A FIRST COURSE IN NUMBER THEORY

K.C. Chowdhury

Asian Books Private Limited

A FIRST COURSE IN NUMBER THEORY

K.C. Chowdhury
Professor of Mathematics
Gauhati University, Assam

Asian Books Private Limited
7/28, Mahavir Lane, Vardan House, Ansari Road,
Darya Ganj, New Delhi-110002

"This page is Intentionally Left Blank"

Asian Books Private Limited

Corporate and Editorial office
7/28, Mahavir Lane, Vardan House, Ansari Road, Darya Ganj, New Delhi-110 002.
E-Mail: asian@nda.vsnl.net.in; purobi@asianbooksindia.com
World Wide Web: http://www.asianbooksindia.com
Phones: 23287577, 23282098, 23271887, 23259161 Fax: 91-11-23262021

Sales Offices

Bangalore	103, Swiss Complex No. 33, Race Course Road, Bangalore-560 001 Phones: 22200438, Fax: 91-80-22256583, Email: asianblr@airtelbroadband.in
Chennai	Palani Murugan Building No.21, West Cott Road, Royapettah, Chennai-600 014, Phones: 28486927, 28486928, Email: asianmds@vsnl.net
Delhi	7/28, Mahavir Lane, Vardan House, Ansari Road, Darya Ganj, New Delhi-110 002, Phones: 23287577, 23282098, 23271887, 23259161; Fax: 91-11-23262021 E-Mail: asian@nda.vsnl.net.in
Guwahati	6, G.N.B. Road, Panbazar, Guwahati, Assam-781 001 Phones. 0361-2513020, 2635729 Email: asianghy1@sancharnet.in
Hyderabad	3-5-1101/1/B IInd Floor, Opp. Blood Bank, Narayanguda, Hyderabad-500 029 Phones: 24754941, 24750951, Fax: 91-40-24751152 Email: hydasian@hd2.vsnl.net.in, hydasian@eth.net
Kolkata	10 A, Hospital Street, Calcutta-700 072 Phones: 22153040, Fax: 91-33-22159899 Email: calasian@vsnl.com
Mumbai	Showroom: 3 & 4, Ground Floor, Shilpin Centre, 40, G.D. Ambekar Marg, Wadala, Mumbai-400 031; Phones : 22619322, 22623572, Fax: 24159899
Noida	G-20, Sector 18, Atta Market, Noida Ph: 9312234916, Email: asiannoida@asianbooksindia.com
Pune	Shop No. 5-8, G.F. Shaan Brahma Com., Near Ratan Theatre, Budhwar Peth Pune-02; Phones: 24497208, Fax: 91-20-24497207 Email: asianpune@asianbookindia.com

© Authors

1st Published: 2004
Ist Reprint 2007
ISBN: 978-81-8629-965-4

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording and/or otherwise, without the prior written permission of the publisher.

Published by **Kamal Jagasia** for Asian Books Pvt. Ltd., 7/28, Mahavir Lane, Vardan House, Ansari Road, Darya Ganj, New Delhi-110 002

Laser Typeset at *Add Computers Delhi*
Printed at Yashprinto Delhi

To HAMIDA

Preface

In this book, I tried to cover those topics on Elementary Number Theory, which are the essential ingredients for a beginner. Most of these topics are included in the syllabus of Mathematics (major) course for undergraduate students as well as some parts in post graduate level in the universities of Northeast as well as other Indian universities. I hope the book will find a wide appeal.

Due to the undeniable historical importance of the subject, the Theory of Numbers has always occupied a unique position in the world of Mathematics. Because of the basic nature of its problems, number theory has a fascinating appeal for the leading mathematicians as well as for thousands of amateurs. There is no denying of the fact that the elementary theory of numbers should be considered as one of the best subjects for early Mathematical instructions. It requires no long preliminary training; the content is well defined and familiar and above all, other than any other part of mathematics – the methods of inquiry adhere very much to the scientific approach.

This book is the outcome or to be more precise, the ramification of lecture notes on Number Theory that I once attended in Panjab University, Chandigarh and also the ones I taught to the students of Gauhati University at postgraduate level.

The book is divided into eight chapters. The first chapter dealt with the construction of natural numbers and integers on the basis of Peano's axioms, the fundamental building blocks of the Theory of Numbers, keeping in note that in most cases, the importance of fundamental hypotheses (axioms) has always been overlooked, the real taste of elementary number theory being lost. As such in this chapter I tried to bring into the forefront the passage (or the path) of formation of integers from natural numbers (similarly, though not included, the rational numbers from the integers), to be more precise how Peano's axioms help one to give almost all the properties of Natural numbers or how axiom of induction *et al* lead one to the principle of Mathematical induction and the like leading to the equivalence of well ordering property of positive integers.

Next principal discussion in this chapter is on the theory of divisibility introducing different relevant ideas such as greatest common divisor, least common multiple, different scales of numeration, and nonetheless on the most important topic, the Prime Numbers.

The next chapter –Congruences and its Basic Properties includes elementary properties of congruences, residue systems, Fermat's Little theorem, applications of congruences, some Tests of Divisibility by primes (including latest Ramanaiah technique) and the Solutions of Congruences leading to Chinese Remainder Theorem.

In the third chapter, I delved into another part of Algebraic Congruences giving the technique of Reduction of Congruence into parts together with other two major components –the Primitive Roots and the Theory of Indices. The most important and interesting topic of elementary number theory viz., different Arithmetic Functions such as Euler's function, Divisor Function, Sum, Product, Mobius Function and their properties together with Mobius Inversion Formula find their places in the fourth chapter.

The fifth chapter encompasses Farey sequences, Continued Fractions and Pell's Equations, which provide much insight into many Mathematical problems, in the nature

"This page is Intentionally Left Blank"

"This page is Intentionally Left Blank"

of numbers. Though C.D.Olds remarks that continued fractions might have been discovered accidentally, yet, we should not cease to think the attitude reflected in its creative and artistic behaviour. The link of Irrational numbers with Rational numbers has been dealt with an inclination mainly towards the application of Farey sequences. Quadratic irrationals have also found their proper place in the discussion of the applications of continued fractions. Together Pell's Equations and Fibonacci numbers have been included and thus the importance of continued fractions etc have been properly justified.

The sixth chapter comprises of Quadratic Residues, Legendre's and Jacobi's Symbols together with the Quadratic Reciprocity Law – which can be marked as one of the precious jewels in the crown of 'The Queen of Mathematics' – The Theory of Numbers (As D.M.Burton has remarked).

Homogeneous Quadratic Diophantine equations, different problems on sum of Squares together with two important discussions viz., on Fermat's Last Theorem and Waring's problem have been included in the seventh chapter.

The last chapter is just only a collection of solved problems of elementary number theory related to different Mathematical Olympiads. Here I would like to express my deep sense of gratitude towards the authors of the books, from which the problems have been included.

There are examples and exercises at the end of each chapter to authenticate the theory and for drill in calculations. Answers to some of these are provided at the end for verification.

I extend my thanks to Mr. D Bhattacharya of Asian Books Private Ltd., for having taken keen interest in the preparation of the manuscript and almost compelling me to bring it up within a short time.

During the preparation of the book I have benefited up to a great extent from the works of several authors including K.H.Rogen, J.Hunter, H.Gupta, C.D.Olds, Gundala Ramanaiah, different issues of College Journals of Mathematical Association of America, etc. A special debt of thanks goes to his student and now his colleague Dr. H.K.Saikia, whose generous help at every stage for its development was indispensable. Last but not least, I must not fail to mention the names of my two children Kunal and Maitrayee for their ever-ready involvement from typing to comparing the manuscript. I would acknowledge any suggestion for further improvement of this book and would readily accept the responsibility for any error or shortcomings that remains within.

Author

Contents

NUMBER SYSTEM

1.1 FROM NATURAL NUMBERS TO INTEGERS

1.1.1 Introduction: Structure of Number System

We start with a few undefined terms and a few axioms or postulates and deduce from these all the properties of the number system as a logical consequence. This is the method same as that of deductive construction successfully employed by the ancient Greeks in creating a theory of knowledge about geometry. It was left to G.Peano (1899), an Italian mathematician and logician. He propounded that all the properties of number system follow from only a few assumptions (peano's axioms) regarding natural numbers.

Peano's axioms, which involve the association with a given object x, a unique object called the *Successor of* x, are stated as follows:

Peano's Axioms

Suppose $\mathbb{N}$ is a nonempty set such that

1. $1 \in \mathbb{N}$
2. If $n \in \mathbb{N}$ then $n' (= n + 1) \in \mathbb{N}$ (n' is called *successor of* n)
3. There is no element in $\mathbb{N}$ whose successor is 1.
4. If $n' = m'$ then $n = m$ for $n, m \in \mathbb{N}$
5. If K is a set with elements from $\mathbb{N}$ such that
   (i) $1 \in K$
   (ii) $k \in K$, gives $k' \in K$ $(k' = k' + 1)$
   Then $K = \mathbb{N}$

Definition: This set $\mathbb{N}$ called the *set of natural numbers*

Remark: (4) ensures that no two natural numbers are same.
(3) ensures that 1 is the least number of $\mathbb{N}$
(5) is known as *the axiom of induction.*

Symbolically, if $A \subseteq \mathbb{N}$ such that $1 \in A$ and $n' \in A$ whenever $n \in A$, then $A = \mathbb{N}$.

Definition: Peano's axioms lead us to *define '+' (Addition) in* $\mathbb{N}$ as follows:

For $n \in \mathbb{N}$, *we define*

(i) $n' = n + 1$

(ii) $m + n' = (m + n)'$ for all $m, n \in \mathbb{N}$

Similarly one may define another *operation '.' (Multiplication)* in $\mathbb{N}$ as follows:

For $n \in \mathbb{N}$

(i) $n \,.\, 1 = n$

(ii) $m \,.\, n' = mn + m$ for all $m, n \in \mathbb{N}$

These two are sufficient to deduce the associative, commutative and cancellation laws for addition, multiplication and also the distributive law viz. $(m + n) + p = m + (n + p)$, $m + n = n + m$, $m \,.\, n = n \,.\, m$, $(m + n) \,.\, p = m \,.\, p + m \,.\, p$.

Note: Reader may note that for the cancellation laws of addition and multiplication, negative or reciprocal of a number is nowhere necessary. Peano's axioms are sufficient for these.

Example 1. Prove that: $1 + 2 + \ldots + n = \dfrac{n(n+1)}{2}$ (using axiom of induction)

Solution: Let $P = \left\{ n \mid 1 + 2 + 3 + \ldots + n = \dfrac{n(n+1)}{2} \right\}$

Now $1 = \dfrac{1.(1+1)}{2}$, so $1 \in p$

Assume $k \in P$.

$\therefore \quad 1 + 2 + \ldots + k = \dfrac{k.(k+1)}{2}$

Now $1 + 2 + \ldots + (k + 1) = (1 + 2 + \ldots + k) + (k + 1)$

$$= \frac{k.(k+1)}{2} + (k + 1)$$

$$= (k + 1)\left(\frac{k}{2} + 1\right)$$

$$= \frac{(k+1)(k+2)}{2}$$

$\therefore \quad k + 1 \in P$

So, by axiom of induction, $P = N$

$\therefore$ for all $n \in \mathbb{N}$, $1 + 2 + \ldots + n = \dfrac{n(n+1)}{2}$.

Definition: For $m, n \in \mathbb{N}$ we say m *is greater than* n, written $m > n$ (or $n < m$) if for some $p \in \mathbb{N}$, we have $m = n + p$.

1.1.2 Properties of addition, multiplication and order in the set of natural numbers

If m, n, p are any natural numbers then,

1. $m + n$, $m \cdot n$ are natural numbers **(Closure property)**
2. $m + (n + p) = (m + n) + p$
   $m \cdot (n \cdot p) = (m \cdot n) \cdot p$ } **(Associative property)**
3. $m + n = n + m$
   $m \cdot n = n \cdot m$ } **(Commutative property)**
4. If $m + p = n + p$, then $m = n$ **(Law of cancellation for addition in an equation)**
5. $(m + n) \cdot p = m \cdot p + m \cdot p$ **(Distributive law)**
6. (i) if $m + p < n + p$ then $m < n$ } **Low of cancellation for addition and**
   (ii) if $mp < np$ then $m < n$ } **multiplication in an inequation**

   $[m, n, p \in \mathbb{N}]$

Example 2. If $m, n, p \in \mathbb{N}$ then prove that $m + (n + p) = (m + n) + p$

Proof: First fix m, n

Consider the set $P = \{p \in \mathbb{N}, \mid m + (n + p) = (m + n) + p\}$

Here, $m + (n + 1) = m + n' = (m + n)' = (m + n) + 1$

$\therefore$ $1 \in P$

Now for $k \in P$, we have $m + (n + k) = (m + n) + k$

and $m + (n + k') = m + (n + k)' = m + ((n + k) + 1) = (m + n + k)'$

$= ((m + n) + k') = (m + n) + k'$

So, $k' \in P$.

Thus by axiom of induction, $P = \mathbb{N}$

$\therefore$ $m + (n + p) = (m + n) + p$, for all $m, n, p \in \mathbb{N}$.

Example 3. If $m, n, p \in \mathbb{N}$ then $m \cdot (n + p) = m \cdot n + m \cdot p$

Solution: Consider the set $P = \{p \in \mathbb{N} \mid m \cdot (n + p) = m \cdot n + m \cdot p\}$

Now, $m \cdot (n + 1) = m \cdot n' = m \cdot n + m = m \cdot n + m \cdot 1$

$\therefore$ $1 \in P$

Let $k \in P$.

So, $m \cdot (n + k) = m \cdot n + m \cdot k$

Now $m \cdot [n + k'] = m \cdot (n + k)' = m (n + k) + m = (mn + mk) + m$

$= mn + (mk + m) = m \cdot n + mk'$

So, by axiom of induction $k' \in \mathbb{N}$

$\therefore$ $P = \mathbb{N}$.

1.1.3 Law of Trichotomy of Natural Numbers

Given any two natural numbers m and n, one and only one of the following is true.

(i) $m = n$,
(ii) $n > m$
(iii) $m > n$

Note: Law of Trichotomy can be proved, using the Peano's axioms

1.1.4 Law of Cancellation

If $m, n, p \in \mathbb{N}$, such that $m \cdot p = n \cdot p$ then $m = n$

Proof: It is sufficient if we show that neither $m > n$ nor $n > m$ is true.

Suppose $m > n$.

Then $m = n + k$ for some $k \in \mathbb{N}$

$\therefore$ $m \cdot p = (n + k) \cdot p = n \cdot p + k \cdot p$

$\therefore$ $m \cdot p > n \cdot p$ and this is not possible.

$\therefore$ $m > n$.

Similarly, $n > m$

Hence $m = n$.

1.1.5 Open Statement: Solution and Inverse Operation

Although the system of natural numbers developed affords a good model of a deductive structure it is incomplete in some respect. It cannot answer all the questions even with respect to the binary operation defined on it. This is because with respect to every operation we always think of an inverse or an opposite operation. If an operation is to be thought of as a command to do some action, the inverse operation is in the nature of asking a question to do the opposite effect. Thus in mathematics if we write $9 + 3$ it means add 3 to 9 (to get 12). But the symbol $9 - 3$ means, 'What is that number which when added to 3 gives 9?'

In the long course of its development mathematicians have developed a highly symbolic language, which uses only statements, which are either true or false but not both. Mathematical language does not need to use other forms of sentences. Questions have no place in the body of proof. Mathematicians have circumvented this difficulty by allowing sentences which have the form of statements but which are ***open*** with respect to their truth or falsity. They use variables as a device. Thus the equation $9 - 3$ is converted into an open statement $9 = 3 + x$. The number, which makes this open statement true, is called our **solution of the open statement.** In the given case our solution is 6. We also say that '6' has been obtained by subtracting 3 from 9. We observe that if we wish to restrict ourselves to the set of natural numbers then an open sentence $4 = 13 + x$ has no solution. In other words subtraction, the inverse operation of addition, cannot always be carried out in the set of naturals.

What can we say about multiplication? Consider the question $3 \cdot x = 15$.

Obviously its solution is $x = 5$.

But an open statement such as $9 \cdot x = 4$ has no solution in the set of natural numbers. Inverse operation of that of multiplication is called *division.* We observe that in this sense division cannot always be carried out in the set of naturals.

We therefore need a set of numbers in which these inverse operations can always be carried out. We know that the set of integers fulfils this need with respect to subtraction. In this sense the set of integers is an extended set of the set of naturals. For this purpose we have, at this stage only some limited information about naturals viz., the

natural numbers, order relation in natural numbers, the properties of the two binary operations defined on natural numbers and use logical reasoning as the only means to achieve this end.

1.1.6 Relations

Sometimes ordered pairs of $A \times B$ (A, B are two sets) may be further classified according to a specified rule or according to a relation between elements a of A and elements b of B; only those elements (ordered pairs) being chosen for which it is true that the said relation between a and b is satisfied.

For instance $A \neq B$, each a set of positive integers. Let the relation between elements a and b be specified by the rule $a^2 = b$. The some of the elements of the ordered pairs that must be chosen are (1, 1), (2, 4), (3, 9) ..... An ordered pair of the type (4, 2) cannot be chosen

$\because \quad 4^2 \neq 2$

Definition: A relation between any two elements is called a *binary relation.* A 'relation' may be denoted by a letter such as R. Then $a\,R\,b$ stands for the statement "a is R – related to b." Any subset of $A \times B$ is called a relation from A to B. Thus we say that every known relation gives rise to a specific subset and every subset can be supposed to be formed in accordance to some relation though not specifically known. We then identify every subset of $A \times B$ with a specific relation. The two statements $x\,R\,y$ and $(x, y) \in R$ are then equivalent.

Some class of relations plays a very important role in mathematics.

Amongst these is a class of *equivalence relations.*

In order that a relation R may be an equivalence relation in a given set A it has to fulfill the following conditions:

(a) For every $x \in A$, $x\,R\,x$ holds (reflexive)

(b) For $x, y \in A$ if $x\,R\,y$ holds then $y\,R\,x$ holds (symmetric).

(c) For $x, y, z \in A$ if $x\,R\,y$, $y\,R\,z$ hold then $x\,R\,z$ holds. (Transitive)

Why are equivalence relations so very important? Because of the three properties of the equivalence relation all the elements, which are related to each other, form a class, and elements, which are not related to each other, belong to distinct classes. Thus every equivalence relation helps further classification of a set on which it is defined. Collection of these disjoint classes is known as a *partition* of the set.

If R is an equivalence relation defined on a set A then R partitions the set A.

1.1.7 We now see that *integers are equivalence classes defined in* $\mathbb{N} \times \mathbb{N}$

Consider the set $\mathbb{N} \times \mathbb{N}$ and define a relation in $\mathbb{N} \times \mathbb{N}$ such that $(m, n)\ R\ (p, q)$ if and only if $m + q = n + p$.

And it can be seen that R is an equivalence relation in $\mathbb{N} \times \mathbb{N}$ and hence R partitions.

$\mathbb{N} \times \mathbb{N}$ into mutually disjoint classes *called an integer viz., [(m, n)]*

The following are some such equivalence classes representing the integers

(1, 5), (1, 4), (1, 3), (1, 3), (1, 1), (2, 1), (3, 1), (4, 1), (5, 1) →
(2, 6), (2, 5), (2, 4), (2, 3), (2, 2), (3, 2), (4, 2), (5, 2), (6, 2)
(3, 7), (3, 6), (3, 5), (3, 4), (3, 3), (4, 3), (5, 3), (6, 3), (7, 3)
↓

1.1.8 Order in the Set of Integers

If $(p, q) \in [(m, n)]$ and $n < m$ then $q < p$ for,

$\because$ $(p, q)\ R\ (m, n)$ we have $p + n = q + m$,

$\because$ $n < m$, $n + t = m$, for some $t \in \mathbb{N}$. So $p + n = q + (n + t)$ and, $p = q + t$.

$\therefore$ $q < p$

1.1.9

The set $\mathbb{N} \times \mathbb{N}$ can be arranged into square arrays of rows and columns such as,

$$\begin{array}{ccccc}
(1,1) & (2,1) & (3,1) & (4,1) & (5,1) \\
(1,2) & (2,2) & (3,2) & (4,2) & (5,2) \\
(1,3) & (2,3) & (3,3) & (4,3) & (5,3) \\
(1,4) & (2,4) & (3,4) & (4,4) & (5,4)
\end{array}$$

The diagonal of this array is a set of ordered pairs whose components are equal.

Every ordered pair to the right of this diagonal has the property that its first component is greater than the second. Every ordered pair to the left of the diagonal has the property that its first component is less than the second.

If the equivalence classes $[(m, n)]$ is such that $m < n$ then we say $[(m, n)]$ is a *positive integer* and if $n < m$ then the corresponding class denotes a *negative integer.*

The class $(m, m + p)$ for some $p \in \mathbb{N}$, is the integer p and the class $(m + q, m)$ for some $q \in \mathbb{N}$ is the integer $-q$.

To denote the *diagonal integer* we use the symbol 0.

We denote this *set of integers by* $\mathbb{Z}$.

1.1.10 In the set $\mathbb{Z}$ of integers we define addition and multiplication as follows:

For any two integers $a = [(m, n)]$ and $b = [(p, q)]$,

$$a + b = [(m + p, n + q)], \text{ and}$$
$$a \,.\, b = [(mp + nq, mq + np)]$$

and that these are well defined can be seen easily. With these definitions it is easy to establish the Ring properties viz.,

Closure property: $a + b$, $a \,.\, b$ are integers

Associative property: $a + (b + c) = (a + b) + c$

$$a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c$$

Property of zero: $a + 0 = 0 + a = a$ (0 is called the additive identity for the set of integers and it is unique)

Distributive property: $a \,.\, (b + c) = a \,.\, b + a \,.\, c,$

$(b + c) \,.\, a = b \,.\, c + b \,.\, a$

Additive inverse: For every integer a there is an integer b such that $a + b = b + a = 0$ {for the integer $a = [(m, n)]$ the integer $-a = [(n, m)]$ has this property]

For the sake of completeness we just state the following properties of integers;

(a) If $a, b \in \mathbb{Z}$ then the equation $a + x = b$ has a unique solution in the set of integers.

(b) Sum and product of two positive integers is positive.

(c) Product of two negative integers is positive.

(d) Product of a positive and a negative integer is negative.

(e) Given two integers a, b one and only one of the following holds.

(i) $a - b$ is positive

(ii) $a - b$ is negative,

(iii) $a - b = 0$

We write $a > b$ if $a - b$ is positive

$a < b$ if $a - b$ is negative

(f) If $a + c = b + c$ then $a = b$

(g) If $a \,.\, c = b \,.\, c, c \neq 0$ then $a = b$

(h) If $a + c > b + c$ then $a > b$

(i) If $a \,.\, c > b \,.\, c, c > 0$ then $a > b$.

(j) If $a \,.\, c > b \,.\, c, c < 0$ then $b > a$.

1.1.11 Structure of Integers

The correspondece

$$[(x, x + n)] \to n, (n \in \mathbb{N}]$$

is such that it preserves addition and multiplication, in the following sense:

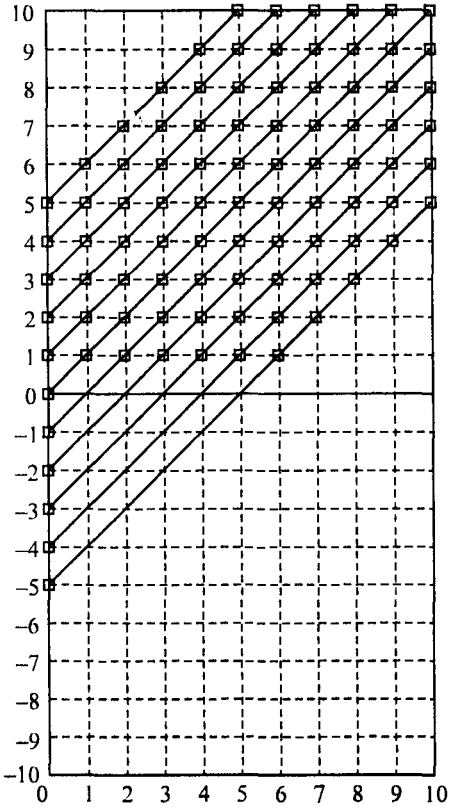
(i) $[(x, x + n_1)] + [(p, p + n_2)] = [(x, x + \overline{n_1 + n_2})]$

(ii) $([(x, x + n_1)] \,.\, [(p, p + n_2)] = [(x, x + \overline{n_1 . n_2})]$

Because of these properties positive integers are identified with corresponding natural numbers

Although the set of integers is much richer in structural properties than the set of natural numbers an equation of the type $a \,.\, x = b$; $a, b \in \mathbb{Z}$ does not have always a solution in the set. It therefore requires to be extended into a larger set (of rational). We shall not undertake to carry out this extension here.

1.1.12 Geometrical link between the set of natural numbers and that of integers:



Consider the equivalence classes of the set of ordered pairs of natural numbers as described below:

(1) {(1, 2), (2, 3), (3, 4), (1, 5), (1, 6), ...} as lattice points on the line $y = x + 1$
(2) {(1, 3), (2, 4), (3, 5), (4, 6), (5, 7), ...} as lattice points on the line $y = x + 2$
(3) {(1, 4), (2, 5), (3, 6), (4, 7), (5, 8), ...} as lattice points on the line $y = x + 3$
... .
(i) {(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), ...} as lattice points on the line $y = x$
(ii) {(2, 1), (3, 2), (4, 3), (5, 4), (6, 5), ...} as lattice points on the line $y = x - 1$
(iii) {(3, 1), (4, 2), (5, 3), (6, 4), (7, 5), ...} as lattice points on the line $y = x - 2$
(iv) {(4, 1), (5, 2), (6, 3), (7, 4), (8, 5), ...} as lattice points on the line $y = x - 3$
... ...
etc.

It is seen that these lines meet the vertical infinite line on left at the points shown, representing what we have wanted; giving thereby the set of *representing-points* of the equivalence classes denoting the integers.

Hence these points are in one-one correspondence with the set of integers.

In above we have seen that there is a one-one correspondence between the set of positive integers and the set of natural numbers which preserves addition and multiplication; the terms "natural numbers 'and "positive integers 'will hereafter mean one and the same thing. *So the axiom of induction can then be restated as:*

If a set of positive integers (i) contains 1 (ii) contains the positive integer $n + 1$ whenever it contains the positive integer n; then this set contains all the positive integers."

Definition: If a, b, c are positive integers such that $a < b < c$ or $c < b < a$ we say that *b is between a and c*

Theorem 1.1. There is no integers between a and $a + 1$

Proof: If possible, let m be an integer such that $a < m < a + 1$ ...(1)

$\because a < m$, there exists a positive integer p such that $a + p = m$

If $p = 1$, $a + 1 = m$. But from (1), $m < a + 1$; so that, $p \neq 1$. If $p > 1$, let $p = g + 1$ for some positive integer g.

Then, $a + (g + 1) = m$

i.e., $(a + 1) + g = m$

So, $a + 1 < m$

This contradicts $m < a + 1$

$\therefore$ there is no positive integer p such that $a + p = m$ and $a < m < a + 1$

Hence there is no integer m such that $a < m < a + 1$.

The axiom of induction gives rise two methods of proof known as the first and the second Principle of mathematical induction.

1.1.13 First Principle of Mathematical Induction

Theorem 1.2. Let $P(n)$ be a statement defined for any positive integer.

If (i) $P(1)$ is true, and (ii) $P(n + 1)$ is true whenever $P(n)$ is true, then $P(n)$ is true for all positive integral values of n.

Proof: Let M be the set of positive integers for which $P(n)$ is true.

Then $1 \in M$, $\because P(1)$ is true.

Let $n \in M$. It follows that $P(n)$ is true. But then $P(n + 1)$ is also true, so that $n + 1 \in M$.

$\therefore$ by the axiom of induction M contains all the positive integers.

$\therefore$ $P(n)$ is true for all positive integers n.

1.1.14 Second Principle of Mathematical Induction

Theorem 1.3. Let $P(n)$ be a statement defined for any positive integer n.

If (i) $P(1)$ is true, and $P(n + 1)$ is true whenever $P(k)$ is true for all $k \leq n$, then $P(n)$ is true for all positive integral, values of n.

Proof: Let M be the set of positive integers n such that $P(k)$ is true for all positive integers $k \leq n$.

Now $1 \in M$, $\because P(1)$ is true.

Let $n \in M$. $\therefore P(k)$ is true for all positive integers $k \leq n$.

But then $P(n + 1)$ is true. It follows that $P(k)$ is true for all positive integers $k \leq n + 1$.

So, $n + 1 \in M$

$\therefore M$ is the set of all positive integers Hence; $P(n)$ is true for all positive integers n.

Definition: Least element of a set of positive integers

An element a of a set A of positive integers is said to be *"a least element"* of A if for every element b of A ($b \neq a$), $a < b$ (one can show easily that this element is unique)

1.1.15 Well Ordering Property of (WOP) of Positive Integers

Theorem 1.4. Every non-empty subset of $\mathbb{N}$ contains a least element.

Proof: Let S be a non-empty subset of $\mathbb{N}$.

Suppose S does not contain a least number. Then $1 \notin S$

Let $A = \{m \mid m \in \mathbb{N}, m < k\}$ (every $k \in S$)

Observation:

(i) $1 \in A$

(ii) If $a \in A$ then $a' \in A$, because $a \in A$ gives $k > a$

or $k \geq a'$ $(= a + 1)$.

But $k = a'$ gives that a' is the least element of S.

So, $k \neq a'$

And

$\therefore k > a'$ or $a' < k$. Thus, $a' \in A$ and by axiom of induction it follows that $A = \mathbb{N}$ and

$\therefore S = \phi$ which is not true. And hence the theorem is proved.

The fact that every non-empty subset of positive integers has a least element is known as:

Well Ordering Principle of (WOP) of Positive Integers

Example 4. Assuming the WOP of positive integers, prove the axiom of induction.

Solution: Suppose $S \neq \mathbb{N}$

$\therefore$ there exists an $s \in \mathbb{N}$, such that $s \notin S$.

Let $T = \{m \mid m \in \mathbb{N}, m \notin S\}$

Observation: $T \neq \phi$ and $T \cap S = \phi$, $T \subseteq \mathbb{N}$ and so by WOP, T contains a least element (say) t.

By hypothesis,

$S \subseteq \mathbb{N}$ such that

(i) $1 \in S$

(ii) if $k \in S$

then $k' \in S$.

So, $1 \in S$ gives $1 \notin T$

$\therefore$ $t \neq 1$

or $t > 1$ or $t > t - 1 > 0$.

$\because$ t is the least element of T, $t - 1 \notin T$. So, $t - 1 \in S$. And

$\therefore$ by (ii) $(t - 1) + 1 = t \in S$ and also, $t \in T$ which is a contradiction. Hence $S = \mathbb{N}$.

Theorem 1.5. The well ordering principle and the axiom of induction are equivalent (from above it follows).

Example 5. Prove that there is no natural number in between 0 and 1.

Solution: Let $S = \{x \mid x \in \mathbb{N}, 0 < x < 1\}$

We show that $S = \phi$. Suppose $S \neq \phi$.

$\therefore$ S is a nonempty set of positive integers. So, by WOP of positive integer, S contains a least number a (say).

$\therefore$ $0 < a < 1$ or, $0 < a^2 < a < 1$ or, $0 < a^2 < 1$ or, $a^2 \in S$ and $a^2 < a$

And it contradicts the assumption that a is the least element of S.

Hence $S \neq \phi$ is wrong.

$\therefore$ $S = \phi$.

Property 1.6. If b is an integer > 1 then for any integer $r \geq 0$, $b^r > r$

Proof: Proof is by induction. For $r = 0$ this is trivially true. We therefore assume $r \geq 1$

Let $P(r)$ be the statement: "$b^r > r$ for integer $r \geq 1$"

$P(1)$ is true.

Assume that $P(r)$ is true, so that $b^r > r$

We show that $P(r + 1)$ is true.

Now, $b^{r+1} = b^r . b$

$\because$ $b \geq 2$, $b^{r+1} \geq b^r . 2$

$\therefore$ $b^{r+1} \geq b^r(1 + 1)$

$\geq b^r + b^r$

$\geq b^r + 1$ (1 is the least positive integer)

$\geq r + 1$

It follows that $P(r)$ is true for all $r \geq 0$. Otherwise we may proceed as follows:

$\because$ $b - 1 > 0$, we have $b - 1 \geq 1$

Multiplying both sides by the positive integer $(1 + b + ... + b^r)$,

We get, $(b - 1)(1 + b + b^2 + ... + b^r) \geq 1 + b + ... + b^r$

i.e., $b^{r+1} \geq 1 + b + ... + b^r \geq r + 1$,

$\because$ $b^r > 1$ for every r.

$\therefore$ $b^r > r$ for every r.

Example 6. Let b be an integer greater than 1 and let $c_0, c_1, c_2, \ldots c_r$ be integers between 0 and $b-1$ inclusive, with $c_r > 0$. Put $n = c_0 + c_1 b + c_2 b_2 + \ldots + c_r b_r$. Then show that $b^r \le n \le b^{r+1}$

Solution: We have $c_0 + c_1 b + c_2 b^2 + \ldots + c_{r-1} b^{r-1} \ge 0$,

$\because$ every number in this expression is non-negative, it follows that $n \ge c_r b^r$.

By assumption, $c_r \ge 1$.

$\therefore$ $n \ge b^r$.

Also $0 \le c_i \le b-1$ for each, $0 \le i \le r$

$\therefore$ $c_0 \le b-1$

$c_1 b \le (b-1)b$

$c_2 b^2 \le (b-1)b^2$

$c_r b^r \le (b-1)b^r$

$\therefore$ $c_0 + c_1 + c_2 b^2 + \ldots + c_r b^r$

$\le (b-1)(1 + b + b^2 + \ldots + br)$

$= b^{r+1} - 1$

$\le b^{r+1}$

$\therefore$ $b^r \le n \le b^{r+1}$

Example 7. $\sqrt{2}$ is irrational

Solution: Suppose that $\sqrt{2}$ is rational. Then there would exist positive integers a and b with $\sqrt{2} = \frac{a}{b}$.

Consequently the set $S = \{k\sqrt{2} \mid k \text{ and } k\sqrt{2} \text{ are positive integers}\}$ $(\ne \phi) \subseteq \mathbb{Z}^+$ $(S \ne \phi$, because $a = b\sqrt{2} \in S\})$.

$\therefore$ by WOP S has a smallest element, say $s = t\sqrt{2}$.

We have $s\sqrt{2} - s = s\sqrt{2} - t\sqrt{2} = (s-t)\sqrt{2}$.

Since $s\sqrt{2} = 2t$ and s are both integers,

$s\sqrt{2} - s = (s-t)\sqrt{2}$ – must also be an integer.

Furthermore, it is positive since

$s\sqrt{2} - s = s(\sqrt{2} - 1)$

and $\sqrt{2} > 1$.

It is less than s since $s = t\sqrt{2}$, $s\sqrt{2} = 2t$, and $\sqrt{2} < 2$.

This contradicts the choice of s as the smallest positive integer in S.

It follows that $\sqrt{2}$ is irrational.

1.2 DIVISIBILITY THEORY

1.2.1 Division Algorithm

Theorem 1.7. Given $a, b \in \mathbb{Z}$, $b > 0$, then there exists $q, r \in \mathbb{Z}$, such that $a = bq + r$, $0 \le r < b$

Proof: Let $S = \{bx \mid x \in \mathbb{Z}, bx \leq a\}$

Obviously $S \subseteq \mathbb{Z}$. Again, for given $a, b \in \mathbb{Z}$, there exists an $n \in \mathbb{Z}$ such that

$$bn \geq -a$$

or $$-bn \leq a$$

or $$b(-n) \leq a$$

or $$b(-n) \in S$$

$\therefore S \neq \phi$. Thus, S is a non-empty subset of $\mathbb{Z}$, which is bounded above ($bx \leq a$).

$\therefore S$ contains a largest element, (say) bq ($q \in \mathbb{Z}$). So, $bq \leq a$. Hence,

$$a = bq + r (r \geq 0).$$

Now we prove : $r < b$. If not, suppose $r \geq b$ (and $\therefore r - b \geq 0$)

Then, $$a = bq + r = bq + b + r - b = b(q + 1) + s, \quad [s = (r - b) \geq 0]$$

$$= bq' + s, s \geq 0$$

$\therefore$ $$a = bq + r = bq' + s, (s \geq 0)$$

or, $$bq' \leq a$$

or $$bq' \in S \text{ and}$$

$\therefore$ $$bq \geq bq'$$

or $b \leq 0$ and is a contradiction with $b > 0$.

Hence $$r < b.$$

$\therefore a = bq + r$ where $0 \leq r < b$.

Now we prove:

Theorem 1.8. *Given* $a, b \in \mathbb{Z}, b \neq 0$, then there exists $q, r \in \mathbb{Z}, 0 \leq r < |b|$ such that $a = bq + r$

Proof $\because 0 \neq b \in \mathbb{Z}, |b| > 0,$

$\therefore$ by theorem 1.7,

$$a = |b| q_1 + r, \text{ for } q_1, r \in \mathbb{Z}, 0 \leq r < |b|$$

$$= (\pm b) q_1 + r$$

$$= b(\pm q_1) + r$$

$$= bq + r$$

Thus, $$a = bq + r, 0 \leq r < |b|, \pm q_1 = q \in \mathbb{Z}$$

Remark: q and r are unique

If possible let $$a = bq_1 + r_1, 0 \leq r_1 < b$$

and $$a = bq_2 + r_2, 0 \leq r_2 < b$$

$\therefore$ $$0 = b(q_1 - q_2) + (r_1 - r_2)$$

or $$|b| |q_1 - q_2| = |r_1 - r_2| \quad \text{...(*)}$$

Again, $$0 \leq r_1 < |b| \quad \text{...(i)}$$

$$0 \leq r_2 < |b|$$

or $-|b| \leq -r_2 < 0$ ...(ii)

Adding (i) and (ii),

$$0 - |b| < r_1 - r_2 < |b|$$

or $|r_1 - r_2| < |b|$

or $|b||q_1 - q_2| < |b|$ [by (*)]

or $|q_1 - q_2| < 1$

or $|q_1 - q_2| \leq 0$

And the only possibility is $|q_1 - q_2| = 0$.

$\therefore$ $q_1 = q_2$ and from (*) $r_1 = r_2$.

Definition:

(1) $a = bq + r$ is called *the principle of division identity of integer.*

(2) q is called *the quotient of division*

(3) r is called *the remainder of division.*

We now look the above mentioned division algorithm from another angle.

Consider $a = 17$, $b = 59$

Clearly a does not divide b. We understood that division is repeated subtraction. This way, each time the subtraction is being repeated if the remainder $b - a > a$. After a finite number of steps, at a certain stage remainder will be less than a. In this process we get the following multiples of a viz. a, $2a$, $3a$, $4a$, ... qa, $(q + 1)\, a$

And we get either b = one of these positive integers for some q,

or, $qa < b < (q + 1)\, a$

and this gives, $qa \leq b < (q + 1)\, a$

which gives $b - aq < a$.

If $b - aq = r$

then, $b = aq + r$

where, $0 \leq r < a$

This is what is known as division Algorithm [observe that this is not a proof.]

We now give another proof of division algorithm

Theorem 1.9. To an integer $a \geq 0$ and an integer $b \geq 1$ there exist two unique integers q and r such that $a = qb + r$ with $0 \leq r < b$.

Proof: Now, If $b = 1$, then $a = a \cdot 1 + 0$ and the result is true.

So we now assume: $b > 1$

If $a = 0$, we take $q = 0, r = 0$

If $a < b$ we have $q = 0, r = a$

If $a = b$, take $q = 1$ and $r = 0$

We have $a - b < a$ if $a > b$

Consider the case, $a > b$. Then $0 < a - b < a$.

Suppose $P(a) \equiv a = bq + r$, $0 \leq r < b$, for all integers $a > 0$, $b \geq 1$

$P(1)$ is true, for $1 = 0 \cdot b + 1$

Assume that $P(k)$ is true for all $k \leq a$.

$\because$ $0 < a - b < a$, there are integers q_1, r

$0 \leq r < b$, such that $a - b = bq_1 + r \quad 0 \leq r < b$

So, $a = b(q_1 + 1) + r = bq + r, 0 \leq r < b \quad (q = q_1 + 1)$

Hence $P(a)$ is true. Thus $P(a)$ is true $\forall\ a > 0$.

Uniquencess part is same as in the previous method.

The theorem can be extended to include the case of all integers a where a is negative.

Note 1. If $r = 0$ we say that b divides a (or a is a divisor of b, or b is a factor of a) and is written as $a \mid b$; otherwise $a \nmid b$.

Note 2. $b \mid a$ gives $a = bq$, $q \in \mathbb{Z}$ and

$b \nmid a$ gives $a = bq + r$, $r \in \mathbb{Z}$, $0 < r < b$

Example 8. $1 \mid a\ a \in \mathbb{Z}$

If $1 \nmid a$, then $a = 1 \cdot q + r$ when $0 < r < 1$. But there is no integer in between 0 and 1. Thus, $1 \mid a$, $\forall\ a \in \mathbb{Z}$.

Example 9. (Similarly) $-1 \mid a$, $\forall\ a \in \mathbb{Z}$.

Example 10. If $a \mid b$ then $\pm a \mid \pm b$; $\forall\ a, b \in \mathbb{Z}$

Solution: $\because a \mid b$, we have

$$b = aq, (q \in \mathbb{Z})$$
$$= (-a)(-q) = (-a)q_1, (q_1 \in \mathbb{Z})$$

$\therefore \quad -a \mid b.$

Example 11. If $a \mid b$, $b \mid c$ then $a \mid c$

Solution: $\because a \mid b$, we have

$$b = aq_1, (q_1 \in \mathbb{Z}) \text{ and } b \mid c$$

$\therefore$ $$c = bq_2, (q_2 \in \mathbb{Z})$$

or
$$c = bq_2$$
$$= (aq_1)q_2$$
$$= a(q_1 q_2)$$
$$= aq_3$$

where $q_3 = q_1(q_2 \in \mathbb{Z})$ or $a \mid c$

Example 12. $a \mid b$ gives $a \mid k b$, $k \in \mathbb{Z}$.

Example 13. If $a \mid b$, $a \mid c$ then $a \mid kb + lc$, $k, l \in \mathbb{Z}$

Example 14. $a \mid b$, $b > 0$ gives $b > a$

Proof: (i) if $a < 0$ then (obviously) $b > a$

(ii) and $a > 0$, $a \mid b$ gives $b = aq$, $q \in \mathbb{Z}$

Now, $q > 1 \Rightarrow aq > a$

or $b = aq > a$

or $b > a.$

Example 15. $ac \mid bc$, $c \neq 0$ gives $a \mid b$

Proof: If $ac \mid bc$ then $bc = (ac)\, q$, $(q \in \mathbb{Z})$

or $c(b - aq) = 0$

or $b - aq = 0 \quad (\because c \neq 0)$

or $b = aq$

$\therefore \quad a \mid b.$

Example 16. If $a \mid b$, $b \mid a$, $a, b \in \mathbb{Z}$, then $a = \pm b$

Example 17. If $a \mid b$ then $|a| \mid\mid |b|$

Some results 1.10

1. if $a \mid b$ then $\pm a \mid \pm b$
2. if $a \mid b$, $b \mid c$ then $a \mid c$
3. if $ac \mid bc$ then $a \mid b$, if $c \neq 0$
4. if $a \mid b$ then $a \mid bx$ for every x, $x \in \mathbb{Z}$
5. $a \mid b$, $a \mid c$ give $a \mid (b + c)$ and $a \mid (b - c)$
6. $a \mid b$, $a \mid c$ give $a \mid (bx \pm cy)$, $x, y \in \mathbb{Z}$

1.2.2 Greatest Common divisor (gcd)

Let $a, b \in \mathbb{Z}$, $a, b \neq 0$.

Then, obviously $|a| + |b| > 0$. Let $S = \{x \mid x$ is a common positive divisor of a and $b\}$

We have, $1 \mid n, \forall\, n \in \mathbb{Z}$

$\therefore \quad 1 \mid a,\ 1 \mid b$ and $1 \in S$

$\therefore \quad S \neq \phi$

Now if $x \mid a$ then $x \mid |a|$ and if $x \mid b$ then $x \mid |b|$

Then, $x \mid |a| + |b|$ gives $x \leq |a| + |b|$

$\therefore$ S is a non empty set of positive integers which is bounded above

$\therefore$ S has a largest element, (say) g.

Definition: This g is called the greatest common divisor (GCD) of a and b.

Note: (i) g exists and $g \geq 1$

(ii) we write $(a, b) = g$.

Theorem 1.11. Let $a, b \in \mathbb{Z}$, $a, b \neq 0$ [or $a, b \in \mathbb{Z}^*$ $(=\mathbb{Z} - \{0\})$] $(a, b) = g$, then,

(i) there exists $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = g$

(ii) for $d \in \mathbb{Z}$, if $d \mid a$, $d \mid b$ then $d \mid g$

Proof: Consider $S = \{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}$

Now, $\quad |a| + |b| > 0$

$\Rightarrow \quad \pm a \pm b > 0$

or, $\quad a \cdot (\pm 1) + b \cdot (\pm 1) > 0$

or, $\quad |a| + |b| \in S.$

$\therefore$ $S\ (\neq \phi) \subseteq N$ and so by WOP, S contains a least element (say)m which is of the form $ax + by$ (say),

$$m = ax_0 + by_0,\ x_0, y_0 \in \mathbb{Z}$$

Assert, $\quad m = g$

To prove our assertion we are to show that

(A) m is a common divisor of a and b ($m \mid a$ and $m \mid b$)

(B) If $d \mid a$ and $d \mid b$ then $d \mid m$.

Proof: Suppose, $m \nmid a$

$\therefore$ $\quad a = mq + r,\ 0 \le r < m,\ q, r \in \mathbb{Z}$ ...(i)

or $\quad r = a - mq$

$= a - q(ax_0 + by_0)$

$= a(1 - qx_0) + b\ (-qy_0)$

$= ax' + by'\ ;\ x', y' \in \mathbb{Z}$

gives $\quad r \in S,$

$\therefore$ $\quad r \ge m$ ...(ii)

which is a contradiction to (i).

Hence $m \mid a$ and similarly $m \mid b$

(B) Again, $d \mid a,\ d \mid b$

give $d \mid ax_0,\ d \mid by_0$

or $\quad d \mid ax_0 + by_0 = m$

$\therefore$ $\quad d \le m$

$\therefore$ $\quad m = g = ax_0 + by_0.$

Note: Incidentally we have proved here that $d \mid m = g$,

i.e. If $\quad d \mid a,\ d \mid b$

then $\quad d \mid (a, b)$

And g *is the least positive integer of the form* $ax + by$

[The greatest common divisor can be characterized in the following two ways:

1. it is the least positive value of $ax + by$ where x and y range over all integers
2. it is the positive common divisor of a and b which is divisible by any common divisor.

Corollary 1.12. If $(a, b) = 1$ then there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$ [Put $g = 1$]

Conversely, if $a, b \in \mathbb{Z}^+$ and for $x, y \in \mathbb{Z}$, $ax + by = 1$ then $(a, b) = 1$

Proof: Suppose $(a, b) = d$

Then, for some $x, y \in \mathbb{Z}$ we have $ax + by = d$. And, given that $ax + by = 1$.

$\because$ 1 is the least positive integer, but d is the least positive integer of the form $ax + by$.

$\therefore$ $d = 1$.

Definition: If $(a, b) = 1$, then a, b are said to be **relatively prime.**

Theorem 1.13. Any non-void set of integers closed under addition and subtraction consists of zero alone or else consists of the least positive element and all the multiples of this element.

Proof: Let S be any non empty set of integers closed under addition and subtraction.

Let an integer $a \in S$. Then $a - a \in S$.

$\therefore$ $0 \in S$. Also $0 - a \in S$

$\because$ $a, -a \in S$, of these two, at least one is positive.

By WOP, the set of all positive elements of S will contains a least element, say d. We wish to show that every element of S is an integral multiple of d and conversely.

It is clear that if n is any positive integer,

$$nd = d + d + \ldots + d \ (n \text{ times}), \ \therefore \ nd \in S$$

$\therefore$ Thus any integral multiple of d is in S. Suppose now that $k \in S$

If d does not divide k, then by division algorithm

$$k = q \cdot d + r, \ q, r \in \mathbb{Z} \text{ and } 0 \leq r < d$$

Now,

$\because$ k and qd are elements of S and S is closed under subtraction, $r = k - q \cdot d$ is also a member of S.

$\therefore$ We must have $r = 0$.

Thus, every element of S is a multiple of d.

Example 18. $(4, 9) = 1$ $\therefore$ 4 and 9 are relatively prime

$(16, 15) = 1$ $\therefore$ 16 and 15 are relatively prime

Example 19. If $a, b, k \in \mathbb{Z}$, then $(a + kb, b) = (a, b)$

Solution: Let $(a, b) = d$, $(a + kb, b) = d_1$

Now $d \mid a, d \mid b$

gives $d \mid a + kb$.

And, $d \mid a + kb, d \mid b$

gives $d \mid d_1 \ (= (a + kb, b)$ ...(i)

Again, $(a + kb, b) = d_1$

gives $d_1 \mid a + kb, d_1 \mid b$

or $d_1 \mid (a + kb) - kb = a$

or $d_1 \mid a$, also $d_1 \mid b$

$\therefore$ $d_1 \mid (a, b) = d$ ...(ii)

So, from (i) and (ii), we get $d = d_1$.

Example 20. $a \nmid bc$, $(a, b) = 1$, $a, b, c \in \mathbb{Z}$. Then $a \mid c$

Solution: $(a, b) = 1 \Rightarrow ax + by = 1$ for some $x, y \in \mathbb{Z}$.

Then, $acx + bcy = c$ and $a \mid bc$

$\Rightarrow$ $a \mid acx + bcy$

or $a \mid c$.

Example 21. Show that for any positive integer m and a, b (not both zero) $(ma, mb) = m\,(a, b)$

Solution: If x, y are two integers then by above (ma, mb) = least positive value of $x \,.\, ma + y \,.\, mb = m$ (least positive value of $xa + yb$) $= m\,(a, b)$.

Definition: The greatest common divisor can be calculated by successive division and this process is known as *Euclidean Algorithm.*

For suppose a_0 and a_1 are two positive integers; then by division algorithm we have integers q_1 and a_2 such that

$$a_0 = q_1 a_1 + a_2,\ 0 \le a_2 < a_1$$

If $a_2 = 0$,

then $d = a_1 \qquad [d = (a_0, a_1)]$

If $a_2 \neq 0$

then divide a_1 by a_2. There exist integers q_2 and a_3 such that

$$a_1 = q_2 \,.\, a_2 + a_3 \text{ with } 0 \le a_3 < a_2.$$

If $a_3 = 0$

then $d = a_2$

If $a_3 \neq 0$ then we divide a_2 by a_3. There are integers q_3 and a_4

Such that $a_2 = q_2 a_3 + a_4,\ 0 \le a_4 < a_3.$

Proceeding in this way, we observe that the remainders are getting reduced successively since $a_2 > a_3 > a_4$ ... etc. After a finite number of steps say k, the remainder ak would be such that a_{k-1} is a multiple of a_k, so that the remainder for the k^{th} division is zero. We write this as follows:

$$\begin{aligned}
a_0 &= q_1 \,.\, a_1 + a_2 \\
a_1 &= q_2 \,.\, a_2 + a_3 \\
a_2 &= q_3 \,.\, a_3 + a_4 \\
&\cdots\ \cdots\ \cdots \\
&\cdots\ \cdots\ \cdots \\
a_{k-2} &= q_{k-1} \,.\, a_{k-1} + a_k \\
a_{k-1} &= q_k \,.\, a_k
\end{aligned}$$

Now we show that a_k is the g.c.d. of a_0 and a_1

From above we see that $a_k \mid a_{k-1}$. From the equation preceding the last, we get $a_k \mid a_{k-2}$, since a_k divides both the terms on the right. From the equations that precedes it, we conclude similarly that $a_k \mid a_{k-3}$. Continuing up the list in this way, we find that $a_k \mid a_0$ and $a_k \mid a_1$. We now show that if $b \mid a_0$ and $b \mid a_1$ then $b \mid a_k$.

$\because$ $b \mid a_0$ and $b \mid a_1$, the first equation above shows that $b \mid a_2$.

$\because$ $b \mid a_1$ and $b \mid a_2$ the second equation above shows that $b \mid a_3$. Continuing down the list we see that $b \mid a_k$

$\therefore$ $a_k = (a_0, a_1)$.

Definition: If $d \mid a_1, a_2, \ldots, a_n$ such that d is the greatest among the common positive divisors of $a_1, a_2, \ldots, a_n$ then d is called the ged of $a_1, a_2, \ldots, a_n$ and is denoted $d = (a_1, a_2, \ldots, a_n)$

Theorem 1.14. If $d = (a_1, a_2, \ldots, a_n)$, there are integers $x_1, x_2, \ldots, x_n$ such that
$d = a_1x_1 + a_1x_1 + a_2x_2 + \ldots + a_nx_n$ *(Extension)*

Proof: Let $S = \{a_1x_1 + a_2x + \ldots + a_nx_n \mid x_1, x_2, \ldots, x_n \in \mathbb{Z}\}$

Now here $\mid a_1 \mid \in S$, $\mid a_1 \mid = a_1\ sgna_1$ here, $x_1 = sgn\ a_1$, $x_2 = x_3 = \ldots = x_n = 0$.

[*sgn* stands for the word 'sign']

Thus S has a least positive member, d_0 say. We show that every member is divisible by d_0. By division algorithm, if m is any member of S, we have

$$m = d_0q + r,\ 0 \le r < d_0$$

Then $r = m - d_0q$.

Now $d_0 = a_1x_1 + a_2x_2 + . + a_nx_n$

and $m = a_1y_1 + a_2y_2 + \ldots + a_ny_n$,

for some integers $x_1, x_2, \ldots x_n$ and $y_1, y_2, \ldots y_n$.

Thus $r = a_1(y_1 - qx_1) + a_2(y_2 - qx_2) + \ldots + a_n(y_n - qx_n) \in S$

$\therefore$ by the definition of d_0 and by $0 \le r < d_0$, it follows that d_0 is a positive common divisor of $a_1, a_2, \ldots a_n$. Hence $d_0 \mid d$, by the definition of d.

But $d \mid a_i$ $(i = 1, 2, \ldots n)$ and $d_0 = a_1x_1 + a_2x_2 + .+ a_nx_n$; thus $d \mid d_0$.

$\therefore$ $d \le d_0$. Hence $d = d_0$ and the result follows.

Theorem 1.15. If $d = (a_1, a_2, \ldots a_n)$, then an integer d_1 is a common divisor of $a_1, a_2, \ldots a_n$ if and only if $d_1 \mid d$

Proof: If $d_1 \mid d$, then,

$\because$ d is a common divisor of $a_1, a_2, \ldots a_n$, it follows that $d_1 \mid a_i$ $(i = 1, 2, \ldots n)$. Thus d_1 is a common divisor of a_1, a_2, a_n.

Convensely, suppose that d_1 is a common divisor of $a_1, a_2, \ldots, a_n$. By the above theorem, there are integers $x_1, x_2, \ldots, x_n$ such that $d = a_1x_1 + a_2x_2 + \ldots + a_mx_m$.

Hence $d_1 \mid d$.

Theorem 1.16. If $a_1, a_2, \ldots a_n$ are nonzero integers and if $d_1 = a_1$, $d_2 = (d_1, a_2)$, $d_3 = (d_2, a_3) \ldots, d_n = (d_{n-1}, a_n)$, then $d_n = (a_1, a_2, \ldots, a_n)$

Proof: (is left as an exercise.)

Example 22. Express (726, 275) in the form $m \cdot 726 + n \cdot 275$

Solution:

1	275	726	2
	176	550	
1	99	176	1
	77	99	
2	22	77	3
	22	66	
	+	11	

$\therefore \quad 726 = 275.2 + 176$

$275 = 176.1 + 99$

$176 = 99.1 + 77$

$99 = 77.1 + 22$

$77 = 22.3 + 11$

$22 = 11.2$

Thus 11 is g.c.d

$\therefore \quad 11 = 77 - 22.3 = 77 - (99 - 77.1)3$

$= 77.4 - 99.3 = (176 - 99.1)4 - 99.3 = 176.4 - 99.7$

$= 176.4 - (275 - 176.1).7$

$= 176.11 - 275.7 = (726 - 275.2)\,11 - 275.7$

$= 726.11 - 275.29$

Thus $11 = m \cdot 726 + n \cdot 275$, where $m = 11$, $n = -29$.

Example 23. Prove that $4 \nmid (n^2 + 2)$ for any integer n

Solution: (i) Let n be an odd number. Then n^2 is also odd and

$\therefore \quad n^2 + 2$ is also an odd number. Hence $4 \nmid (n^2 + 2)$

(iv) Let n be an even number, then $4 \mid n^2$. Hence when 4 divides $n^2 + 2$, a remainder 2 is left.

$\therefore \quad 4 \nmid (n^2 + 2)$.

Example 24. Show that g.c.d. of $a + b$ and $a - b$ is either 1 or 2 if $(a, b) = 1$

Solution: *Case I.* Let $f = (a + b, a - b)$. Then

$f = m(a + b) + n(a - b)$

$= (m + n)a + (m - n)b = m'a + n'b.$

But $(a, b) = 1,$

$\therefore \quad f = 1$ [Some steps are missing!]

Case II. If $a = b$, then $(a, a) = 1$ gives $a = 1$. Then

$(a + b, a - b) = (2, 0) = 2.$

$\therefore$ The g.c.d. is either 1 or 2.

Example 25. If $(a, 4) = 2$ and $(b, 4) = 2$, prove that $(a + b, 4) = 4$

Solution: From hypothesis,

$a = 2a_1,$ where a_1 is an odd number

$b = 2b_1,$ where b_1 is an old number

$\therefore \quad a_1 + b_1 = 2m$ (say) as the sum of two odd numbers is always even.

So, $(a + b, 4) = 2(a_1 + b_1, 2) = 2(2m, 2) = 4(m, 1)$

$= 4$ (as $(m, 1) = 1$).

Example 26. If $x - y$ is even, then show that $x^2 - y^2$ is divisible by 4, x and y being positive integers.

Solution $\because$ $x - y$ is even, x and y should either be both odd or both even.

$\therefore$ $x + y$ is also even

Hence, $x^2 - y^2 = (x + y)(x - y)$

= (Multiple of 2) . (Multiple of 2)

= Multiple of 4 = an expression divisible by 4.

Example 27. Show that the difference between any number and its square is even.

Solution: $n^2 - n = n(n - 1)$ = Product of two consecutive number. Hence one of the two must be even.

$\therefore$ this number is divisible by 2.

Example 28. If $4x - y$ is $M(3)$, show that $4x^2 + 7xy - 2y^2$ is $M(9)$, [$M(n)$ denotes a multiple of n.]

Solution: $4x^2 + 7xy - 2y^2 = (4x - y)(x + 2y)$

$= (4x - y)\{(4x - y) - 3(x - y)\}$

$= M(3)\{M(3) - M(3)\}$

$= M(9)$.

Example 29. Show that the square of any integer b is of the form $4k$ or $8k + 1$.

Solution: By division algorithm, any integer b is representable as

$2q$ or $2q + 1$.

If $b = 2q$, then $b^2 = 4q^2$. Thus b^2 is of the form $4k$.

If $b = 2q + 1$, then $b^2 = 4q^2 + 4q + 1 = 4q(q + 1) + 1$.

$\because$ $q(q + 1)$ is divisible by 2, we get that b^2 is of the form $8k + 1$.

Example 30. Find all integers n such that $n^2 + 1$ is divisible by $n + 1$

Solution: Let n be an integer such that $n + 1 \mid n^2 + 1$.

Note that $n + 1 \mid (n + 1)(n - 1)$ i.e, $n + 1 \mid n^2 - 1$.

Hence, $n + 1 \mid (n^2 + 1) - (n^2 - 1)$ i.e., $n + 1 \mid 1$.

$\therefore$ $n + 1 = \pm 1, \pm 2$. So, $n = -3, -2, 0, 1$.

1.17 Some Properties

1. If $(a, b) = d$ then, $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$
2. If $a \mid bc$ and $(a, b) = 1$ then, $a \mid c$
3. If $c \neq 0$, $c \mid a$, $c \mid b$, $\left(\frac{a}{c}, \frac{b}{c}\right) = 1$ then $c = (a, b)$

Example 31. Prove that the fraction $\frac{21+n}{14n+3}$ is irreducible for every natural number n.

Solution: It is sufficient if we show that $(21 + n, 14n + 3) = 1$

Now, $21n + 4 = 1\,(14n + 3) + (7n + 1)$ [Dividing by $14n + 3$]

$14n + 3 = 2(7n + 1) + 1$ [Dividing by $7n + 1$]

$7n + 1 = 1\,.\,(7n + 1)$ [Dividing by 1]

Hence by Euclidean algorithm, $(21n + 4, 14n + 3) = 1$. Hence, the fraction $\frac{21+n}{14n+3}$ is irreducible for every natural numbers.

1.2.3 Lowest Common Multiple (L.C.M)

Consider $a, b \in \mathbb{Z}$. Let $S = \{x \mid x \in \mathbb{Z}^+$ and x is a common multiple of a and $b\}$ or, $= \{x \mid x \in \mathbb{Z}^+, a \mid x$ and $b \mid x\}$)

Now $a \mid a$ gives $a \mid \mid a \mid$ or, $a \mid \mid a \mid \mid b \mid$ or, $a \mid \mid ab \mid$ Similarly $b \mid \mid ab \mid$ and $\mid ab \mid \in \mathbb{Z}^+$. So, $\mid ab \mid \in S$.

$\therefore \quad S \neq \phi$.

Thus, S is a non-empty set of positive integers.

Hence by WOP, S has a least element(say)m.

Definition: This m is called the *lowest common multiple (LCM) of a and b*, written as $[a, b]$ or $\{a, b\}$

Definition: The integers $a_1, a_2, ..., a_n$, all different from zero, have common multiple b if $a_i \mid b$ for $i = 1, 2, ..., n$. The least of the positive common multiples is called *the least common multiple* of $a_1, a_2, ..., a_n$ and is denoted by $[a_1, a_2, .., a_n]$

Theorem 1.18. If $m = [a_1, a_2, ..., a_n]$ then there exists ℓ such that $a_i \mid \ell$, $i = 1, 2, ..., n$ if and only if $m \mid \ell$

Proof: Let $m \mid \ell$

Now, $a_i \mid m$, for $i = 1, 2, ..., n$

And, $m \mid \ell$ gives $a_i \mid \ell$, $(i = 1, 2, ..., n.)$

Conversely, let $a_i \mid \ell$ $(i = 1, 2, ..., n.)$.

Suppose, $m \nmid \ell$.

Then $\ell = mq + r$ $(0 < r < m)$

or, $r = \ell - mq$

Now, $a_i \mid \ell$, $a_i \mid m$ give $a_i \mid r$, $(i = 1, 2, ..., n)$

But m is least such that $a_i \mid m$, $(i = 1, 2, ..., n)$.

Hence $m \mid \ell$.

Theorem 1.19. If $m = [a, b]$ and $a \mid x$, $b \mid x$, then $m \mid x$ (i.e., m divides every common multiple of a and b.)

Proof: Follow from Theorem 1.18 above.

Theorem 1.20. If $(a, b) = 1$, then $[a, b] = |ab|$

Proof: Given that $1 = (a, b) = (|a|, |b|)$

Let $m = [a, b] = [|a|, |b|]$

Now $m = [|a|, |b|]$

gives $|a| m, |b| | m$

or $m = |a| q, \quad \therefore \quad |b| | |a| q$

$\therefore$ $|b| | q \qquad (\because (|a|, |b|) = 1)$

or, $|a|, |b| | |a| q \ (=m)$

or $|ab| \leq m$

But m is the least common multiple of a and b

$\therefore$ $m = |ab|$.

Example 32. For $a, b \in \mathbb{Z}^*$, $d = ax_0 + by_0$ is the smallest positive integer of the form $ax + by$, $(x, y, x_0, y_0 \in \mathbb{Z})$. Prove that $d = (a, b)$.

Solution: For, $ax + by$ and d, by Division Algorithm

we get $q, r \in \mathbb{Z}$ such that

$$ax + by = dq + r, \ (0 \leq r < d)$$
$$= q\,(ax_0 + by_0) + r$$

or $r = a(xqx_0) + b(y - qy_0) = ax' + by', \ x', y' \in \mathbb{Z}$

And d is the smallest positive integer of this type,

$\therefore$ $r = 0.$

Thus $ax + by = dq,$

for $x, y \in \mathbb{Z}$ and so $d \mid ax + by$. In particular, $d \mid a$, $d \mid b$ $(x = 0, y = 1, x = 1, y = 0)$

If $d_1 \mid a$, $d_1 \mid b$ then

$$d_1 \mid ax_0 + by_0 = d \text{ or } d_1 \mid d.$$

Hence $d = (a, b).$

Theorem 1.21. If b is any common multiple of $a_1, a_2, \ldots, a_n$, then $[a_1, a_2, \ldots, a_n] \mid b$. (In other words, if $h = [a_1, a_2, \ldots, a_n]$ then $0, \pm h, \pm 2h, \pm 3h, \ldots$ comprise all the multiples of $a_1, a_2, \ldots, a_n$.

Proof: Let $m \mid a_1, a_2, \ldots, a_n$ and $m \nmid h$

Then by division algorithm,

$$m = qh + r, \text{ for } 0 \leq r < h.$$

We now prove that $r = 0.$

If $r \neq 0$ then for each i as we have, $a_i \mid h$, and also $a_i \mid m$ so we have $a_i \mid r$. Thus r is a positive common multiple of $a_1, a_2, \ldots, a_n$ and this is a contradiction to the fact that h is the least positive of all common multiples.

Theorem 1.22. For $m > 0$, $[ma, m\,b] = m[a, b]$

Proof: Let $M = [ma, m\,b]$.

Then $ma \mid M$ and $mb \mid M$.

So we have

$$M = mx.$$

If $[a, b] = x_1$ we note that $a \mid x_1$, $b \mid x_1$, $am \mid mx_1$, $bm \mid mx_1$ and so $mx \mid mx_1$. Thus $x \mid x_1$. Also, $am \mid mx$, $bm \mid mx$, $a \mid x$, $b \mid x$ and so $x_1 \mid x$.

Hence $x = x_1$

$\therefore$ $M = mx = mx_1 = m[a, b]$.

$\therefore$ $[ma, mb] = m[a, b]$.

Theorem 1.23. $[a, b] \,.\, (a, b) = |\, a\, b\,|$

Proof: It is sufficient if we prove the result for positive integers only (why?)

First we consider the case: $(a, b) = 1$

Suppose $[a, b] = M$. Then, $M = ma$ for some m. Then $b \mid ma$ and $(a, b) = 1$. .

So $b \mid m$. Hence, $b \leq m$, $ba \leq ma$. But ba, being a positive common multiple of b and a, cannot be less than the least common multiple, and so $b = M$.

$\therefore$ $ba = ma = [a, b]$

Now we come to the general case:

Let $(a, b) = g(> 1)$. Then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

So by the above result we have $\left[\frac{a}{g}, \frac{b}{g}\right] = \frac{a}{g}.\frac{b}{g}$.

And this gives, $[a, b]\,(a, b) = ab$.

Example 33. If $(a, b) = 1$ then $a!b! \mid (a + b - 1)!$

Solution: Let $\dfrac{(a+b-1)!}{(a-1)!b!} = c$

and $\dfrac{(a+b-1)!}{a!(b-1)} = d$

Then $(a + b - 1)! = (a - 1)!\, b!\, c = a!(b - 1)!d$

And so $bc = ad$. $\because (a, b) = 1$, then $a \mid c$, that is, $c = ar$.

Thus $(a + b - 1)! = a!b!r$, which implies that $a!b! \mid (a + b - 1)!$.

Hence the resultant follows.

Example 34. Prove that the product of r consecutive integers is divisible by $r!$

Proof Let $P_n = n(n + 1)\,(n + 2) \ldots (n + r - 1)$.

Then, $P_{n+1} = n(n + 1)\,(n + 2) \ldots (n + r)$

$$\therefore \quad P_{n+1} - P_n = (n+1)(n+2)\ldots(n+r-1)\{(n+r)-n\}$$
$$= (n+1)(n+2)\ldots(n+r-1)\,r$$
$$= \frac{P_n}{n} r$$
$= r$ times the product of $(r-1)$ consecutive integers.

We now use induction as follows: Assume that the product of $(r-1)$ consecutive integers is divisible by $(r-1)!$,

Therefore, $P_{n+1} - P_n = r \,.\, m(\{r-1)!\} = m(r!)$

$\therefore \quad P_2 - P_1 = m(r!)$; But $P_1 = r!$; So, $P_2 = m(r!)$

$\therefore$ by induction $P_3, P_4, \ldots, P_n$ are all multiples of $r!$

Again the product of any two consecutive integers is divisible by 2!. Hence conclude that the product of any three consecutive integers is divisible by 3!, and so on.

1.3 THEORY OF SCALES OF NUMERATION

In the decimal system of numeration the digits 1, 2, 3, 4, 5, 6, 7, 8, 9 and 0 are used. Can we think of any other system using some or all of these digits? We have a few such systems viz., The decimal system and the binary system

We observe the following:

$$13 = 1 \,.\, 2^3 + 1 \,.\, 2^2 + 0 \,.\, 2 + 1 = (1101)_2$$
$$31 = 1 \,.\, 2^4 + 1 \,.\, 2^3 + 1 \,.\, 2^2 + 1 \,.\, 2 + 1 = (11111)_2$$
$$387 = 1 \,.\, 2^8 + 0 \,.\, 2^7 + \,.\, 2^6 + 1 \,.\, 2^5 + 1 \,.\, 2^4 + 0 \,.\, 2^3 + 1 \,.\, 2^2 + 1 \,.\, 2 + 1$$
$= (101110111)_2$ the binary representation of the number 387.

On the other hand

$$13 = 1 \,.\, 10 + 3;\ 31 = 3 \,.\, 10 + 1;\ 387 = 3 \,.\, 10^2 + 8 \,.\, 10 + 7$$

We now observe the following:

The ordinary decimal notation uses the representation of integers in the scale of 10 in the binary system and the same is in the scale of 2 etc.,

We now discuss some general result in this regard.

Theorem 1.24. Let S be a positive integer. If n is a positive integer such that

$$b_n S^n + b_{n-1} S^{n-1} + \ldots + b_1 S + b_0 = 0$$

where the integers b_i are such that

$$|b_i| \leq S - 1,$$

then $\quad b_i = 0 \ (i = 0, 1, 2, \ldots, n)$

Proof: From $b_n S^n + b_{n-1} S^{n-1} + \ldots + b_1 S + b_0 = 0$ we have

$$b_0 = k_0 S \text{ for some integer } k_0$$

Thus $\quad |b_0| \geq S$ unless $k_0 = 0$ and so $b_0 = 0$

Then we have

$$b_n S^n + b_{n-1} S^{n-1} + \ldots + b_1 S = 0$$

and so for some integer k_1 we have

$$b_1 = k_1 S$$

and in the same way we have

$$b_1 = 0 \text{ and so on.}$$

Hence finally we have $b_i = 0$ for all i.

Theorem 1.25. Suppose S is a positive integer (>1). Then each positive integer a can be expressed uniquely in the form

$$a = c_n S^n + c_{n-1} S^{n-1} + \ldots + c_1 S + c_0,$$

where $0 \le c_i \le S - 1$ $(i = 0, 1, 2, \ldots, n-1)$ and $0 < c_n \le S - 1$

Proof: Let a be a given integer and $B = \{k \in \mathbb{Z}^+ | \ S^{k-1} > a\}$

$\because S > 1$, S^{k+1} tend to infinity as k tends to infinity. Thus B is a non-empty subset of positive integers and therefore it contains a least element, say n.

Then $$S^n \le a < S^{n+1} \qquad \ldots(*)$$

and n is uniquely determined. By division algorithm we have,

$$a = c_n S^n + a_1 \qquad \ldots(**)$$

where $$0 \le a_1 < S^n \qquad \ldots(***)$$

Also form (*) $\quad 0 < c_n \le S - 1$. [how?]

Again using division algorithm we have

$$a_1 = c_{n-1} S^{n-1} + a_2, \qquad \ldots (****)$$

where $\quad 0 \le a_2 < S^{n-1}$.

Also by (**) $\quad 0 \le c_{n-1} \le S - 1$.

Thus from (**) and (****)

$$a = c_n S^n + c_{n-1} S^{n-1} + a_2.$$

Similarly we can deduce that there are c_i $(i = 0, 1, 2, \ldots, n)$ integers such that

$$a = c_n S^n + c_{n-1} S^{n-1} + \ldots + c_1 S + c_0,$$

where $0 \le c_i \le S - 1$ $(i = 0, 1, 2, \ldots, n-1)$ and $0 < c_n \le S - 1$ hold (that the expression is unique is left as an exercise).

The above stated expression is called the representation of a in the scale of S. The integer S *is called the base* of the scale.

Example 35. To illustrate base b notation, note that $(236)_7 = 2 \cdot 7^2 + 3 \cdot 7 + 6$ and $(10010011)_2 = 1 \cdot 27 + 1 \cdot 24 + 1 \cdot 21 + 1 = 147$

Computers use base 8 or base 16 for display purpose. In base 16, or, hexadecimal, notation there are 16 digits, usually denoted by 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *A*, *B*, *C*, *D*, *E*, *F*. The letters *A*, *B*, C, *D E* and *F* are used to represent the digits that correspond to 10, 11, 12, 13, 14 and 15 (written in decimal notation)

Example 36. To convert $(A35B0F)_{16}$ from hexadecimal notation to decimal notation we write

$(A35B0F)_{16} = 10 \cdot 16^5 + 3 \cdot 16^4 + 5 \cdot 16^3 + 11 \cdot 16^2 + 0 \cdot 16 + 15 = (10705679)_{10}$

A simple conversion is possible between binary and hexadecimal notation. We can write each hex digit as a block of four binary digits according to the corresponding given in the following table:

Hex digit	Binary digit	Hex digit	Binary digit
0	0000	8	1000
1	0001	9	1001
2	0010	*A*	1010
3	0011	*B*	1011
4	0100	*C*	1100
5	0101	*D*	1101
6	0110	*E*	1110
7	0111	*F*	1111

Convert $(2FB3)_{16}$ from hex to binary

Here each hex digit is converted to a block of four binary digits (the initial zero in the initial block $(0010)_2$ corresponding to the digit(2) 16 are omitted). And thus the corresponding binary representation is $(10111110110011)_2$

And to convert from binary to hex, if we take $(11110111101001)_2$ then we break this into blocks of four starting from the right. The blocks are from right to left, 1001, 1110, 1101, and 0011. And thus we get in hex as $(3DE9)_{16}$

When performing base r addition, subtraction and multiplication by hand, we can use the same familiar technique as use in decimal addition.

Example 37. To add $(1101)_2$ and $(1001)_2$ we write

1			*1*	
	1	1	0	1
+	1	0	0	1
1	0	1	1	0

Where we have indicated carries by 1's in italics written above the appropriate column. We found the binary digits of the sum by noting that $1 + 1 = 1 \cdot 2 + 0$, $0 + 0 + 1 = 0 \cdot 2 + 1$, $1 + 0 + 0 = 0 \cdot 2 + 1$, and $1 + 1 + 0 = 1 \cdot 2 + 0$.

To subtract $(101110)_2$ from $(11011)_2$ we have

	–1			
1	1	0	1	1
1	0	1	1	0
		1	0	1

Where –1 in italics above a column indicates a borrow. We found the binary digits of the difference by noting that $1 - 0 = 0 \cdot 2 + 1$, $1 - 1 + 0 = 0 \cdot 2 + 0$, $0 - 1 + 0 = -1 \cdot 2 + 1 \cdot 1 - 0 - 1 = 0 \cdot + 0$, and $1 - 1 + 0 = 0 \cdot 2 + 0$.

To multiply $(1101)_2$ and $(1110)_2$ we write

				1	1	0	1
			×	1	1	1	0
				0	0	0	0
			1	1	0	1	
		1	1	0	1		
	1	1	0	1			
1	0	1	1	0	1	1	0

We first multiplied $(1101)_2$ by each of $(1110)_2$, shifting each time by the appropriate number of places, and then we added the appropriate integers to find our product.

To divide $(11101)_2$ by $(111)_2$, we let $q = (q_2q_1q_0)_2$. We subtract $2^2(111)_2 = (11100)_2$ once from $(11101)_2$ to obtain $(1)_2$, and once more to obtain a negative result, so that $q_2 = 1$. Now $R_1 = (111010)_2 - (11100)_2 = (1)_2$. We find that $q_1 = 0$, since $R_1 - 2(111)_2$ is less than zero, and likewise $q_0 = 0$. Hence, the quotient of the division is $(100)_2$ and the remainder is $(1)_2$.

1.4 PRIME NUMBERS

If $a = 1$ then a has only one positive divisor viz. 1. If $|a| \neq 1$, then a has at least two positive divisors viz, 1 and $|a|$.

The **numbers** of positive divisors of a is **1** if $a = 1$ and > 1 if $|a| \neq 1$.

Definition: If $a > 0$ and a has exactly two positive divisors then a is called a *prime number.*

Definition: If $a > 0$ and a has more than two positive divisors, then a is called *a composite number.*

Remark: (i) 1 is not a prime number for, it has only 'one' positive divisor.
(ii) If p is a prime number then, 1 and p are the only positive divisors of p

Lemma 1.26. If p is a prime, then $(p, a) = 1$ or $p \mid a$.

Proof: Suppose $(a, p) = d$

Then, $d \mid p$, $d \mid a$ and p being a prime, it therefore follows that $d = 1$ or $d = p$

If $d = 1$ then we are done and if $d = p$ then from above it follows that $p \mid a$.

Hence either $d = 1$ or $d \mid a$ i.e., $(a, p) = 1$ or $p \mid a$.

Properties 1.27. If p is a prime and $p \mid ab$ then, $p \mid a$ or $p \mid b$, where $a, b \in \mathbb{Z}$

Proof: Let $p \nmid a$, then $(p, a) = 1$

$\therefore$ $\exists\ x, y \in \mathbb{Z}$ such that

$$px + ay = 1$$

And this gives, $pbx + aby = b$ ...(i)

Now $p \mid ab$

gives $ab = pk,\ k \in \mathbb{Z},$

$\therefore$ from (i) we get, $pbx + pky = b$

or $p(bx + ky) = b$

or $pq = b, \quad q \in \mathbb{Z}$

$\therefore$ $p \mid b$

Similarly if $p \nmid b$, then $p \mid a$.

Extension 1.28. If $p \mid a_1 . a_2 ..., a_n$ then, $p \mid a_1$, or $p \mid a_2$, or $..p \mid a_n$

(**proof** is repeated application of the above result.)

Corollary 1.29. If $p \mid p_1 . p_2 . ... p_n$ (p's are primes) then, p is one of $p_1, p_2, ..., p_n$

Proof: By Extension 1.28, $p \mid p_1 p_2 ..., p_n$ gives either $p \mid p_1$ or, $p \mid p_2 p_3 ... p_n$. If $p \nmid p_1$, then again by the same result we have $p \mid p_2$ or $p \mid p_3 p_4 ... p_n$. Hence with a finite number of application of the same result we get that $p \mid p_i$, for some i.

And

$\because$ p is a prime we must have

$$p = p_i.$$

Converse of the theorem 1.30. Let $p > 1$ and p has the property that if for any a, $b \in \mathbb{Z}$ $p \mid ab$ gives $p \mid a$ or $p \mid b$, then is a prime.

[**Note:** Both the theorems can be combined as **for** $a, b \in \mathbb{Z}$, $p \mid ab$ gives $p \mid a$ **or** $p \mid b$ *if and only if p is a prime.*]

Proof: Suppose p is not a prime. Then it is composite.

$\therefore$ $q \in \mathbb{Z}^+$ such that $q \mid p$ and $q \neq 1, p$ i.e. $1 < q < p$.

$\therefore$ $p = qr,\ 1 < r < p$

Now $p \mid p = qr$ gives $p \mid q$ or $p \mid r$.

But both q and r are positive integers ($< p$).

$\therefore$ $p < q$ or r. So we meet a contradiction.

$\therefore$ our assumption is wrong. So, p is prime.

Example 38. If $n = ab$, then at least one of a and b must be less than n [Left as exercise]

Theorem 1.31. If $a \neq 1$, $a \in Z$, a must have a prime factor.

Proof: Case (i) If a is a prime then a is itself a prime factor.

Case (ii) Let a be not prime. And $S = \{d \mid d > 1, d \in \mathbb{N}, d \mid a\}$

Now $|a| \mid a, |a| > 1$ gives $|a| \in S$.

$\therefore$ $S \neq \phi$.

$\therefore$ S is a non empty set of positive integers, and by W.O.P it has a least integer, say, p.

Assert: p is a prime

For $p \in S$, $p > 1$, $p \mid a$. So 1 and p are positive divisors of p. If possible let $q \neq p$ and $q \mid p$, $q \in \mathbb{N}$.

$\therefore \quad q < p$ ...(i)

But $p \mid a$, $q \mid p \Rightarrow q \mid a$ and so, $q \in S$

$\therefore \quad q \geq p$ and this contradicts (i)

Hence p is prime.

Properties 1.32. Every integer n (> 1) can be expressed as a product of finite number of primes.

Proof: If the integer is a prime then it itself stands as a product with a single factor. Otherwise by above theorem we have a prime factor p_1 such that

$$n = p_1 n_1, \ 1 < n_1 < n.$$

If n_1 is not a prime then again by the same result we have another prime p_2 such that $n_2 = p_2 n_3$, $1 < n_3 < n_2$. Similarly for n_3. This process of writing each composite number that arises as a product of factors gives us $n > n_2 > n_2 > n_3 > ...$, a descending chain of positive integers and it must therefore terminate after a finite steps.

Thus we can write n as a product of finite number of primes.

Remark: Every integer can be expressed as product of primes.

for $n = \pm[p_1 n_1]$, p_1 is prime, $1 < p_1 < n$

$= \pm[p_1 . p_2 . n_2] \ 1 < p_2 < n_1$

$= .....$

$= \pm[p_1 . p_2 . p_3 . ..., p_n]$; p's need not be all different.

[$n = 100 = 2 \times 50 = 2 \times 2 \times 25 = 2 \times 2 \times 5 \times 5$]

Note: Disregarding the order in which the primes are written, every natural number can be expressed as a product of primes and this is the result that we are going to prove below. Before giving the proof of the theorem we note the following.

Does the fundamental theorem need a proof at all? As Prof. *H R* Gupta says "Has any one ever come across an example where the theorem has failed? The following example will convince the reader about the necessity of a proof. [Selected Topics in Number Theory; *H* Gupta ABACUS PRESS, 1980]

Take the set {1, 4, 7, 10, 13, 22, 25, 28, 31, ...} of natural numbers. It is easy to see that the set is closed under multiplication. Call an element of the set a '*prime*' if it has exactly two divisors in the set. Thus, the primes of the set are 4, 7, 10, 19, 22, 25, 31,..

We observe that 100 belongs to the set and it can be written as a product of the primes of the set in two distinct ways:

$$100 = 4.25; \text{ also } 100 = 10.10.$$

Fundamental Theorem of Arithmetic (also know as unique factorization theorem) 1.33. The presentation of n(> 1), as a product of primes is unique apart from the order of factors.

Proof: Suppose that $n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$, where $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ are primes and suppose that the primes are ordered so that $p_1 \leq p_2 \leq \ldots \leq p$ and $q_1 \leq q_2 \leq \ldots \leq q_s$. We now prove that $r = s$ and $p_i = q_i$ $(i = 1, 2, \ldots r)$

The proof will be by induction.

The result is true for $n = 2$. Suppose that it is true for 2, 3, ..., $n - 1$ and consider the number n.

If n is a prime the result is true. Suppose n is not a prime. Then in the expression $n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$ we have $r > 1$ and $s > 1$. Then $p_1 = q_j$ and $q_1 = p_i$ for some i and j (by corollary 1.29) $\because p_1 \leq p_i = q_1 \leq q_j = p_1$, it follows that $p_1 = q_1$

Then the integer $\frac{n}{p_1}$ is such that $1 < \frac{n}{p_1} < n$, and we have

$$\frac{n}{p_1} = p_2 \ldots p_r = q_2 \ldots q_s.$$

Thus from the inductive hypothesis $r = s$ and $p_i = q_i$ (i = 2 ,,,... r) Hence $r = s$ and $p_i = q_i$ $(i = 1, 2, \ldots r)$

And the result follows by induction.

In the application of the fundamental theorem we frequently write any integer (> 1) in the form, sometimes called the "fundamental form"

$$n = p_1^{a_1} . p_2^{a_2} \ldots p_k^{a_k}$$

One may prove the above result if this form is used to write.

Proof: Suppose $n = p_1^{a_1} . p_2^{a_2} \ldots p_k^{a_k} = \ldots q_1^{b_1} . q_1^{b_2} \ldots q_j^{b_j}$, p's and q's are primes ....(*)

Assume that, $p_1 < p_2 < p_3 < \ldots < p_k$ and also $q_1 < q_2 < q_3 < \ldots < q_j$

Now $p_1 \mid p_1^{a_1} . p_2^{a_2} \ldots p_k^{a_k}$ (obviously).

$\therefore$ $p_1 \mid q_1 q_2 \ldots q_j$ So, $p_1 \mid q_1^{b_i}$, for some i $\in \{1, 2, \ldots, j\}$ so, $p_1 \mid q_i$,

Hence, $p_1 = q_i$.

$\therefore$ every p is some q.

Similarly, starting from right p's and q's are arranged in ascending order, so follows that $p_1 = q_1$, $p_2 = q_2$. and $k = j$.

Now to prove that $a_i = b_i$.

If not, say $b_i > a_i$. Dividing (*) by $p_i^{a_i}$, we get

$$p_1^{a_1} \; p_2^{a_2} . p_{i-1}^{a_{i-1}} \; p_{i+1}^{a_{i+1}} \ldots p_k^{a_k} = p_1^{b_1} \; p_1^{b_2} \ldots . p_i^{b_i - a_i} \ldots p_k^{b_k}$$

Hence $p_i \nmid$ LHS.

But $p_i \mid$ RHS and is contradiction. Thus

$$a_j = b_j.$$

Corollary 1.34. If $n \in \mathbb{Z}$ then $n = \pm p_1^{a_1} \; p_2^{a_2} \ldots . p_k^{a_k}$, $p_1 < p_2 < \ldots < p_k$

Theorem 1.35. There are infinitely many primes.

Proof: Suppose 2, 3, 5, 7, 11, ..., p be the finite set of primes up to p. Then let

$$q = 2.3.5.7.11 \ldots p + 1$$

Now q is not divisible by any of the primes 2, 3, 5, 7, 11, ..., p because if q is divided by any of these primes 1 is left as remainder.

Hence q is either a prime number itself or is divisible by some prime between p and q; in either case there is a prime number greater than p.

$\therefore$ the number of primes is not finite.

Theorem 1.36. No rational algebraic formula can represent prime numbers only.

Proof: If possible let the formula

$$a + bx + cx^2 + dx^3 + \ldots + kx^n \qquad \ldots(1)$$

represents prime numbers only.

When $x = m$, let its value be p.

Then $$p = a + bm + cm^2 + dm^3 + \ldots + km^n$$

When $x = m + np$, (1) gives

$$a + b\,(m + np) + c\,(m + np)^2 + \ldots + k\,(m + np)^n$$

i.e., $a + bm + cm^2 + dm^3 + \ldots + km^n + a$ multiple of p

$= p + a$ multiple of p

$= M(p)$, where symbol $M(p)$ stands for multiple of p

= an expression divisible by p

Hence, when $x = m + np$, (1) does not give a prime number.

This shows that there is no simple general formula for the n^{th} prime p_n, i.e., a formula by which we can calculate the value of p_n for any given n.

Theorem 1.37. There are arbitrarily large gaps in the series of primes. (In other wise, there exist k consecutive numbers composite whose length exceeds any given number k.

(given any positive integer n, there exist n consecutive composite integers.)

Proof: Consider the integers

$(k + 1)! + 2$, $(k + 1)! + 3$ .... $(k + 1)! + k$, $(k + 1)! + k + 1$.

Each of these numbers is a composite number because the number n divides $(k + 1)! + n$ if $2 \le n \le k + 1$ and these are the k consecutive integers which are composite.

Hence the theorem.

Example 39. There are infinitely many primes of the form $4n + 3$

Solution: Suppose 2, 3, 5, 7, 11 ... p are the primes up to p, and let $q = 2^2.3.5 \ldots p - 1$,

Now q is of the form $4n + 3$ and is not divisible by any of the prime 2, 3, 5 ... p. It cannot be a product of primes of the form $4n + 1$ only, because the product of two numbers of this form is of the same form. It is therefore either a prime or divisible by a prime of the form $4n + 3$, greater than p. Hence there are infinite number of primes of the form $4n + 3$.

Example 40. Prove that there are an infinite number of composite numbers among the numbers represented by the polynomial $f(x) \equiv a_0x^n + a_1x^{n-1} + \ldots + a_n$, where $n > 0$, a_0, a_1, ..., a_n are integers and $a_0 > 0$.

Solution: Suppose m is an integer such that $f(m) > 1$ and $f(x) > 0$ for $x \geq m$.

Suppose, $f(m) = M$.

Then all the numbers given by

$$f(m + Mt),\ t = 1, 2, \ldots$$

are composite as they are multiples of M.

Thus the result follows.

Example 41. Prove that $\frac{1}{2}+\frac{1}{3}+\frac{1}{3}+\ldots+\frac{1}{n} = S_n$ is never an integer.

Solution: Let k = largest of k_i, where $2k^i \leq n$

And $P = \Pi m$, m odd and $m \leq n$

Now $2^{k-1}PS_n = 2^{k-1}.3.5.7 \ldots S_n$

$$= 2^{k-1}3.5.7 \ldots \left(\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots+\frac{1}{n}\right)$$

= a sum all of whose terms are integers except the term

$2^{k-1}.3.5.7 \ldots \frac{1}{2^k}$ which is a fraction $\frac{3.5.7\ldots}{2}$

Thus, $2^{k-1}PS_n$ = a fraction. But $2^{k-1}P$ is an integer.

Hence S_n is not an integer.

Example 42. Let $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ can not be a prime for any x

Solution: Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, a's $\in \mathbb{Z}$

$f(x) = 0$ for at most n values

$f(x) = 1$ for at most n values

$f(x) = -1$ for at most n values.

Thus $f(x) = 0, 1, -1$, for at most $3n$ values.

$\therefore\ \exists\ y \in \mathbb{Z}$ such that $|f(y)| > 1$

Let $b = |f(y)|$

Consider $f(br + y) = a_0 + a_1 (br + y) + a_2 (br + y)^2 + \ldots a_n (br + y)^n$

$= f(y) + b.g(r)$

But, $b = |f(y)| \Rightarrow b \mid f(y)$ and also $b \mid b.g(r)$

$\therefore$ $b \mid f(br + y)$.

$f(br + y)$ is prime $\Rightarrow f(br + y) = \pm b$

$f(br + y) = \pm b$ for at most $2n$ values of r.

$\therefore$ for other values of r, it is composite.

$\therefore$ $f(x)$ is not a prime for any x.

Example 43. For what non trivial values of a and k, $a^k + 1$ will be prime?

Solution: Cases

(i) $a = 1$, $a^k + 1 = 1^k + 1 = 1 + 1 = 2$, a prime

(ii) $k = 1$, $a^k + 1 = a + 1$ is a prime if $a = p - 1$, p is a prime.

(iii) $a \neq 1$, $k \neq 1$

Let $a > 1$, $k > 1$.

If a is odd, a^k is odd then $a^k + 1$ is even.

$\therefore$ $a^k + 1$ is not a prime, if a is odd.

(iv) $a > 1$, $k > 1$, a is even and k is odd, $a + 1 \mid a^k + 1 \Rightarrow a^k + 1$ is not prime

(v) $a > 1$, $k > 1$, a is even and k is even.

Let $k = 2^{k_1} k_2$, k_2 is odd, $k_1 \geq 1$.

$$\therefore \quad a^k + 1 = a^{2^{k_1} k_2} + 1 = \left(a^{2^{k_1}}\right)^{k_2} + 1 = b^{k_2} + 1;$$

$\therefore$ $b + 1 \mid b^{k_2} + 1$ gives $b^{k_2} + 1$ is not prime

and k_2 is odd and $\neq 1$ gives $a^k + 1$ is not a prime.

$\therefore$ $a^k + 1$ is may be prime if $k_2 = 1$

(vi) $a > 1$, $k > 1$, a is even, k is even and of the form 2^{k_1} and then $a^k + 1 = a^{2^{k_1}} + 1$ is prime for some k_1. In particular, $2^{2^r} + 1$ is prime for some r.

Definition: $F_m = 2^{2^m+1}$ are called *Fermat number*

Fermat conjectured that F_m is prime for all $m \in \mathbb{Z}$.

$F_0 = 3$, $F_1 = 5$, $F_3 = 257$, $F_4 = 65537$, that $F_5 = 2^{2^5} + 1 = 4{,}294{,}967{,}297$ is not a prime was shown by Euler in 1732.

At the beginning Fermat conjectured that all the Fermat numbers are primes. In 1732, Euler pointed out that F_5 is a composite. This negated the Fermat conjecture. So, there are some primes and others are composite in Fermat numbers.

Up to now, we know only that the first five Fermat numbers

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$$

are primes and other 49 numbers F_n are composite; their respective n's are:

5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18,
19, 20, 21, 23, 25, 26, 27, 30, 32, 36, 38,
39, 42, 52, 55, 58, 63, 73, 77, 81, 117,
125, 144, 150, 207, 226, 228, 250, 267,
268, 284, 426, 452, 556, 744, 1945,

Besides these we do not know whether or not there are infinitely many Fermat primes. No new Fermat prime has been discovered for the last 30 years(since 1995), so many people conjecture that there are no more Fermat primes. This is still one of the unsolved problems in the theory of numbers.

The following elementary proof that $641 \mid F_5$ is due to G. Bennett (which does not explicitly involve division)

Example 44. The Fermat number F_5 is divisible by 641

Proof: We put $a = 2^7$ and $b = 5$, so that

$$1 + ab = 1 + 2^7.5 = 641$$

it is easily seen that

$$1 + ab - b^4 = 1 + (a - b^3)\, b = 1 + 3b = 2^4$$

But this implies that

$$\begin{aligned} F_5 &= 2^{2^5} + 1 = 2^{32} + 1 \\ &= 2^4a^4 + 1 \\ &= (1 + ab - b^4)a^4 + 1 \\ &= (1 + ab)a^4 + (1 - a^4b^4) \\ &= (1 + ab)\,[a^4 + (1 - ab)(1 + a^2b^2)] \text{ which gives } 641 \mid F_5. \end{aligned}$$

Conjecture: F_m is prime for finite number of m: Prove or disprove

Example 45. $d = (a^{2^m} + 1, a^{2^n} + 1) \mid 2$ if $m \neq n$

Solution: Given that $m \neq n$. Suppose $m < n$

$\therefore$ $n = m + k$, say. Then,

$a^{2^m} = x$ say. Then,

$$a^{2^n} = a^{2^{m+k}} = a^{2^m 2^k} = (a^{2^m})^{2^k} = x^{2^k}$$

Now $x + 1 \mid x^{2^k} - 1$, $k \geq 1$. Now

$$\begin{aligned} d &= (a^{2^m} + 1,\ a^{2^{m+k}} + 1) \\ &= (x + 1,\ x^{2^k} + 1) \mid x^{2^k} - 1,\ x^{2^k} + 1. \end{aligned}$$

$\therefore$ $d \mid x^{2^k} - 1,\ x^{2^k} + 1 \Rightarrow d \mid 2.$

Corollary 1.38. $(F_m, F_n) = 1$

Proof: (left as an exercise)

Note: Let us consider $a^k - 1$

(1) $a - 1 \mid a^k - 1$ $\therefore$ $a^k - 1$ may be a prime if $a = 2$

(2) $a = 2$, let $k = 1m$ (i.e. We are assuming $1 < 1 < k$; $1 < m < k$, that k is composite $\therefore 2^k - 1 = (2^1)^m - 1 \Rightarrow 2^1 - 1 \mid (2^1)^m - 1$. $\because 1 > 1$, $2^k - 1$ is not a prime if k is composite.

(3) $a^k - 1$ may be a prime if $a = 2$, $k > 1$ and k is a prime.

Numbers of the form $M_n = 2^n - 1$ $n > 1$ are called Mersenne numbers after a French monk Marin Mersenne who made an incorrect but provocative assertion concerning their primality. Those Mersenne numbers which happen to be prime are said to be Mersenne primes.

Definition: *If p is a prime then* $Mp = 2^p - 1$ is called a *Mersenne prime.*

(4) Mersenne said that Mp is a prime for $p \leq 257$. Subsequently it is found that Mp is a prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 257$

(5) There are also mistakes as, $p = 61$ gives Mp a prime.

Among the Mersenne numbers, there are some primes and others are composites. Up to now (*1995*) we know only the following *31* Mersenne primes for which the respective p's are

2, 3, 5, 7, 13, 17, 19, 31, 61, 81, 107, 127,
521, 601, 1279, 2203, 2281, 3217, 4253,
4423, 9689, 9941, 11213, 19937, 21701,
23209, 44497, 86243, 110503, 132049, 216091

$2^{6972593} - 1$ is the 38^{th} known Mersenne prime discovered on June 1, *1999* by one of the 12000 participants in the *Great Internet Mersenne Prime search.* It was also the first megaprime found (prime with more than a million digits). Some websites predict that the first bevaprime (prime with more than a billion digits) will be found by 2006. The complete list of the record primes found since 1951, the first year that an electronic computer found one, shows that 24 of these 26 record primes are Mersenne primes.

Lemma 1.39. The product of the numbers of the form $4m + 1$ is of the form $4m + 1$

Proof: $n_1 = 4k + 1$, $n_2 = 41 + 1$.

Then, $n_1 . n_2 = (4k + 1)(41 + 1) = 4m + 1$, for $m \in N$

Lemma 1.40. The product of the numbers of the form $4m + 3$ is of the for $4m + 1$.

Lemma 1.41. The product of the number of the form $4m + 1$ and $4m + 3$ is of the form $4m + 3$.

(Proofs are left as exercises).

Theorem 1.42. Show that there are infinite numbers of primes of the form (*a*) $4m + 3$, (*b*) $6m + 5$.

Proof: (*a*) If $p \neq 2$, then $p \equiv 1 (\text{mod } 4)$ or $p \equiv 3 (\text{mod } 4)$

Let us assume that there are finite number of primes of the form $4m + 3$, viz.

$$p_0 = 3, p_1 = 7, p_2 = 11, p_3 ..., p_n.$$

Consider $k = 4p_1 . p_2 ... p_n + 3 = 4M + 3$(say)

Case (i): If k is prime then it is a new prime of the form $4m + 3$. Similarly we may get another new prime and so on.

$\therefore$ the number of primes of the form $4m + 3$ is infinite.

Case (ii): If k is not a prime, Then $k = k_1.k_2.k_3 ... k_q$, (k_i is a prime). All the k_i's cannot be of the form $4m + 1$, since their product is of the form $4m + 3$.

$\therefore$ at least one of them, say k_1 is of the form $4m + 3$

$\therefore$ $k_1 \mid k$ But, $p_1 \nmid k$, $p_2 \nmid k$, .. $p_n \nmid k$. So, $k_1 \neq p_1, p_2, ... p_n$.

$\therefore$ k_1 is a new prime.

Similarly, we may get another new prime and so on.

$\therefore$ the number of primes of the form $4m + 3$ is infinite.

[The above problem can be stated in the following way also: The arithmetic progression:

3, 7, 11, 15, 19, ... and 5, 11, 17, 23, 29, ... contain an infinitude of primes. A famous theorem in number theory viz., *the theorem due to Dirichlet* reads: the arithmetic progression a, $a + b$, $a + 2b$, ... contains infinitely many primes if the integers a and b (both positive) are relatively prime, that is if $(a, b) = 1$]

Theorem 1.43. If p_n is the n^{th} prime number, then $p_n < 2^{2^n}$

Proof: Proof will be by induction. It is clear that

$$p_1 = 2 < 2^{2^1}.$$

Assume $p_i < 2^{2^i}$, $i < k + 1$, and let $N \leq p_1 \ldots p_k + 1$ [N is a prime]. Then

$$N < 2^{2^{k+1}}.$$

Example 46. $F_0F_1 \ldots F_{n-1} = F_n - 2$, where $F_n = 2^{2^n} + 1$.

Solution: We prove it by induction

If $n = 1$, then $F_0 = F_1 - 2$.

$\because$ $F_0 = 3$, $F_1 = 5$ the formula is valid when $n = 1$. Assuming the formula holds for $n - 1$, then

$$\begin{aligned} F_0F_1 \ldots F_{n-1} &= (F_{n-2} - 2)F_{n-1} \\ &= (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1) = \left(2^{2^{n-1}}\right)^2 - 1 \\ &= 2^{2^n} - 1 = F_n - 2 \end{aligned}$$

Hence the result.

Example 47. Show that $\exists k \in \mathbb{N}$ for which $1.2.3 \ldots (n-2)(n-1) + 1 = n^k$ is true when $n > 5$ ... (*)

Solution: Case (i): Let n be composite. Let $d \mid n$, $d \neq 1$

$\therefore$ $d \mid$ RHS $(=n^k)$ of (*)

But, $d \nmid$ LHS, a contradiction, n cannot be composite.

Case (ii): Let n be a prime.

(*) gives,

$$1.2.3 \ldots (n-2)(n-1) = n^k - 1 = (n-1)\{n^{k-1} + \ldots n + 1\}$$

Dividing by $(n - 1)$,

$$1.2.3 \ldots (n-2) = n^{k-1} + n^{k-2} + \ldots +$$

When $n > 5$, the product on the left contains a factor 2 and $\frac{1}{2}(n - 1)$.

$\therefore$ LHS is divisible by $2\frac{1}{2}(n-1)$. But, RHS is not. {$\because$ when we put $n = 1$, then RHS $1 + 1 + + 1 = k \neq 0$.

Example 48. If p is a prime greater than 3 then show that $2p + 1$ and $4p + 1$ cannot be primes simultaneously.

Solution: $\because$ p is a prime greater than 3, p is either of the type $3k + 1$ or $3k + 2$. If p is of the type $3k + 1$ then $2p + 1 = 2(3k + 1) + 1 = 6k + 3 = 3(2k + 1)$. Hence, $3 \mid 2p + 1$ and $2p + 1$ cannot be a prime. Similarly, if p is of the type $3k + 2$ then $3 \mid 4p + 1$ and it cannot be a prime.

Example 49. If a is a composite integer, and q is its least positive divisor, then $q \leq \sqrt{a}$.

Solution: $\because$ q is a divisor of a, we have

$$a = qa_1.$$

So here, $a_1 \geq q$.

Hence $a \geq q^2$ that is,

$$q \leq \sqrt{a}.$$

Example 50. If m is a composite integer, prove that the following integer is so too:

$$n_m = \underbrace{11.....11}_{m \text{ times}}$$

Proof: Let $m = ab$. Then

$$10^m - 1 = (10^a)^b - 1 = (10^a - 1)(10^{a(b-1)} + ... + 10^a + 1),$$

or $$\underbrace{9\,11.....11}_{m \text{ times}} = 9\underbrace{11.....11}_{a \text{ times}}(10^{a(b-1)} + ... + 10^a + 1)$$

or $$\underbrace{11.....11}_{m \text{ times}} = \underbrace{11.....11}_{a \text{ times}}(10^{a(b-1)} + ... + 10^a + 1)$$

Thus $n_a \mid n_m$. Hence if n_m is a prime integer then so is m.

Note: (i) But the converse is not true. For $n_3 = 111 = 3.37$ and $n_5 = 11111 = 41.271$ are both composite.

(ii) We know that $n_2, n_{19}, n_{23}, n_{317}$ are prime integers. 50 years after the discovery of n_{23}, n_{317} in 1978 using the computer, it was conjectured that the next such prime would be n_{1031} but the conjecture has not yet been proved.

Example 51. If p is a prime then prove that there exist no positive integers a and b such that $a^2 = pb^2$

Solution Suppose there are two positive integers a and b such that $a^2 = pb^2$ and let $(a, b) = d$. Then $a = da_1$, $b = db_1$, $(a_1, b_1) = 1$. Substituting this in above we get

$$a_1^2 = pb_1^2. \text{ Obviously } p \mid a_1^2 \text{ and then } p \mid a_1$$

Putting $a_1 = pa_2$, we have

$$a_2^2 p = b_1^2. \text{ Clearly } p \mid b_1^2 \text{ and then } p \mid b_1.$$

$\therefore$ p is a common divisor of a_1 and b_1. And this is a contradiction with the fact that $(a_1, b_1) = 1$ Hence the result.

Example 52. If a, b are relatively primes, and $d \mid ab$, then there exist unique d_1 and d_2 with $d_1 \mid a$, $d_2 \mid b$ such that $d \mid d_1 d_2$

Solution: Suppose $a = p_1^{a_1} \; p_r^{a_r}$, $b = q_1^{b_1} \ldots q_s^{b_s}$

Then $ab = p_1^{a_1} \ldots p_r^{a_r} q_1^{b_1} \ldots q_s^{b_s}$

$d = p_1^{t_1} \ldots p_r^{t_r} q_1^{k_1} \ldots q_s^{k_s}$, $0 < t_i < a_i$, $0 < k_i < b_i$

Let $d_1 = p_1^{t_1} \ldots p_r^{t_r}$, $d_2 = q_1^{k_1} \ldots q_s^{k_s}$.

Then $d = d_1 d_2$, and clearly d_1, d_2 are unique.

Hence the result follows.

Example 53. If n is a positive integer and $p = 4n + 3$, $q = 8n + 7$ are two primes, then $q \mid Mp$

Solution: (Left as an exercise)

Note: Hence we have

$$23 \mid M_{11}, \quad 47 \mid M_{21}, \quad 167 \mid M_{81}, \quad 263 \mid M_{121}$$
$$359 \mid M_{177}, 388 \mid M_{191}, 479 \mid M_{321}, 503 \mid M_{251}$$

Example 54. If p is a prime > 5 prove that $(p - 1)!$ is divisible by $(p - 1)^2$

Solution: $\because$ $p > 5$, $(p - 1)!$ has factors 2, $p - 1$, $\frac{p-1}{2}$ as $p - 1$ is even. Hence $(p - 1)!$ divisible by $(p - 1)^2$.

1.5 INTEGRAL PART OF n: $[n]$

$[n]$ means the integral part of n or in other words $[n]$ means the largest integer $\leq n$

$$[5] = 5, [4] = 4, \left[4\frac{2}{3}\right] = 4[-5.79] = -6 \text{ etc.}$$

The function $\{n\} = n - [n]$ is called the fractional part of n.

Thus $$\{4\} = 0, \left[4\frac{2}{3}\right] = \frac{2}{3}, \{5.76\} = .76$$

Observe: $\frac{40}{3} = 13.333..$, $\frac{40}{3} = 4.44 \ldots$, $\frac{40}{27} = 1.481...$

$$\therefore \quad \left[\frac{40}{3}\right] + \left[\frac{40}{3^2}\right] + \left[\frac{40}{3^3}\right] = 13 + 4 + 1 = 18$$

Now we prove the following theorem.

Theorem 1.44. The power with which a given prime number p enters into the product $n!$ is

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

Proof: The number of factors of the product $n!$ which are multiples of p is $\left[\frac{n}{p}\right]$, such numbers are $p, 2p, 3p, \ldots$

The numbers of factors of the product $n!$ are multiples of p^2 is $\left[\frac{n}{p^2}\right]$

The number of the factors of the product $n!$ which are multiples of p^3 is $\left[\frac{n}{p^3}\right]$ and so on.

Here each factor of the product $n!$ which is a multiple of the maximal p^m is counted m times by the above process as a multiple of $p, p^2, p^3, \ldots$ and finally p^m

Hence the highest power of p contained in $n! = \left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots.$

Example 55. Find the highest power of 3 which is contained in 1000!

Solution: The required number

$$=\left[\frac{1000}{3}\right]+\left[\frac{1000}{3^2}\right]+\left[\frac{1000}{3^3}\right]+\left[\frac{1000}{3^4}\right]+\left[\frac{1000}{3^5}\right]+\left[\frac{1000}{3^6}\right]$$

$$= 333 + 111 + 37 + 12 + 4 + 1 = 498.$$

Example 56. Find the number of multiples of 7 among the integers from 200 to 500.

Solution: Here $\left[\frac{500}{7}\right] = 71$ and $\left[\frac{199}{7}\right] = 28$ the required number is $71 - 28 = 43$.

Example 57. If x is a positive real number and n is a positive integer, then among the integers from 1 to x, the number of multiples of n is $\left[\frac{x}{n}\right]$.

Solution: We know $\left[\frac{x}{n}\right] \le \frac{x}{n} < \left[\frac{x}{n}\right] + 1$

So we have $\left[\frac{x}{n}\right]n \le x \le \left\{\left[\frac{x}{n}\right]+1\right\}n$

Thus among the integers from 1 to x, the multiples of n are only $n, 2n, \ldots \left[\frac{x}{n}\right]n$,

The total of which is $\left[\frac{x}{n}\right]$. Hence the result.

Now we prove the following theorems

Theorem 1.45.

(a) If $m \in \mathbb{Z}$, then $[m + \alpha] = m + [\alpha]$.

(b) For $\alpha, \beta \in \mathbb{Z}$, $[\alpha + \beta] - 1 \le [\alpha] + [\beta] \le [\alpha + \beta] \le [\alpha] + [\beta] + 1$

Proof: (a) Let $\alpha = [\alpha] + \theta,\ 0 \le \theta < 1$

And $m = [m]$

Then, $[m + \alpha] = [[m] + [\alpha] + \theta] = [m] + [\alpha] = m + [\alpha].//$

(b) $[\alpha + \beta] = [[\alpha] + \theta + [\beta] + \phi],\ 0 \le \theta, \phi < 1$

$= [[\alpha] + [\beta] + (\theta + \phi)],\ 0 \le \theta + \phi < 2$

$= [\alpha] + [\beta] + [\theta + \phi]$, by theorem (a)

$\therefore \quad [\alpha + \beta] \ge [\alpha] + [\beta]$

Again $[\alpha + \beta] - [\theta + \phi] = [\alpha] + [\beta]$

And $[\alpha + \beta] - 1 \le [\alpha] + [\beta], \quad [\because (\theta + \phi) \le 1]$

$\therefore \quad [\alpha + \beta] - 1 \le [\alpha] + [\beta] \le [\alpha + \beta]$ ...(*)

Again, $[\alpha + \beta] = [\alpha] + [\beta] + [\theta + \phi] \le [\alpha] + [\beta] + 1$ ...(**)

Combining (*) and (**) we get

$$[\alpha + \beta] - 1 \le [\alpha] + [\beta] \le [\alpha + \beta] \le [\alpha] + [\beta] + 1.//$$

Example 58. For any x, $[x] + [-x] = 0$ or -1 according as x is an integer or a fraction.

Solution: If x an integer then $[x] = x$ and $[-x] = -x$

Therefore, $[-x] + [x] = 0$

Suppose x is not an integer then,

$x = [x] + \theta,\ 0 \le \theta < 1$

Then, $-x = -[x] - \theta$

$= -[x] - 1 + (1 - \theta) = -[x] - 1 + \theta_1,\ (0 \le \theta_1 < 1)$

Therefore, $[-x] = -[x] - 1$ or, $[-x] + [x] = -1$.

Example 59. If a be a real number, c an integer > 0, prove that

$$\left[\frac{[a]}{c}\right] = \left[\frac{a}{c}\right].$$

Solution: Let $a = [a] + \theta, \quad 0 \le \theta < 1$

$[a] = cq + r, \quad q, r \in z$

$0 \le r < c$

$\therefore \quad a = cq + r + \theta$

Then, $\left[\frac{[a]}{c}\right] = \left[q + \frac{r}{c}\right] = q$ and $\left[\frac{a}{c}\right] = \left[q + \frac{r+\theta}{c}\right] = q$

Hence the result.

Example 60. If n is a positive integer then

$$[x] + \left[x + \frac{1}{n}\right] + \ldots + \left[x + \frac{n-1}{n}\right]\Bigg] = [nx]$$

Solution: Write $f(x) = \left[x + \frac{1}{n}\right] + \ldots + \left[x + \frac{n-1}{n}\right] - [nx]$

Then $f(x) = f\left(x + \frac{1}{n}\right)$ $\left[\text{Note: } [x] = \left[x + \frac{1}{n}\right]\right]$

(**Hint:** Consider the range $0 \le x < \frac{1}{n}$)

Example 61. Suppose that a and b are irrational numbers such that $\frac{1}{a} + \frac{1}{b} = 1$.

Show that every nonnegative integer can be uniquely expressed as either $[ka]$ or $[kb]$ for some integer k.

Solution: Reduce to the case $1 < a < 2$, and hence $b > 2$.

Let n be an integer such that $[ka] < n < n + 1 \le [(k + 1)a]$.

Since $a = \frac{b}{b-1}$, we have

$$k\frac{b}{b-1} < n < n + 1 < k\frac{b}{b-1} + \frac{b}{b-1}, \text{ from which we get}$$

$$0 < nb - kb - n < nb - kb - n + b - 1 < b.$$

The first inequality implies $n < (n - k)b$.

The last inequality implies $(n - k)\, b - 1 < n$;

$\therefore \quad [(n - k)b] = n.$

For uniqueness, suppose

$$[ka] = [kb].$$

Then, if $k > 0$, then $[a] = [b]$.

But since $\frac{1}{a} + \frac{1}{b} = 1$, one of a and b must be greater than 2, and the other less than 2.

EXERCISES 1.1

1. Prove by *axiom of induction* that
   (i) $2^n \rangle n$, for all $n \in \mathbb{N}$
   (ii) 4 divides $n(n + 1)(n + 2)(n + 3)$ for all $n \in \mathbb{N}$
   (iii) $1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$.
2. By the *principle of mathematical induction* prove that: [(i) to (x)]
   (i) $na + nb = n(a + b)$
   (ii) $1 \le n$
   (iii) $ma + na = (m + n)a$
   (iv) $1.2 + 2.2^2 + 3.2^3 + \ldots + n.2^n = (n - 1)\, 2^{n+1} + 2$

(v) $\frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+\ldots+\frac{1}{n.(n+1)}=\frac{n}{n+1}$

(vi) $3.1.2 + 3.2.3 + 3.3.4 + \ldots + 3.n.(n+1) = n(n+1)(n+2)$

(vii) $1^2 - 2^2 + 3^2 - 4^2 + \ldots + (-1)^{n-1}n^2 = (-1)^{n-1}\frac{n(n+1)}{2}$

(viii) For all integers $n \geq 2$, the product of n odd integers is odd

(ix) $3^{2n} - 1$ is divisible by 8

(x) $x^n - y^n$ is divisible by $x - y$

(xi) Prove by induction the permutation formula

$$p(n, m) = m(m-1)(m-2) \ldots (m-n+1)$$

(xii) Show that in the proposition $P(n)$: $2^n > 2n + 1$, $n \in \mathbb{N}$, although $P(k) \Rightarrow P(k+1)$, yet the proposition is not true in $\mathbb{N}$.

3. Prove the commutative law of addition and multiplication for the positive integers

4. For $m, n, p \in \mathbb{N}$, prove the following:

(i) if $m + p = n + p$ then $m = n$

(ii) If $m + p < n + p$ then $m < n$

(iii) If $m.p < n.p$ then $m < n$

(iv) $m.(n.p) = (m.n).p$

5. Prove the law of Trichotomy for natural numbers (using Peano's Axioms).

6. Using properties of integers, prove that for any two integers a, b

(i) $a - 0 = a$

(ii) $-(a - b) = -a + b$

(iii) $(-a)(-b) = ab$

(iv) $a(-b) = -(ab)$

(v) $a(-b) = -(ab)$

(vi) If $ab = 0$ then $a = 0$ or $b = 0$.

7. Prove that $-0 = 0$.

8. Use the well ordering property to show that $\sqrt{3}$ is irrational number.

EXERCISES 1.2

1. For $m \in \mathbb{N}$, prove that $(ma, mb) = m(a, b)$, $a, b \in \mathbb{N}$.

2. Prove that $d \mid a, d \mid b \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$.

3. Prove that $(a, b) = d \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

4. Prove that $(a, b) = (a, b \pm a) = (a, b + na) = (a + nb, b)$.

5. Find the greatest common divisor d of the numbers 963,657 and find the integers m and n such that $d = m.657 + n.963$.
6. Find the values of m, n to satisfy
   (i) $198.m + 243.n = 9$
   (ii) $71.m - 50.n = 1$
   (iii) $93.m - 81$, $n = 3$.
7. If x, y are integers, find the least positive value of
   (i) $963x + 99y$
   (ii) $121x + 891y$.
8. Prove that if $(a, b) = 1$ and $(b, c) = 1$ then $(ac, b) = 1$.
9. Show that if $ad\text{-}bc = 1$ then $(a + b, c + d) = 1$.
10. If $a + b \neq 0$, $(a, b) = 1$, and p is an odd prime, then prove that
$$\left(a + b, \frac{a^p + b^p}{a + b}\right) = 1 \text{ or } p.$$
11. Prove that $(a + b, a - b) \geq (a, b)$.
12. Prove that, if $a \mid m$, $b \mid m$ and if $(a, b) = 1$ then $ab \mid m$.
13. Determine whether the following assertions concerning integers are true of false. If true, prove the result, and if false, give a counter example
   (i) If $b \mid a^2 + 1$ then $b \mid a^4 + 1$
   (ii) If $b \mid a^2 - 1$ then be $\mid a^4 - 1$
   (iii) If p is a prime and $p \mid a$, $p \mid a^2 + b^2$ then $p \mid b$
   (iv) If p is prime and $p \mid a$, $p \mid a^2 + 6b^2$ then $p \mid b$.
14. If a and b are integers, b being non-zero, then prove that there are unique integers q and r such that $a = qb + r$ where $-\frac{1}{2} \mid b \mid \leq r \leq \frac{1}{2} \mid b \mid$ [In this case, r is called the *least absolute remainders of a with respect to b*].
15. If $(a, b) = 1$ then show that $(a + b, a - b) = 1$ or 2.
16. Prove : $4 \nmid n^2 + 2$ for any integer n.
17. If $(a, 4) = (b, 4) = 2$, then prove that $(a + b, 4) = 4$.
18. If for $k \in \mathbb{Z}$, $M(k)$ stands for multiple of k then
$$4xy - y \text{ is } M(3) \Rightarrow 4x^2 + 7xy - 2y^2 \text{ is } M(9).$$
19. Using the Euclidean algorithm find the greatest common divisor (g*cd*) of
   (i) 7468 and 2464
   (ii) 2689 and 4001
   (iii) 2947 and 3997
   (iv) 1109 and 4999.
20. Find the greatest common divisor g of the numbers 1819 and 3587, and find integers x and y to satisfy $1819x + 3587y = g$.

21. Find the values of x and y to satisfy

(a) $243x + 198y = 9$

(*b*) $71x - 50y = 1$

(c) $43x + 64y = 1$

(d) $93x - 81y = 3$

(e) $6x + 10y + 15z = 1$.

22. Prove that the product of three consecutive integers is divisible by 6; of four consecutive integers by 24.

23. Two integers are said to be of the same parity if they are both even or both odd: if one is even and the other is odd, they are said to be of opposite parity, or of different parity.

Given any two integers, prove that their sum and their difference are of the same parity.

24. Prove:

(i) that $n^2 - n$ is divisible 2 for every integer n;

(ii) that $n^3 - n$ is divisible by 6;

(iii) that $n^5 - n$ is divisible by 30.

25. Prove that if x and y are both odd, then $x^2 + y^2$ is even but not divisible by 4.

26. Prove that any integer is of the form $3k$ or of the form $3k + 1$ or of the form $3k + 2$.

27. Prove that if an integer is of the form $6k + 5$ then it is necessarily of the form $3k - 1$, but not conversely.

28. Prove that the square of any integer of the form $5k + 1$ is of the same form.

29. Prove that the square of any integer is of the form $3k$ or $3k + 1$ but not of the form $3k + 2$.

30. Prove that no integers x and y exist satisfying $x + y = 100$ and $(x, y) = 3$.

31. Prove that there are infinite pairs of integers x and y satisfying $x + y = 100$ and $(x, y) = 5$.

32. Prove that $[a, b] = \dfrac{ab}{(a, b)}$.

33. If $D = \dfrac{d}{(b, d)}$ and $B = \dfrac{b}{(b, d)}$, then show that $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{(aD + cB)}{[b, d]}$.

{Discuss the relationship between this equation and the addition of fractions by means of a 'common denominator'}.

34. Prove that $(a + b, a - b) \mid (a, b)$.

35. Prove that if a and b are nonzero integers, then $(a, b) \mid [a, b]$.

36. Let $\langle m \rangle$ be the set of all integral multiples of the integer m. Then prove that $\langle m \rangle \cap \langle n \rangle = \langle [m, n] \rangle$.

37. A sequence a_n is such that $a_1 = a$, $a_2 = b$ and $a_n = ca_{n-1} + ea_{n-2}$ if $n > 2$.
(a) Prove that, if $d = (a, b)$, then $d \mid a_n$ for all $n \geq 1$
(*b*) Prove that, if $f = (a_m, a_{m-1})$ and $(f, e) = 1$ then $f \mid d$.

38. Prove that if a and b are positive integers such that $(a, b) = [a, b]$, then $a = b$.

39. Evaluate $(n, n + 1)$ and $[n, n + 1]$ when n is a positive integer.

40. Find the values of (a, b) and $[a, b]$ if a and b are positive integers such that $a \mid b$.

41. Prove that $(a, b) = (a + b, [a, b])$.

42. The sum of two positive integers is 5264 and their least common multiple is 200, 340. Determine the two integers.

43. Find the highest power of 2 in $(2r - 1)!$.

44. Prove that the number $\dfrac{(n_1 + n_2 + \ldots + \ldots n_k)!}{n_1!.n_2!\ldots n_k!}$ is an integer.

45. If $r = \dfrac{4}{3}$, prove that there are infinitely many positive integers n such that $[nr]$ are primes.

EXERCISES 1.3

1. Convert $(1999)_{10}$ from decimal to base 7 notations. Convert $(6105)_7$ from base 7 to decimal notation.

2. Convert $(89156)_{10}$ from decimal notation to base 8 notation. Convert $(706113)_8$ from base 8 notation to decimal notation.

3. Convert $(10101111)_2$ from binary to decimal notation and $(999)_{10}$ from decimal to binary notation.

4. Convert $(ABCDEF)_{16}$, $(DEFACED)_{16}$, and $(AOB)_{16}$ from hexadecimal to binary.

5. Add $(101111011)_2$ and $(1100111011)_2$.

6. Add $(100001000111101)_2$ and $(11111101011111)_2$

7. Subtract $(11010111)_2$ from $(1111000011)_2$.

8. Subtract $(11110101)_2$ from $(1101101100)_2$.

9. Multiply $(11101)_2$ and $(110001)_2$

10. Add $(1234321)_5$ and $(2030104)_5$, $(3314430)_5$

11. Subtract $(434421)_5$ from $(4434201)_5$

12. Multiply $(1234)_5$ and $(3002)_5$

13. Add$(ABAB)_{16}$ and $(BABA)_{16}$

14. Subtract $(CAFE)_{16}$ from $(BAD)_{16}$

15. Multiply $FACE_{16}$ and BAD_{16}

EXERCISES 1.4

1. Show that there are infinitely many primes of the form $6n - 1$.
2. Show that there are infinitely many primes of the form $4n - 1$.
3. Find the canonical decomposition of the numbers
   (a) 82798848
   (b) 8105722663500.
4. Show that the product of numbers of the form $6k + 1$ is of the same form.
5. Prove that any prime of the form $3k + 1$ is of the form $6k + 1$.
6. Prove that any positive integer of the form $3k + 2$ has a prime factor of the same form; similarly for each of the form $4k + 3$ and $6k + 5$.
7. If x and y are prime to 3, prove that $x^2 + y^2$ cannot be a perfect square.
8. If $(a, b) = p$, a prime, what are the possible values of (a^2, b)? of (a^3, b)? of (a^2, b^2).
9. Evaluate (ab, p^4) and $(a + b, p^4)$ given that $(a, p^2) = p$ and $(b, p^3) = p^2$ where p is a prime.
10. If p is a prime and $p \mid (a^2 + b^2)$ and $p \mid (b^2 + c^2)$ then prove that $p \mid (a^2 \pm c^2)$.
11. If a prime integer $p > 3$, then prove that $2p + 1$ and $4p + 1$ cannot be prime simultaneously.
12. If $a_1 + a_2 + \ldots + a_r = n$ and all a's ≥ 0, then prove that $\dfrac{n!}{a_1!a_2!a_3!\ldots a_r!}$ is an integer.
13. Prove that if $a \geq 3$ and $n \geq 2$, then $a^n - 1$ is composite
14. Show that highest power of 2 contained in $(2^r - 1)!$ is $2^r - r - 1$
15. Show that the highest power of n which is contained in $(n^r - 1)!$ is $\dfrac{n^r - nr + r - 1}{n - r}$.
16. Show that $[x] + \left[x + \dfrac{1}{2}\right] = [2x]$ whenever x is any real number.
17. Show that $[2x] + [2y] \geq [x] + [y] + [x + y]$ whenever x and y are real numbers.
18. Show that if x and y are real numbers then $[xy] \geq [x]\,[y]$. What is the situation when both x and y are negative? When one of x and y is negative and the other positive.
19. Show that $\left[x + \dfrac{1}{2}\right]$ is the integer nearest to x (when there are two integers equidistant from x it is the larger of the two).
20. Show that $\sum_{j=0}^{n-1} [x + j/n] = [nx]$ whenever x is a real number and n is a positive integer.

❑❑❑

2

CONGRUENCES AND ITS BASIC PROPERTIES

Carl Freidrich Gauss in his *Disquisitions Arithmeticae,* a milestone in number theory codified an idea related to some bizarre arithmetic, which he found it ideal for handling questions of divisibility.

Consider a clock, numbered with the hours 0, 1, 2, ... 11. Such a clock has its own peculiar arithmetic. For example, since three hours after 5 o'clock is 8 o'clock, we could say that $3 + 5 = 8$, as usual. But 3 hours after 10 o'clock is 1 o'clock, and 3 hours after 10 o'clock is 2 o'clock; so by the same token, $3 + 10 = 1$ and $3 + 11 = 2$. Though it is not so standard (!) nevertheless, this '*clock arithmetic*' has a great deal going for it including almost *all of the usual laws of algebra.* Following Gauss, we describe it as arithmetic to the modulus 12, and replace '=' by the symbol '≡' as a remainder that some *monkey-business* (in IAN STEWART's words) is going on. The relation '≡' is called *congruence.* In arithmetic modulo (modulus) 12, all multiples of 12 are ignored. so $12 + 1 = 13 \equiv 1$, since $13 = 12 + 1$ and we may ignore 12.

Thus *Congruence* is a statement about divisibility slightly different point of view more than the convenient notation. It helps in easily discovering proofs and the same can suggest new problems leading to new and interesting topics.

2.1 ELEMENTARY PROPERTIES OF CONGRUENCES

Definition: Let $a, b, m \in \mathbb{Z}$, $m > 0$.

Then, *a is said to be congruent to b modulo m* if and only if $m \mid a - b$ and is written as

$$a \equiv b(\text{mod } m)$$

Remark: $30 \equiv 0 \pmod 5$, $5 \equiv 5(\text{mod})$

In general $a \equiv a(\text{mod } m)$ for any $m > 0$ and $a \equiv 0(\text{mod } m)$ if $m \mid a$

Theorem 2.1. The relation ≡ is an equivalence relation.

Proof: $\because$ for any $m\ (>0) \in \mathbb{Z}$, $m \mid 0$ and $a - a = 0$, for any $a \in \mathbb{Z}$,

it follows that $m \mid a - a$, $a \in \mathbb{Z}$.

$\therefore$ $$a \equiv a(\text{mod } m) \qquad \text{...(i)}$$

Next suppose for $a, b \in \mathbb{Z}$, $a \equiv b(\text{mod } m)$

Then $m \mid a - b$

or $m \mid b - a$

$\therefore$ $b \equiv a(\text{mod } m)$.

$\therefore$ $a \equiv a(\text{mod } m)$

gives $b \equiv a(\text{mod } m)$ ...(ii)

Finally suppose, for $a, b, c \in \mathbb{Z}$ such that

$a \equiv b(\text{mod } m)$,

$b \equiv c(\text{mod } m)$,

then $m \mid a - b$, $m \mid b - c$ and

$\therefore$ $m \mid (a - b) + (b - c) = a - c$

so, $a \equiv c(\text{mod } m)$

$\therefore$ $a \equiv b(\text{mod } m)$,

$b \equiv c(\text{mod } m)$,

gives $a \equiv c(\text{mod } m)$.

$\therefore$ "$\equiv$" is an equivalence relation.

Property 2.2. $a \equiv b(\text{mod } m)$ if and only if a and b have the same principal remainder on division by m.

Proof: Let $a \equiv b(\text{mod } m)$ and $a = mq_1 + r$, $0 \leq r < m$.

We prove that

$b = mq_2 + r$ (same r).

Now, $a \equiv b(\text{mod } m)$

or $b \equiv a(\text{mod } m)$

gives $b - a = mq_3 \quad (q_3 \in \mathbb{Z})$

or $b = a + mq_3 = mq_1 + r + mq_3 = m(q_1 + q_3) + r$

$= mq_2 + r$.

$\therefore$ $b = mq_2 + r$

Conversely, let $a = mq_1 + r$

And $b = mq_2 + r$, $0 \leq r < m$

Then, $a - b = m(q_1 - q_2) = mq_3, \quad (q_3 \in \mathbb{Z})$

or $m \mid a - b$

or $a \equiv b(\text{mod } m)$.

Some properties 2.3. $a \equiv b(\text{mod } m)$, $c \equiv d(\text{mod } m)$. Then

(i) $a + c \equiv b + d(\text{mod } m)$

(ii) $a - c \equiv b - d(\text{mod } m)$

(iii) $ac \equiv bd(\text{mod } m)$

(iv) $ax + cy \equiv bx + dy(\text{mod } m)$

(v) $a \equiv b(\text{mod } m)$ and $d \mid m$ $(d > 0)$, then $a \equiv b(\text{mod } d)$

(Proofs are left as exercise).

Extensions 2.4. If $a_i = b_i (\text{mod } m)$, $i = 1, 2, \ldots n$.

then, $\Sigma s_i a_i \equiv \Sigma s_i b_i \,(\text{mod } m)$, $(i = 1, 2, \ldots, n)$. ...(i)

$\Pi a_i \equiv \Pi b_i \,(\text{mode } m)$ ...(ii)

Property 2.5. $an \equiv bn(\text{mod } m)$ if and only if $a \equiv b\left(\text{mod}\frac{m}{(m, n)}\right)$

Proof Let $(m, n) = d$, then $d \mid m$, $d \mid n$

or $m = dm_1$, $n = dn_1$ with $(m_1, n_1) = 1$, $m_1, n_1 \in \mathbb{Z}$.

Now suppose, $an \equiv bn(\text{mod } m)$ then, $m \mid an - bn$

or $m \mid (a - b)\, dn_1$

or $dm_1 \mid (a - b)dn_1$

or $m_1 \mid (a - b)n_1$

or $m_1 \mid a - b$ $[\because (m_1, n_1) = 1]$

or $a \equiv b(\text{mod } m_1)$

$\therefore$ $a \equiv b\left(\text{mod}\frac{m}{(m, n)}\right)$.

Conversely, let $a \equiv b\left(\text{mod}\frac{m}{(m, n)}\right)$.

Then $a \equiv b\left(\text{mod}\frac{m}{d}\right)$ $[d = (m, n)]$

or $a \equiv b(\text{mod } m_1)$

or $m_1 \mid a - b$

or $m_1 \mid (a - b)n_1$

or $dm_1 \mid (a - b)dn_1$

or $m \mid (a - b)n$

$\therefore$ $an \equiv bn(\text{mod } m)$.

Observe: $an \equiv bn(\text{mod } m)$ does not give $a \equiv b(\text{mod } m)$ in general. [how?]

Corollary 2.6. $an \equiv bn(\text{mod } m)$, $(m, n) = 1$ gives $a \equiv b(\text{mod } m)$
(Restricted cancellation)

Example 1. $8 \times 7 \equiv 2 \times 7(\text{mod } 6)$, $(7, 6) = 1$, then, $8 \equiv 2(\text{mod } 6)$

Example 2. Find the remainder when $2^{73} + 14^3$ is divided by 11

Solution: $2 \equiv 2(\text{mod } 11)$

or $2^2 \equiv 4(\text{mod } 11)$

or $2^4 \equiv 4^2 \equiv 16 \equiv 5(\text{mod } 11)$

or $2^8 \equiv 5^2 \equiv 25 \equiv 3 (\text{mod } 11)$

or $2^{10} \equiv 3 \times 2^2 \equiv 12 \equiv 1 (\text{mod } 11)$

or $2^{70} \equiv 1 (\text{mod } 11)$

or $2^{70} \times 2^3 \equiv 8 (\text{mod } 11)$

or $2^{73} \equiv 8 (\text{mod } 11)$, ...(i)

Again, $14^3 = (11 + 3)^3 \equiv 3^3 (\text{mod } 11)$

$\equiv 27$

$\equiv 5 (\text{mod } 11)$ ...(ii)

From (i) and (ii), we get,

$2^{73} + 14^3 \equiv 8 + 5 \equiv 13 \equiv 2 (\text{mod } 11)$

$\therefore$ Remainder is 2.

Example 3. Prove that $2^p + 3^p$ is not a perfect power

(i.e., a perfect square, perfect cube etc.), if p is a prime number.

Solution: Case I: $p = 2$

Then $2^2 + 3^2 = 13$ is not perfect power

Case II: p is odd

then, $$2^p + 3^p = (2 + 3) \sum_{k=0}^{p-1} (-1)^k 2^{p-1-k} 3^k$$

then, $$\sum_{k=0}^{p-1} (-1)^k 2^{p-1-k} 3^k \equiv \sum_{k=0}^{p-1} (-1)^k 2^{p-1-k} (-2)^k$$

$\equiv p \cdot 2^{p-1} (\text{mod } 5)$ $[\because 3 \equiv -2 (\text{mod } 5)]$

So, if $p \neq 5$, then $2^p + 3^p = 5n$,

where $n \not\equiv 0 (\text{mod } 5)$, so that $2^p + 3^p$ is not a perfect power.

Again, $2^5 + 3^5 = 275$ is not a perfect power.

Example 4. Find the smallest value of $| 36^m - 5^n |$, where m and n are natural numbers.

Solution: The unit digits of 36^m is 6 for all m and of 5^n is 5 for all n respectively.

$\therefore$ the unit digit of $| 36^m - 5^n |$ is 1 or 9

$\therefore$ the least possible value of $| 36^m - 5^n |$ may be 1.

And then, $36^m - 5^n = \pm 1$

$\therefore$ $36^m \pm 1 = 5^n$.

Suppose $36^m + 1 = 5^n$

But, $36 \equiv 1 (\text{mod } 5)$ gives

$36^m \equiv 1 (\text{mod } 5)$

$\therefore$ $36^m + 1 \equiv 1 + 1 \equiv 2 (\text{mod } 5)$

Again, $5^n \equiv 0 (\text{mod } 5)$.

Hence $2 \equiv 0 (\text{mod } 5)$, a contradiction.

Suppose, $36^m - 1 = 5^n$

And $36^m - 1 \equiv 0 - 1 \equiv -1 \pmod 4$

and $5^n \equiv 1 \pmod 4$

$\therefore$ $1 \equiv -1 \pmod 4$, a contradiction.

So the least possible value cannot be 1 ; it may be 9.

$\therefore$ $36^m - 5^n = \pm 9$ and this gives,

$36^m \pm 9 = 5^n$

which is not possible, for $36 = 0 \pmod 3$

$\therefore$ $36^m = 0 \pmod 3$ and $9 \equiv 0 \pmod 3$

give $36^m \pm 9 \equiv 0 \pmod 3$

but $5^n \not\equiv 0 \pmod 3$.

The least possible value cannot be 9.

Hence the next least possible value is 11

Now we see that really,

$36 - 25 = 11$ (for $m = 1$ $n = 2$)

Hence 11 is the least possible value of $| 36^m - 5^n |$.

Example 5. Show that $10^n + 3.4^{n+2} + 5$ is divisible by 9

Solution: Suppose, $f(n) = 10^n + 3 \times 4^{n+2} + 5$

Then, $f(n+1) = 10^{n+1} + 3 \times 4^{n+3} + 5$

$= 10 \times 10^n + 3 \times 4 \times 4^{n+2} + 5$

$= 10 \times 10^n + 10 \times 3 \times 4^{n+2} - 6 \times 3 \times 4^{n+2} + 5$

$= 10 \times f(n) - 6 \times 3 \times 4^{n+2} - 45$

$\therefore$ $f(n+1) - f(n) = 9 \times f(n) - 18 \times 4^{n+2} - 45$

$= 9 (f(n) - 2 \times 4^{n+2} - 5)$

$\equiv 0 \pmod 9$

or $f(n+1) - f(n) \equiv 0 \pmod 9$

Now, $f(1) = 10 + 192 + 5 = 207 \equiv 0 \pmod 9$

From above we see that

$f(n) \equiv 0 \pmod 9$

if and only if $f(n+1) \equiv 0 \pmod 9$

Hence by induction

We get $f(n) \equiv 0 \pmod 9$, for all n.

Thus,

$10^n + 3 \times 4^{n+2} + 5$ is divisible by 9.

Example 6. Show that $3^{4n+2} + 5^{2n+1} \equiv 0 \pmod{14}$

Solution: Suppose $f(n) = 3^{4n+2} + 5^{2n+1}$

Then, $f(n+1) = 3^{4n+6} + 5^{2n+3}$

$= 3^4 \times 3^{4n+2} + 5^2 \times 5^{2n+1}$

$= 81 \times 3^{4n+2} + 81 \times 5^{2n+1} - 56 \times 5^{2n+1}$

$= 81 f(n) - 56 \times 5^{2n+1}$.

Thus, $f(n+1) - 81 f(n) = -56 \times 2^{n+1}$

$\equiv 0 (\text{mod } 14)$

i.e., $f(n+1) - 81 f(n) \equiv 0 (\text{mod } 14)$

Now if $f(n) \equiv 0 (\text{mod } 14)$

then by above $f(n+1) \equiv 0 (\text{mod } 14)$.

Again, $f(1) = 3^6 + 5^3$

$= 729 + 125$

$= 854$

$\equiv 0 (\text{mod } 14)$.

$\therefore$ by induction,

$f(n) \equiv 0 (\text{mod } 14)$, for all n.

2.2 COMPLETE RESIDUE SYSTEM, REDUCE RESIDUE SYSTEM

We now discuss the following division for some purpose.

Consider the integer 6. And,

$\mathbb{Z} = \{....., -5, -4, -3, -2, -1, 0, +1, +2, +3, +4, +5 .....\}$

We note that any integer divided by 6 will give us the remainder

0, 1, 2, 3, 4 or 5

Thus the *set of integers* when divided by 6

give the remainder 0 is $[0] = \{..... -24, -18, -12, -6, 0, 6, 12, 18, 24, ...\}$

give the remainder 1 $[1] = \{..... -23, -17, -11, -5, 1, 7, 13, 19, 25, ...\}$

give the remainder 2 $[2] = \{....., -22, -16, -10, -4, 2, 8, 14, 20, 26, ...\}$

give the remainder 3 $[3] = \{....., -21, -15, -9, -3, 3, 9, 15, 21, 27, ...\}$

give the remainder 4 $[4] = \{....., -20, -14, -8, -2, 4, 10, 16, 22, 28, ...\}$

give the remainder 5 $[5] = \{....., -19, -13, -7, -1, 5, 11, 17, 23, 29, ...\}$

Observe: $[0] \cup [1] \cup [2] \cup [3] \cup [4] \cup [5] = \mathbb{Z}$

and for any $(0 \leq) r, s (\leq 5), r \neq s, [r] \cap [s] = \varnothing$.

So it is observed that for any $m \in \mathbb{Z}^+$, there are m classes, $C_0, C_1 \ldots C_{m-1}$ in the equivalence relation congruence modulo m. In fact C_r, (for each $r = 0, 1, ..., m-1$) consists of all the integers of the type $km + r$, $r = 0, 1, ...$

Definition: The sets $C_0, C_1, ..., C_{m-1}$ are congruence classes (mod m).

Definition: If $x_i \in C_i$, $(i = 0, 1, ..., m-1)$ then m integers $x_0, x_1, x_2, ..., x_{m-1}$ are said to form a *complete set of residues mod m*(*c.s.r. mod m*).

Example 7. If for $m = 6$, a c.s.r(mod 6) is $\{12, -23, 8, -9, 4, 11\}$

Another c.s.r(mod 6) is $\{-24, 19, 14, -3, -8, 17\}$

Remark: A csr(mod m) has the properties:

(i) It contains m elements

(ii) Every pair of elements is incongruent mod m

i.e., $x_i \not\equiv x_j \pmod m$ if $i \neq j$,

or $x_i \equiv x_j \pmod m$ if and only if $x_i = x_j$

Note: The csr mod m, $\{0, 1, 2, ..., m-1\}$ is *called simplest csr(mod m)*

Addition and multiplication of residue classes mod m are as follows:

$C_q + C_r = C_{q+r}$, if $q + r < m$

$= C_t$, if $q + r \geq m$ and t is the remainder when $q + r$ is divided by m

$C_q . C_r = C_{qr}$, if $qr < m$

$= C_t$, if $q.r \geq m$ and t is the remainder when $q.r$ is divided by m

Example 8. If $m = 6$, then

$$C_1 + C_3 = C_4,$$
$$C_5 + C_4 = C_9 = C_3,$$
$$C_2 . C_4 = C_8 = C_2 \text{ etc.}$$

Theorem 2.7.

(a) If $S = \{x_0, x_1, ..., x_{m-1}\}$ is a csr (mod m) and if $b \in \mathbb{Z}$ then $A = \{ax_0 + b, ax_1 + b, ..., ax_{m-1} + b\}$ is also a csr(mod m)

(b) If $(m.n) = 1$ and $S_1 = \{x_0.x_1, ..., x_{m-1}\}$ is a csr(mod m)

and $S_2 = \{y_0, y_1, ..., y_{n-1}\}$ is a csr(mod n)

then the set $S = \{nx_i + my_j \mid i = 0, 1, ..., m-1, j = 0, 1, ..., n-1\}$ is a csr(mod mn)

Proof: (a)

(i) Obviously there are m elements

(ii) We now prove $ax_i + b \not\equiv ax_j + b \pmod m$ if $i \neq j$.

Suppose $ax_i + b \equiv ax_j + b \pmod m$.

Then $x_i \equiv x_j \pmod m$ ($\because (a, m) = 1$), and it is not possible. [for S is a csr (mod m)]

Hence A is a csr(mod m).

(b) (i) Obviously there are mn elements.

(ii) We prove $nx_i + my_j \not\equiv nx_k + my_j \pmod{mn}$

Given, S_1 is a csr (mod m).

$\therefore$ $x_i \not\equiv x_k \pmod m$, which gives $m \nmid x_i - x_k$

And so, $x_i - x_k = mq_1 + r_1$, $r_1 \neq 0$

Hence $n(x_i - x_k) = mnq_1 + r_1 n$, $r_1 n \neq 0$ ...(i)

Similarly, $m(y_j - y_1) = mnq_2 + r_2m,\ r_2m \neq 0$ ...(ii).

Adding (i) and (ii),

$$n(x_i - x_k) + m(y_j - y_k) = mnq + (r_1n + r_2m)$$

And this gives $mn \nmid n(x_i - x_k) + m(y_j - y_1)$ [why?]

And hence, $nx_i + my_j \not\equiv nx_k + my_1 (\text{mod } mn)$.

Hence, S is a csr (mod m).

Observation: Consider $m \in \equiv \mathbb{Z}^+$, and for $a, b \in \mathbb{Z}$, $a \equiv b (\text{mod } m)$.

Then, $C_a + C_b = C_{a+b}$ and $C_a.C_b = C_{ab}$

or $\bar{a} + \bar{b} = \overline{a+b}$ and $\bar{a}.\bar{b} = \overline{a.b}$,

where $\bar{a} = \bar{b}$ if and only if $a \equiv b (\text{mod } m)$ [write $\bar{x}$ for C_x]

Suppose $\mathbb{Z} = \{C_0, C_1, ..., C_{m-1}\}$

$= \{\bar{0}, \bar{1}, \bar{2}, ... \overline{m_{-1}})$

$= \bar{x}, \bar{y}, \bar{z}, ..., \} (x \in \bar{0}, y \in \bar{1}, z \in \bar{2}, ...)$. Then

Theorem 2.8. In $\mathbb{Z}_m$ if the addition and multiplication are defined above, then $\mathbb{Z}_m$ is a commutative ring with unity. (left as an exercise).

Note: This ring will be a field if m is a prime p i.e., $\mathbb{Z}_p$ is a field.

Lemma 2.9. $a \equiv b (\text{mod } m)$ gives $(a, m) = (b, m)$

Proof: $a \equiv b (\text{mod } m)$

or $b - a = mk$

or $a = b - mk$.

Now if $(a, m) = d_1$ and $(b, m) = d_2$,

Then, $d_1 \mid a$, $d_1 \mid m$ and $d_2 \mid b$, $d_2 \mid m$

or $a = d_1k_1,\ m = d_1k',\ b = d_2k_2,\ m = d_2k''$.

Then $a = b - mk = d_2k_2 - d_2k''k = d_2k_3$, where $k_3 = k_2 - kk''$

i.e., $a = d_2k_3$

or $d_2 \mid a$

Again $d_2 \mid a$ and $d_2 \mid m$

gives $d_2 \mid (a, m) = d_1$

Similarly, $d_1 \mid d_2$ gives $d_1 = d_2$.

Note: The following example justifies that the *converse of this lemma is not true.*

$(1, 4) = 1 = (3, 4)$, but $1 \not\equiv 3 (\text{mod } 4)$.

Definition: A set of integers r_i, where $(r_i, m) = 1$, $r_i \not\equiv r_j (\text{mode } m)$ $i \neq j$ and such that every a with $(a, m) = 1$ is congruent modulo m to some member r_i of the set, is said to be *a reduced set of residues mod m.*

Reduced set of modulo m can be obtained by deleting from a complete set of residues modulo m those members that are not relatively prime to m.

A reduced set of residues therefore consists of the numbers of a complete system, which are relatively prime to the modulus.

Example 10. {1, 2, 3, ... 40, 41, 42} is the complete set of residue mod 42

$$\{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 41\}$$

is the reduced system of residue modulo 42.

Example 10. Exhibit the complete residue system modulo 17 composed entirely of multiples of 3.

Also find the reduced residue set modulo 17.

Solution: The complete set of residue modulo 17 is

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$$

Now these numbers are to be changed in the multiples of 3
so that they may represent the same number modulo 17;

And thus the required set is

$$\{0, 18, 36, 3, 21, 39, 6, 24, 42, 9, 27, 45, 12, 30, 48, 15, 33\}$$

And the reduced residue set is same as the complete set of residue modulo 17 for 17 is a prime number (and so each number in the set of the complete residue is prime to 17).

Theorem 2.10. If m is prime, then show that $(a + b)^m \equiv a^m + b^m \pmod{m}$

Proof: $(a + b)^m = a^m + {}^mC_1 a^{m-1} b + {}^mC_2 a^{m-2} b^2 + \ldots + {}^mC_r a^{m-r} b^r + \ldots + b^m$

and it is seen that (Example 32, Ch 1)
the product of r consecutive integers is always divisible by $r!$

So the coefficient of each term of the above expansion is an integer.

$\because$ m is a prime, no factor of $r!$ is a divisor of it,

Moreover $m \nmid r$, so $m \nmid$ any factor of $r!$

$\therefore$ $r! \mid (m-1)(m-2) \ldots (m-r+1)$

Hence, $${}^mC_r = \{m.(m-1).(m-2) \ldots \frac{(m-r+1)}{r!}$$

is divisible by m for all $r \leq m - 1$

$\therefore$ $$(a + b)^m \equiv a^m + b^m \pmod{m}.$$

Theorem 2.11. If m is a prime, then prove that

$$(a + b + c + \ldots + \ldots)^m \equiv a^m + b^m + c^m + \ldots \pmod{m}$$

Proof: (**Hint:** Take $b + c + d + \ldots = p$, use the above theorem and repeat the same.

Theorem 2.12: If $m \equiv 1 \pmod{p^n}$, then $m^p \equiv 1 \pmod{p^{n+1}}$, where $n > 0$ and p is a prime.

Proof: $\because$ $m \equiv 1 \pmod{p^n}$, we write $m = 1 + \lambda p^n$, for some integer λ

Again $np \geq n + 1$. .

Now, $m^p = (1 + \lambda p^n)^p = \ldots = \ldots = 1 + \alpha\, p^{n+1}$

[*students are asked to calculate in details and fill up the missing steps*]

$\therefore$ $m^p \equiv 1 (\text{mod } p^{n+1})$.

Theorem 2.13. If $a \equiv b (\text{mod } m)$, $a \equiv b (\text{mod } n)$, $(m, n) = 1$ then $a \equiv b (\text{mod } mn)$

Proof $a \equiv b (\text{mod } m)$, $a \equiv b (\text{mod } n)$ give, $m \mid a - b$ and $n \mid a - b$

Thus, $a - b = mk = n\ell$ (for some k, ℓ).

$\because$ $(m, n) = 1$ and $mk = n\ell$ gives $n \mid mk$

$\therefore$ we have $n \mid k$.

So, $k = nt$(for some t).

$\therefore$ $a - b = mnt$

and this gives,

$mn \mid a - b$,

in other words $a \equiv b (\text{mod } mn)$.

2.3 SOME APPLICATIONS OF CONGRUENCES- (FERMAT'S LITTLE THEOREM, EULER'S THEOREM, WILSON'S THEOREM, CONVERSES AND THEIR APPLICATIONS)

Note: Before discussing arithmetic functions or Euler's function in particular we want to discuss Fermat's little theorem (though the same may be proved with the help of Euler's theorem!)

Theorem 2.14. Fermat's theorem (This is known as *Fermat's Little Theorem* to distinguish it from the famous conjecture known as *Fermat's Last Theorem.*)

If p is a prime and $(a, p) = 1$ (i.e., $p \nmid a$), then $a^{p-1} \equiv 1 (\text{mod } p)$

Proof: From theorem 2.10, we have

$$(\alpha_1 + \alpha_2 + \ldots \alpha_a)^p \equiv \alpha_1^p + \alpha_2^p + \ldots + \alpha_a^p (\text{mod } p)$$

Consider $\alpha_1 = \alpha_2 = \ldots = \alpha_a = 1$, then we have

$a^p \equiv a (\text{mod } p)$

or $a^{p-1} \equiv 1 (\text{mod } p)$.

Note: If p is a prime then for any integer a and b we have

$ab \equiv 0 (\text{mod } p)$

gives $a \equiv 0 (\text{mod } p)$

or $b \equiv 0 (\text{mod } p)$ [$p \mid ab$ gives $p \mid a$ or $p \mid b$]

Corollary 2.15. For any prime p and any integer a, prove that $a^{\frac{p-1}{2}} = \lambda p \pm 1$, for some positive integer λ.

Proof: By Fermat's theorem we have (except for $p = 2$)

$$a^{p-1} \equiv 1 (\text{mod } p)$$

or $$a^{p-1} - 1 \equiv 0 (\text{mod } p)$$

or $$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 (\text{mod } p)$$

Now $\because$ $(a^{\frac{p-1}{2}} - 1)$ or $(a^{\frac{p-1}{2}} + 1) \equiv 0 (\text{mod } p)$,

$\therefore$ $(a^{\frac{p-1}{2}} - 1)$ or $(a^{\frac{p-1}{2}} + 1)$ is a multiple of p i.e., λp.

$\therefore$ $a^{\frac{p-1}{2}} = \lambda p \pm 1$.

Application of Fermat's theorem

Example 11. If p is a prime to a then, prove that

$$a^{p^{n-1}(p-1)} \equiv 1 (\text{mod } p^n)$$

Proof: By *Fermat theorem* we have, $a^{p-1} = 1 (\text{mod } p)$ ...(*)

and by the theorem 2.12,

$$m \equiv 1 (\text{mod } p^n) \text{ gives}$$
$$m^p \equiv 1 (\text{mod } p^{n+1}) \quad \text{...(**)}$$

Combining (*) and (**) we have

$$a^{p(p-1)} \equiv 1 (\text{mod } p^2)$$

$$a^{p^2(p-1)} \equiv 1 (\text{mod } p^3)$$

... ...

... ...

$$a^{p^{n-1}(p-1)} \equiv 1 (\text{mod } p^n).$$

Example 12. Show that $n^7 - n$ is divisible by 42

Solution: $n^7 - n = n(n^6 - 1)$

$= n(n^{7-1} - 1)$ and $\because$ 7 is prime, we therefore have

by *Fermat theorem,* $n^7 - n = n(n^{7-1} - 1) \equiv 0 (\text{mod } 7)$

or $n^7 - n = M(7)$

and also, $= n(n^6 - 1)$

$= n(n+1)(n-1)(n^4 + n^2 + 1)$

Moreover, $(n-1)\, n\, (n+1)$ being the product of three consecutive integers is divisible by $3! = 6$ and $(7, 6) = 1$

Hence $n^7 - n$ is divisible by $7 \times 6 = 42$.

Example 13. $5^{10} - 3^{10}$ is divisible by 11

Solution 3, 5, 11 are primes

Therefore $5^{10} = 5^{11-1} \equiv 1 (\text{mod } 11)$

and $3^{10} = 3^{11-1} \equiv 1 \pmod{11}$ (*Fermat's theorem*)

$\therefore$ $5^{10} - 3^{10} \equiv 0 \pmod{11}$

and we get, $5^{10} - 3^{10} = M(11)$.

Example 14. Prove that every square number is of the form $5k - 1$, $5k$, $5k + 1$ where n is some positive integer.

Solution: Suppose N is any number

Case I: $(5, N) = 1$

$N^4 - 1 = N^{5-1} - 1 \ (\equiv 0 \ mod \ 5) = M(5)$ (*Fermat's theorem*)

So, $(N^2 - 1)(N^2 + 1) = M(5)$ which gives, $N^2 - 1$ or $N^2 + 1$ is $M(5)$.

Hence, $N^2 = 5k \pm 1$.

Case II: $(5, N) \neq 1$,

$\therefore$ $(5, N) = 5$

Then, $N^2 = 5^2 k$

Hence the result.

Example 15. Find the last unit digit of 3^{400}

Solution $3^4 \equiv 1 \pmod{5}$, and $3^4 \equiv 1 \pmod{2}$ (*Fermat*)

$\therefore$ $3^4 \equiv 1 \pmod{10}$ [theorem 2.2.7]

or $3^{4n} \equiv 1 \pmod{10}$

$\therefore$ $3^{400} = 3^{4\,100} \equiv 1 \pmod{10}$

$\therefore$ the last digit is 1.

Note: The converse of Fermat's theorem is not true.

In other words, if $a^{m-1} \equiv 1 \pmod{m}$, m need not be prime.

Example 16. $2^{340} \equiv 1 \pmod{341}$, 341 is not prime

$\because$ $341 = 11.31$.

To discuss one *partial converse* of it we first note the following

Definition: If $(a, m) = 1$, and λ is the smallest positive integer such that

$$a^{\lambda} \equiv 1 \pmod{m},$$

i.e., $a^{\lambda} \equiv 1 \pmod{m}$,

$a^k \not\equiv 1 \pmod{m}$, for $0 < k < \lambda$,

then λ is called the order of a modulo m.

Theorem 2.16. $a^n \equiv 1 \pmod{m}$ and d is the order of a modulo m, then $d \mid n$.

Proof: By Division algorithm, $n = qd + r$, $0 \leq r < d$, $q, r \in Z$

Now $a^n = a^{qd+r} = (a^d)^q . a^r$,

Gives $a^r \equiv 1 \pmod{m}$.

Hence $r = 0$, that is, $n = qd$.

Thus the statement holds.

Theorem 2.17. If q is a prime factor of the Mersenne number

$$M_p = 2^p - 1 \text{ then } q > p.$$

Proof: If $p = 2$ then the result is true.

Suppose p is odd.

Now $q \mid (2^p - 1)$ gives $2^p \equiv 1 \pmod{q}$ $\because$ p is prime, by Theorem 2.16 we know that the order of 2 modulo q is p. By *Fermat's theorem*

$2^{q-1} \equiv 1 \pmod{q}$. Thus $p \mid (q - 1)$, that is,

$q > p$.

[student will try the proof without using Theorem 2.16].

[Also the above result reveals that there are infinitely many primes.]

Theorem 2.18. The prime factor of Mersenne number M_p $(p > 2)$ has the form $2pt + 1$

Proof: If q is a prime factor of M_p then by Theorem 2.16, $p \mid q - 1$.

$\because$ q is odd, $2 \mid q - 1$. Hence $2p \mid (q - 1)$, that is

$q = 2pt + 1$, and so the theorem is proved.

Theorem 2.19. The odd prime factor of $a^{2^n} + 1$ $(a > 1)$ is of the form $2^{n+1}.t + 1$

Proof: Proof will be by induction.

For $n = 0$ the result is trivial.

Assume that the result is true $n - 1$,

So, $a^{2^{n-1}} + 1 \equiv 0 \pmod{q_1}$, $q_1 = 2^n t_1 + 1$

Let $a^{2^n} + 1 \equiv 0 \pmod{q}$, or $\left(a^2\right)^{2^{n-1}} + 1 \equiv 0 \pmod{q}$

By induction hypothesis we have

$q = 2^n t + 1$.

Now $a^{2^n} + 1 \equiv 0 \pmod{q}$

or $a^{2^n t} \equiv (-1)^t \pmod{q}$,

or $a^{q-1} \equiv (-1)^t \pmod{q}$

or $(-1)^t \equiv 1 \pmod{q}$ [*Fermat theorem*]

Now $t = 2t_2$ [$\because$ t is even for $q > 2$]

Hence, $q = 2^{n+1} t_2 + 1$.

Thus the theorem is proved.

[**Note:** for $n = 1$, the prime factor $a^2 + 1$ is of the form $4t + 1$]

Theorem 2.20. Every prime factor of the Fermat number F_n $(n > 2)$ is of the form $2^{n+2}t + 1$.

Proof: Suppose q is a prime actor of F_n.

Now $\left(F_{n-1}\right)^{2^{n+1}} = \left(2^{2^{n-1}} + 1\right)^{2^{n+1}}$

$$= \left(2^{2^n} + 2^{2^{n-1}+1}\right)^{2^n}$$

$$\equiv \left(2^{2^{n-1}+1}\right)^{2^n}$$

$$\equiv \left(2^{2^n}\right)^{2^{n-1}+1}$$

$$\equiv (-1)^{2^{n-1}+1} \equiv -1 (\text{mod } F_n)$$

or $$\left(F_{n-1}\right)^{2^{n+1}} + 1 \equiv 0 (\text{mod } F_n)$$

Then q is a prime factor of $\left(F_{n-1}\right)^{2^{n+1}} + 1$ also.

If q is an odd prime factor of $\left(F_{n-1}\right)^{2^{n+1}} + 1$ then $q = 2^{n+2}t + 1$ [above theorem].

Thus it follows that every prime factor of F_n is of the form $2^{n+2}t + 1$.

Note: It is to be noted that a reduced residue set modulo m is obtained by deleting from a complete residue set modulo m those members that are not relatively prime to m and all such sets contain the same number of members, and this number is *denoted by* $\Phi(m)$. Thus, this leads us to a function called *the Euler's phi-function* and is denoted by Φ.

In other words when m is a positive integer, $\Phi(m)$ denotes the number of positive integers not exceeding m and which are relatively prime to m[$\Phi(m)$ = number of a's , $(a \leq m)$, such that $(a, m) = 1$]

So, $\Phi(1) = 1$ (the only number n such that, $(n, 1) = 1$ is 1 itself)
$\Phi(2) = 1$ (the only number n such that, $(n, 2) = 1$ is : 1
$\Phi(3) = 2$ (the only number n such that, $(n, 3) = 1$ are 1, 2)
$\Phi(4) = 2$ (the only number n such that, $(n, 4) = 1$ are 1,3)
$\Phi(5) = 4$ (the only number n such that, $(n, 5) = 1$ are 1, 2, 3, 4)
$\Phi(6) = 2$ (the only number n such that, $(n, 6) = 1$ are 1,5)
$\Phi(7) = 6$ (the only number n such that, $(n, 7) = 1$ are 1,2, 3, 4, 5, 6)
$\Phi(8) = 4$ (the only number n such that, $(n, 8) = 1$ are 1, 3, 5, 7)

If p is a prime then

$\Phi(p) = p - 1$ (the only number n such that, $(n, p) = 1$ are 1, 2, 3, 4, ..., $(p - 1)$)

Note: Here 1 is considered as prime to all the numbers.)

Theorem 2.21. Euler's theorem

$$(a, m) = 1 \text{ gives } a^{\Phi(m)} \equiv 1 (\text{mod } m)$$

Proof: We use the following

Lemma: If $\{r_1, r_2, \ldots r_{\Phi(m)}\}$ is a r.r.s. (mod m) and if $(a, m) = 1$ then
$\{ar_1, ar_2, \ldots, ar_{\Phi(m)}\}$ is also r.r.s. (mod m)

Now $r_i \not\equiv r_j (\text{mod } m)$, $(1 \le i, j \le \Phi(m), i \ne j)$

and $r_i \equiv ar_j (\text{mod } m)$, for some i and j.

Then multiplying we get

$$r_1.r_2, \ldots r_{\Phi(m)} \equiv ar_1.ar_2 \ldots ar_{\Phi(m)} (\text{mod } m)$$

and by restricted cancellation law

$$r_2 \ldots r_{\Phi(m)} \equiv r_2 \ldots r_{\Phi(m)} a^{\Phi(m)} (\text{mod } m) \ (\because (r_1, m) = 1).$$

Similarly, $\because (r_2, m) = 1, (r_3, m) = 1, \ldots (r_{\varphi(m)}, m) = 1$, we get cancelling $r_2, r_3, \ldots, r_{\varphi(m)}$

$$1 \equiv a^{\varphi(m)}(m).$$

$$\therefore \quad a^{\varphi(m)} \equiv 1(m).$$

Corollary 2.22. Fermat's theorem: $a^p \equiv a(\text{mod } p) \quad \forall\ a \in \mathbb{Z}$

Proof: Euler's theorem states that $a^{\varphi(m)} \equiv 1(\text{mod } m)$ if $(a, m) = 1$.

When m is prime p, we then get,

$$a^{\varphi(p)} \equiv 1 \ (\text{mod } p) \text{ and } p \text{ being a prime, } \varphi(p) = p - 1.$$

Thus, $a^{\varphi(p)} \equiv 1(\text{mod } p)$,

if $(a, p) = 1$ i.e., $a \not\equiv 0(\text{mod } p)$ and obviously, $a \equiv a(\text{mod } p)$.

Multiplying, (if $a \not\equiv 0(\text{mod } p)$), $a^p \equiv a(\text{mod } p)$ and if $a \equiv 0(\text{mod } p)$, then this result is obviously satisfied.

$$\therefore \quad a^p \equiv a(\text{mod } p) \ \forall\ a \in \mathbb{Z}.$$

Note: For $p = 7$,

$$1^7 \equiv 1(\text{mod } 7),$$
$$2^7 \equiv 2(\text{mod } 7),$$
$$3^7 \equiv 3(\text{mod } 7) \text{ ..etc}$$
$$7^7 \equiv 7 \ (\text{mod } 7),$$
$$14^7 \equiv 14(\text{mod } 7)$$

If $a \not\equiv 0(\text{mod } p)$ i.e. if $(a, p) = 1$, then

$$a^{p-1} \equiv 1 \ (\text{mod } p) \text{ e.g.}$$
$$1^6 \equiv 1(\text{mod } 7),$$
$$2^6 \equiv 1(\text{mod } 7),$$
$$3^6 \equiv (\text{mod } 7).$$
$$7^6 \not\equiv 1(\text{mod } 7).$$

Remark: Direct converse of Fermat's theorem is not true.

Theorem (Partial converse of Fermat theorem) 2.23. If $a^{m-1} \equiv 1(\text{mod } m)$ and $a^n \not\equiv 1(\text{mod } m)$ for any proper divisor of $m - 1$, then m is a prime.

Proof: Theorem 2.16 asserts that $m - 1$ is the order of a modulo m.

Euler's theorem states that

$$a^{\varphi(m)} \equiv 1(\text{mod } m).$$

Hence $\varphi(m) \ge m - 1$.

But for any integer $m > 1$, we must have

$$\varphi(m) \leq m - 1.$$

$\therefore$ $\varphi(m) = m - 1$, that is m is prime.

Note: Positive factor of $47 - 1 = 46$ are 1, 2, 23, 46

And $45^{23} = (47 - 2)^{23} \equiv (-2)^{23} \equiv -1 \pmod{47}$

or $(45^{23})^2 = 45^{46} \equiv (-1)^2 \equiv 1 \pmod{47}$ also

$45^2 \not\equiv 1 \pmod{47}$, thus 47 is prime.

The converse of above is not true (The converse states that: When m is prime and $n \mid (m - 1)$ then $a^n \not\equiv 1 \pmod{m}$.

For example, when $m = 5$, $a = 4$, we have

$$4^2 \equiv 1 \pmod{5}.$$

Theorem 2.24. *Wilson's theorem:*

If p is prime, then

$$(p - 1)\,! + 1 \equiv 0 \pmod{p}$$

$$[\text{or } (p - 1)\,! \equiv -1 \pmod{p}]$$

Proof: $\mathbb{Z}p = \{\overline{0}, \overline{1}, \overline{2}, \ldots\ldots, \overline{p-1}\}$ is a csr (mod p).

and $S = \{\overline{1}, \overline{2}, \overline{3}, \ldots\ldots, \overline{p-1}\}$ is r.r.s. (mod p).

We know that $\mathbb{Z}p$ is a field.

$\therefore$ non-zero element has its inverse. i.e., if $\alpha \in S$,

then, $b.\alpha = \overline{1} \in S$.

[b is called the inverse of α in S(denoted α^{-1}) and α is called the inverse of b in S(denoted $\alpha = b^{-1}$.)]

Now $\overline{1}.\overline{1} = \overline{1}$ therefore, inverse of $\overline{1}$ is $\overline{1}$. Thus, $\overline{1}^{-1} = \overline{1}$

or $\overline{p-1} = \overline{-1}, \overline{p-1}.\overline{p-1} = \overline{-1}.\overline{-1} = \overline{1}$

$\therefore$ inverse of $\overline{p-1}$ is $\overline{p-1}$ itself.

Case (i): $p = 2$ gives $(2 - 1)! + 1 \equiv 0 \pmod{2}$. Verified.

Case (ii): $p = 3$ gives $(3 - 1)! + 1 \equiv 0 \pmod{3}$. Verified.

Case (iii): $p \geq 5$

Consider $\mathbb{Z}p = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-2}, \overline{p-1}\}$ is a csr (mod p).

Now $S = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ is r.r.s (mod p)

We know that $\mathbb{Z}p$ form a field.

$\therefore$ every nonzero element of $\mathbb{Z}p$ has a unique inverse.

Let $S_1 = \{\overline{2}, \overline{3}, \overline{5}, \ldots, \overline{p-2}\}$ [i.e. $S_1 = S \backslash \{\overline{1}, \overline{p-1}\}$

If $\overline{a} = \alpha \in S_1$, $2 \leq a \leq p - 2$, then inverse of α is not α. Because, if it is so, then,

$$\alpha.\alpha^{-1} = \overline{a}.\overline{a}, \text{ or } \overline{1} = \overline{a}^{-2} \text{ or, } a^2 \equiv 1 \pmod{p}$$

or $p \mid a^2 - 1$

or $$p \mid (a+1)(a-1)$$

or $$p \mid a+1 \text{ or, } p \mid a-1$$

and this is impossible as $2 \leq a \leq p-2$.

$\therefore$ $\alpha \in S_1$ gives $\alpha^{-1} \in S_1$ such that

$$\alpha \neq \alpha^{-1}$$

$\therefore$ inverse of $\alpha_1(=\overline{2}) \in S_1$ is $\alpha_1^{-1}(\neq\overline{2})\ S_1$ and so on.

$\therefore$ the elements in S_1 can be paired as

$$(\alpha_1, \alpha_1^{-1}), (\alpha_2, \alpha_2^{-1}), \ldots$$

$\therefore$ $\alpha_1.\alpha_1^{-1}.\alpha_2\alpha_2^{-1} \ldots = \overline{2}\cdot\overline{3}\cdot\overline{5}\ldots\cdot\overline{p-2}$ in some order. Thus we get

$$\overline{2}\cdot\overline{3}\cdot\overline{5}\ldots\cdot\overline{p-2} = \overline{1}\,\overline{1}\,\overline{1}\,\overline{1} = \overline{1}$$

or, $$\overline{1}\,\overline{2}\cdot\overline{3}\cdot\overline{5}\ldots\cdot\overline{p-2}\,\overline{p-1} = \overline{1}\,\overline{1}\,\overline{1}\ldots\overline{p-1} = -\overline{1}$$

or $$\overline{1\cdot 2\cdot 3\ldots\cdot p-1} = -\overline{1} \text{ so, } \overline{p-1!} = -\overline{1}$$

Hence $$(p-1)! \equiv -1 (\text{mod}\, p).$$

Theorem 2.25. *Converse:* If $n > 1$, $(n-1)! + 1 \equiv 0 (\text{mod}\ n)$ then, n is a prime.

Proof: If n is not a prime, then n is composite

Let, $$n = mk,\ 1 < m,k < n, \quad \text{i.e. } 2 \leq m,\ k \leq n-1$$

Then $$(n-1)! + 1 \equiv 0 (\text{mod}\ mk)$$

or, $$mk \mid (n-1)! + 1$$

or $$m \mid (n-1)! + 1.$$

But $m \mid (n-1)!$. $\because$ $m \in \{2, 3, \ldots, n-1\}$ gives $m \mid 1$ impossible $\because$ $m \neq 1$.

Similarly for k. Therefore, n cannot be composite.

Hence n is a prime.

Example 17. Show that $(m-1)! \equiv (m-1) \bmod (1 + 2 + 3 + \ldots + (m-1))$ if and only of m is a prime.

Solution: First we assume that

$$(m-1)! \equiv (m-1) \bmod (1 + 2 + 3 + \ldots + (m-1)).$$

Then $$(m-1)! \equiv (m-1) \bmod \left(\frac{m(m-1)}{2}\right)$$

Case I: Let m be odd.

$\therefore$ $m-1$ is even and so, $\dfrac{m-1}{2}$ is an integer.

Now $$\frac{m-1}{2}.m \mid (m-1)! - (m-1)$$

or $$m \mid (m-1)! - (m-1) \text{ or } m \mid (m-1)! + 1$$

or $$(m-1)! + 1 \equiv 0 (\text{mod}\ m)$$

$\therefore$ m is a prime, by converse of Wilson's theorem.

Case II: Let m be even. Then $\frac{m}{2}$ is an integer

Now $(m-1)! \equiv (m-1) \bmod ((m-1)\frac{m}{2})$

or $(m-1)\frac{m}{2} \mid (m-1)! - (m-1)$

or $\frac{m}{2} \mid (m-1)! - m + 1$

or $\frac{m}{2} \mid 1$

[$\because \frac{m}{2} \mid (m-1)!$ and $\frac{m}{2} \mid m$ (obviously)] gives $m \mid 2$ or $m = 2$, which is a prime, Hence.

Conversely, let m be a prime

Case I: Let $m = 2$: Then,

$(2-1)! \equiv (2-1) \pmod 1$, which is true.

Case II: Let $m = p \geq 3$, Then

$$1 + 2 + \ldots + (p-1) = \frac{p-1}{2}p = p\frac{p-1}{2}.$$

Now, $\because$ $\frac{p-1}{2} \mid (p-1)!$ and, $\frac{p-1}{2} \mid p-1$.

$\therefore$ $\frac{p-1}{2} \mid (p-1)!, \frac{p-1}{2} \mid (p-1)$

$\therefore$ $\frac{p-1}{2} \mid (p-1)! - (p-1)$

or $(p-1)! \equiv (p-1) \pmod{\frac{p-1}{2}}$

By Wilson's theorem,

$(p-1)! \equiv -1(p)$ or $(p-1)! \equiv (p-1) \pmod p$,

$\therefore$ $(p-1)! \equiv (p-1) \bmod (\frac{p-1}{2}.p)$

or $(p-1)! \equiv (p-1) \bmod (1 + 2 + 3 + \ldots + (p-1))$.

Example 18. If p is an odd prime and $k + 1 = p - 1$ then show that

$k!\ 1! + (-1)^k \equiv 0 \pmod p$. [Left as exercise]

Example 19. If p is a prime, then show that $2\ \{(p-3)!\} + 1 \equiv 0 \pmod p$

Solution:

$$2\ \{(p-3)!\} + 1 = 2\{(p-3)!\} + 1$$

$$= \frac{2\{(p-1)!\}}{(p-1)(p-2)} + 1$$

$$= \frac{2\{(p-1)!\} + (p-1)(p-2)}{(p-1)(p-2)}$$

$$= \frac{2\{(p-1)!\}+2+p^2-3p}{(p-1)(p-2)}$$

$$= \frac{2\{(p-1)!+1\}+p^2-3p}{(p-1)(p-2)}$$

By Wilson's theorem,

$$(p-1)! + 1 \equiv 0 (\text{mod } p)$$

and $p^2 - 3p \equiv 0 (\text{mod } p)$ and, $p \nmid (p-1)$, $p \nmid (p-2)$,

$\therefore$ $2\{(p-3)!\} + 1 \equiv 0 (\text{mod } p)$.

Example 20. Show that any integer n is congruent modulo 9 to the sum of its digits.

Solution: Suppose n contains $m + 1$ digits a, b, c, d, j beginning from the left.

Then $n = a \times 10^m + b \times 10^{m-1} + c \times 10^{m-2} + \ldots + i \times 10 + j$

(called the *extended notation* of n)

Now, $10 = 9 + 1 \equiv 1 (\text{mod } 9)$,

$10^2 = 9 \times 11 + 1 \equiv 1 (\text{mod } 9)$

$10^3 = 9 \times 111 + 1 \equiv 1 (\text{mod } 9)$,

.....

$10^m = 9 \times 111 \ldots\ldots m \text{ times} + 1 \equiv 1 (\text{mod } 9)$

$\therefore$ $n \equiv a + b + c + \ldots + i + j (\text{mod } 9)$

$=$ sum of the digits (mod 9).

Example 21. The necessary and sufficient condition that a positive integer n can be divided by 3 is that the sum of its digits is divisible by 3.

Solution: Suppose the number in the extended notation is

$$n = a_0 + a_1\, 10 + a_2 10^2 + \ldots + a_{k-1} 10^{k-1},\ 0 \le a_i < 10$$

Now $10 \equiv 1 (\text{mod } 3)$

or $a_0 + a_1 10 + a_2 10^2 + \ldots + a_{k-1} 10^{k-1}$

$\equiv a_0 + a_1 + a_2 + \ldots + a_{k-1} (\text{mod } 3)$

Thus $n \equiv 0 (\text{mod } 3)$ if and only if $a_0 + a_1 + a_2 + \ldots + a_{k-1} \equiv 0 (\text{mod } 3)$.

Example 22. Show that a positive integer n is divisible by 7 if and only if $\sum_{i=0}^{k-1} (-1)^i a_i \equiv 0 (\text{mod } 7)$, where $a_k, \ldots a_2, a_1, a_0$ are the digits of n from the left, $0 \le a_i < 1000$.

Solution: Let $n = a_0 + a_1 1000 + a_2 1000^2 + \ldots + a_k 1000^{k-1},\ 0 \le a_i < 1000,$

Now, $(a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) = \sum_{i=0}^{k-1} (-1)^i a_i \equiv 0 (\text{mod } 7)$

[**Note:** $1000 \equiv -1 (\text{mod } 7)$].

Example 23. Show that 637693 is divisible by 7

Solution: $n = 637693 = 693 + 637 \times 1000$; $a_0 = 693$, $a_1 = 637$

Therefore, $a_0 - a_1 = 693 - 637 = 56 \equiv 0 (\text{mod } 7)$

Thus, the number is divisible by 7.

Example 24. If $n = a_m \times 10^m + a_{m-1} \times 10_{m-1} + a_{m-2} \times 10^{m-2} + ... + a_1 \times 10 + a_0$ be the decimal expansion of n, $0 \le a_m, a_{m-1}, a_{m-2}, ... a_1, a_0 \le 9$, and $T = a_0 - a_1 + a_2 - ... + (-1)^m$. Then $11 \mid n$ if and only if $11 \mid T$.

Solution: We write $P(x) = \sum_{i=0}^{m} a_k x^k$

Now $10 \equiv -1 (\text{mod } 11)$ gives $P(10) \equiv P(-1) (\text{mod } 11)$.

But $P(1) = N$ and $P(-1) = a_0 - a_1 + a_2 - ... + (-1)^m = T$.

So $N \equiv T (\text{mod } 11)$

Thus 11 divides n if and only if 11 divides T.

We are much pleased to include the following test of divisibility with due permission from the author Prof. Gundala Ramanaiah (and the same has been named after his name).

Ramanaiah Technique of Tests of Divisibility by Primes.

The divisibility criterion for any prime depends on the 'period' of the prime and when the period/semi periods are small.

Definition: *Period of a prime:*

The period of a prime p is defined as the least positive integer r such that

$$10^r \equiv 1 (\text{mod } p) \quad ...(1)$$

Example 25. Find the periods of the primes 37 and 41.

$$10^2 \equiv 26 (\text{mod } 37), 10^3 \equiv 1 (\text{mod } 37).$$

$\therefore$ 37 has period 3.

$$10^2 \equiv 18 (\text{mod } 41), 10^3 \equiv 16 (\text{mod } 41), 10^4 \equiv -4 (\text{mod } 41), 10^5 \equiv 1 (\text{mod } 41)$$

$\therefore$ 41 has period 5.

If the period of the primes p is even, say $r = 2s$, then,

$10^{2s} \equiv 1 (\text{mod } p)$ which implies that

$$10^s \equiv -1 (\text{mod } p) \quad ...(2)$$

The other alternative, $10^s \equiv -1 (\text{mod } p)$ contradicts the hypothesis that $2s$ is the period.

Definition: We call s as the semi-period of p. It is the least positive integer satisfying (2) and is a divisor of $\frac{p-1}{2}$.

Example 26. Find the semi-period s of the primes 137 and 9091

$10^2 \equiv -37 (\text{mod } 137)$

$10^3 \equiv -96 (\text{mod } 137)$

$10^4 \equiv -1 (\text{mod } 137)$

$\therefore$ $s = 4$ for 137.

$10^4 \equiv 909 (\text{mod } 9091)$

$10^5 \equiv -1 (\text{mod } 9091)$

$s = 5$ for 9091.

Table 1 and 2 give the odd periods r and semi periods s for all primes less than 500 while table 3 gives all primes less than 100,000 with r and s not more than 10. There is no regular pattern of occurrences of r and s. It is interesting to note that there are only 19 primes less than 1000,000 whose r and s are not more than 10.

Table 1 Primes less than 500 odd periods r.

P	3	31	37	41	43	53	67	71	79	83	107	151	163
r	1	15	3	5	21	13	33	35	13	41	53	75	81

P	173	191	199	227	239	271	277	283	307	311	317
r	43	95	99	113	7	5	69	141	153	155	79

P	347	359	397	431	439	443	467	479
r	173	179	99	215	219	221	233	239

Table 2 Primes less than 500 with even periods $2s$.

P	7	11	13	17	19	23	29	47	59	61	73	89	97	101	103
s	3	1	3	8	9	11	14	23	29	30	4	22	48	2	17

P	109	113	127	131	137	139	149	157	167	179	181	193
s	54	56	21	65	4	23	74	39	83	89	90	96

P	197	211	223	229	233	241	251	257	263	269	281	293
s	49	15	111	114	116	15	25	128	131	134	14	73

P	313	331	349	337	353	367	373	379	383	389	401	409
s	156	55	168	58	16	183	93	189	191	194	100	102

P	419	421	433	449	457	461	463	487	491	499
s	209	70	216	16	76	230	77	243	245	249

Table 3 Primes less than 1000,000 with r or s not more than 10

P	3	37	41	239	271	4649
s	1	3	5	7	5	7

P	7	11	13	17	19	73	101	137	3541	9091	9901	27961	52579
s	3	1	3	8	9	4	2	4	10	5	6	10	9

DIVISIBILITY CRITERIA

Let p be a prime with period r. Consider a number N comprising n digits where $n > r$,

$$N = d_{n-1} \ldots d_2 d_1 d_0 = \sum_{j=0}^{r-1} d_j 10^j + \sum_{j=r}^{2r-1} d_j 10^j + \ldots$$

Since $10^r \equiv 1 (\text{mod } p)$, we find

$$N = (d_{r-1} \ldots d_2 d_1 d_0) + (d_{2r-1} \ldots d_r) + \ldots (\text{mod } p) \quad \ldots(3)$$

Hence we obtain the divisibility criterion.

Rule 1.

(i) If r is the period of p; divide the digits of N into blocks of r digits starting from the right. (The last block may contain fewer digits.).

(ii) Find the sum N_0 of the numbers in the blocks.

(iii) Then N_0 and N leave the same remainder when they are divided by P.

If N_0 contains more than r digits apply the rule to N_0.

If s is the semi-period of prime p, then using the relation

$10^s \equiv -1 (\text{mod } p)$, we find, in this case, that

$$N = (d_{s-1} \ldots d_2 d_1 d_0) + (d_{2s-1} \ldots d_r) + \ldots \equiv (\text{mod } p) \quad \ldots(4)$$

Hence we obtain the divisibility criterion.

Rule 2.

(i) If s is the semi-period of p, divide the digits into blocks of s digits from the right (The last bloc may contain fewer digits).

(ii) Find the alternate sum (4), say N_0.

(iii) Then N and N_0 leave the same remainder when they are divided by p.

Note:

(i) It may be noted that Rule 1 can be applied for all primes (other than 2 and 5) irrespective of whether the period is even or odd.

(ii) However in case of even periods it is better to use Rule 2 with s as the semi-period.

Since $s = 1$ for $p = 11$, Rule 2 gives that N is divisible by 11 if and only if the alternate sum $d_0 - d_1 + d_2 - \ldots$ is divisible by 11.

$R = 3$ for $p = 37$, therefore N is divisible by 37 if and only if $d_2 d_1 d_0 + d_5 d_4 d_3 + \ldots$ is divisible by 73.

Example 27.

Test $N = 2356710825$ is divisible by 37.

From Table 1 we find $r = 3$, if $p = 32$. Here $N = \underline{2356710825}$

Therefore $825 + 710 + 356 + 2 = 1893 = \underline{1893}$

$893 = 1 = 894 = N0$

By actual division of 894 by 37 we find that the remainder is 6.

Hence N also leaves 6 as remainder when divided by 37.

Note the advantage of the rule:

(i) We have divided a three-digit number instead of original 10-digit number.

(ii) The advantage is much more if one is testing a number with, say, 100 digits.

Example 28.

Test if $N = 2779104276$ is divisible by the prime 9091.

$S = 5$ for $p = 9091$

Therefore $N = \underline{2779104276} = 04276 - 27791 = -23515 = -9091\,x3 + 3758$

Therefore N leaves the remainder 3758.

Note: The advantage of criteria for divisibility by primes in the Rule 1 which is to be used for primes with odd period r and Rule 2 for primes with even period $2s$ lies in the fat:

One has to carry out division of a number with at most r or s digits instead of the original number with n digits.

These rules can be used to reduce computation time while finding the prime factors of large numbers.

2.4 SOLUTIONS OF CONGRUENCES

The ancient Greek mathematician Diophantine (C 250 C.E.) wrote extensively on equation which has two or more than two unknowns. Such an equation is called an *indeterminate equation.* A system of equations is said to be indeterminate if the number of equations is less than that of the unknowns. In this type of equations we usually look for the solutions in a restricted class of numbers such as positive integers, negative integers, or integers.

2.4.1 Linear Indeterminate Equations

Theorem 2.26. (i): $a, b \in \mathbb{Z}$, $a \neq 0$ then $ax + b = 0$ has a unique solution in integers if and only if $a \mid b$.

Proof: Let there exist $x_0 \in \mathbb{Z}$ such that $ax_0 = -b$. Then, $x_0 = -\frac{b}{a} \in \mathbb{Z}$ gives $a \mid b$

Next suppose $a \mid b$. Then $b = ak$, $(k \neq 0) \in \mathbb{Z}$. Therefore $-k$ is a solution.

Theorem 2.7. (ii): $ax + by = c$ ...(1) $a, b \in \mathbb{Z}$; $a \neq 0 \neq b$

The necessary and sufficient condition that the equation (1) will have a solution in integers is $(a, b) \mid c$.

Necessary part: Let (1) have solution.

Then $\exists\ x_0, y_0 \in \mathbb{Z}$ such that

$$ax_0 + by_0 = c \qquad \text{...(2)}$$

Let $(a, b) = d$

$\therefore$ $d \mid a$, $d \mid b$ gives

$$d \mid ax_0 + by_0 = c$$

$\therefore$ $d = (a, b) \mid c$.

Sufficient part: Let $d = (a, b) \mid c$. To prove that (1) has solution

As $d \mid c$ we have $c = dc_1$

And $(a, b) = d$ gives $\exists\ x'y' \in \mathbb{Z}$ such that

$$d = ax' + by'.$$

Multiplying by c_1 we get

$$a(c_1x' + b(c_1y') = dc_1,$$

or $$ax_1 + by_1 = c$$

therefore, (x_1, y_1) is a solution of (1).

Remark: (1) will have a solution if and only if $d = (a, b) \mid c$. Therefore, we have

$$d \mid a \text{ or } a = da_1, \text{ (say)}$$
$$d \mid b \text{ or } b = dc_1, \text{ (say)}$$
$$d \mid c \text{ or } c = dc_1, \text{ (say)}$$

Putting in (1) we get

$$da_1x + db_1y = dc_1,$$

or $$a_1x + b_1y = c_1 \quad ...(3)$$

when $$(a_1, b_1) = 1.$$

$\therefore$ Every consistent equation of the general type (1) can be converted to the type (3) in which (coefficient of x, coefficient of y) = 1. So instead of considering (1) we need consider the solution of (3).

2.4.2 To Find the Solution of Equation of the Type

$$ax + by = c \quad ...(1)$$

$$a \neq 0 \neq b;\ a, b, c \in \mathbb{Z}$$

Suppose one solution of (1) is known, (in the upper line) say (x_0, y_0);

To find the other solutions:

(x, y) and (x_0, y_0) will be solutions of (1) if

$$\left.\begin{aligned} ax + by &= c \\ ax_0 + by_0 &= c \end{aligned}\right\} ...(2)$$

The set (2) is equivalent to

$$\left.\begin{aligned} ax_0 + by_0 &= c \\ a(x - x_0) + b(y - y_0) &= 0 \end{aligned}\right\} ...(3)$$

but 1st of (3) is satisfied, $\because$ (x_0, y_0) is a solution by assumption.

To have a solution of (1) we get

$$a(x - x_0) + b(y - y_0) = 0$$

or $$a \mid b\ (y - y_0)$$

or $$a \mid y_0 - y \qquad (\because (a, b) = 1)$$

or $$y_0 - y = \text{at},$$

or $$y = y_0 - \text{at}\ (t \in \mathbb{Z})$$

Putting this value in (3) we get,

$$a(x - x_0) + b(-at) = 0$$

or $$x = x_0 + bt.$$

Theorem 2.28. Therefore, where (x_0, y_0) is a particular solution of (1) the general solution is

$$x = x_0 + bt$$
$$y = y_0 - at,\ t \in \mathbb{Z}.$$

Example 29. Solve: $11x - 33y = 22$

Solution: As (11,33) = 11, dividing by 11 we get

$$x - 3y = 2$$

[**Note:** Here (1,3) = 1] and $x = 5, y = 1$ is a solution (Euclidean algorithm may be used).

$\therefore$ $$x = x_0 + bt = 5 + (-3)t = 3 - 3t,$$
$$y = y_0 - at = 1 - 1t = 1 - t.$$

$\therefore$ the general solution is

$$(5 - 3t,\ 1 - t),\ t \in \mathbb{Z} \text{ i.e., } (5, 1), (2, 0), (8, 2), \ldots.$$

Example 30. Solve $525x + 231y = 42$

Solution: As (525,231) = 21, dividing by 21, we get

$$25x + 11y = 2$$

Now (25, 11) = 1, and so by Euclidean Algorithm we get,

$$25 \times (4) + 11 \times (-9) = 1$$

Hence, $$x = 2 \times 4 = 8,$$
$$y = 2 \times (-9) = -18$$

is a solution of the given equation. Therefore, the required solution is

$$\left.\begin{aligned} x &= 8 + 11t, \\ y &= -18 - 25t \end{aligned}\right\} t \in \mathbb{Z}.$$

There are various ways of obtaining a particular solution. When the coefficients of the given equation are not large, it can be found by inspection. However *the process of successively diminishing the coefficients is sometimes very convenient.*

Here the *method is due to Euler,* which is best illustrated by the following example:

Example 31. Solve: $738x + 621y = 45$ ...(1)

Solution: From (1) $y = \dfrac{-738x + 45}{621}$, (solving for y)

$$= -x + \frac{-117x + 45}{621},\ (\because\ y \text{ has the smallest coefficient in absolute})$$

$$= -x + t, \text{ say, } t$$

$$= \frac{-117x + 45}{621}\ (\in \mathbb{Z})$$

Therefore, $621t + 117x = 45$ ...(2)

Therefore, $x = \dfrac{-621t + 45}{117}$ ($\because$ coefficient of x is least)

$= -5t + \dfrac{-36t + 45}{117}$

$= -5t + u$, say, $u = \dfrac{-36t + 45}{117}$ ($\in \mathbb{Z}$)

Therefore, $117u + 36t = 45$ ...(3)

Therefore, $t = \dfrac{-117u + 45}{36} = -3u + 1 + \dfrac{-9u + 9}{36} = -3u + 1 + v$, say,

where $v = \dfrac{-9u + 9}{36}$ i.e., $36v = -9u + 9$, say, $v \in \mathbb{Z}$

or $4v + u = 1$ ...(4)

Therefore, $u = 1 - 4v$

To obtain one solution, we pick up a convenient value of v, say, $v = 0$ and work back through the chain of equations

$v = 0$

$u = -4v + 1$

$t = -3u + 1 + v = -2$

$x = -5t + u = 11$

$\therefore$ $x = 11, y = -13$ is a solution.

We are now asked to find all solutions of $ax + by = c$ ...(1)

Such that $x \geq 0, y \geq 0$ ...(i)

Solving as above we get $\left.\begin{matrix} r = x_0 + bt \\ s = y_0 - at \end{matrix}\right\} t \in \mathbb{Z}$

Now r will be positive if $x_0 + bt > 0$, i.e., $t > -\dfrac{x_0}{b}$

s will be positive if $y_0 - at > 0$ i.e., $t < \dfrac{y_0}{a}$

$\therefore$ for positive solution $-\dfrac{x_0}{b} < t < \dfrac{y_0}{a}$

The smallest allowable value for t is $\left[-\dfrac{x_0}{b}\right] + 1 = \left[-\dfrac{x_0}{b} + 1\right]$

and the greatest is $-\left[-\dfrac{y_0}{a} + 1\right]$

Therefore, $\left[-\dfrac{x_0}{b} + 1\right] \leq t \leq -\left[-\dfrac{y_0}{a} + 1\right]$ for which (1) will give positive solution

$\{-4, -3, -2, -1, 0, 1, 2, 3, ...\} \cap (6, 5, 4, 2, 10, -1, -2, -3,.\}$

2.4.2 Number of Solutions

$$N = \left(-\left[-\frac{y_0}{a}+1\right]\right) - \left(\left[-\frac{x_0}{b}+1\right]\right)$$

$$= -\left[-\frac{y_0}{a}\right] - 1 - \left[-\frac{x}{b}\right] - 1 + 1$$

$$= -\left(-\left[\frac{y_0}{a}\right] + \left[-\frac{x_0}{b}\right] + 1\right)$$

Now, $$\left[-\frac{y_0}{a} - \frac{x_0}{b}\right] \le \left[-\frac{y_0}{a}\right] + \left[-\frac{x_0}{b}\right] + 1$$

$$\le \left(\left[-\frac{y_0}{a} - \frac{x_0}{b}\right] + 1\right)$$

$$[\because [\alpha + \beta] \le [\alpha] + [\beta] + 1 \le [\alpha + \beta] + 1$$

gives $$-\left[-\frac{y_o}{a} - \frac{x_0}{b}\right] \ge -\left(\left[-\frac{y_0}{a}\right] + \left[-\frac{x_0}{b}\right] + 1\right) \ge -\left(\left[-\frac{y_0}{a} - \frac{x_0}{b}\right] + 1\right)$$

or $$-\left(\left[-\frac{y_0}{a} - \frac{x_0}{b}\right] + 1\right) \le N \le -\left[-\frac{y_0}{a} - \frac{x_0}{b}\right]$$

or $$-\left(\left[-\frac{ax_0 + by_0}{ab}\right] + 1\right) \le N \le -\left(\left[-\frac{ax_0 + by_0}{ab}\right]\right)$$

or $$-\left(\left[-\frac{c}{ab}\right] + 1\right) \le N \le -\left[-\frac{c}{ab}\right].$$

Example 32. Find the positive integer solution of the indeterminate equation;

$$7x + 19y = 213$$

Solution: Divide the equation by the smaller coefficient 7. Then we get

$$x = \frac{213 - 19y}{7} = 30 - 2y + \frac{3 - 5y}{7}$$

$\because$ x is an integer, y is also an integer. Thus

$$\frac{3 - 5y}{7} = u$$

is also an integer. The above now becomes

$$5y + 7u = 3,$$

Dividing by 5 we get

$$y = \frac{3 - 7u}{5} = -u + \frac{3 - 2u}{5},$$

or $$2u + 5v = 3.$$

Now we see that, $u = -1$, $v = 1$ is a solution. Hence, $x = 25$, $y = 2$. Thus, the general solution is

$$x = 25 + 19t,\ y = 2 - 7t$$

For positive solution we have

$$25 + 19t > 0,\ 2 - 7t > 0,$$

We required $$-\frac{25}{10} < t < \frac{2}{7}$$

Hence $t = 0$ or $t = -1$.

Therefore, the required positive integer solutions are

$$\left.\begin{matrix} x = 25 \\ y = 2 \end{matrix}\right\} \qquad \left.\begin{matrix} x = 6 \\ y = 9 \end{matrix}\right\}$$

$$\left[\text{since}, -\left(\left[-\frac{c}{ab}\right]+1\right) \le N \le -\left[-\frac{c}{ab}\right]\right]$$

Number of solutions: $-\left(\left[-\frac{213}{7\times 9}\right]+1\right) \le N \le -\left[-\frac{213}{7\times 13}\right]$ gives

$-(-2 + 1) \le N \le -(-2)$ which gives $1 \le N \le 2$ i.e. Number of solutions is 2.

Example 33. Solve $50x + 45y + 36z = 10$.

Solution: (This is a Diophantine equation in three unknowns.)

We decompose the given equation into two equations as follows:

$$50x + 45y = 5t,$$
$$5t + 36z = 10$$

We see that $(t, -t)$ and $(-70, 10)$ are the solutions respectively of the above two. So the general solutions are

$$x = t + 9k_1 \qquad \text{and} \qquad t = -70 + 36k_2$$
$$y = -t - 10k_1 \qquad z = 10 - 5k_2$$

Eliminating t we obtain the required solutions

$$x = -70 + 9k_1 + 36k_2$$
$$y = 70 - 10k_1 - 36k_2$$
$$z = 10 - 5k_2$$

or

$$x = 2 + 9k_1$$
$$y = -2 - 10k_1 - 36k_2$$
$$z = -5k_2.$$

(Student may try the same problem using Euler's method also).

Example 34. If $(a, b, c) = 1$, prove that any solution of the Diophantine equation $ax + by + cz = k$ can be expressed as

$$x = x_0 + b_1t_1 - u_1ct_2,$$
$$y = y_0 - a_1t_1 - u_2ct_2,$$

$$z = z_0 + dt_2,$$

where (x_0, y_0, z_0) is a solution of the given equation, $d = (a, b)$, $a = da_1$, $b = db_1$, u_1, u_2 are positive integers satisfying $a_1u_1 + b_1u_2 = 1$, t_1, t_2 are any integers.

Solution: Given that (x_0, y_0, z_0) is a solution of the given equation.

Therefore, we have

$$ax + by + cz = k$$

$$ax_0 + by_0 + cz_0 = k$$

or $$d\{a_1(x - x_0) + b_1(y - y_0)\} = -c(z - z_0).$$

$\because$ $(d, c) = 1$, $\exists$ an integer t_2 such that $z = z_0 + dt_2$.

Thus we have

$$a_1(x - x_0) + b_1(y - y_0) = -ct_2.$$

$\because$ $$a_1u_1 + b_1u_2 = 1,$$

Then $a_1(-u_1ct_2) + b_1(-u_2ct_2) = -ct.$

$\therefore$ $\exists$ an integer t_1 such that

$$x = x_0 + b_1t_1 - u_1ct_2,$$

$$y = y_0 - a_1t_1 - u_2ct_2.$$ [Theorem: 2.28]

Thus we have

$$x = x_0 + b_1t_1 - u_1ct_2,$$

$$y = y_0 - a_1t_1 - u_2ct_2,$$

$$z = z_0 + dt_2.$$

2.5 ALGEBRAIC CONGRUENCES

Suppose $f(x) \in \mathbb{Z}[x]$, $f(x) = 2x^2 - x + 1$ (say)

e.g., $$3x^2 - 2x + 1, x^3 + x + 1 \in \mathbb{Z}[x]\ x^3 + \frac{1}{2x - 2} \notin \mathbb{Z}[x], 2x\ 2, 1, 0 \in \mathbb{Z}[x].$$

$$f(x) = a_0 + a_1x + a_2x_2 + \ldots\ a_nx^n + \ldots$$

$f(x)$ is of degree n, if $a_n \neq 0$ and $a_{n+1} = a_{n+2} = \ldots = 0$

e.g., $x^2 \div x + 1$ is of degree 2

$x + 2$ is of degree 1

2 is of degree 0:

Remark: 0 is a also a polynomial which has no degree.

Definition: Suppose $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + a_{n+1}x^{n+1} + .., m \in \mathbb{Z}$.

Then $$f(x) \equiv 0 (\text{mod}\, m)$$ ...(1)

or, $$m \mid f(x)$$

$f(x)$ is said to be of degree n mod m if $m \dagger a_n$ *i.e.,*

$$a_n \equiv 0 (\text{mod}\ m) \text{ and } m \mid a_{n+1}, a_{n+2}, \ldots \text{ etc.}$$

e.g. $2 - 3x + 4x^2 + 6x^3 + 8x^4$ is of degree 3(mod 4),

is of degree 4(mod 5),

is of degree 1(mod 2).

Definition: a is said to be a solution of $f(x) \equiv 0 (\text{mod } m)$

if $f(a) \equiv 0(m)$ (i.e., $m \mid f(a)$)

e.g., $f(x) = x^2 - 1$ is the polynomial and $m = 8$

Then, $f(1) = 1 - 1 = 0$ or $8 \mid f(1)$, $\therefore$ 1 is a solution

$f(2) = 2^2 - 1 = 3$ or $8 \dagger f(2)$ $\therefore$ 2 is not a solution

$f(3) = 3^2 - 1 = 8$ or $8 \mid f(3)$ $\therefore$ 3 is a solution

$f(4) = 4^2 - 1 = 15$ or $8 \dagger f(4)$ $\therefore$ 4 is not a solution

$f(5) = 5^2 - 1 = 24$ or $8 \mid f(5)$ $\therefore$ 5 is a solution

etc.,

e.g., $f(x) = x^2 - 3$ is the polynomial, $m = 5$;

$f(1) = 12 - 3 = -2$ or $5 \dagger f(1)$ $\therefore$ 1 is not a solution

$f(2) = 22 - 3 = 1$ or $\dagger f(2)$ $\therefore$ 2 is not a solution

$f(3) = 6$ or $5 \dagger f(3)$ $\therefore$ 3 is not a solution

$f(4) = 13$ or $5 \dagger f(4)$ $\therefore$ 4 is not a solution

In an ordinary equation there must have solution but in congruence there may not have solution at all.

Theorem 2.29. If a is a solution of $f(x) \equiv 0(\text{mod } m)$ ...(1)

and $b \equiv a(m)$

then b is also a solution of (1)

Proof: $b \equiv a(m)$ or $b = a + \lambda m$, or $a = b + \mu m$ $(-\lambda = \mu)$

We have $f(a) = 0(\text{mod } m)$ i.e., $m \mid f(a)$

And $f(b) = f(a + \lambda m)$

$= a_0 + a_1 + (a + \lambda m) + a_2(a + \lambda m)^2 + \ldots + a_n(a + \lambda m)^n$

$= (a_0 + a_1 a + a_2 a_2 + \ldots + a_n a^n) + m\Phi(\lambda)$, say.

Therefore, $f(b) = f(a) + m\Phi(\lambda)$

Now $m \mid f(a)$, $m \mid m\Phi(\lambda)$ gives $m \mid f(b)$.

$\therefore$ b is a solution.

Remark: If one solution of (1) can be found then infinitely many others can be obtained, but related to each other's mod m.

Therefore we speak in terms to be a solution of

$$f(x) \equiv 0(\text{mod } m) \text{ if and only if } f(a) \equiv 0(\text{mod } m)$$

If a_1 and a_2 are solutions of (1), then these will be considered as distinct if and only if $a_1 \not\equiv a_2(\text{mod } m)$.

So instead of considering the number of solutions of (1) the proper consideration will be the number of residue classes.

Hence, by the number of solutions of a congruence mod m we shall mean the maximum number of solutions incongruent in pairs.

According to this definition there cannot be more than m solutions for any given congruence mod m, since there are m different residue classes to be considered.

Definition: The congruence of the type

$$ax + b \equiv 0 (\text{mod } m) \qquad \ldots.(*)$$

is called a linear congruence in one unknown

Theorem 2.30. If $(a, m) = 1$, then (*) has a unique solution

[One solution means one residue class.]

Proof: Euler Theorem states that $(a, m) = 1$

gives $a^{\Phi(m)} \equiv 1 (\text{mod } m)$

Multiplying (*) by $a^{\Phi(m)-1}$ we get

$$a^{\Phi(m)-1} ax \equiv -b\, a^{\Phi(m)-1} (\text{mod } m)$$

or $$a^{\Phi(m)} x \equiv -b\, a^{\Phi(m)-1} (\text{mod } m)$$

or $$x \equiv -ba^{\Phi(m)-1} (m)$$

$\therefore$ the solution is $-ba^{\Phi(m)-1}$ and this is unique.

Theorem 2.31. If $(a, m) = d\ (> 1)$, then (*) has a solution

if and only if $d \mid b$ [i.e., $\frac{b}{d} = d_3 \in \mathbb{Z}$]

Proof: $d \mid m$, $d \mid a$, we have $m = dd_1$ and $a = dd_2$ [i.e., $\frac{m}{d} = d_1$, $\frac{a}{d} = d_2$]

Suppose $ax + b \equiv 0 (\text{mod } m)$ is solvable.

Then $dd_2 x + b \equiv 0 (\text{mod } dd_1)$ is solvable and this gives,

$$dd_2 x + b \equiv 0 (\text{mod } d)$$

$$b \equiv 0 (\text{mod } d)$$

or $$d \mid b.$$

Conversely, assume that, $d \mid b$, then $b = dd_3$

Now $d_2 x + d_3 \equiv 0 (\text{mod } d_1)$ has a unique solution say, y $(\because (d_1, d_2) = 1)$

So, $d_2 y + d_3 \equiv 0 (\text{mod } d_1)$

or $dd_2 y + dd_3 \equiv 0 (\text{mod } dd_1)$

or $ay + b \equiv 0 (m)$

$\therefore$ (*) has a solution, say, y.

Theorem 2.32. If in (*) $d \mid b$, then (*) has d solutions $(m = dd_1, a = dd_2, b = dd_3)$

These are given by

$$x_1, x_1 + \frac{m}{d}, x_1 + 2\frac{m}{d}, \ldots, x_1 + (d-1)\frac{m}{d}$$

where x_1 is the solution, unique modulo $\frac{m}{d}$, of the linear congruence

$$\frac{a}{d} x + \frac{b}{d} \equiv 0 (\text{mod } \frac{m}{d})$$

Proof: $d_2 x + d_3 \equiv 0 (\text{mod } d_1)$ has a unique solution $(\because (d_2, d_1) = 1)$ (say, x_1)

So $d_2x_1 + d_3 \equiv 0(\text{mod } d_1)$ gives, $\frac{a}{d}x_1 + \frac{b}{d} \equiv 0(\text{mod } \frac{m}{d})$

Now the solutions of $ax + b \equiv 0(\text{mod } m)$ are the integers u such that $u \equiv x_1(\text{mod } d_1)$ that is

$$u = x_1 + td_1 \ (= x_1 + \frac{m}{d}t)$$

If $t \in \{0, 1, 2, ..., d - 1\}$ then u takes d values, no two of which are congruent modulo m.

If t is given any other values, the corresponding u will be congruent modulo m to one of these d values.

[*Thus we have: The linear congruence in one unknown* (*), *where* $(a, m) = 1$, *has exactly one solution* $x \equiv -ba^{\Phi(m)-1}$ *(mod m)*

When $(a, m) = d > 1$, (*) *has solution if and only if* $d \mid b$, *in which case* (*) *has d solutions*

$$x_t \equiv a + \frac{m}{d}t(\text{mod } m),\ t \in \{0, 1, 2, ..., d - 1\}$$

Example 35. **Solve:** $39x \equiv 65(\text{mod } 52)$

Solution: Here $a = 39$, $m = 52$,

$\therefore$ $d = (a, m) = (39, 52) = 13$

$13 \mid 65$.

$\therefore$ The equation has solutions. And it has 13 solutions.

The reduced congruence is $3x \equiv 5(\text{mod } 4)$ which has unique solution, $\because$ $(3, 4) = 1$ viz., $x \equiv 3(\text{mod } 4)$.

$\therefore$ we can take x_0 as 3

$\therefore$ general solution of given congruence are given by

$$x = x_0 + \frac{m}{d}t = 3 + \frac{52}{13}t = 3 + 4t$$

where $x \in \{0, 1, 2, 3, ..., 51\}$

Solutions are 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51 (mod 52)

i.e., the solutions are $\{0, 1, 2, 3, ..., 51) \cap \{x \mid x = 3 + 4t\}$.

Example 36. Solve: $3x + 2 \equiv 0(\text{mod } 7)$ ...(1)

Solution: $\because$ $(3, 7) = 1$, the congruence has only one incongruent solution

$\therefore$ $1 = 7 - 3 \times 2$ or $-2 = -14 + 3.4$ ...(2)

Comparing (1) and (2) we get,

$$3x \equiv -14 - 3 \times 4 \equiv 3 \times 4(\text{mod } 7).$$

$\therefore$ $x \equiv 4(\text{mod } 7)$ is the solution.

Example 37. Find the least positive solution of $13x \equiv 9(\text{mod } 25)$

Solution: $\because$ $(13, 25) = 1$, the congruence has a single solution (Observe:

$$13\overset{1}{)}35 - 13 = 12\overset{1}{)}13 - 2 = 1\overset{12}{)}12 - 12 = 0$$

$\therefore$ $35 = 13 \times 1 + 12$

$13 = 12 \times 1 + 1$

$12 = 12 \times 1$

$\therefore$ $1 = 13 - 12 \times 1 = 13 - (25 - 13 \times 1)$

$= 13 \times 2 - 25 \times 1$

Then $9 = 13 \times 2 \times 9 - 25 \times 1 \times 9,$

which gives, $9 = 13 \times 18 - 25 \times 9 \equiv 13x \pmod{25}$

$\therefore$ $x \equiv 18 \pmod{25}.$

Example 38. Solve: $207x \equiv 6 \pmod{18}$

Solution: From the given equation we have, $(18 \times 11 + 9)\, x \equiv 6 \pmod{18}$

or $9x \equiv 6 \pmod{18}$

or $3x \equiv 2 \pmod{6}$

$\because$ $(3, 6) = 3$ and $3 \nmid 2$, the equation has no solution.

Example 39. Solve $259x \equiv 5 \pmod{11}$

Solution: $259 = 11 \times 25 + 6.,$

or $259 \equiv 6 \pmod{11},$

$\therefore$ we get, $6x \equiv 259x \equiv 5 \pmod{11}$

So, $6x \equiv 5 \pmod{11}.$

Now the above has only one solution.

We observe that among 0, 1, 2, ..., 10, $x = 10$ satisfies the above.

Hence $x \equiv 10 \pmod{11}$ is the only solution.

Example 40. Solve $7x \equiv 5 \pmod{256}$ ...(1)

Solution: $\because$ $(256,7) = 1$, the equation has only one solution

We note $7\overset{36}{)}256 - 252 = 4\overset{1}{)}7 - 4 = 3\overset{1}{)}4 - 3 = 1\overset{3}{)}3 - 3 = 0$

$\therefore$ $256 = 7 \times 26 + 4,\ 7 = 4 \times 1 + 3,\ 4 = 3 \times 1 + 1,\ 3 = 3 \times 1$

or $1 = 4 - 3 \times 1 = 4 - (7 - 4) \times 1$

$= 4 \times 2 - 7 \times 1 = (256 - 7 \times 36) \times 2 - 7 \times 1$

$= 256 \times 2 - 73 \times 7$

or $5 = 5 \times 1 = 5 \times (256 \times 2 - 73 \times 7)$

$= 256 \times 10 - 73 \times 35$

or $5 \equiv -73 \times 35 \pmod{256}$ ...(2)

$\therefore$ (1) and (2) give,

$7x \equiv -73 \times 35 \pmod{256}$

or $x \equiv -73 \times 5 \equiv -365 \equiv 147 (\text{mod } 256)$

or 147(mod 256) is the solution.

Example 41. Solve $222x = 12(\text{mod } 18)$

Solution: $\because$ $222 \equiv 6(\text{mod } 18)$,

$\therefore$ $6x \equiv 12(\text{mod } 18)$

$\because$ $(6, 18) = 6$ and $6 \mid 12$, there are exactly 6 incongruent solutions,

now $6x \equiv 12(\text{mod } 18)$ gives $x \equiv 2(\text{mod } 3)$

$\therefore$ $x = 2, 5, 8, 11, 14, 17$ are solutions (mod 18).

Example 42. Solve $111x = 75(\text{mod } 321)$

Solution: Here $(111,321) = 3$ and $3 \mid 75$.

$\therefore$ the congruence has three solutions.

Now from the given congruence we have,

$$37x \equiv 25(\text{mod } 107)$$

We note

$$37\overline{)107}^{2} - 74 = 33\overline{)37}^{1} - 33 = 4\overline{)33}^{8} - 32 = 1\overline{)4}^{4} - 4 = 0$$

Now, $107 = 37 \times 2 + 33$

$37 = 33 \times 1 + 4$

$33 = 4 \times 8 + 1$

$4 = 4 \times 1$

$\therefore$ $1 = 33 - 4 \times 8$

$= 33 - (37 - 33 \times 1) \times 8$

$= 33 \times 9 - 37 \times 8$

$= (107 - 37 \times 2) \times 9 - 37 \times 8$

$= 107 \times 9 - 37 \times 26$

or $1 = 107 \times 9 - 37 \times 26$

or $25 = 25 \times 107 \times 9 - 25 \times 37 \times 26$

$\equiv -25.37 \times 26(\text{mod } 107)$

or $25 \equiv -25 \times 37 \times 26(\text{mod } 107)$

Now the above congruence is

$37x = 25(\text{mod } 107)$.

And $25 \equiv -25.37.26$

So, we get $\equiv 37x(\text{mod } 107)$

or $-25 \times 26 \equiv x(\text{mod } 107)$

or $x \equiv -25 \times 26 \equiv 99(\text{mod } 107)$

$\therefore$ the required solutions are

$x = 99, 99 + 107, 99 + 2 \times 107(\text{mod } 321)$

or $x = 99,206,313(\text{mod } 321)$.

Note: Suppose our congruence is $ax + b \equiv 0 \pmod{m}$

Then we have, $my \equiv b \pmod{a}$

If y_0 is a solution, then

$$x_0 = \frac{my_0 - b}{a}$$ is the solution of the given congruence.

When $a < m$, to solve this congruence is easier than to solve the given one.]

Example 43. Solve: $863x \equiv 880 \pmod{2151}$

Solution The given congruence takes the form

$$2151y \equiv -880 \pmod{863}$$

And this takes the form

$$425y \equiv -880 \pmod{863} \qquad [863 \times 2 + 425 = 2151]$$

or $$85y \equiv -176 \pmod{863} \qquad [\because (425, 880) = 5]$$

Again in the same style,

$$863z \equiv 176 \pmod{85}$$

Then, $$13z \equiv 6 \pmod{85} \qquad [863 = 85 \times 10 + 13,\ 176 = 85 \times 2 + 6]$$

also, $$85w = -6 \pmod{13}$$

or $$7w = -6 \pmod{13}$$

Hence, $w_0 = 1$

$\therefore$ $$z_0 = \frac{85 + 6}{13} = 7$$ } ...(*)

$$y_0 = \frac{863.7 - 176}{85} = 69,$$

$$x_0 = \frac{2151.69 + 880}{863} = 173$$

Thus the required solution is $x \equiv 173 \pmod{2151}$ $\because$ (863, 2151) = 1 the given congruence has only one solution.

2.6 SOLUTIONS OF THE PROBLEMS OF THE TYPE: ax + by + c = 0

Example 44. Solve $5x + 11y = 92$

Solution: The problem is equivalent to $92 = 11y + 5x$

or $$92 \equiv 11y \pmod{5}$$

and $\because$ $$92 \equiv 2 \pmod{5},$$

$$11 \equiv 1 \pmod{5}$$

$\therefore$ $$2 \equiv y \pmod{5},$$

or $$y \equiv 2 \pmod{5}$$

Hence all values of y must be of the form

$$y = 2 + 5n.$$

So, $5x = 92 - 22 - 55n = 70 - 55n$

$\therefore$ $x = 14 - 11n$

Hence, $\left.\begin{aligned} x &= 14 - 11n \\ y &= 2 + 5n \end{aligned}\right\}$ for all integral values of n.

And the same may be put in the form

$$\left.\begin{aligned} x &\equiv 14 (\text{mod } 11) \\ y &\equiv 2 (\text{mod } 5). \end{aligned}\right\}$$

Example 45. Find all solutions in positive integers of

$$5x + 3y = 52$$

Solution: The given equation is equivalent to

$$5x \equiv 52 (\text{mod } 3),$$

$\because$ $5 \equiv 2 (\text{mod } 3)$

and $52 \equiv 1 (\text{mod } 3)$,

We have, $2x \equiv 5x \equiv 52 \equiv 1 (\text{mod } 3)$,

i.e., $2x \equiv 1 (\text{mod } 3)$

or $2x \equiv 4 (\text{mod } 3)$

$\therefore$ $x \equiv 2 (\text{mod } 3)$

or $x = 2 + 3k$

Now from the given equation we get

$$3y = 52 - 5x = 52 - 5\,(2 + 3k)$$
$$= 42 - 15k.$$

or $3y = 42 - 15k$

or $y = 14 - 5k$

$\therefore$ the solutions are $(2 + 3k, 14 - 5k)$, for all integral values of k.

Example 46. Solve $2x + 7y \equiv 5 (\text{mod } 12)$

Solution: The given congruence is equivalent to

$$2x + 7y = 5 + 12z \qquad \ldots(*)$$

or $7y + 2(x - 6z) = 5$

i.e., equivalent to $7y \equiv 5 (\text{mod } 2)$ [**Note:** Here $(2, 12) = 2$]

and the congruence has a solution ($\because$ $(7, 2) = 1$)

$\because$ $7 \equiv 1 (\text{mod } 2)$,

We get $7y \equiv y (\text{mod } 2)$

And $5 \equiv 1 (\text{mod } 2)$ gives

$y \equiv 1 (\text{mod } 2)$ is a solution.

The value of y are 1, 3, 5, 7, 9, 11(mod 12).

Again the (*) gives $2x + 7y \equiv 5 (\text{mod } 12)$

or $2x \equiv 5 - 7y (\text{mod } 12)$

or $x \equiv (5 - 7y) (\text{mod } 6)$

Now the corresponding solutions for x are 5, 4, 3, 2, 1, 0 mod 6)

$\therefore$ Solutions (mod 12) are

(5, 1); (11, 1); (4, 3); (10, 3); (3, 5); (9, 5);
(2, 7); (8, 7); (1, 9); (7, 9); (0, 11); (6, 11).

Example 47. Solve: $x + 2y + 3z = 1$

Solution: The given equation is equivalent to

$$x + 2y = 1 - 3z \equiv 1 \pmod 3$$

i.e., $$x + 2y \equiv 1 \pmod 3$$

Now we consider, $x \equiv 1 \pmod 2$ [as in above example]

Put $x = 1 + u$ then $2y + 3z = 1 - x$

$$= 1 - (1 + u)$$

or $$2y + 3z = -u$$

or $$2y \equiv -u \pmod 3$$

$$\equiv -u - 3u$$

$$\equiv -4u \pmod 3$$

or $$y \equiv -2u \pmod 3$$

or $$y \equiv -2u + 3v$$

$\therefore$ $$3z = -u - 2y$$

$$= -u - 2(-2u + 3v)$$

$$= 3u - 6v$$

or $$z = u - 2v$$

Hence, $$x = 1 + u,$$

$$y = -2u + 3v,$$

$$z = u - 2v,$$ where u, v are integers.

So, the solutions are

$(1 + u, -2u + 3v, u - 2v)$ where u and v are integers.

Example 48. Solve $x + 2y + 3z = 10$

Solution: The given equation is equivalent to

$$x + 2y \equiv 10 \pmod 3$$

We now consider the congruence,

$$x \equiv 10 \pmod 2$$

Let $$x = 10 + u,$$

$\therefore$ $$2y + 3z = 10 - x = 10 - 10 - u$$

or $$2y + 3z = -u$$

or $$2y \equiv -u \pmod 3,$$

or $$2y \equiv -4u \pmod 3,$$

or $$y \equiv -2u \pmod 3$$

or $y = -2u + 3v,$

Then, $3z = -u - 2y$

$= -u - 2(-2u + 3v)$

$= 3u - 6v$

or $z = u - 2v$

$\therefore$ $x = 10 + u,$

$y = -2u + 3v,$

$z = u - 2v.$

Hence the solution is $(10 + u, -2u + 3v, u - 2v)$.

Note: It is sometimes convenient that we solve the congruence by using indeterminate equation

Example 49. Solve: $111x \equiv 75 (\text{mod } 321)$

Solution: $\because (111, 321) = 3$ and $3 \mid 75$ it follows that the given congruence has 3 solutions.

Now the given congruence reduces to

$$37x \equiv 25 (\text{mod } 107) \quad ...(*)$$

Now we solve the indeterminate equation

$$37u + 107v = 25,$$

Solving this equation we get $u = -8$, $v = 3$. Hence

$$x \equiv -8 \equiv 99 (\text{mod } 107) \text{ is a solution of (*)}$$

$\therefore$ the required 3 solutions are

$$x \equiv 99, 99 + 107 = 206, 99 + 214 = 315 (\text{mod } 321)$$

2.7 SIMULTANEOUS CONGRUENCES

Theorem 2.33. The systems of congruences

$$x \equiv a (\text{mod } m)$$

$$x \equiv b (\text{mod } n)$$

has a solution if and only if

$$a \equiv b (\text{mod } (m, n))$$

If this condition is satisfied, then (*) has only one unique solution modulo $[m, n]$.

Proof: Suppose $x \equiv c$ be a solution of a given system, then

$c \equiv a (\text{mod } m)$,

$c \equiv b (\text{mod } n)$

Thus $a \equiv b (\text{mod } (m, n))$,

[Observe: $m \mid c - a$, $n \mid b - a$ gives, $(m, n) \mid c - a$, $(m, n) \mid c - b$ or $(m, n) \mid a - b$]

And hence the necessary condition holds.

Conversely suppose

$$a \equiv b (\text{mod } (m, n))$$

then by Theorem 2.31. we know that the congruence

$$my \equiv b - a(\text{mod } n)$$

has solution $$y \equiv d(\text{mod } n).$$

Hence we obtain $$a + md \equiv a(\text{mod } m),$$

$$a + md \equiv b(\text{mod } n)$$

Thus $x \equiv a + md$ is a solution of the given system.

Hence the sufficient condition holds

Now suppose x_0 and y_0 are the solution of the system.

$\therefore$ $$x_0 \equiv y_0(\text{mod } m)$$

$$x_0 \equiv y_0(\text{mod } n)$$

give $$m, n \mid x_0 - y_0$$

or $$[m, n] \mid x_0 - y_0$$

or $$x_0 \equiv y_0 \,(\text{mod } [m, n])$$

And this means that the given congruence has only one solution. modulo $[m, n]$

Note: From above we see that the congruences

$$x \equiv a_1(\text{mod } m_1)$$

$$x \equiv a_2(\text{mod } m_2)$$

$$\ldots \ldots \ldots$$

$$\ldots \ldots \ldots$$

$$x \equiv a_n(\text{mod } m_n)$$

has a solution if and only if $a_i = a_j(\text{mod } (m_i, m_j))$, $i, j = 1, 2, \ldots, n$

and has only one solution modulo $[m_1, m_2, \ldots, m_n]$.

Remark: If $(m_1, m_2) = 1$ then the above congruence has always a common solution.

Example 50. Determine the common solution of

$$x \equiv 5(\text{mod } 8)$$

and $$x \equiv 4(\text{mod } 9).$$

Solution: From the first one we get

$x = 5 + 8t$ and putting this values in the second one we get

$$5 + 8t \equiv 4(\text{mod } 9)$$

or $$8t \equiv -1(\text{mod } 9).$$

Multiplying this by 8 and

$\because$ $$8 \times 8 \equiv 1(\text{mod } 9)$$

or $$t \equiv -8 \equiv 1(\text{mod } 9)$$

We get, $$t = 1 + 9r$$

and $$x = 5 + 8t = 5 + 8(1 + 9r) = 13 + 72r.$$

Now to determine the common solution of

$$x \equiv 5(\text{mod } 8)$$

and $$x \equiv 4(\text{mod } 9)$$

it can be seen that it is possible to have common solutions.

Now we find the condition under which such type of a set of congruences may have common solutions

We note that if $m = p_1^{n_1} \cdot p_2^{n_2} \cdots p_r^{n_r}$.

Then $A \equiv B(\text{mod } m)$ if and only if all the congruences

$A \equiv B(\text{mod } p_1^{n_1})$

$A \equiv B(\text{mod } p_2^{n_2})$

.....

$A \equiv B(\text{mod } p_r^{n_r})$

hold.

Thus, the system

$ax \equiv b(\text{mod } m)$ has the same solutions as the system of simultaneous congruences

$ax \equiv b(\text{mod } p_1^{n_1})$

$ax \equiv b(\text{mod } p_2^{n_2})$

..... and

$ax \equiv b(\text{mod } p_r^{n_r})$

Observe

Example 51. The congruence

$$3x \equiv 11(\text{mod } 2275)$$

This is equivalent to the following:

$$3x \equiv 11(\text{mod } 25)$$
$$3x \equiv 11(\text{mod } 7)$$
$$3x \equiv 11(\text{mod } 13) \qquad (\because 2275 = 5^2 \times 7 \times 13)$$

This type of explanation leads one to give the problem for searching for the common solution of a system of congruences.

Theorem 2.34. *Chinese remainder theorem* named after Sun – Tsu, believed to be the first mathematician who studied special cases of this theorem.

Let $m_1, m_2, ..., m_n$ be integers each greater than 1 and co prime to each other. Then the following congruences

$$x \equiv a_1(\text{mod } m_1)$$
$$x \equiv a_2(\text{mod } m_2)$$
.....
.....
$$x \equiv a_n(\text{mod } mn)$$

has a solution x_0 and for any general solution x,

$$x \equiv x_0 (\text{mod } m_1.m_2 ..., m_n)$$

Proof: Let $m = m_1.m_2 ... m_n$

Then, each of $\frac{m}{m_1}, \frac{m}{m_2}, ..., \frac{m}{m_n}$ is an integer and that

$$(\frac{m}{m_1}, m_1) = 1, (\frac{m}{m_2}, m_2) = 1, ..., (\frac{m}{m_n}, m_n) = 1.$$

Now applying the result: *if* $(a, m) = 1$, *then* $ax \equiv b (mod\ m)$ *has a solution,* we see that there are integers $b_1, b_2, ..., b_n$ such that

$$\frac{m}{m_1} b_1 \equiv 1 (\text{mod } m_1),$$

$$\frac{m}{m_2} b_2 \equiv 1 (\text{mod } m_2),$$

.....

$$\frac{m}{m_n} b_n \equiv 1 (\text{mod } m_n),$$

Now it is easy to follow that

$$\frac{m}{m_1} b_1 \equiv 0 (\text{mod } m_2), \text{ or } (\text{mod } m_3), ... \quad (\text{mod } m_r)$$

$$\frac{m}{m_2} b_2 \equiv 0 (\text{mod } m_1), \text{ or } (\text{mod } m_3), ... \quad (\text{mod } m_n)$$

.....

$$\frac{m}{m_n} b_n \equiv 0 (\text{mod } m_1), \text{ or } (\text{mod } m_3), ... \quad (\text{mod } m_{n-1})$$

Now we define $x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2 + ... + \frac{m}{m_n} b_n a_n$ then we have

$$x_0 \equiv \frac{m}{m_1} b_1 a_1 (\text{mod } m_1)$$

$$\equiv a_1 (\text{mod } m_1)$$

$$\equiv a_1 (\text{mod } m_1)$$

or

$$x_0 \equiv \frac{m}{m_2} b_2 a_2 (\text{mod } m_2)$$

$$\equiv a_2 (\text{mod } m_2)$$

.....

.....

Thus, x_0 is a common solution of the original congruences.

If x_0 and x_1 are both common solutions of

$$x \equiv a_1 (\text{mod } m_1),$$
$$x \equiv a_2 (\text{mod } m_2),$$
$$\ldots\ldots\ldots,$$
$$x \equiv a_r (\text{mod } m_r) \text{ then}$$
$$x_0 \equiv x_1 (\text{mod } m_1),$$
$$x_0 \equiv x_1 (\text{mod } m_2),$$
$$\ldots \ldots\ldots\ldots\ldots\ldots$$
$$x \equiv a_r (\text{mod } m_r) \text{ hence}$$
$$x_0 \equiv x_1 (\text{mod } m).$$

Example 52. Find the least natural number which when divided by 7, 10 and 11 leaves in order the remainders 1, 6 and 2.

Solution: Here we have to find a common solution of the congruences

$$x \equiv 1 (\text{mod } 7)$$
$$x \equiv 6 (\text{mod } 10)$$
$$x \equiv 2 (\text{mod } 11)$$

We can let $x = 7x_1 + 1.$

Then we must have $7x_1 \equiv 5 (\text{mod } 10)$

Multiplying both sides of this congruence by 3 (the associate of 7 modulo 10), we

Get $x_1 \equiv 15 \equiv 5 (\text{mod } 10).$

[Observe: $7x_1 \equiv 5 (\text{mod } 10)$

or $21x_1 \equiv 15 (\text{mod } 10)$ (*Note 10 = 7 + 3*)

or $20x_1 + x_1 \equiv 10 + 5 (\text{mod } 10)$

or $x_1 \equiv 5 (\text{mod } 10)]$

Let $x_1 = 10x_2 + 5,$

so that $x = 70x_2 + 36$

This will satisfy the third congruence of the set, if and only if

$$70x_2 \equiv -34 (\text{mod } 11);$$

i.e., $4x_2 \equiv -1 (\text{mod } 11)$

Again multiplying the sides of the congruence by 3, the associate of 4 modulo 11, 23 get

$$x_2 \equiv -3x_1 \equiv 8 (\text{mod } 11).$$

This means that for some integer x_3, we have

$$x_2 = 11x_3 + 8$$

Hence $x = 770x_3 + 596 \equiv 596 (\text{mod } 770)$

$\therefore$ the required number is 596.

Using the Chinese remainder theorem, we will have

$$x_0 = \frac{m}{m_1}b_1a_1 + \frac{m}{m_2}b_2a_2 + ... + \frac{m}{m_n}b_na_n$$

$$m = 770$$

$$\frac{m}{m_1} = 110$$

$$\frac{m}{m_2} = 77$$

$$\frac{m}{m_n} = 70$$

These give $b_1 = 3, \quad b_2 = 3, \quad b_3 = 3$

(It is a mere chance that the b's have turned out to be equal)

Hence

$$x_0 = 1 \times 110 \times 3 + 6 \times 77 \times 3 + 2 \times 70 \times 3 + 2136 \equiv 596 (\text{mod } 770)$$

or $$x_0 = 596 (\text{mod } 770)$$

Example 53. Solve $x \equiv 2(\text{mod } 3)$

$x \equiv 3(\text{mod } 5)$

$x \equiv 2(\text{mod } 7)$

Solution: $3 \times 5 \times 7 = 3 \times 35 = 5 \times 21 = 7 \times 15$

And $35.2 = 1(\text{mod } 3), 21.1 = (\text{mod } 5), 15.1 = 1(\text{mod } 7)$

Then $35 \times 2 \times 2 + 21 \times 1 \times 3 + 15 \times 1 \times 2 = 140 + 63 + 30 = 233$

Hence the required solution is $233 \equiv 23 \pmod{105}$.

Example 54. Find all integers that satisfy simultaneously

$x \equiv 2(\text{mod } 3)$

$x \equiv 3(\text{mod } 5),$

$x \equiv 5(\text{mod } 2)$

Solution: Here, $3 \times 5 \times 2 = 3 \times 10 = 5 \times 6 = 2 \times 15$

And $1 \times 10 \equiv 1(\text{mod } 3), 1 \times 6(\text{mod } 3), 1 \times 15(\text{mod } 2)$

$\therefore$ $x = 1 \times 10 \times 2 + 1 \times 6 \times 3 + 1 \times 15 \times 5$

$= 20 + 18 + 75$

$\equiv 113(\text{mod } 30)$

$\equiv 23(\text{mod } 30).$

Example 55. Solve: $x \equiv 6(\text{mod } 17)$

$x \equiv 17(\text{mod } 24)$

$x \equiv 13(\text{mod } 33)$

Solution: Here 24 and 33 are not co-prime.

If $x \equiv 17(\text{mod } 24)$ then, $x - 17$ is divisible by 24, then so is 3 and 8.

Similarly if $x \equiv 13(\text{mod } 33)$ then $x - 13$ is divisible by 3 and 11.

Hence the given congruence can be written as

$$x \equiv 6(\text{mod } 17) \quad ...(1)$$
$$x \equiv 17(\text{mod } 3) \quad ...(2)$$
$$x \equiv 17(\text{mod } 8) \quad ...(3)$$
$$x \equiv 13(\text{mod } 3) \quad ...(4)$$
$$x \equiv 13(\text{mod } 11) \quad ...(5)$$

If (2) and (4) hold, then

$17 \equiv 13(\text{mod } 3)$, but this impossible.

So the given simultaneous congruence has no solution.

Example 56. Solve $x \equiv 5(\text{mod } 18)$
$x \equiv -1(\text{mod } 24)$
$x \equiv 17(\text{mod } 33)$

Solution The given congruences are equivalent to

$$x \equiv 1(\text{mod } 2) \quad ...(1)$$
$$x \equiv 5(\text{mod } 9) \quad ...(2)$$
$$x \equiv -1(\text{mod } 3) \quad ...(3)$$
$$x \equiv -1(\text{mod } 8) \quad ...(4)$$
$$x \equiv 2(\text{mod } 3) \quad ...(5)$$
$$x \equiv 6(\text{mod } 11) \quad ...(6)$$

If $x \equiv 5(\text{mod } 9)$, then $x \equiv -1(\text{mod } 3)$ and $x \equiv 2(\text{mod } 3)$ so, we discard (3) and (4) and we consider $x \equiv 5(\text{mod } 9)$, $x \equiv -1(\text{mod } 8)$, $x \equiv 6(\text{mod } 11)$

$$x \equiv 1(\text{mod } 2) \quad ...(i)$$
$$x \equiv 5(\text{mod } 9) \quad ...(ii)$$
$$x \equiv -1(\text{mod } 8) \quad ...(iii)$$
$$x \equiv 6(\text{mod } 11) \quad ...(iv)$$

By using Chinese remainder theorem, we get the solution as

$$x = 743 + 792k$$

or $$x \equiv 743 \text{ mod } (792).$$

Example 57. Solve $x \equiv -2(\text{mod } 12)$
$x \equiv 6(\text{mod } 10)$
$x \equiv 1(\text{mod } 15)$

Solution: *We express the given system as the product of primes and we get,*

$$x \equiv -2(\text{mod } 2^2)$$
$$x \equiv -2(\text{mod } 3)$$
$$x \equiv 6(\text{mod } 2)$$
$$x \equiv 6(\text{mod } 5)$$
$$x \equiv 1(\text{mod } 3)$$
$$x \equiv 1(\text{mod } 5)$$

From $x \equiv -2 (\text{mod } 2^2)$

$x \equiv 6 (\text{mod } 2)$

$x \equiv -2 (\text{mod } 3)$

$x \equiv 1 (\text{mod } 3)$

$x \equiv 6 (\text{mod } 5)$

$x \equiv 1 (\text{mod } 5)$

we have $x \equiv -2 (\text{mod } 22)$, $x \equiv 1 (\text{mod } 3)$, $x \equiv 1 (\text{mod } 5)$ respectively.

Thus the given system is equivalent to

$x \equiv -2 (\text{mod } 22)$

$x \equiv 1 (\text{mod } 3)$

$x \equiv 1 (\text{mod } 5)$

And the required solution is $x \equiv 46 (\text{mod } 60$.

EXERCISES 2.1

1. Show that if $2n + 1$ and $3n + 1$ are both perfect square then n is divisible by 40.
2. Show that $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots r$ if and only if $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$
3. Let n be an integer. Show that if $2 + 2\sqrt{28n^2 + 1}$ is an integer, then it must be a perfect square.
4. Prove that $n^6 - 1$ and $n^{12} - 1$ both are divisible by 7 if $(n, 7) = 1$
5. Prove that $x^{12} - y^{12}$ is divisible by 13 if x and y are prime to 13.
6. Prove that $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is an integer for all integral values of n.
7. Show that the number $2^{1093} - 2$ is divisible by 2186, 1093^2
8. Prove that 12^{th} power of any number is of the form $13n$ or $13n + 1$
9. Prove that 8^{th} power of any number is of the form $17n$ or $17n \pm 1$
10. Show that $n^{36} - 1$ is divisible by 33744 if n is prime to 2, 3, 19, 37.
11. Prove that if $n^4 + 4$ is composite when $n > 1$.
12. Prove that if p is a prime then $(p - 2r)!(2r - 1)! - 1$ is divisible by p

EXERCISES 2.2

1. Exhibit a reduced residue system for the modulus 15.
2. Exhibit a reduced residue system for the modulus 12.
3. Exhibit a reduced residue system for the modulus 30.
4. Find out a reduced residue system modulo 7 composed of entirely powers of 3.
5. If $(a, m) = 1$ and the quantities $a, 2a, 3a, 4a, \ldots, (m - 1)$ a are divided by m, then prove that the remainders are all different.

6. Deduce from above that if a is prime to m, and c is any number, then m terms of the Arithmetic Progression $c, c + a, c + 2a, ..., c + (m - 1)a$ when divided by m will leave the same remainder as the terms of the series

$$c, c + 1, c + 2, ..., c + (m - 1)$$

though not necessarily in this order and therefore the remainders will be

$$0, 1, 2, ..., (m - 1)$$

7. Show that $2, 4, 6, ..., 2m$ is a complete reside system modulo m if m is odd.

EXERCISES 2.3

1. Prove that M_{11} is composite.
2. Prove that F_5 is composite.

   (**Hint:** Prime integers not greater than 2^{2^4} and of the form $2^{3+2}t + 1 = 123t + 1$ are only 257, 641.

   Here $F_5 = 641 \times 6700417$.)
3. Show that, if a is any integer, then $a^2 + a + 1 \equiv 1 (\text{mod } 3)$ or $a + a + 1 \equiv 0 (\text{mod } 3)$
4. Prove that the necessary and sufficient condition that a number is a multiple of 11 is that the difference between the sum of odd digits and the sum of even digits is a multiple of 11.
5. Find the necessary and sufficient condition that a positive integer n can be divided by 13. Use your answer to decide whether 13 is a factor of 637639.
6. If p and q are two different primes, prove that $p^{q-1} + q^{p-1} \equiv 1 (\text{mod } pq)$
7. If $a > 0$, $b > 0$ and $(a, b) = 1$, show that there exist $m > 0$, $n > 0$ such that

$$a^m + b^n \equiv 1 (\text{mod } ab)$$

8. If p is prime $a \nmid p$ then prove that
   (i) if a is odd then $a^{p-1} + (p - 1)^a \equiv 1 (\text{mod } p)$
   (ii) if a is even then $a^{p-1} - (p - 1)^a \equiv 1 (\text{mod } p)$
9. Show that the product of two consecutive even numbers is a multiple of 8. Using Fermat theorem, hence deduce that for prime $p(> 5)$, $p^4 \equiv 1 (\text{mod } 240)$.

EXERCISES 2.4

1. Solve the following equations:
   (i) $2072x + 1813y = 2849$
   (ii) $8x - 18y + 10z = 16$
   (iii) $4x + 10y + 14z + 6t = 20$
2. Solve the system of linear equations:

$$x + 2y + 3z = 10$$
$$x - 2y + 5z = 4$$

3. Find the sum of all positive integers each of which has 2 digits and has remainder 4 when divided by 4.
4. A cock is worth Rupees 50, a hen Rupees 30, and three chickens together are worth Rupees 10, how many cocks, hens and chicks, totalling 100, can be bought for Rupees 1000?
5. What positive integer becomes a square when it is increased by 100 and when it is increased by 168?
6. Find the positive integers x and y such that $x(x + y) = 6$.
7. A person purchased 19 of item A and 20 of item B with rupees 1909. What are the possible numbers of the item A he may purchase.
8. When the quotient-obtained by dividing the sum of a number and three times the another number by the number obtained on increasing the first by 2-is added to 1 the second number is obtained. What are the possible values of the first number?

EXERCISES 2.5

A. How many solutions of the following congruences do have?

1. $12x \equiv 4 (\text{mod } 3)$
2. $30x \equiv 40 (\text{mod } 15)$
3. $15x \equiv 25 (\text{mod } 35)$
4. $25x \equiv 0 (\text{mod } 45)$
5. $353x \equiv 254 (\text{mod } 400)$

B. Solve the following congruences's

1. $256x \equiv 179 (\text{mod } 337)$
2. $1215x \equiv 560 (\text{mod } 2755)$
3. $3x \equiv 1 (\text{mod } 125)$

EXERCISES 2.6

Solve in integers

1. $7x + 5y = 5$
2. $3x + 5y = 1$
3. $10x - 7y = 17$
4. Prove that $ax + by = a + c$ is solvable if and only if $ax + by = c$ is solvable
5. If $(a, b, c) = 1$, show that $ax + by = c$ is solvable if and only if $(a, b) = 1$
6. Prove that $ax + by = c$ is solvable if nd only if $(a, b) = (a, b, c)$
7. Given that $ax + by = c$ has two solutions (x_0, y_0) and (x_1, y_1) with $x_1 = 1 + x_0$ and given that $(a, b) = 1$, prove that $b = \pm 1$.

EXERCISES 2.7

1. Find all the integers that give the remainders 1, 2, 3 when divided by 3, 4, 5 respectively
2. Find the least two positive integers having the remainders 2, 3, 2 when divide by 3, 5, 7 respectively.

EXERCISES 2.8

Solve the following congruences simultaneously

1. $x \equiv 1 (\text{mod } 3), x \equiv 1 (\text{mod } 5), x \equiv 1 (\text{mod } 7)$
2. $x \equiv 1 (\text{mod } 4), x \equiv 0 (\text{mod } 3), x \equiv 5 (\text{mod } 7)$
3. $x \equiv 3 (\text{mod } 4), x \equiv 2 (\text{mod } 5), x \equiv 6 (\text{mod } 7)$
4. $x \equiv 3 (\text{mod } 8), x \equiv 11 (\text{mod } 20), x \equiv 1 (\text{mod } 15), x \equiv 91 (\text{mod } 120)$

EXERCISES 2.9

Solve the following congruences

1. $158x \equiv -22 (\text{mod } 194)$
2. $194 \equiv -22 (\text{mod } 158)$
3. $1001x \equiv 433 (\text{mod } 4845)$
4. $9x \equiv 6 (\text{mod } 24)$

EXERCISES 2.10

Solve the simultaneous congruences:

1. $x \equiv 3 \text{ mod } 7, x \equiv -2 \text{ mod } 11,$
2. $x \equiv -2 \text{ mod } 11, x \equiv 8 \text{ mod } 22$
3. $x \equiv 3 \text{ mod } 7, x = 7 \text{ mod } 12, x \equiv 8 \text{ mod } 13$
4. $x \equiv 2 \text{ mod } 7, x \equiv -2 \text{ mod } 11, x \equiv 8 \text{ mod } 13, x \equiv -3 \text{ mod } 17$
5. $x \equiv -2 \text{ mod } 11, x \equiv 8 \text{ mod } 13, x \equiv 9 \text{ mod } 14, x \equiv 1 \text{ mod } 15, x \equiv -39 \text{ mod } 17$
6. $x \equiv 3 \text{ mod } 7, x \equiv -2 \text{ mod } 11, x \equiv 8 \text{ mod } 13, x \equiv -3 \text{ mod } 17, x \equiv 5 \text{ mod } 18$
7. $x \equiv 7 \text{ mod } 12, x \equiv 9 \text{ mod } 14$
8. $x \equiv 7 \text{ mod } 12, x \equiv 1 \text{ mod } 15$
9. $x \equiv 7 \text{ mod } 12, x \equiv 5 \text{ mod } 18$
10. $x \equiv 9 \text{ mod } 14, x \equiv 5 \text{ mod } 18$

EXERCISES 2.11

Solve the following simultaneous congruences

1. $3x \equiv 5 (\text{mod } 22), 11x \equiv 3 (\text{mod } 28), 5x \equiv 89 (\text{mod } 99)$
2. $9x \equiv 6 (\text{mod } 24), 12x \equiv 14 (\text{mod } 26)$

3. $x \equiv 1 (\text{mod } 2)$
$x \equiv 2 (\text{mod } 3)$
$x \equiv 3 (\text{mod } 5)$

4. $x \equiv 1 (\text{mod } 3)$
$x \equiv 3 (\text{mod } 5)$
$x \equiv 5 (\text{mod } 7)$

5. $3x \equiv 1 (\text{mod } 5)$
$4x \equiv 6 (\text{mod } 14)$
$5x \equiv 11 (\text{mod } 3)$

3

ALGEBRAIC CONGRUENCES AND PRIMITIVE ROOTS

3.1 ALGEBRAIC CONGRUENCES

Definition: $f(x) = a_0x^n + a_1x^{n-1} + = \ldots + a_n \equiv 0(\text{mod } p)$ ...(1)

$[(a_0, p) = 1$ i.e., $p \dagger a_0)]$

is called the *general form of a congruence with prime modulo p.* Substituting all the integers of a complete system of residue modulo p for x in (1) we may have all its solutions.

When n or p is large enough we note the following.

(i) If some a_i $(i \leq n) > p$, we reduce them to less than p.

(ii) If the degree of $f(x)$ is not less than p, we divide $f(x)$ by $x^p - x$ and obtain $r(x)$ and $q(x)$ as follows (Division algorithm in $\mathbb{Z}[x]$)

$$f(x) = (x^p - x)\, q(x) + r(x)$$

where deg $(r(x))$ less than p. Thus we get

$$f(x) \equiv r(x) \text{ (mod } p)$$

[using $x^p \equiv x(\text{mod } p)$ corollary to Fermat theorem]

It is seen that the incongruent solutions of $f(x)$ and $r(x)$ are identical.

(iii) Hence the problem of solution of (1) becomes that of solving

$$r(x) \equiv 0(\text{mod } p)$$

and the calculation becomes simpler, as deg $r(x) <$ deg $f(x)$

(iv) If $f(x) \equiv f_1(x) f_2(x) \text{ (mod } p)$

then to solve (1) is to solve

$$f(x) \equiv f_1(x) \text{ (mod } p)$$

and $f(x) \equiv f_2(x) \text{ (mod } p)$

(v) The difficulty of calculation is now greatly reduced, as deg $f_1(x)$, deg $f_2(x) <$ deg $f(x)$

(vi) If $x \equiv a(\text{mod } p)$ is a solution of (1) then as (i) above

$$f(x) = (x - a)\, q(x) + r,$$

and we have $r \equiv 0 (\text{mod } p)$

Thus, $f(x) \equiv (x - a)\, q(x) (\text{mod } p)$ [i.e., $x - a$ is a factor of $f(x)$ modulo p)

(vii) The problem of solving (1) becomes that of solving

$q(x) \equiv 0 (\text{mod } p)$ and thus the calculation is diminished.

It is to be noted that the only method of solving the congruence of the type (1) is by substitution.

Though the above reductions have efficacy for some special cases, they are of no use in general.

Example 1. Solve: $f(x) = x^7 - 2x^6 - 7x^5 + x + 2 \equiv 0 (\text{mod } 5)$

Solution: $x^7 \equiv x^3 (\text{mod } 5)$

$2x^6 \equiv 2x^2 (\text{mod } 5)$

$7x^5 \equiv 7x (\text{mod } 5)$

or $x^7 - 2x^6 - 7x^5 + x + 2 = x^3 - 2x^2 - 7x + x + 2 \equiv x^3 - x + 2 (\text{mod } 5)$

or $x^2 - x + 2 \equiv 0 (\text{mod } 5)$

Substituting the complete residue systems –2, –1, 0, 1, 2 (mod 5), for x, we obtain the 3 required solutions,

i.e., $x \equiv -1, 1, 2 (\text{mod } 5)$.

Example 2. Solve: $x^2 - 1 \equiv 0 (\text{mod } p)$, [$p$ is a prime]

Solution: Suppose x_0 is solution of the given congruence. Then

$x_0^2 - 1 \equiv 0 (\text{mod } p)$

or $p \mid x_0^2 - 1$

or $p \mid x_0 - 1$ or $x_0 + 1$

or $x_0 - 1 \equiv 0 (\text{mod } p)$ or $x_0 + 1 \equiv 0 (\text{mod } p)$

or $x_0 \equiv 1$ or $-1 (\text{mod } p)$

or $x_0 \equiv 1$ or $p - 1 (\text{mod } p)$[taking x_0 for the least positive residue.]

Thus 1 and $p - 1$ are the solutions of the given congruence.

Example 3. Solve: $x^{p-1} - 1 \equiv 0 (\text{mod } p)$

Solution: By Fermat theorem we have that

$x^{p-1} - 1 \equiv 0 (\text{mod } p)$

is true for every number x relatively prime to p. Hence we have $p - 1$ different solutions

$x \equiv 1, 2, 3, ..., p - 1 (\text{mod } p)$.

Theorem 3.1. The number of solutions of congruences

$$f(x) = a_0 x^n + a_1 x^{n-1} + = ... + a_n \equiv 0 (\text{mod } p) \quad ...(1)$$

is at most n $[(a_0, p) = 1$ i.e., $p \dagger a_0)]$

Remark: Maximum number of solutions is $n (\text{mod } p)$

Proof: The statement is correct if (1) has no solution

Suppose it has a solution $x_1 (\text{mod } p)$

Then

$$a_0 x_1^{\,n} + a_1 x_1^{\,n-1} + = \ldots + a_n \equiv 0 (\text{mod } p) \qquad \ldots(2)$$

Now (1) – (2) gives,

$$a_0 (x^n - x_1^{\,n}) + a_1 (x^{n-1} - x_1^{\,n-1}) + \ldots + a_{n-1} (x - x_1) \equiv 0 (\text{mod } p) \qquad \ldots(3)$$

Which any x satisfying (1) must also satisfy (3) can be written as

$$(x - x_1) [a_0 (x^{n-1} - \ldots) + a_1 (x^{n-2} + \ldots) + \ldots] \equiv 0 (p)$$

or

$$(x - x_1) [a_0 x^{n-1} + b_1 x^{n-2} + \ldots + \ldots b_{n-1}.] \equiv 0 (p) \qquad \ldots(4)$$

(b's are functions of a's and x's)

$\because$ $p \mid$ then L.H.S. of (4), it must divide at least one of them.

$\therefore$ any x satisfying (1) must satisfy either.

$$x - x_1 \equiv 0 (p) \qquad (\text{i.e., } x \equiv x_1 (\text{mod } p))$$

or

$$a_0 x^{n-1} + b_1 x^{n-2} + \ldots + \ldots b_{n-1}.] \equiv 0 (p) \qquad \ldots(5)$$

The first alternative yields again x_1,

The second may or may not yield a solution.

If 2nd has not given any solution, the number of solution of (1) is 1[i.e., $x_1 (\text{mod } p)$ and the theorem is proved.

If (5) has solution, say, $x_2 (\text{mod } p)$ then (5) can be written as

$$(x - x_2) (a_0 x^{n-2} + c_1 x^{n-3} + \ldots + \ldots c_{n\cdot}] \equiv 0 (p) \qquad \ldots(6)$$

where $x_2 (\text{mod } p)$ is a solution of (5) and therefore of (1)

If $a_0 x^{n-2} + \ldots + \ldots \equiv 0 (\text{mod } p)$ has no solution, then the number of solution is 2 and the theorem is proved, and so on.

Ultimately we may get a congruence $a_0 x + g \equiv 0 (\text{mod } p)$,

which it has a unique solution, $\because$ $(p, a_0) = 1$

$\therefore$ the number of solution is now n.

Hence the number of solution is at most n.

The following result gives the condition that a congruence of n^{th} degree has exactly n distinct solutions.

Theorem 3.2. The necessary and sufficient condition that a congruence of n^{th} degree.

$f(x) \equiv 0 (\text{mod } p)$ has n different solutions is that

$f(x)$ is a factor of $x^p - x$ mod p, where $p \geq n$.

Proof: Suppose $x^p - x \equiv q(x) f(x) + r(x)$, where $r = 0$ or deg $r(x) < n$.

If $f(x) \equiv 0 \pmod p$ has n solutions then these are solutions of $x^p - x \equiv 0 (\text{mod } p)$ also, and

$\therefore$ they are solutions of $r(x) \equiv 0 (\text{mod } p)$ also.

Now deg $r(x) < n$, it therefore follows that

The coefficient of $r(x)$ are multiples of p, that is, $r(x) = 0$.

Hence $x^p - x \equiv q(x)f(x)(\text{mod}\, p)$.

Conversely,

Suppose $x^p - x \equiv q(x)f(x)(\text{mod}\, p)$. And

(i) The number of solutions of $f(x) \equiv 0(\text{mod}\, p) < n$,

$\because$ the number of solutions of $q(x) \equiv 0(\text{mod}\, p) \leq p - n$,

The number of solutions of $q(x)f(x) \equiv 0(\text{mod}\, p))$ is less than p. And this is not the case.

$\therefore$ $f(x) \equiv 0(\text{mod}\, p)$ has n solutions.

Hence the theorem follows.

3.2 REDUCTION OF

$$f(x) \equiv 0(\text{mod}\, m) \qquad ...(1)$$

to the solutions

$$f(x) \equiv 0(\text{mod}\, p^{\alpha}):$$

Theorem 3.3. If $m > 0$, $m = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, p's are primes

$$1 < p_1 < p_2 < p_3 < p_4 \ldots < p_n,$$

then the solutions of (1) depend upon the solutions of

$$f(x) \equiv 0(p_i^{\alpha_i}), \qquad (i = 1, 2, .., n) \quad ...(2)$$

Proof: Obviously, $f(x) \equiv 0(m)$

gives $f(x) \equiv 0(p_i^{\alpha_i})$, $(i = 1, 2, ..., n)$

So, every solution of (1) is a solution of various congruences (2)

Conversely, suppose that all solution of (2) can be found. Let us suppose that a_1, a_2, ... $a_n \in \mathbb{Z}$ have been found so that

$$f(a_1) \equiv 0(p_1^{\alpha_1}),$$

$$f(a_2) \equiv 0(p_2^{\alpha_2}),$$

.....

$$f(a_n) \equiv 0(p_n^{\alpha_n})$$

[That $f(a_i) \equiv 0(p_i^{\alpha_i})'$ $(i = 1, 2, \ldots n)$],

i.e., $x \equiv a_1(p_1^{\alpha_1})$ is a solution of first congruence of (2) i.e. $f(x) = 0(p_1^{\alpha_1})$

$x \equiv a_2(p_2^{\alpha_2})$ is 2^{nd} ..... $f(x) \equiv 0(p_2^{\alpha_2})$

.....

$x \equiv a_n(p_n^{\alpha_n})$ is a ..... n^{th} .... $f(x) \equiv 0(p_n^{\alpha_n})$

Then, $\because (p_i^{\alpha_i}, p_j^{\alpha_j}) = 1, (i \neq j)$, by Chinese remainder theorem there exists $a \in \mathbb{Z}$ such that

$$a \equiv a_1(p_1^{\alpha_1}),$$

$$a \equiv a_1(p_2^{\alpha_2})$$

...

$$a \equiv a_k(p_n^{\alpha_n}) \quad \text{with}$$

$$f(a_i) \equiv 0(\text{mod } p_i^{\alpha_i})$$

then $\because$ $f(a) \equiv f(a_i) \equiv 0(p_i^{\alpha_i})$, $i = 1, 2, ..., k$ with $a \equiv a_1 \pmod{p_1^{\alpha_1}}$

i.e., $f(a) \equiv 0(p_1^{\alpha_1})$,

$$f(a) \equiv 0(p_2^{\alpha_2})$$

...

$$f(a) \equiv 0(p_n^{\alpha_n})$$

$\therefore$ $f(a) \equiv 0(\text{mod } p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n})$

$\equiv 0(\text{mod } m)$

$\therefore$ a is a solution $f(x) \equiv 0(m)$

and if $a \equiv b(m)$,

then $f(b) \equiv 0(m)$, i.e., b is a solution

$\therefore$ $x \equiv a(\text{mod } m)$ is a solution of (1)

Hence each distinct set of the system of several congruences (2) leads to a distinct solution of the given congruences (1).

Note:

(i) Thus if there are N_i incongruent solutions ai of $f(x) \equiv 0(\text{mod } p_i^{\alpha_i})$, then there will be $N = N_1.N_2 \ldots N_k$ incongruent solutions a of $f(x) \equiv 0(\text{mod } p_i^{\alpha_i})$.

(ii) If $N_i = 0$ for some i, the congruence (1) has no solution.
If the positive integer m (> 1) has the prime decomposition

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

And if $f(x)$ is any polynomial in x with integral coefficients then

(iii) The algebraic congruence

$f(x) \equiv 0(\text{mod } m)$ is soluble if and only if each of the congruences.

$$f(x) \equiv 0(\text{mod } p_i^{\alpha_i})(i = 1, 2, .n)$$

is soluble.

(iv) If N and N_i $(i = 1, 2, ., n)$ denote the numbers of roots of $f(x) \equiv 0(\text{mod } m)$ and $f(x) \equiv 0(\text{mod } p_i^{\alpha_i})$ respectively,

then $N = N_1.N_2 \ldots N_n$.

Working Principle of solution of congruence of higher degree::

(1) $m = p_1^{\alpha_1} . p_2^{\alpha_2} \ldots . p_n^{\alpha_n}$ And $f(x) \equiv 0(\text{mod } m)$, $m > 0$

(2) $f(x) \equiv 0(\text{mod } m)$ is equivalent to the set of congruences

$$f(x) \equiv 0(\text{mod } p_i^{\alpha_i}) \quad (i = 1, 2,.n) \qquad ...(*)$$

(3) If some one congruence of (*) has no solution then the given congruence also has no solution.

(4) Suppose each one of (*) has solution.

(5) An integer u is a root of the given congruence if any only if for each i we have an a_i such that

$$u \equiv a(\text{mod } p_i^{\alpha_i})$$

(6) Use now the Chinese remainder theorem.

Example 4. Solve: $x^2 + x + 7 \equiv 0(\text{mod } 15)$

Solution: Here, $15 = 3 \times 5$

Now the congruence,

$$x^2 + x + 7 \equiv 0(\text{mod } 15)$$

has solution if and only if each of the congruences

$$x^2 + x + 7 \equiv 0(\text{mod } 5)$$

and $x^2 + x + 7 \equiv 0(\text{mod } 3)$ has solution.

But trying the values $0, \pm 1, \pm 2$, we see that the congruence $x^2 + x + 7 \equiv 0(\text{mod } 15)$ has no solution.

Hence the given congruence has no solution.

Example 5. Solve: $x^2 + x + 7 \equiv (\text{mod } 189)$ ...(*)

Solution: Here $189 = 3^3 \times 7$

Now (*) has solution if and only if

$$x^2 + x + 7 \equiv 0(\text{mod } 3^3)$$

and $x^2 + x + 7 \equiv 0(\text{mod } 7)$ have solutions.

Now we see that $x \equiv 4, 13, -5(\text{mod } 27)$ are the solution of

$$x^2 + x + 7 \equiv 0(\text{mod } 3^3)$$

and that $x \equiv 0, -1(\text{mod } 7)$ are the solution of

$$x^2 + x + 7 \equiv 0(\text{mod } 7)$$

$\therefore$ we get in total 6 pairs of values and using Chinese remainder theorem we get

$$u \equiv -77, -14, -140, -50, 13, -113 \pmod{189}$$

as solutions of the given congruence.

Theorem 3.4. If $\alpha > 1$, then the solution of

$$f(x) \equiv 0 \pmod{p^{\alpha}} \qquad \ldots(1)$$

depends upon the solutions of

$$f(x) \equiv 0 \pmod{p^{\alpha - 1}}, \quad (\alpha \geq 2) \qquad \ldots(2)$$

Proof: We begin by observing: .

Each solution x of (1) is obviously a solution of (2).

Consequently,

All solutions of (1) must be included among the solutions of (2).

In other words,

If x is a solution of (1), it must be possible for us to find a solution X of (2)

So that $x \equiv X(p^{\alpha - 1})$

i.e., x must have the form

$$x = X + t\, p^{\alpha - 1}, \text{ for a suitably chosen integer } t.$$

We will suppose then that

All solutions X of (2) have been found

And we shall check each of these in turn to see if one or more integers t can be found

So that $x = X + t\, p^{\alpha - 1}$ will be a solution of (1),

for we are certain from above discussion that this is the only way that solutions of the later congruence can arise.

In the attempt to find suitable values of t we may use the result

$$F(a + h) = F(a) + hF'(a) + h^2 \frac{F''(a)}{2!} + \ldots + h^n \frac{F^{(n)}(a)}{n!},$$

for this equation allows us to write

$$f(x) = f(X + t\, p^{\alpha - 1})$$

$$= f(X) + t\, p^{\alpha - 1} f'(X) + (t\, p^{\alpha - 1})^2 \frac{f''(X)}{2!} + \ldots + (t\, p^{\alpha - 1})^n \frac{f^{(n)}(X)}{n!},$$

where n is the degree of the polynomial f.

$\because$ we are seeking solution x of (1) and

$\because$ for $\alpha > 1$ it is clear that

$(p^{\alpha - 1})^2 \equiv 0(p^{\alpha})$, we are left with the following restriction,

or $$f(x) + t\, p^{\alpha - 1} f'(X) \equiv 0(p^{\alpha}).$$

However, by hypothesis,

$$f(X) \equiv 0(p^{\alpha})$$

So there exists an integer M such that

$$f(X) = M\, p^{\alpha - 1}.$$

$\therefore$ the congruence restriction on t may be replaced by

$$M + tf'(X) \equiv 0(p) \qquad ...(*)$$

To (*) we may apply, theorem Theroem 2.32:

There is one solution t if

$$f'(X) \not\equiv 0(\text{mod}\, p) \qquad [\text{i.e., } p \nmid f'(X) \text{ i.e., } (p, f'(x)) = 1]$$

There is no solution t

if $$f'(X) \equiv 0(\text{mod}\, p)$$

and $$M \not\equiv 0(\text{mod}\, p) \qquad [\text{i.e., } p \nmid M]$$

$$\ldots p \ldots \text{ if } f'(x) \equiv 0(\text{mod}\, p)$$

and $$M \equiv 0(\text{mod}\, p)$$

Using the results we have at hand a definite method (when a > 1) of discovering every possible solution of $f(x) \equiv 0(p^{\alpha})$, if we have previously found every solution of

$$f(x) \equiv 0(p^{\alpha - 1}).$$

Hence the theorem.

We summarize the above result in the following

Note: If X is a root of the algebraic congruence

$$f(x) \equiv 0(p^{\alpha - 1}) \ (\alpha \geq 2) \qquad ...(*)$$

Satisfying $0 \leq X \leq p^{\alpha - 1}$, and if $f'(x)$ is the formal derivative of $f(x)$, then

(i) if $f'(X) \not\equiv 0(\text{mod}\, p)$, there is a unique root of $f(x) \equiv 0(p^{\alpha})$ corresponding to X.

(ii) if $f'(X) \equiv 0(p)$, there are p roots of (*) corresponding to X when

$$f(x) \equiv 0(p^{\alpha})$$

and no such root when $f(X) \not\equiv 0(\text{mod}\, p^{\alpha})$

Remark: By repeated application of this theorem the problem reduces to solving

$$f(x) \equiv 0(p).$$

Example 6. If $M = 1 \times 3 \times 5 \ldots \times (p - 2)$ where p is an odd prime, show that

$$M^4 \equiv 1(\text{mod}\, 16)$$

$$M^4 \equiv 1(\text{mod}\, p)$$

Solution: We shall show that

$$M^4 \equiv 1(\text{mod}\, 16) \qquad ...(1)$$

$$M^4 \equiv 1(\text{mod}\, p) \qquad ...(2)$$

To prove (1)

$\because$ $(M, 16) = 1$, $\Phi(16) = 8$. Hence by Euler's theorem

$$M^4 \equiv \pm 1(16)$$

But, $M^4 \not\equiv -1(\text{mod}\, 16)$ because if $M^4 \equiv -1(\text{mod}\, 16)$ then $M^2 \equiv \sqrt{-1}\,(\text{mod}\, 16)$ which is impossible.

$\therefore \quad M^4 \equiv 1 (\text{mod } 16).$

To prove (2)

$\therefore \quad M = (p-2) \times (p-4) \times \ldots \times 5 \times 3 \times 1$

$M \equiv (-1)^{(p-1)/2}\, 2 \times 4 \times 6 \ldots \times (p-3) \times (p-1) (\text{mod } p)$

We get $M^2 \equiv 1 \times 2 \times 3 \times 4 \times 5 \ldots \times (p-1) \times (-1)^{(p-1)/2}$

$\equiv (p-1)!\, (-1)^{(p-1)/2} (\text{mod } p).$

Now we know that $(p-1)! \equiv -1 (\text{mod } p)$ (Wilson)

$\therefore \quad M^2 \equiv (-1)\, (-1)^{(p-1)/2} \equiv \pm 1 (\text{mod } p)$

$\therefore \quad M^4 \equiv 1 (\text{mod } p).$

Example 7. If $(X+1)\,(X+2) \ldots (X+p-1) = X^{p-1} + A_1 X^{p-2} + \ldots + A_{p-1}$

And p is an odd prime, prove that

$A_r \equiv 0(p)$, for $r = 1, 2, \ldots, p-2$ and $A_{p-1} \equiv -1(p)$, [Left as exercise]

Example 8. Solve: $f(x) = x^3 + x - 19 \equiv 0 (\text{mod } 7^2)$

Solution: Let us first consider the congruence

$$x^3 + x - 19 \equiv 0 (\text{mod } 7) \qquad \ldots(**)$$

We observe $0, \pm 1, \pm 2, \pm 3\}$ is the complete set of residues (mod 7) and checking these integers, it can be seen that

$x \equiv -1, -3 (\text{mod } 7)$ are the two roots of (**)

Now $f'(-1) = 4 \equiv 0 (\text{mod } 7)$

$f(-1) = 7(-3)$

and $4t - 3 \equiv 0 (\text{mod } 7)$

has the unique solution $t \equiv -1 (\text{mod } 7)$.

Then by above theorem

$x \equiv -8 (\text{mod } 7^2)$

is the root of (*) corresponding to the

root $x \equiv -1 (\text{mod } 7)$ of (**)

Again $f'(-3) \equiv 0 (\text{mod } 7)$

and $f(-3) \equiv 0 (\text{mod } 7^2)$.

Hence there are seven roots of (*) corresponding to the roots

$x \equiv -3 (\text{mod } 7)$ of (**) given by

$x \equiv -3 + 7t (\text{mod } 7^2)$ with $t = 1, 2, \ldots, 7$; and they are

$x \equiv 4, 11, 18, 25, 32, 29, 46 (\text{mod } 7^2)$

Thus (*) has eight incongruent roots (mod 7^2).

Example 9. Solve: $x^3 - 2x + 6 \equiv 0 (\text{mod } 125)$

Solution: $f(x) = x^3 - 2x + 6 \equiv x^3 - 2x + 1 \equiv 0 (\text{mod } 5)$ has two solutions

$x \equiv 1, 2.$

Consider $x = 1$

Then $f(1) = 5 \equiv 0(\text{mod } 5)$

$f'(1) = 1 \not\equiv 0(\text{mod } 5)$

$\therefore$ there is a unique roo for $x \equiv 1$ [Theorem 3.4 Note]

or $1 + t_1 \equiv 0(\text{mod } 5)$

Now we get $t_1 = -1$; hence

$x_2 = 1 + 5t_1 \equiv -4(\text{mod } 25)$ is a solution of $f(x) \equiv 0(\text{mod } 25)$

Again,

$\because$ $f(-4) = 46$ and the solution of

$-2 + 46t_2 \equiv 0(\text{mod } 5)$

or $-2 + t_2 \equiv 0(\text{mod } 5)$ is $t_2 \equiv 2(\text{mod } 5)$,

So that required solution is

$x \equiv -4 + 25.2 \equiv 46(\text{mod } 125)$.

Next we consider

$X_1 = 2$

Then $f(2) = 0 \not\equiv 0(\text{mod } 5)$

$f'(2) = 10 \not\equiv (\text{mod } 5^2)$

The congruence

$2 + 10t_1 \equiv 0(\text{mod } 5)$ has no solution

Hence the given congruence in this case also has no solution

Thus the given congruence has only one solution

$x \equiv 46(\text{mod } 125)$.

Example 10. Solve: $x^3 + 3x + 1 \equiv 0(\text{mod } 75)$

Solution: Let $f(x) \equiv x^3 + 3x + 1 \equiv 0(\text{mod } 75)$ ...(i)

Here we solve the following two congruences

$x^3 + 3x + 1 \equiv 0(\text{mod } 3)$ ...(ii)

$x^3 + 3x + 1 \equiv 0(\text{mod } 5^2)$ ...(iii)

It can be easily seen that (ii) has only one root viz., $x \equiv 2(\text{mod } 3)$

Now to solve (iii) we give attention to

$x^3 + 3x + 1 \equiv 0(\text{mod } 5)$ ...(iv)

This congruence has two roots, viz $x \equiv 1, 2(\text{mod } 5)$

Now $f'(1) = 6 \not\equiv 0(\text{mod } 5)$, $f(1) = 5.1$ and $6t + 1 \equiv 0(\text{mod } 5)$ has the unique solution

$t \equiv -1(\text{mod } 5)$. If follows that

$x \equiv -4(\text{mod } 5^2)$ is the root of (iii)

Again $f'(2) = 0(\text{mod } 50$ and $f(2) \not\equiv 0(\text{mod } 5^2)$

So there is no root of (iii) corresponding to the root $x \equiv 2(\text{mod } 5)$

Now we solve the simultaneous congruences

$$x \equiv 2(\text{mod } 3)$$
$$x \equiv -4(\text{mod } 5^2)$$

So by Chinese remainder theorem

We get the only root $x \equiv -4(\text{mod } 75)$.

3.3 PRIMITIVE ROOTS

We have already discussed

(i) Euler's Theorem: $a^{\Phi(p)} \equiv 1(p)$, $a^{\Phi(m)} \equiv 1(\text{mod } m)$, $(a, m) = 1$

(ii) Fermat's Theorem: $a^p \equiv a(\text{mod } p)\ \forall\ a$

Definition: If $(a, m) = 1$, then the least positive integer r such that $a^r \equiv 1(\text{mod } m)$ is called *the order of a(mod m)*

or, we say that *a belongs to the exponent r(mod m)*' if r is the smallest positive integer such that $a^r \equiv 1(\text{mod } m)$

Euler's theorem states that such an r exists, where $r \leq \Phi(m)$

e.g., $m = 7$

1 = order of 1 mod 7, $\because 1^1 \equiv 1(7)$, 1 = smallest such that $1^r \equiv 1(\text{mod } 7)$

3 = order of 2 mod 7, $\because 2^3 \equiv 1(7)$, 3 = smallest such that $2^r \equiv 1(7)$

6 = order of 3 mod 7 $\because 3^6 \equiv 1(7)$, 6 = smallest such that $3^r \equiv 1(\text{mod } 7)$

3 = order of 4(mod 7) $\because 4^3 \equiv 1(7)$, 3 = smallest such that $4^r \equiv 1(\text{mod } 7)$

6 = order of 5(mod 7) $\because 5^6 \equiv 1(7)$, 6 = smallest such that $5^r \equiv 1(\text{mod } 7)$

2 = order of 6(mod 7) $\because 6^2 \equiv 1(7)$, 2 = smallest such that $6^r \equiv 1(\text{mod } 7)$

Remark: If $(a, m) = d > 1$

then there is no such integer r, for $a^r \equiv 1(m)$ $\therefore a^r = 1 + \lambda m$, $\lambda \in Z$ or, $a^r - \lambda m = 1$

Now $(a, m) = d$

$\therefore d \mid a$; m gives $d \mid a^r - \lambda\ m$ or, $d \mid 1$ and is impossible

Hence there is no such integer.

Definition: If order of $a(\text{mod } m)$ is equal to $\Phi(m)$, then *a is said to be a primitive root of m*, e.g., 3, 5 are the primitive roots of 7

Theorem 3.5. If $(a, m) = 1$ and if r is the order of $a(\text{mod } m)$, then

(i) $1, a, a^2, a^3, \ldots a^{r-1}$ are incongruent mod m

(ii) If $n \in \mathbb{N}$ and $n > r$, then there exists a unique integer s in $0 \leq s < r$ for which $a^n \equiv a^s(\text{mod } m)$

(iii) $a^n \equiv 1(\text{mod } m)$ if and only if $r \mid n$

(iv) If $b \equiv a(\text{mod } m)$, then the order of $b(\text{mod } m)$ is equal to the order of $a(\text{mod } m)$

Proof:

(i) If not, suppose $a^u \equiv a^v(\text{mod } m)$ with $0 \leq u < v \leq r - 1$

Then $0 < v - u < n$, and

$$a^u \equiv a^v$$
$$\equiv a^{u+(v-u)}$$
$$\equiv a^u.a^{v-u} \pmod{m},$$

$\because$ $(a, m) = 1$

$\therefore$ $(a^u, m) = 1$

We get

$a^{v-u} \equiv 1 \pmod{m}$, which is impossible

$\because$ $v - u < r$ = order of a (mod m),

Hence.

(ii) $\exists$ unique q and s such that $n = rq + s$, $0 \le s < r$

Then $a^n = a^{rq+s} = (a^r)^q.a^s$

$\equiv 1^q a^s$

$\equiv a^s \pmod{m}$.

or $a^n \equiv a^s \pmod{m}$.

(iii) By (ii) above $a^n \equiv 1^0$ iff $s = 0$, i.e., $n = rq$ iff $r \mid n$

(iv) If $b \equiv a \pmod{m}$ then, $b^r \equiv a^r \pmod{m}$ for every $r \in \mathbb{N}$

Thus, $b^r \equiv 1$ iff $a^r \equiv 1$.

Corollary 3.6. If r is the order of $a \pmod{m}$, then $r \mid \Phi(m)$

Proof: By Euler's theorem $a^{\Phi(m)} \equiv 1 \pmod{m}$

By (iii) $a^n \equiv 1 \pmod{m}$ iff $r \mid n$,

$\therefore$ comparing we get

$r \mid \Phi(m)$.

Remark: For any given integer a prime to m i.e., $(a, m) = 1$ there is an unique order $r \pmod{m}$ which is a divisor of $\Phi(m)$

The question arises whether each positive divisor of $\Phi(m)$ and in particular $\Phi(m)$ itself must be the order (mod m) of some integer a.

The answer is in negative.

Definition: If order of a (mod m) = $\Phi(m)$, then a is said to be a primitive root of m.

e.g., order of 5 mod 7 is $6 (= 7 - 1) = \Phi(7)$.

$\therefore$ 5 is a primitive root of 7(i.e., $5^6 \equiv 1 \pmod{7}$)

order of 2(mod 7) is 3 ($2^3 \equiv 1 \pmod{7}$)

$\therefore$ 2 is not primitive root of 7

If a is a primitive of m, then the integers $1, a, a^2, \ldots, a^{\Phi(m)}$ are incongruent mod m by the theorem (i) above.

Consequently, these integers form a reduced set of residues (mod m).

In other words the congruence classes consisting of integers prime to m are the classes

$$\{1, a, a^2, a^3, ..., a^{\Phi(m)-1}\}$$

It follows that,

If a is a primitive root of m then $G_m = 1, a, a^2, a^3, ..., a^{\Phi(m)-1}\}$

the multiplicative group of congruence classes prime to m is cyclic.

Conversely, if this group of order $\Phi(m)$ is cyclic and is generated by an integer a then it has order $\Phi(m)$ (mod m).

Remark: A positive integer m has a primitive root if and only if the multiplicative group G_m is cyclic,

Note:

(1) The every positive integer m has not a primitive root.

(2) $m = 1$ is a trivial case.

(3) $m = 2$ gives,

$$\Phi(2) = 1, (1) \text{ and } 1^1 = 1^{\Phi(2)} \equiv 1(\text{mod } 2)$$

$\therefore$ $m = 2$ has a primitive root 1

$m = 4$ gives, $\Phi(4) = 2, (1, 3,) 1^1 \equiv 1(\text{mod } 4), 2^1 \not\equiv 1(\text{mod } 4), 2^2 \not\equiv 1(\text{mod } 4)$

$\therefore$ 1 and 2 are not primitive roots mod 4

$$3^{\Phi(4)} = 3^2 \equiv 1(\text{mod } 4), 3^1 \not\equiv 1(\text{mod } 4)$$

$\therefore$ 3 is a primitive root of 4

$m = 6$ gives, $\Phi(6) = 2, (1, 5,) 5^1 \not\equiv 1(\text{mod } 6), 5^{\Phi(6)} \equiv 5^2 \equiv 1(\text{mod } 6).$

$\therefore$ 5 is a primitive root

$m = 8$ gives, $\Phi(8) = 4, (1, 2, 3, 5, 7), 3^1 \not\equiv 1(\text{mod } 8), 3^2 \equiv 1(\text{mod } 8)$

$\therefore$ order of 3(mod 8) is $2 \neq 4$

$\therefore$ 3 is not a primitive root of 8,

$$5^1 \not\equiv 1(\text{mod } 8)$$

$$5^2 \equiv 1(\text{mod } 8)$$

$\therefore$ order of 5(mod 8) is $2 \neq 4$.

So 5 is not a primitive root of 8.

$$7 \not\equiv 1(\text{mod } 8), 7^2 \equiv 1(\text{mod } 8)$$

$\therefore$ order of 7 mod 8 is $2 \neq 4$ and

So 7 is not a primitive root of 8

Thus 8 has no primitive root.

Exercise 11. For $m = 9$ students are asked to verify.

Theorem 3.7.

(i) If a belongs to exponent h modulo m, then $h \mid \Phi(m)$

(ii) $a^j \equiv a^k(\text{mod } m)$ iff $h \mid (j - k)$

(iii) a^k belongs to the exponent $\frac{h}{(h, k)}(\text{mod } m)$

Proof:

(i) Done

(ii) $j > k$, say, $(a, m) = 1$

Then, $a^j \equiv a^k \pmod m$

if and only if $a^{j-k} \equiv 1 \pmod m$ $(a^h \equiv 1 \pmod m)$

where h is the order of a (mod m))

if and only if $h \mid (j - k)$

(iii) $(a^k)^j \equiv 1 \pmod m$

if and only if $a^{kj} \equiv 1 \pmod m$

if and only if $h \mid kj$

if and only if $\frac{h}{(h,k)} \mid \frac{kj}{(h,k)} = \frac{k}{(h,k)} j$

i.e., $\frac{k}{(h,k)} \mid j$ $\left[\because \left(\frac{h}{(h,k)}, \frac{k}{(h,k)}\right) = 1\right]$

$\therefore$ the least value of $j = \frac{h}{(h,k)}$

and

$\therefore$ the order of a^k is $\frac{h}{(h,k)}$.

Theorem 3.8. If the order of a and b modulo m are λ and μ respectively and $(\lambda, \mu) = 1$, then the order of ab modulo m is $\lambda\mu$.

Proof: Suppose the order of ab modulo m is k.

$\because$ $a^\lambda \equiv 1,\ b^\mu \equiv 1 \pmod m$,

$\therefore$ $(ab)^{\lambda\mu} = (a^\lambda)^\mu (b^\mu)^\lambda \equiv 1 \pmod m$.

Hence $k \mid \lambda\mu$

Now $(ab)^{k\lambda} = (a^\lambda)^k b^{k\lambda} = b^{k\lambda}$

or, $1 \equiv b^{k\lambda} \pmod m$

or, $b^{k\lambda} \equiv 1 \pmod m$

or, $\mu \mid k\lambda$

Then, as $(\lambda, \mu) = 1$, $\mu \mid k$. Similarly $\lambda \mid k$

Hence $\lambda\mu \mid k$

$\therefore$ $k = \lambda\mu$.

Example 12. If k (> 1) and n are positive integers then show that $\Phi(k^n - 1)$ is a multiple of n

$k^n - 1 = 0 \pmod{(k^n - 1)}$ $k^n \equiv 1 \pmod m$ (where $m = k^n - 1$) ....(1)

Now $k^r \not\equiv 1 \pmod m$ if $r < n$

Because if $k^r \equiv 1 \pmod m$, for $r < n$

Then $k^r - 1 \equiv 0 (\text{mod } k^n - 1)$ $k^n - 1 \mid k^r - 1, r < n$

which is impossible.

$\therefore$ n is the least positive integer satisfying (1).

In other words n is the order of k mod m.

$\therefore$ $n \mid \Phi(m)$ (by the former theorem)

i.e., $n \mid \Phi(k^n - 1)$, i.e., $\Phi(k^n - 1) = nq$.

Example 13. If p and $q = 4p + 1$ are both odd primes, then 2 is a primitive root of q.

Proof: $\because$ $\varphi(q) = 4p$, the order of 2 modulo q is only one of the following numbers

$$1, 2, 4, p, 2p \text{ and } 4p$$

As p is prime, $p \equiv 1(\text{mod } 2)$ and $q \equiv 5(\text{mod } 8)$.

$\because$ $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ we see that 2 is a quadratic no residue of q; thus

$$2^{2p} \equiv -1(\text{mod } q)$$ [Ref: chapter vi]

Hence the order of 2 modulo q is not $2p$. Evidently it is not the factor 2 or p or $2p$, nor 1 or 4. Therefore the order of 2 modulo q is 4pie., 2 is the primitive root of q.

Lemma 3.9. If p is an odd prime and $d \mid p - 1$ $(d > 0)$ then

(i) The algebraic congruence $x^d - 1 \equiv 0(\text{mod } p)$ has exactly d *incongruence roots,* and

(ii) $\Phi(d)$ of these roots have order $d(\text{mod } p)$

Proof: Consider

$$x^d - 1 \equiv 0(p) \quad \ldots(1)$$

Now $d \mid p - 1$

or, $x^{p-1} - 1 = (x^d - 1) f(x)$,

where $f(x) = x^{p-1-d} + x^{p-1-2d} + \ldots + x^d + 1$

or $x^{p-1} - 1 \equiv 0(p)$ $\quad \ldots(2)$

and (2) has $p - 1$ incongruence roots mod p.[by Fermat's theorem]

If a is one of them,

then $a^{p-1} - 1 = (a^d - 1) f(a) \equiv 0(p)$,

Consequently

$$p \mid a^d - 1 \text{ or }, f(a)$$

i.e. Either $a^d - 1 \equiv 0(\text{mod } p)$

or $f(a) \equiv 0(\text{mod } p)$ $\because$ p is prime.

Thus each of $p - 1$ incongruent roots of (2) is either a root of (1) or a root of the algebraic congruence $f(x) \equiv 0(p)$ ... (3)

But (1) has not more than d incongruent roots (former theorem)

(1) Has not more than $p - 1 - d$ incongruent roots

And all together they have $p - 1$ roots

But $d + (p - 1 - d) = p - 1$

$\therefore$ it follows that

(1) Has exactly d incongruent roots.

Suppose now that one of these roots, b, say, has order $d \pmod p$,

Then $1, b, b^2, .., b^{d-1}$ are all roots of (1) and incongruent (mod p).

Thus they form a complete set of roots (mod p) of (1)

If b^α is one of them and has order $d_1 \pmod p$,

Then $((b^\alpha)^{d_1} = b^{\alpha d_1} \equiv 1 \pmod p)$

But d is the order of b i.e., $b^d \equiv 1 \pmod p$.

$\therefore$ $d \mid \alpha d_1$

Thus, d_1 is the smallest positive integer such that $d \mid \alpha d_1$.

It follows that

$$d_1 = d \text{ iff } (d, \alpha) = 1.$$

$\because$ there are $\Phi(d)$ values of x such that $(x, d) = 1$,

$\therefore$ if the algebraic congruence (1) has one root of order $d \pmod p$, then it has $\Phi(d)$ *incongruent roots of order d (mod p).*

Theorem 3.10. The necessary and sufficient condition that a is a primitive root of m is that

$$a, a^2, ..., a^{\Phi(m)}$$

form the reduced system of m.

Proof: Suppose that a is a primitive root of modulo m. Then $(a, m) = 1$

And any two integers among

$$a, a^2, .., a^{\Phi(m)} \quad ....(*)$$

are incongruent modulo m. [For $a^i \equiv a^j \pmod m$ $(i \neq j)$ or, $a^{i-j} \equiv 1 \pmod m$, $i - j < \Phi(m)$ and this is not true as a is a primitive root modulo m.]

Hence the set (*) is a reduced residue system of m.

Conversely,

If (*) is a reduced residue system of m, then any two integers of the system are incongruent modulo m.

Thus $a^k \equiv 1 \pmod m$, $0 < k < \Phi(m)$

Hence the order of a modulo m is $\Phi(m)$

Thus a is a primitive root of m.

Note: If a is a primitive root of m, then the reduced residue system of m can be expressed as a geometric progression of the form $a, a^2, ..., a^{\Phi(m)}$

And this is useful in many cases.

Theorem 3.11. If $m = p_1^{\alpha_1} . p_2^{\alpha_2} ... p_k^{\alpha_k}$ has a primitive root then m must be of the form

$$2^k, p^k, 2p^k$$

Proof: Suppose a is a primitive rot of m.

Then $(a, m) = 1$

Hence, $(a, p_1^{\alpha_1}) = 1$

$\therefore$ by Euler's theorem,

$$a^{\phi(p_i^{\alpha_i})} \equiv 1 (\text{mod } p_i^{\alpha_i})$$

Suppose $M = \left[\phi(p_i^{\alpha_i}), \ldots, \phi(p_k^{a_k})\right]$ [L . C . M] Then

$$a^M \equiv 1 (\text{mod } p_i^{\alpha_i}),$$

Hence $a^t \equiv 1 (\text{mod } m)$

$\because$ a is a primitive root of m, so $\Phi(m) \mid M$

$\because$ $\Phi(m) = \phi(p_i^{\alpha_i}) \ldots \phi(p_k^{a_k})$ is the multiple of M, $M \mid \Phi(m)$ and hence $M = \Phi(m)$.

$\therefore$ $$\left[\phi(p_i^{\alpha_i}), \ldots, \phi(p_k^{a_k})\right] = \phi(p_i^{\alpha_i}) \ldots \phi(p_k^{a_k})$$

Thus $\phi(p_i^{\alpha_i}), \ldots, \phi(p_k^{a_k})$ are relatively prime.

Again $\Phi(2^r) = 2^{r-1}$, $\Phi(p^r) = p^{r-1}(p-1)$, p is an odd prime.

Hence

(i) The number of odd prime factors of m cannot be greater than 1.

(ii) If odd prime factors and even prime factors exist simultaneously, then the power of an even prime factor also cannot be of greater than 1.

(iii) Hence if m has primitive roots then m must be in one of the following forms
$$2^k, p^k, 2p^k$$

The following result shows that 2^k, p^k, $2p^k$ are the only integers with primitive roots

Theorem 3.12. An integer m has a primitive roots if and only if $m = 2$, 4, p^k or $2p^k$ where p is an odd prime and k is a positive integer.

Proof: (A) $m = 2^k$

(i) If $k = 1$, then $m = 2$, $\Phi(m) = 1$. and clearly 1 is a primitive root.

(ii) If $k = 2$, then $m = 4$, $\Phi(m) = 2$, and 3 is the primitive root.

(iii) If $k \geq 3$, then $\Phi(m) = 2^{k-1}$

Now reduced residue system of m is made up of odd integers

$\therefore$ $m = 2^k$ has no primitive roots

if $$a^{2^{k-2}} \equiv 1 (\text{mod } 2^k) \quad \ldots(*)$$

We now prove this by induction.

It is clear that

$$a^2 \equiv 1(\text{mod}\, 2^3)$$

$\therefore$ (*) is true for $k = 3$

Assume that the result is true for k.

Now $$a^{2^{k-1}} = \left(a^{2^{k-2}}\right)^2 = (1 + 2^k t)^2 \equiv 1(\text{mod}\ 2^{k+1})$$

$\therefore$ (*) is true for $k + 1$.

Thus the result is true by induction.

$\therefore$ 2^k, for $k = 1, 2$ has primitive roots; but for $k \geq 3$ there are no primitive roots.

(B) p^n, $2p^n$, where p is an odd prime and n is a positive integer, have primitive roots.

Proof Consider p^n, where p is an odd prime.

Case I $n = 1$, i.e., for p

Take $d = p - 1$ in the lemma 3.9

$\therefore$ there are $\Phi(p-1)$ incongruent roots of $x^{p-1} \equiv 1(p)$ of order $p - 1(\text{mod}\ p)$. Thus the prime p has $\Phi(p-1)$ i.e., $\Phi(\Phi(p)$ incongruent primitive roots.

Case II p^n, $n \geq 2$

Let g be a primitive root of p

i.e., $$g^{\Phi(p)} \equiv 1(\text{mod}\, p)$$

and $\Phi(p)$ is the least positive integer to satisfy this equation.

And this gives

$$g^{p-1} - 1 \equiv 0(\text{mod}\ p) \text{ and } (g, p) = 1.$$

We show that g can be so chosen that

$$g^{p-1} - 1 \not\equiv 0(\text{mod}\, p^2)$$

Now, $g + p \equiv g(\text{mod}\ p)$ or, $g + p$ is also a primitive root of p.

And

$$\begin{aligned}(g+p)^{p-1} - g^{p-1} &= ((g+p) - g)\,((g+p)^{p-2} + (g+p)^{p-3}g + \ldots + g^{p-2}) \\ &= p(g^{p-2} + pN_1 + g^{p-2} + pN_2 + \ldots + g^{p-2}) \\ &= p((p-1)\,g^{p-2} + p(N_1 + N_2 + \ldots)) \\ &= p(-g^{p-2} + Np),\ n \in \mathbb{N}\end{aligned}$$

or $$[(g+p)^{p-1} - 1] - (g^{p-1} - 1) = (g+p)^{p-1} - g^{p-1}$$

$$\equiv -pg^{p-2}(\text{mod}\ p^2)$$

$$\not\equiv 0(\text{mod}\, p^2)$$

$[\because (g, p) = 1$ gives p does not divide g and, so $-g^{p-2}]$

or $$(g+p)^{p-1} - 1 \not\equiv (g^{p-1} - 1)\ (\text{mod}\ p^2)$$

Hence the primitive roots

g and $g + p$ of p

cannot both be the roots of the algebraic congruence

$$x^{p-1} - 1 \equiv 0 (\text{mod}\, p^2)$$

Thus we may suppose that g can be so chosen that

$$g^{p-1} - 1 \not\equiv 0 (\text{mod}\, p^2)$$

We now deduce by induction that

for all $n \geq 2$, $\quad g^{p^{n-2}(p-1)} - 1 \not\equiv 0 (\text{mod}\, p^n)$ ...(2)

I. This result is true for $n = 2$

II. Assume that (2) is true for n

Then, on noting that

$$g^{p^{n-2}.(p-1)} = g^{\phi(p^{n-1})}$$
$$\equiv 1 (\text{mod}\, p^{n-1})$$

And $\quad g^{p^{n-2}(p-1)} = 1 + k_n p^{n-1}$, where K_n is a constant and $(p, K_n) = 1$

We get, $\quad g^{p^{n-1}(p-1)} = (g^{p^{n-2}.(p-1)})^p$
$$= (1 + K_n p^{n-1})^p$$
$$= 1 + K_{n+1} p^n$$

where $\quad K_{n+1} = K_n + {}^pC_2\, K_n^2 p^{n-2} + \ldots + K_n^p p^{(p-1)n-p}$
$$\equiv K_n (\text{mod}\, p)$$

and so $\quad p \nmid K_{n+1}$ $\qquad \because, p \nmid K_n$

i.e., $\quad (p, K_{n+1}) = 1$

Consequently, $g^{p^{n-1}(p-1)} - 1 \not\equiv 0 (\text{mod}\, p^{n+1})$

Suppose now that

g has order $d (\text{mod}\, p^n)$.

$\therefore \quad d \mid \Phi(p^n) = p^{n-1}(p-1)$ ...(i)

$\because$ d is order of $g (\text{mod}\, p^n)$,

$\therefore \quad g^d \equiv 1 (\text{Mod}\, p^n)$,

we also have

$$g^d \equiv 1 (\text{mod}\, p)$$

But g is a primitive root of p

and $\therefore, \quad g^{\Phi(p)(=p-1)} \equiv 1 (\text{mod}\, p)$

and $\quad (p-1)$ is the least such positive integer,

$\therefore \quad p - 1 \mid d$ ...(ii)

(i) and (ii) give d is of the form

$(p-1)p^0, (p-1)p^1, (p-1)p^2, \ldots (p-1)p^{n-1}$

It follows that

$$d = p^r(p-1) \text{ with } 0 \leq r \leq n-1$$

If $d \neq p^{n-1}(p-1)$,

then $d \mid p^{n-2}(p-1)$

and so, $g^{p^{n-1}(p-1)} \equiv 1 (\text{mod}\, p^n)$ $(\because g^d \equiv 1 (\text{mod}\, p^n)$

And it contradicts (2)

$\therefore$ $d = p^{n-1}(p-1)$

and

$\therefore$ g is a primitive root of p^n

Hence,

p^n has primitive root, $n \geq 2$.

Case III $2p^n$ $(n \in \mathbb{N})$.

Let g_1 be a primitive root of p^n,

then $g_1 + p^n$ is also a primitive root

Let g be the odd integer of the pair g_1 and $g_1 + p^n$

and

$\therefore$ $(g, 2p^n) = 1$.

Suppose now that g has order $d (\text{mod}\, 2p^n)$,

$\therefore$ $d \mid (2p^n)$.

Then, $g^d \equiv 1 (\text{mod}\, 2p^n)$

so that $g^d \equiv 1 (\text{mod}\, p^n)$.

Also $g^{\Phi(p^n)} \equiv 1 (\text{mod}\, p^n)$

and $\Phi(p^n)$ is the least such integer

and this gives

$$\Phi(p^n) \mid d \quad \text{...(i)}$$

$$\therefore \quad d \mid \Phi(2p^n) = \Phi(2)\,\Phi(p^n) = \Phi(p^n) \quad \text{...(ii)}$$

$\therefore$ (i) and (ii) give

$$d = \Phi(p^n)$$

Consequently

$$d = \Phi(p^n) = \Phi(2p^n).$$

$\therefore$ g is a primitive root of $2p^n$

Thus $2p^n$ has primitive root.

Theorem 3.13. If g is a primitive root of p, then when $g^{p-1} \not\equiv (\text{mod}\, p^2)$, g is a primitive root of p^k; when $g^{p-1} \equiv 1 (\text{mod}\, p^2)$, $g + p$ is a primitive root of p^k

Proof: Given that

g is a primitive root of p

$\therefore$ $g^{p-1} \equiv 1 (\text{mod}\, p)$.

Then, $g^{p-1} \not\equiv 1 (\text{mod}\, p^2)$, or $g^{p-1} \equiv 1 (\text{mod}\, p^2)$

Now $g^{p-1} \not\equiv 1 (\text{mod}\, p^2)$ or $g^{p-1} = 1 + ph,\ p + h$.

Suppose the order of g modulo p^k be λ, then $\lambda \mid \Phi(p^k)$ i.e. $\lambda \mid p^{k-1}(p-1)$. Write,

$$p^{k-1}(p-1) = \lambda s$$

Now $g^\lambda \equiv 1 (\text{mod } p^k)$ or, $g^\lambda \equiv 1 (\text{mod } p)$ and hence,

$(p-1) \mid \lambda$, or $\lambda = (p-1)\, t$.

Thus

$$p^{k-1}(p-1) = \lambda s$$

or $$p^{k-1}(p-1) = (p-1)\, ts$$

or $$p^{k-1} = ts,$$

i.e. $$t = p^e,\ e \leq k-1.$$

Hence

$$\lambda = p^e(p-1)$$

If $e < k-1$, then $e+2 \leq k$

and hence $$g^\lambda \equiv 1 (\text{mod } p^{e+2}).$$

But $$g^\lambda = g^{p^e(p-1)} = \left(g^{p-1}\right)^{p^e} =$$

$$(1+hp)^{p^e} \equiv 1 + hp^{e+1} (\text{mod } p^{e+2}),$$

Then $$hp^{e+1} \equiv 0 (\text{mod } p^{e+2}).$$

Hence, $$h \equiv 0 (\text{mod } p)$$

And this is not true of $ph \not\equiv 0 (\text{mod } p^2)$

$\therefore$ $$e = k-1.$$ Thus

$$\lambda = p^{k-1}(p-1) \text{ or } \lambda = \Phi(p^k)$$

Hence g is a primitive root of p^k

Now $g+p$ is also a primitive root of p

or $$g^{p-1} \equiv 1 (\text{mod } p)$$

$\therefore$ $(g+p)^{p-1} - 1 = g^{p-1} - 1 + p(p-1)g^{p-2} \equiv p(p-1)g^{p-2} (\text{mod } p^2)$

$\because$ $(g, p) = 1,$

$p \nmid g^{p-2}$ and

$\therefore$ $$(g+p)^{p-1} \equiv 1 (\text{mod } p^2)$$

From above it is seen that $g+p$ is the primitive root of p^k

Hence the result.

Theorem 3.14. If a is a primitive root of an odd prime p, then

$$\left(a^{2k+1}\right)^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$$

Proof: Suppose $\left(a^{2k+1}\right)^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$

Then $\left(a^{2k+1}\right)^{\frac{p-1}{2}} = a^{\frac{2k+1}{2}(p-1)} \equiv 1 (\text{mod } p)$

$\because$ a is a primitive root of p,

$\frac{2k+1}{2}$ must be an integer, and is not possible

Hence $\left(a^{2k+1}\right)^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$.

Example 14. Find the primitive root of 41

Solution: Here $p = 41$

$p - 1 = 40$

$\frac{p-1}{2} = 20$

Now $3^2 = 9, 3^4 = 81 \equiv -1, 3^6 \equiv -9, 3^{16} \equiv 1, 3^{20} \equiv -1.$

Hence 3 is not the solution of the congruence $x^{\frac{40}{2}} = x^{20} \equiv 1 (\text{mod } 41)$.

As $\frac{p-1}{5} = 8$, and

$2^2 = 4, 2^4 = 16, 2^8 = 256 \equiv 10,$

we see that 2 is not a solution of the congruence $x^{\frac{40}{5}} = x^8 \equiv 1 (\text{mod } 41)$.

Hence, $3^5.2^8 \equiv -3.\ 10 \equiv 11 \text{ mod } (41)$

is a primitive root of 41.

Example 15. Find the primitive root of $m = 3362 = 2.41^2$.

Solution: Computing $11^2 = 121,$ $11^4 = 14641 \equiv -488,$

$11^5 = -325,$ $11^{10} \equiv 105625 \equiv -278,$

$11^{20} \equiv 77284 \equiv -42,$ $11^{40} \equiv 1764 \equiv 83,$

we see that $11^{40} \not\equiv 1 (\text{mod } 41^2)$.

Hence 11 is a primitive root of 41^2.

$\because$ 11 is odd, 11 is also a primitive root of $m = 2.41^2$

Example 16. Find all the primitive roots if $p = 17$

Solution: Here $p - 1 = 16 = 2^4$.

As $3^2 = 9, 3^4 = 81 \equiv 13, 3^8 \equiv 169 \equiv 16,$

$3^8 \equiv 1 (\text{mod } 17)$ and hence 3 is a primitive root of 17.

Moreover, $\because \phi(p-1) = 23 = 8$, and

$$1, 2, 3, 5, 7, 9, 11, 13, 15$$

is the reduced residue set of $p - 1 = 16$, all primitive roots of 17 are

$$3^1 = 3,\ 3^3 = 27 \equiv 10,\ 3^5 \equiv 90 \equiv 5,\ 3^7 \equiv 45 \equiv 11,\ 3^9 \equiv 99 \equiv 14,$$
$$3^{11} \equiv 126 \equiv 7,\ 3^{13} \equiv 63 \equiv 12,\ 3^{15} \equiv 108 \equiv 6,$$

i.e., the integers

$$3, 5, 6, 7, 10, 11, 12, 14.$$

Hence the result.

The following result gives us the number of primitive roots of an integer m

Theorem 3.15. If m has a primitive root, then it has a total of $\phi(\phi(m))$ incongruent primitive roots.

Proof: Suppose g is a primitive root, then

$$g^0, g^1, g^2, \ldots, g^{\phi(m)-1} \qquad \ldots(*)$$

form a reduced residue set modulo m.

$\because$ m and its primitive roots are relatively prime, all the primitive roots of m are all in (*).

Suppose the order of g^i modulo m is k

Then $(g^i)^k = g^{ik} \equiv 1 \pmod{m}$

$\therefore$ $\phi(m) \mid ik$ or, $\dfrac{\phi(m)}{d} \mid k$ [if $(i, \phi(m)) = d$]

But $\left(g^i\right)^{\frac{\phi(m)}{d}} = \left(g^{\phi(m)}\right)^{\frac{i}{d}} \equiv 1 \pmod{m}$

or $k \mid \dfrac{\phi(m)}{d}$

$\therefore$ $k = \dfrac{\phi(m)}{d}$

Thus, the order of g^i modulo m is $\phi(m)$ if and only if $d = 1$

Hence, for any integer i in the reduced residue system of $\phi(m)$, the integers g^i are all primitive roots of m.

$\therefore$ we have $\phi(\phi(m))$ incongruent primitive roots.

Corollary 3.16. Any odd prime p has $\phi(p-1)$ incongruent primitive roots.

Proof: Take $m = p$.

Example 3.17. Using the concept of primitive root prove that

$1^n + 2^n + 3^n \ldots + (p-1)^n \equiv -1$ or $0 \pmod{p}$ according as $p - 1 \mid n$ or $p - 1 \nmid$ in

Case I $p - 1 \mid n$

or $n = (p-1)k$

Fermat's theorem states that

$(a, p) = 1$

gives $a^{\Phi(p)} \equiv 1 (\text{mod}\, p)$

or $a^{p-1} \equiv 1 (\text{mod}\, p)$

or $a^{(p-1)k} \equiv 1^k (\text{mod}\, p)$

or $a^n \equiv 1 (\text{mod}\, p)$

Putting $a = 1, 2, ..., (p-1)$, we get

$1^n \equiv 1 (\text{mod}\, p)$

$2^n \equiv 1 (\text{mod}\, p)$

... ...

... ...

$(p-1)^n \equiv 1 (\text{mod}\, p)$

$\therefore \quad 1^n + 2^n + 3^n \ldots\ldots\ldots + (p-1)^n$

$\equiv (1 + 1 + \text{to}(p-1) \text{ terms}) (\text{mod}\, p)$

$\equiv (p-1) (\text{mod}\, p)$

$\equiv -1 (\text{mod}\, p).$

Case II $p - 1 \nmid n$

If g is a primitive root of p,

Then $g^{\Phi(p)} \equiv 1(p)$ and $\varphi(p)$ is the least positive integer to satisfy this relation

or $g^{p-1} \equiv 1 (\text{mod}\, p)$

$\therefore \quad g^n \not\equiv 1(p)$ [$\because$ n is not a multiple of $p-1$, because $p - 1 \nmid n$

Now the two sets $g, 2g, 3g, ..., (p-1)g$ and $1, 2, 3, ... (p-1)$ $\left.\begin{array}{l} \\ \\ \end{array}\right\}$ $\because (g, p) = 1$, $\because g$ is a primitive root

are equivalent (mod p)

i.e., $jg \equiv i (\text{mod}\, p),\ i, j \in \{1, 2, ..., p-1\}$

or $(jg)^n \equiv i^n (\text{mod}\, p)$

or $\sum_{a=1}^{p-1} (ag)^n \equiv \sum_{a=1}^{p-1} a^n (\text{mod}\, p)$

or $\sum_{a=1}^{p-1} (ag)^n - \sum_{a=1}^{p-1} a^n \equiv 0 (\text{mod}\, p)$

or $(g^n - 1) \sum_{a=1}^{p-1} a^n \equiv 0 (\text{mod}\, p)$

or $\sum_{a=1}^{p-1} a^n \equiv 0 (\text{mod}\, p)$ [$\because g^n - 1 \not\equiv 0 (\text{mod}\, p)$]

or $1^n + 2^n + 3^n \ldots\ldots\ldots + (p-1)^n \equiv 0 (\text{mod } p)$.

Example 18. Show that the product P(of the primitive roots of p is) $\equiv 1 (\text{mod } p)$ except when $p = 3$[p is odd prime],

i.e., P = the product of the primitive roots $\equiv 1 (\text{mod } p)$

[Recall theorem: If a has the order $h (\text{mod } m)$ and $(h, k) = d$, then a^k has the order $\frac{h}{d} (\text{mod } m)$

Corollary If g is a primitive root of m, then g^k is also a primitive root if $(k, \Phi(m)) = 1$

Proof Put $h = \Phi(m)$ in the above theorem and replace a by g

Note If m is a prime p, (i.e., $m = p$) then, cor becomes,

if g is a primitive root (mod p) then g^k is also so, if $(k, p-1) = 1$]

Solution: If g is a primitive root of p the set of primitive rots of p is congruent (mod p) to

$g^1, g^\alpha, g^\beta, \ldots, g^\lambda$, where $\alpha, \beta, \ldots, 1$ are prime to $p-1$ and $< p-1$

[for $p = 13$ they are, g^1, g^5, g^7, g^{11}]

Now if $k < p-1$ and $(k, p-1) = 1$, then, $(p-1-k, p-1) = 1$

Hence, the above series can be distributed into couples such as

$$g^1, g^{(p-1)} - 1; g^\alpha, g^{(p-1)-\alpha}; g^\lambda, g^{(p-1)-\lambda}$$

Now $g^k . g^{(p-1)-k} = g^{p-1} = g^{\Phi(p)} \equiv 1 (\text{mod } p)$.

$\therefore$ $P = (g^1 g^{(p-1)-1}) (\ldots) \ldots (g^\lambda . g^{(p-1)-\lambda})$

$\equiv 1.1.1 \ldots 1 (\text{mod } p)$

$\equiv 1 (\text{mod } p)$.

The only exception occurs

when $k = (p-1) - k$,

or $k = \frac{1}{2}(p-1)$, where $(k, p-1) = 1$.

or $\left(\frac{1}{2}(p-1), p-1\right) = \frac{1}{2}(p-1) = 1$

$\therefore$ $p = 3$.

3.4 THEORY OF INDICES

Primitive roots lead us to another interesting concept analogous to that of logarithm. This is known as indices. Before going to the discussion of indices we first have a look into the technique of how to write the set of reduced residue set of any m.

Note: *We know that if m has primitive root, then its reduced residue system can be expressed as the powers of its primitive roots g, viz.,*

$\{g^0, g^1 \ldots, g^{\phi(m-1)}\}$ and this is the simplest form. Now the question arises when primitive root of m does not exist. We also know that for any odd integer a,

$$a^{2^{k-2}} \equiv 1 (\text{mod } 2^k),\ k \geq 3.$$

In other words, the order of any odd integer modulo 2^k is not greater than 2^{k-2}. If it is possible to find an integer whose order is exactly 2^{k-2}, then we can use its power to express one half of the reduced residue system of 2^k; for the other half we can take their negatives to suppliant it. In this way it is seen that the reduced residue system of 2^k is not fundamentally different from the reduced residue system formed by the powers of the primitive root. And this is also in the simplest form.

Theorem 3.17. The order of 5 modulo $2^k (k \geq 3)$ is 2^{k-2}

Proof: It is sufficient if we show that

$$5^{2^{k-3}} \not\equiv 1 (\text{mod } 2^k) (\text{for then, the order of 5 modulo } 2^k \text{ is } 2^{k-2})$$

So we show that

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} (\text{mod } 2^k),\ (\text{for } k \geq 3) \quad \ldots(1)$$

Proof: Will be by induction.

It is seen that, for $k = 3$, (1) is true.

We assume that (1) is true for $k - 1$

i.e., $5^{2^{k-4}} = 1 + 2^{k-1} + 2^{k-1}.t,$

or $5^{2^{k-3}} = (5^{2^{k-4}})2 = 1 + 2^{k-1} (\text{mod } 2^k)$ and thus (1) is true.

Thus completes the proof.

Theorem 3.18. The set $\{\pm 5^0, \pm 5^1, \ldots, \pm 5^{2^{k-2}-1}\}$ forms the reduced residue system of 2^k

Proof: As $5 \equiv 1 (\text{mod } 4)$, obviously for any i we have $5^i \equiv 1 (\text{mod } 4)$

Hence, $-5^i \equiv -1 (\text{mod } 4)$, and for any two different integers i and j we have $5^k \not\equiv -5^j (\text{mod } 2^k)$. This means that among the integers

$$\pm 5^0, \pm 5^1, \ldots \pm 5^{2^{k-2}-1}$$

any two are incongruent modulo 2^k, and each of them is relatively prime with 2^k and hence the result.

Note: If $m = m_1 m_2$, $(m_1, m_2) = 1$, and the reduced residue system of m^1 and m^2 are respectively

$$a_1, a_2, \ldots a_{\phi(m_1)};\ b_1, b_2, \ldots, b_{\phi(m_2)}$$ and if $a_i \equiv 1 (\text{mod } m_1)$, $b_j \equiv 1 (\text{mod } m_2)$

The $\phi(m_1)\,\phi(m_2) = \phi(m)$ integers

$$a_i b_j,\ i = 1, 2, \ldots, \phi(m_1);\ j = 1, 2, \ldots, \phi(m_2)$$

form a reduced residue system of $m = m_1 m_2$. It is because, $\because (a_i, m_1) = 1$, we may also assume that $(a_i, m_2) = 1$; hence $(a_i, m) = 1$. Similarly, $(b_j, m) = 1$ Consequently $(a_i b_j, m) = 1$, that is $a_i b_j$ and m are relatively prime. Moreover, if

$a_i b_j \equiv a_k b_1 \pmod{m}$, then $a_i b_j \equiv a_k b_1 \pmod{m_1}$, and hence
$a_i \equiv a_k \pmod{m_1}$ i.e., $a_i = a_k$.

Similarly $b_j = b_1$.

Thus among the integers $a_i b_j$ no two are congruent modulo m.]

$\therefore$ these $\phi(m)$ integers $a_i b_j$ form a reduced residue system modulo m.

Example 19. Find the reduced residue system of $m = 40$.

Solution: We note, $40 = 5.2^3$; and the suitable reduced residue system of 5 and 23 respectively are:

$$1, 9, 17, 33; 1, 11, 21, 31$$

$\therefore$ the residue system of 40 is seen from the following table:

×	1	9	17	33
1	1	9	17	33
11	11	$11\times9 \equiv 19$	$11\times17 \equiv 27$	$11\times33 \equiv 3$
21	21	$21\times9 \equiv 29$	$21\times17 \equiv 37$	$21\times33 \equiv 13$
31	31	$31\times9 \equiv 39$	$31\times17 \equiv 7$	$31\times33 \equiv 23$

Thus the reduced residue system is:

$$1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39.$$

Index: Suppose the integer m has a primitive root g. Then the set

$$S = \{g^0, g^1 \ldots, g^{\phi(m)-1}\} \text{ forms a reduced set if residues (mod } m)$$

If a is any integer with $(a, m) = 1$ then $\exists$ (a unique)$r \in \{0, 1, 2, \ldots, \phi(m) - 1\}$ for which $a \equiv g^r \pmod{m}$

Definition: The integer r is called *the index of a to the base* g(mod m); and we write ind_g a or, simply $r = \text{ind } a$, when the base need not to be specifically mentioned.

The definition clearly implies that

$$\text{ind } a = \text{ind } b \Leftrightarrow a \equiv b \pmod{m}.$$

Some properties of indices are as follows:

Theorem 3.19. (i) $\text{ind}(ab) = \text{ind } a + \text{ind } b \pmod{\phi(m)}$

(ii) $\text{ind } a^n \equiv n \text{ ind } a \pmod{\phi(m)}$ $n \geq 1$.

(iii) $\text{ind}_g a \equiv \text{ind } g_1 \; a.\text{ind } g \; g_1 \pmod{\phi(m)}$
where g_1 is also a primitive root of m.

(iv) $\text{ind } 1 = 0$

(v) $\text{ind}(-1) = \frac{1}{2}\phi(m)$, if $m > 2$

Proof: Let $a = r$ and $\text{ind } b = s$; then $ab \equiv g^{r+s} \pmod{m}$.

Consequently

$$\text{ind}\,(ab) \equiv r + s = \text{ind}\,a + \text{ind}\,b \pmod{\phi(m)}$$

and $$a^n \equiv g^{nr} \pmod{m}, \text{ and so}$$

$$\text{ind}\,a^n \equiv nr = n\,\text{ind}\,a \pmod{\phi(m)}$$

(iii) Let $$\text{ind}_{g_1} a = t$$

and $$\text{ind}_g g_1 = \alpha;$$

then $$a \equiv g_1^t \pmod{m}$$

and $$g_1 \equiv g^{\alpha} \pmod{m}.$$

thus $$a \equiv g^{t\alpha} \pmod{m} \text{ and}$$

$\therefore$ $$\text{ind}_g a \equiv t\alpha = \text{ind}_{g_1} a\ \text{ind}_g g_1 \pmod{\phi(m)}$$

(iv) $\because 1 = g^0$, it follows at one that ind $1 = 0$

(v) if $$m = 4$$

then $$\frac{1}{2}\phi(m) = 1$$

$$g = 3$$

and $$-1 \equiv g^t \pmod{4}.$$

Thus (v) holds for $m = 4$.

Now the case $m = p^n$ or $2p^n$, where p is an odd prime and $n \geq 1$

In each case,

$$g^{\phi(m)} - 1 = \left(g^{\frac{1}{2}\phi(m)} - 1 \right)\left(g^{\frac{1}{2}\phi(m)} + 1 \right) \equiv 0 \pmod{m} \qquad \ldots(\&)$$

We now show that $$\left(g^{\frac{1}{2}\phi(m)} - 1, p^n \right) = 1 \qquad \ldots(*)$$

Suppose this is not true.

Then $$p \mid g^{\frac{1}{2}\phi(m)} - 1.$$

Now $$\left(g^{\frac{1}{2}\phi(m)} + 1\right) - \left(g^{\frac{1}{2}\phi(m)} - 1\right) = 2, \text{ and } p \geq 3.$$

Consequently $$p \mid g^{\frac{1}{2}\phi(m)} + 1.$$

It follows that $$p^n \mid g^{\frac{1}{2}\phi(m)} - 1$$

and $\therefore$, $$g^{\frac{1}{2}\phi(m)} - 1 \equiv 0 \pmod{m},$$

We observe g is odd if $m = 2p^n$. By this contradicts the fact that g is a primitive root of m.

Hence (*) is true.

It follows from (&) that

$$g^{\frac{1}{2}\phi(m)} \equiv -1 (\text{mod } m) \text{ and this implies that ind}(-1) = \frac{1}{2}\phi(m)).$$

Using the concept of indices and primitive roots some congruence equation may be solved easily. Some examples are discussed below.

Example 20. For $p = 13$ $g = 2$ is the primitive root and we observe the following:

$$g^0 = 1, g^1 = 2, g^2 = 4, g^3 = 8, g^4 \equiv 3, g^5 \equiv 6, g^6 \equiv 12,$$
$$g^7 \equiv 11, g^8 \equiv 9, g^9 \equiv 5, g^{10} \equiv 10, g^{11} \equiv 7$$

Table 3.1

A	1	2	3	4	5	6	7	8	9	10	11	12
ind a	0	1	4	2	9	5	11	3	8	10	7	6

We already known that if the order of a modulo m is λ then $ar \equiv as(\text{mod } m)$, if and only if $r \equiv s(\text{mod})$, so in case of prime m $a \equiv b(\text{mod } m)$ if and only if ind $a \equiv$ ind $b(\text{mod } \phi(m)$

Now to solve: $11x \equiv 5(\text{mod } 13)$

Solution: given that

$$11x \equiv 5(\text{mod } 13), \text{ now taking indices,}$$
$$\text{ind } 11 + \text{ind } x \equiv \text{ind } 5(\text{mod } 13)$$

From the above table we get

$$\text{Ind } 11 = 7, \text{ ind } 5 = 9,$$

Hence, $7 + \text{ind } x \equiv 9(\text{mod } 13)$.

From the table, $x \equiv 4(\text{mod } 13)$

or $\text{ind } x \equiv 2(\text{mod } 13)$

$\therefore$ $x = 4 (\text{mod})$

Example 21. Solve: $5x^2 + 3x - 10 \equiv (\text{mod } 13)$

Solution: $5x^2 + 3x - 10 \equiv 0(\text{mod } 13)$

or $8.(5x^2 + 3x - 10) \equiv 8.0(\text{mod } 13)$

or $40x^2 + 24x - 80 \equiv 0(\text{mod } 13)$

or $x^2 - 2x - 2 \equiv 0(\text{mod } 13)$

or $(x - 1)^2 \equiv 3(\text{mod } 13)$

Taking indices, we get

$$2\text{ind } (x - 1) \equiv \text{ind}3 (\text{mod } 13)$$

or $2 \text{ ind}(x - 1) \equiv 4(\text{mod } 13)$

Hence, $\text{ind}(x - 1) \equiv 2 \text{ or } 8(\text{mod } 13)$

From the table

$$x - 1 \equiv 4 \text{ or } 9 (\text{mod } 13)$$

$\therefore$ the required solutions are

$$x \equiv 5, 10 (\text{mod } 13).$$

Example 22. If p is an odd prime, $a + b = p$, show that

$$\text{ind } a - \text{ind } b = \frac{p-1}{2} (\text{mod } (p-1))$$

Solution: $\because a \equiv -b (\text{mod } p)$, ind a = ind(-1) + ind d,

and hence

$$\text{ind } a - \text{ind } b \equiv \frac{p-1}{2} (\text{mod } (p-1)).$$

Example 23. Solve the congruence $7x \equiv 13 (\text{mod } 18)$

Solution: $18 = 2.3^2$ and 2 is a primitive root of 3, it follows from the result:

If p is an odd prime then each integer of the form $2p^n$ has primitive root g if $g = \text{odd}\{g_1, g_1 + p^n\}$ where g_1 is a primitive root of p^n.

that 5 is a primitive root of 18.

The corresponding index table for integers prime to 18 is:

Number	1	5	7	11	13	17
Index	0	1	2	5	4	3

Now $7x \equiv 13 (\text{mod } 18)$ if and only if $x.\text{ind } 7 \equiv \text{in } d\ 13\ (\text{mod } \phi(18)) = 6)$.

Consequently we have to solve the linear congruence

$$2x \equiv 4 (\text{mod } 6)$$

This, and

$\therefore$ the given congruence, has two solutions, $x \equiv 2$ and $x \equiv 5 (\text{mod } 6)$.

EXERCISES 3.1

1. Solve the following:
   (i) $3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^8 + 4x^7 + x^6 + 3x^4 + x^3 + 4x^2 + 2x \equiv 0 (\text{mod } 5)$
   (ii) $2x^{17} + 6x^{16} + x^{14} + 5x^{12} + 3x^{11} + 2x^{10} + x^9 + 5x^8 + 2x^7 + 3x^5 + 4x^4 + 6x^3 + 4x^2 + x + 4 \equiv 0 (\text{mod } 7)$
   (iii) $x^{12} \equiv 37 (\text{mod } 41)$
2. If p is prime, then show that

$$1^2.3^2 \ldots (p-2)^2 \equiv (-1)^{\frac{p-1}{2}} (\text{mod } p)$$

$$2^2.4^2 \ldots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} (\text{mod } p)$$

3. Show that if p is a prime number, $n \mid (p-1)$, then $x^n \equiv 1 \pmod{p}$ has n solutions.
4. Solve the following:
   (i) $x^4 + 7x + 4 = 0 \pmod{27}$ (ii) $x^2 - 5x + 7 \equiv 0 \pmod{9}$
   (iii) $x^4 - 8x^3 + 9x^2 + 9x + 14 \equiv 0 \pmod{25}$ (iv) $6x^3 + 27x^2 + 17x + 20 \equiv 0 \pmod{30}$
   (v) $x^3 + x^2 - x - 1 \equiv 0 \pmod{15}$ (vi) $4x^3 + 3x + 43 \equiv 0 \pmod{125}$
5. Find the roots if any of the following congruences
   (i) $x^4 - 3x + 1 \equiv 0 \pmod{5}$ (ii) $x^5 + 3x^3 - x + 2 \equiv 0 \pmod{11}$
   (iii) $x^3 + x^2 + 1 \equiv 0 \pmod{7}$
6. Deduce that $x^3 + x^2 + 1$ is irreducible (mod 7) and find the factorization into irreducible factors of $x^4 - 3x + 1 \pmod{5}$ and $x^5 + 3x^3 - x + 2 \equiv 0 \pmod{11}$
7. Solve the congruences:
   (i) $x^3 + 2x - 3 \equiv 0 \pmod{9}$ (ii) $x^3 + 2x - 3 \equiv 0 \pmod{5}$
   (iii) $x^3 + 2x - 3 \equiv 0 \pmod{45}$ (iv) $x^3 + 4x + 8 \equiv 0 \pmod{15}$

EXERCISES 3.2

1. If p_1, p_2 are odd primes $\alpha = a_1 \pmod{p_1}$, $\alpha \equiv a_2 \pmod{p_2}$, and the order of a_1 modulo p_1 is λ_1, the order of a_2 modulo p_2 is λ_2, prove that the order of a modulo $p_1 p_2$ is the least common multiple $[\lambda_1, \lambda_2]$ of λ_1 and λ_2.
2. Find the primitive roots of 23, 54, 529, 1058.
3. If g and h are two different primitive roots of a prime p, show that
$$\text{ind}_k a = \text{ind}_g a . \text{ing}_k g \ [\text{mod } (p-1)]$$
4. Solve the congruences
   (i) $x^{35} \equiv 17 \pmod{67}$ (ii) $x^3 \equiv 23 \pmod{109}$ (iii) $3x \equiv 5 \pmod{13}$
5. How many primitive roots does the prime 13 have?
6. If a belongs to the exponent h modulo m, prove that no two of $a, a^2, a^3, \ldots, a^h$ are congruent modulo m.
7. If p is an odd prime, how many solutions are there to $x^{p-1} \equiv 1 \pmod{p}$; to $x^{p-1} \equiv 2 \pmod{p}$
8. Prove that if p is a prime and $(a, p) = 1$ and $(n, p-1) = 1$, then $x^n \equiv a \pmod{p}$ has exactly one solution.
9. Given $ab \equiv 1 \pmod{m}$, and that a belongs to the exponent h modulo m, prove that b belongs to the exponent h.
   Then prove that if a prime $p > 3$, the product of all the primitive roots of p is congruent to 1(modulo p).
10. Prove that if a belongs to the exponent 3 modulo a prime p, then $1 + a + a^2 \equiv 0 \pmod{p}$, and $1 + a$ belongs to the exponent 6.

❑❑❑

4

ARITHMETIC FUNCTIONS

4.1 ARITHMETIC FUNCTIONS

An Arithmetic function is an important function with many interesting properties frequently occurred in number theoretic investigations.

Definition: Any function $f: \mathbb{N} \to C$ (= the set of complex numbers) is called an Arithmetic function (**A.F.**)

Example 1. $f: \mathbb{N} \to \mathbb{N}$: $f(n) = n$, $f(n) = n^2$, are arithmetic functions, but, $f(n) = \log n$ ($n \in \mathbb{N}$) is not an arithmetic function.

Definition: Multiplicative Arithmetic functions:

If $f(n)$ is an A.F. such that $f(mn) = f(m) f(n)$ where, $(m, n) = 1$, then $f(n)$ is said to be multiplicative arithmetic function (M.A.F.)

Example 2. If $f(n) = n$, then,

$$f(mn) = mn = f(m) f(n) \text{ so } f \text{ is multiplicative.}$$

And if, $g(n) = 2n$, then,

$$g(mn) = 2mn \neq g(m)\, g(n)$$

$\therefore$ g is not multiplicative.

[we shall call f and $f(n)$ as functions in the same sense.]

Definition: Totally multiplicative Arithmetic function

If $f(n)$ is A.F. such that $f(mn) = f(m) f(n)$ for all m, n, then $f(n)$ is said to be totally multiplicative arithmetic function. (T.M.A.F.)

$$f(n) = n^2 \text{ is totally multiplicative.}$$

Note: The following are *two basic properties of multiplicative functions;*

1. If f and g are multiplicative functions such that $f(p^i) = g(p^i)$ for all primes p and all integers i, then $f(n) = g(n)$ for all positive integers. [Hence $f = g$]
2. If f and g are totally multiplicative functions such that $f(p) = g(p)$ for all primes p, then $f = g$.

Definitions of some important arithmetic functions:

(i) Euler's toutient function $\phi : \mathbb{N} \to \mathbb{N}$ such that for any positive integer a, $\phi(a)$ = number of integers $n(\leq a)$ such that $(n, a) = 1$, $n \in \mathbb{N}$

(ii) The Arithmetic function $d(n)$ [or, $\tau(n)$]: d: $\mathbb{N} \to \mathbb{N}$ such that $d(n)$ = number of divisors of n, $n \in \mathbb{N}$

(iii) σ: $\mathbb{N} \to \mathbb{N}$ such that $\sigma(n)$ = the sum of the divisors of n, $n \in \mathbb{N}$

(iv) σ_k: $\mathbb{N} \to \mathbb{N}$ such that $\sigma_k(n)$ = the sum of the k^{th} powers of n, $n \in \mathbb{N}$

(v) Mobius function μ: $\mathbb{N} \to \mathbb{Z}$ such that, for all $n \in \mathbb{N}$

$$\mu(n) = 1 \quad \text{if } n = 1$$
$$= 0 \quad \text{if } a^2 \mid n \text{ for some } a > 1$$
$$= (-1)^r \quad \text{if } n = p_1 p_2 \ldots p_r,\ p_i \text{ are distinct primes}$$

(vi) $e(n) = 1$, if $n = 1$
$= 0$, if $n > 1$, $n \in \mathbb{N}$

[or, $e(n) = \left[\frac{1}{n}\right]$, $n \in \mathbb{N}$]

(vii) $I(n) = 1$, $n \in \mathbb{N}$

(viii) $P(n) = \prod_{d \mid n} d$, $n \in \mathbb{N}$

4.2 EULER'S FUNCTION

$\Phi : \mathbb{N} \to \mathbb{N}$: $\Phi(n) = 1$ if $n = 1$
= the number of $a(< n)$, such that $(a, n) = 1$, if $n > 1$

Theorem 4.1. For any prime p,

$$\Phi(p) = p - 1$$

Proof: Since p is a prime,

Each of $1, 2, 3, \ldots, p - 1$ is relatively prime to p i.e. for each integer a, $1 \leq a \leq p - 1$ is such that $(a, p) = 1$

Hence $\Phi(p) = p - 1$.

Note: No composite number m exists such that $\Phi(m) = m - 1$ and this was conjectured by Lehmez more than half a century ago and it is yet to be established.

Theorem 4.2. $\Phi(n)$ is multiplicative. [i.e. if $(m, n) = 1$, then $\Phi(mn) = \Phi(m)\,\Phi(n)$]

Proof: Given that $(m, n) = 1$

We consider the product mn. Then the first mn numbers can be arranged in n lines, each containing m numbers. Thus

1	2	,.....,	k	,.....	m
$m+1$,	$m+2$	,.....,	$m+k$	,.....	$m+m$
$2m+1$,	$2m+2$	,.....,	$2m+k$	,.....	$2m+m$
.	.	,.....,	.	,.....	.
.	.	,.....,	.	,.....	.
$(n-1)m+1$,	$(n-1)m+2$	,..... .	$,(n-1)m+k$	,.....	$(n-1)m+m$

Now we consider the vertical column beginning with k.

If $(k, a) = 1$, all the terms of this column will be prime to m

but if k and m have a common divisor, no number in the column will be prime to m.

Now the first row contains $\Phi(m)$ numbers prime to n,

$\therefore$ $\Phi(m)$ vertical columns in each of which every term is prime to n,

Let us suppose that the vertical column which begins with k is one of these.

This column is in A.P., the terms of which when divided by n leaves remainders

$$0, 1, 2, 3, 4, ..., n-2, n-1$$

Hence, The column contains $\Phi(m)$ integers prime to n.

Thus in the table there are

$\Phi(m).\ \Phi(n)$ integers, which are prime to m and also n

and therefore to mn;

i.e., $\Phi(mn) = \Phi(m)\,\Phi(n)$. **[Second proof]**

Proof: To prove the theorem we first note the following lemma.

Lemma 4.3. If $S_1 = \{x_0, x_1, x_2, ..., x_{m-1}\}$ is a c.s.r. (mod m)

and $S_2 = \{y_0, y_1, y_2, ..., y_{n-1}\}$ is a c.s.r. (mod n)

then, $S = \{nx_i + my_j \mid x_i \in S_1, y_j \in S_2\}$ is also a c.s.r. (mod mn).

Proof: Now, $(nx_i + my_j, mn) = 1$

if and only if $(nx_i + my_j, m) = 1$

and $(nx_i + my_j, n) = 1$

if and only if $(nx_i, m) = 1$

and $(my_j, n) = 1$.

So, on the left hand side there are $\Phi(mn)$ integers and on the right hand side there are $\Phi(m)\,\Phi(n)$ integers.

and $\therefore$ $\Phi(mn) = \Phi(m)\,\Phi(n)$.

If p is a prime then $\Phi(p) = p - 1$

Number of a's ($< p$ and $(a, p) = 1$) is $p - 1$

Expression for $\Phi(p^\alpha)$

The numbers from 1 to p^α are as follows:

$1,\quad 2,\quad 3, --, p-1, 1.p, p+1, -, -, 2p, 2p+1, -, -, 3p, -, -, pp$

$p^2+1,\ p^2+2, ---, -, -, -, -, -, -, -, -, -, -, -, -, p.p^2 = p^3$

$p^3+1,\ p^3+2, ---, -, -, -, -, -, -, -, -, -, -, -, -, p4$

. . ---, -, -, -, -, -, -, -, -, -, -, -, -, -

. . ---, -, -, -, -, -, -, -, -, -, -, -, -, $p^{\alpha-1}$

$p^{\alpha-1}+1,\ p^{\alpha-1}+2, ---, -, -, -, -, -, -, -, -, -, -, -, -, p^{\alpha}$

[total $\alpha - 1$ rows]

In each row there are p numbers a's such that $(a, p^{\alpha}) \neq 1$

$\therefore$ there are in total $p^{\alpha-1}.p = p^{\alpha}$ numbers a such that $(a, p^{\alpha}), \neq 1$

$\therefore$ $\Phi(p^{\alpha}) = p^{\alpha} -$ (the number of a's such that (a, p^{α}) ' 1)

$$= p^{\alpha} - p^{\alpha-1} = p^{\alpha}\left(1-\frac{1}{p}\right)$$

Now if $n = p^1 q^m \ldots$ then,

$$= \Phi(p^1 q^m \ldots) = \Phi(p^1).\Phi(q^m) \ldots [\Phi \text{ is multiplicative}]$$

$$= p^1\left(1-\frac{1}{p}\right) \times q^m\left(1-\frac{1}{q}\right) \ldots = p^1 q^m \ldots\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\ldots$$

$$= n\,\Pi\left(1-\frac{1}{p}\right)$$

or, $\Phi(n) = n\,\Pi\left(1-\frac{1}{p}\right)$, p's are distinct prime factors of n.

[Third proof of the multiplicity of Φ]

Proof: Suppose $a = p_1^{\alpha_1}\ p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ and $b = q_1^{\beta_1} q_2^{\beta_2} \ldots . q_s^{\beta_s}$

i.e., $a = \prod_{n=1}^{r} p_n^{\alpha_n}, b = \prod_{m=1}^{s} q_m^{\beta_m}$

$\therefore$ $\Phi(a) = \prod_{n=1}^{r} p_n^{\alpha_n}\left(1-\frac{1}{p_n}\right)$, $\Phi(b) = \prod_{m=1}^{s} q_m^{\beta_m}\left(1-\frac{1}{q_m}\right)$

Since,$(a, b) =$ and $ab = \prod_{n=1}^{r} p_n^{\alpha_n} \prod_{m=1}^{s} q_m^{\beta_m} = \prod_{n=1, m=1}^{r, s} p_n^{\alpha_n} q_m^{\beta_m}$

$\therefore$ $\Phi(ab) = \prod_{n=1, m=1}^{r, s} p_n^{\alpha_n} q_m^{\beta_m}\left(1-\frac{1}{p_n}\right)\left(1-\frac{1}{q_m}\right)$

$$= \prod_{n=1}^{r} p_n^{\alpha_n}\left(1-\frac{1}{p_n}\right)\prod_{m=1}^{s} q_m^{\beta_m}\left(1-\frac{1}{q_m}\right)$$

$$= \Phi(a)\,\Phi(b).$$

Example 3. Solve for x, y, z: : $\Phi(x-5) + \Phi(3y-5) + \Phi(5z-18) = 3$ ....(i), where Φ is the Euler function.

Solution: $\Phi(n)$ = number of a ($< n$) such that $(a, n) = 1$

$= 1$, if $n = 1$

Since, $\Phi(n) \in \mathbb{N}$ therefore,

(i) will be satisfied if and only if $\Phi(x-5) = 1$, $\Phi(3y-5) = 1$, $\Phi(5z-18) = 1$

Now, $\Phi(x-5) = 1$ or, $x - 5 = 1$ or 2 or, $x = 6$ or 7

$\Phi(3y-5) = 1$ or, $3y - 5 = 1$ or 2, but $3y - 5 \neq 2$, $3y - 5 = 1$ or, $y = 2$

$\Phi(5z-18) = 1$ or, $5z - 18 = 1$ or, 2, but $5z - 18 \neq 1$ (since $z \in \mathbb{N}$)

$\therefore$ $5z - 18 = 2$ or, $z = 4$

$\therefore$ the solutions are $\left.\begin{matrix} x=6 \\ y=2 \\ z=4 \end{matrix}\right\}$, $\left.\begin{matrix} x=7 \\ y=2 \\ z=4 \end{matrix}\right\}$.

Example 4. Solve the simultaneous equations:

$$\Phi(x) + \Phi(y) = 2 \quad \text{...(i)}$$

$$\Phi(2x-1) + \Phi(2y) = 3 \quad \text{...(ii)}$$

Solution: From (i) we get $\Phi(x) = 1 \Rightarrow x = 1$ or 2

and, $\Phi(y) = 1$ or, $y = 1$ or 2

Then putting $x = 1$, $y = 1$ in (ii), $\Phi(1) + \Phi(2) = 3$ which is not possible

and, $\Phi(2.1 - 1) + \Phi(2.2) = \Phi(1) + \Phi(4) = 3$ is true.

$\therefore$ $x = 1$, $y = 2$ is a solution and $x = 2$, $y = 1$ is a solution.

and $\Phi(2.2 - 1) + \Phi(2.2) = \Phi(3) + \Phi(4) \neq 3$

$\therefore$ $\left.\begin{matrix} x=1 \\ y=2 \end{matrix}\right\}$; $\left.\begin{matrix} x=2 \\ y=1 \end{matrix}\right\}$ are solutions.

Theorem 4.4. Prove that $\sum_{d \mid n} \phi(d) = n$

Proof: [Method of modified induction]

Let, n have only one distinct prime factor with some positive power

i.e., suppose, $n = p^{\alpha}$, $\alpha \in \mathbb{N}$

$$\therefore \sum_{d \mid p^{\alpha}} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + \ldots + \phi(p^{\alpha})$$

$$= 1 + p - 1 + \ldots + p^{\alpha} - p^{\alpha-1}$$

$$= p^{\alpha}$$

$$= n$$

i.e., the result is true when n is a power of a prime.

Let us assume that the theorem is true when n has k distinct prime factors. Then consider an integer n, which has $(k + 1)$ distinct prime factors.

Let $p^{\alpha} \mid\mid N$ (i.e., $p^{\alpha} \mid N$ and $p^{\alpha+1} \nmid N$)

or $N = p^{\alpha}.n$, say where n has k-factors.

Now if d runs through the divisors of n, then $p^i d$ $(0 \le i \le \alpha)$ runs through the divisors of n.

$$\therefore \sum_{d \mid N} \phi(d) = \phi(d_1) + \phi(p^1 d_1) + \ldots + \phi(p^{\alpha} d_1)$$
$$+ \phi(d_2) + \phi(p^1 d_2) + \ldots + \phi(p^{\alpha} d_2)$$
$$+ \ldots + \ldots + \ldots + \ldots + \ldots$$
$$+ \phi(d_r) + \phi(p^1 d_r) + \ldots + \phi(p^{\alpha} d_r)$$
$$= \sum_{d \mid n} \phi(d) + \sum_{d \mid n} \phi(pd) + \sum_{d \mid n} \phi(p^2 d) + \ldots + \sum_{d \mid n} \phi(p^{\alpha} d)$$
$$= \sum_{d \mid n} \phi(d) + \sum_{d \mid n} \phi(p)\phi(d) + \sum_{d \mid n} \phi(p^2)\phi(d) + \ldots + \sum_{d \mid n} \phi(p^{\alpha})\,\phi(d)$$
$$= \sum_{d \mid n} \phi(d) + \Phi(p) \sum_{d \mid n} \phi(d) + \Phi(p^2) \sum_{d \mid n} \phi(d) + \ldots + \Phi(p^{\alpha}) \sum_{d \mid n} \phi(d)$$
$$= \sum_{d \mid n} \phi(d)\,[1 + \phi(p) + \phi(p^2) + \ldots + \phi(p^{\alpha})]$$
$$= np^{\alpha} = N.$$

or $\sum_{d \mid n} \phi(d) = N.$

Hence by the principle of induction the theorem follows.

Example 5. Prove that $\sum_{1 \le a < n} a = \frac{1}{2} n\phi(n)$, $(a, n) = 1$

Solution: We have

$(a, n) = 1$ gives

$(n - a, n) = 1$

Conclusion: If a is a set of integers such that $(a, n) = 1$, $1 \le a < n$ then, $n - a$ is also the same set as a

i.e., $\sum_{(a,n)=1;\, 1 \le a < n} a = a_1 + a_2 + \ldots + a_{\Phi(n)}$

$= (n - a_1) + (n - a_1) + \ldots + (n - a_{\Phi(n)})$

$\therefore\ 2 \sum_{(a,n)=1;\, 1 \le a < n} a = n + n + \ldots.$ to $\Phi(n)$ terms.

$= n\,\Phi(n)$

or $\sum_{1 \le a < n} a = \frac{1}{2} n\Phi(n).$

Theorem 4.5. Prove that $\phi(ab) = \phi(a)\phi(b)\dfrac{(a,b)}{\phi((a,b))}$

Solution: Suppose $(a, b) = d$

If $a = p_1^{a_1} \ldots p_m^{a_m}$, $b = q_1^{b_1} \ldots q_n^{b_n}$

then, $\phi(ab) = \phi(p_1^{a_1} \ldots p_m^{a_m} q_1^{b_1} \ldots q_n^{b_n})$

$= ab \prod_{p|ab}\left(1-\frac{1}{p}\right)$, p's are distinct prime divisors of ab

or $$\frac{\phi(ab)}{ab} = \prod_{p|ab}\left(1-\frac{1}{p}\right) = \frac{\prod_{p|a}\left(1-\frac{1}{p}\right)\prod_{p|b}\left(1-\frac{1}{p}\right)}{\prod_{p|d}\left(1-\frac{1}{p}\right)}$$, where $d = (a, b)$

$$= \frac{\frac{\phi(a)}{a}\frac{\phi(b)}{b}}{\frac{\phi(d)}{d}} = \frac{1}{ab}\phi(a)\phi(b)\frac{d}{\phi(d)}$$

Thus, $$\phi(ab) = \phi(a)\phi(b)\frac{d}{\phi(d)} = \phi(a)\phi(b)\frac{(a,b)}{\phi((a,b))}$$

Example 6. What are the positive integers a, b that satisfy the expression

$$\phi(ab) = \phi(a) + \phi(b)?$$

Solution By theorem 4.5

$$\phi(ab) = \phi(a)\phi(b)\frac{d}{\phi(d)}, \text{ where } d = (a, b)$$

This gives, $$\frac{\phi(a)+\phi(b)}{\phi(a)\phi(b)} = \frac{d}{\phi(d)}$$

or $$\frac{1}{\phi(a)} + \frac{1}{\phi(b)} = \frac{d}{\phi(d)} \Rightarrow \frac{\phi(d)}{\phi(a)} + \frac{\phi(d)}{\phi(b)} = d$$

or $$\frac{1}{m} + \frac{1}{n} = d, \text{ where, } m = \frac{\phi(a)}{\phi(d)}, n = \frac{\phi(b)}{\phi(d)}.$$

Since

m, n and d are positive integers,

only possible values of m, n and d are:

$d = 2, m = n = 1$ ...(*)

or $d = 1, m = n = 2.$ ...(**)

For the case (*),

$\phi(a) = \phi(b) = 2$ and then, $a = b = 2$

For the case (**),

$$\phi(a) = \phi(b) = 2, \text{ then one of } a, b \text{ is 3 and the other is 4.}$$

Thus the possible values are (2, 2), (3, 4) and (4, 3).

Example 7. Prove that if $\phi(n) \mid n-1$, then there exists no prime p such that $p^2 \mid n$

Solution: Suppose $n = p^a q^b \ldots r^c$, where $p, q, \ldots r$ are all distinct primes and $a \geq 2$. [so $p^2 \mid n$]

Now $\phi(p^a) = p^a - p^{a-1} = p(p^{a-1} - p^{a-2})$

And

$\therefore$ $p \mid \phi(p^a) \mid \phi(n)$

Hence,

$p \mid \phi(n)$ and $p \nmid n-1$.

$\therefore$ $\varphi(n) \neq n-1$.

Example 8. Prove that if n is to a prime and $\phi(n) \mid n-1$, n has at least three distinct prime factors.

Solution: Suppose n has two distinct prime factors

And since, $\phi(n) \mid n-1$, by the preceding example

$n = pq$, where p and q are primes.

Then
$$\frac{n-1}{\phi(n)} = \frac{pq-1}{(p-1)(q-1)}$$
$$= \frac{pq-p-q+1+p+q-2}{(p-1)(q-1)}$$
$$= \frac{(p-1)(q-1)}{(p-1)(q-1)} + \frac{p-1}{(p-1)(q-1)} + \frac{q-1}{(p-1)(q-1)}$$
$$= 1 + \frac{1}{q-1} + \frac{1}{p-1}$$

As $\phi(n) \mid n-1$, $\dfrac{\phi(n)}{n-1}$ is an integer

Moreover, $1 < 1 + \dfrac{1}{p-1} + \dfrac{1}{q-1} \leq 3$, if p and q are primes.

$\therefore$ $\dfrac{1}{p-1} + \dfrac{1}{q-1} = 1$ or 2 which is possible only when $p = q = 2$ or $p = q = 3$; but our assumption says that p and q are distinct. Hence n cannot have two distinct primes.

So n must have at least three distinct primes.

4.3 DIVISOR FUNCTION

$d(n)$ [or, $\tau(n)$]: $d : \mathbb{N} \to \mathbb{N}$ such that $d(n)$ = number of divisors of n, $n \in \mathbb{N}$

We note that

$$d(n) = 1 \text{ if } n = 1$$
$$= 2 \text{ if } n = p(\text{a prime})$$
$$> 2 \text{ if } n \text{ is composite}$$

Expression for $d(n)$

Since

$1, p, p^2, \ldots, p^{\alpha-1}, p^\alpha$ are the divisors of p^α

$\therefore \quad d(p^\alpha) = \alpha + 1$, p is a prime.

In particular, $d(p) = 2$, where p is a prime.

And so on.

$$d(p^\alpha q^\beta) = (\alpha + 1)(\beta + 1)$$

If $n = p_1^{\alpha_1} p_2^{\alpha_2}$

The divisors of n are

1	p_1	p_1^2	—	—	—	$p_1^{\alpha_1}$
p_2	p_2p_1	$p_2p_1^2$	—	—	—	$p_2p_1^{\alpha_1}$
p_2^2	$p_2^2p_1$	$p_2^2p_1^2$				$p_2^2p_1^{\alpha_1}$
—	—	—	—	—	—	—
$p_2^{\alpha_2}$	$p_2^{\alpha_2}p_1$	$p_2^{\alpha_2}p_1^2$	—	—	—	$p_2^{\alpha_2}p_1^{\alpha_1}$

Therefore the number of divisors is $(\alpha_1 + 1)(\alpha_2 + 1)$

Thus, $d(n) = (\alpha_1 + 1)(\alpha_2 + 1)$

Similarly if $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ then

$$d(n) = d\left(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i}\right)$$

$$= (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_i + 1), \qquad (p_i, p_j) = 1, (i \neq j)$$

$$d(4) = d(2^2) = 2 + 1 = 3, \; d(6) = d(2.3) = (1 + 1)(1 + 1) = 4$$

$$d(4320) = d(2^5.3^3.5^1) = (5 + 1)(3 + 1)(1 + 1) = 6.4.2 = 48$$

Theorem 4.6. d is a multiplicative A.F. [To prove that $d(mn) = d(m)\, d(n)$ if $(m, n) = 1$]

Proof: Let, $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i}$, p's are distinct primes; α's are positive integers

$n = q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}$, q's are distinct primes; β's are positive integers.

$$\therefore \quad d(mn) = d\left(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i} q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}\right)$$

$$= (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_i + 1)(\beta_1 + 1)(\beta_2 + 1) \ldots (\beta_l + 1)$$

$$= [(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_i + 1)][(\beta_1 + 1)(\beta_2 + 1) \ldots (\beta_l + 1)],$$

[since $(p_r, q_s) = 1] \; \forall \; 1 \le r \le i, \; 1 \le s \le l$

$$= d(m)d(n).$$

Example 9. Show that $\phi(m) \ge \dfrac{m}{d(m)}$

Solution: Suppose $m = p^a q^b \ldots r^c$

Then, $$\phi(m)d(m) = m\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\ldots\left(1 - \frac{1}{r}\right)(a + 1)(b + 1)\ldots(c + 1)$$

$$\ge m\left(\frac{1}{2}\right)^k .2^k = m$$

[k = the number of distinct prime factors of m]

[**Note:** If $p \ge 2$ then, $-\dfrac{1}{p} \ge -\dfrac{1}{2}$ or, $1 - \dfrac{1}{p} \ge 1 - \dfrac{1}{2} = \dfrac{1}{2}$]

$$\phi(m)d(m) \ge m$$

gives, $$\phi(m) \ge \frac{m}{d(m)}$$

Example 10. $\prod\limits_{d \mid n} d = n^{\frac{1}{2}d(n)}$ [**Hint:** If d is a divisor of n, then so is also $\dfrac{n}{d}$ $(\text{LHS})^2 = n^{d(n)}$]

Example 11. Prove that $d(n)$ is odd if and only if n is a perfect square

Solution: Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i}$

Then, $$d(n) = d\left(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i}\right) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_i + 1)$$

Now $d(n)$ is odd if and only if $(\alpha_i + 1)$ is odd for each i

i.e. if and only if α_i is even for each i

i.e. if and only if $\alpha_i = 2k_i$ for each i

Thus, $$n = p_1^{2k_i} p_2^{2k_2} \ldots p_i^{2k_i} = \left(p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i}\right)^2 = m^2$$

Hence $d(n)$ is odd if and only if n is a perfect square.

Example 12. Find the smallest positive integer having only 10 positive divisors

Solution: Suppose $n = p^a.q^b \ldots r^c$

$$d(n) = d(p^a.q^b \ldots r^c) = \prod_a (a+1) = 10 = 1.10$$

or $= 2.5$

$\therefore \quad (a+1)(b+1) = 1.10$

or $= 2.5$

In the first case, $a = 0$, $b = 9$ give, $n = q^9$

In the second case, $a = 1$, $b = 4$ give, $n = pq^4$

$\therefore$ the required smallest number,

$$n = 3.2^4 = 489.$$

4.4 THE FUNCTION σ

$\sigma : \mathbb{N} \to \mathbb{N}$ such that

$\sigma(n)$ = the sum of the divisors of n

$$= \sum_{d|n} d$$

$$= \sum_{d_i} d_i, \ (1 \le i \le \alpha)$$

$$= \sum_{d_i} d_i, \ d_i \in S, \text{ where } S = \{d_1, d_2, .., d_1\} \text{ is the set of divisors of } n.$$

e.g., $\sigma(1) = 1$, $\sigma(2) = 1 + 2 = 3$, $\sigma(3) = 1 + 3 = 4$, $\sigma(4) = 1 + 2 + 4 = 7$, $\sigma(5) = 1 + 5 = 6$ $\sigma(6) = 1 + 2 + 3 + 6 = 12$ $\sigma(7) = 1 + 7 = 8$ $\sigma(8) = 1 + 2 + 4 + 8 = 15$

Expression for $\sigma(n)$ where n is a power of a prime

We note the divisor of p^α are:

$1, p, ..., p^\alpha$

$$\therefore \quad \sigma(p^\alpha) = 1 + p + p^2 + p^3 + \ldots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

We note here that the divisors of $p^\alpha q^\beta$ are

$$1 \ p \ \ldots \ p^\alpha$$
$$q \ pq \ \ldots \ p^\alpha q$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$q^\beta \ pq^\beta \ \ldots\ p^\alpha \ q^\beta$$

$$\therefore \quad \sigma(p^\alpha q^\beta) = (1 + p + p^2 + p^3 + \ldots + p^\alpha)(1 + q + q^2 + q^3 + \ldots + q^\beta)$$

$$= \frac{p^{\alpha+1} - 1}{p - 1} \times \frac{q^{\beta+1} - 1}{q - 1}.$$

Example 13. Find the smallest positive integer with sum of all its divisors is 15.

Solution: Suppose $n = p^a.q^b \ldots r^c$

Then, $$\sigma(n) = \sigma(p^a.q^b \ldots r^c) = \prod_p \frac{p^{\alpha+1}-1}{p-1} = 15$$

or $$\frac{p^{a+1}-1}{p-1} \times \frac{q^{b+1}-1}{q-1} = 15 = 15 \times 1$$

or, $$= 3 \times 5$$

$\therefore$ $p = 2$, $a = 3$; $q = 2$, $b = -1$ (not allowed) (other factors do not occur)

$\therefore$ the number is $n = 2^3 = 8$.

Example 14. Find σ (2520)

Solution: Divisors of $125 = 5^3$ are $5^0, 5^1, 5^2, 5^3$.

So, $$\sigma(5^3) = 1 + 5 + 5^2 + 5^3$$

Divisors of $3^4 \times 5^3$ are:

$$3^0 \times 5^0, 3^1 \times 5^0, 3^2 \times 5^0, 3^3 \times 5^0, 3^4 \times 5^0$$
$$3^0 \times 5^1, 3^1 \times 5^1, 3^2 \times 5^1, 3^3 \times 5^1, 3^4 \times 5^1$$
$$3^0 \times 5^2, 3^1 \times 5^2, 3^2, \times 5^2, 3^3 \times 5^2, 3^4 \times 5^2,$$
$$3^0 \times 5^3, 3^1 \times 5^0, 2^2 \times 5^3, 3^3 \times 5^3, 3^4 \times 5^3;$$

so $$\sigma(3^4 \times 5^3) = (3^0 + 3^1 + 3^2 + 3^3 + 3^4) \times (5^0 + 5^1 + 5^2 + 5^3).$$

Using the above result:

$$\sigma(2520) = \sigma(2^3 \times 3^2 \times 5^1 \times 7^1)$$
$$= \frac{2^4-1}{2-1} \times \frac{3^3-1}{3-1} \times \frac{5^2-1}{5-1} \times \frac{7^2-1}{7-1}$$
$$= \ldots$$
$$= 15 \times \frac{26}{2} \times 6 \times 8 = 9360.$$

Theorem 4.7. $\sigma(n)$ is multiplicative (i.e. $(m, n) = 1$ then $\sigma(mn) = \sigma(m)\,\sigma(n)$)

Proof: Let, $n = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_i^{\alpha_i}$, $m = q_1^{\beta_1} q_2^{\beta_2} \ldots . q_l^{\beta_l}$: p's and q's are different primes and α's and β's are positive integers

Now, $$\sigma(mn) = \sigma\left(p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_i^{\alpha_i} . q_1^{\beta_1} q_2^{\beta_2} \ldots . q_l^{\beta_l}\right)$$

$$= \frac{{p_1}^{\alpha_i+1}-1}{p_1-1} \times \ldots \times \frac{{p_i}^{\alpha_i+1}-1}{p_1-1} \times \frac{{q_1}^{\beta_l+1}-1}{q_1-1} \times \ldots \times \frac{{q_l}^{\beta_l+1}-1}{q_1-1}$$

$$= \left[\frac{{p_1}^{\alpha_l+1}-1}{p_1-1} \times \ldots \times \frac{{p_i}^{\alpha_l+1}-1}{p_1-1}\right] \times \left[\frac{{q_1}^{\beta_l+1}-1}{q_1-1} \times \ldots \times \frac{{q_l}^{\beta_l+1}-1}{q_1-1}\right]$$

$$= \sigma(n)\,\sigma(m)$$

But it is not totally multiplicative.

Example 15. $m = 18$, $n = 30$. here, $(m, n) \neq 1$and,

$$\sigma(18 \times 30) = \sigma(540) = \sigma(2^3 \times 3^3 \times 5) = 1680$$

And, $\sigma(18)\sigma(30) = \sigma(2 \times 3^2)\,\sigma(2 \times 3 \times 5) = 3 \times 13 \times 3 \times 4 \times 6 = 2808.$

$\therefore$ $\sigma(mn) \neq \sigma(m)\,\sigma(n))$.

Expression for $\sigma(n)$

$$\text{If } n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}, \text{ then } \sigma(n) = \prod_{i=1}^{r} \frac{p_i^{e_i+1} - 1}{p_i - 1}$$

Proof: Here $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, and $\sigma(n)$ is multiplicative.

We have therefore

$$\sigma(n) = \sigma(p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}) = \prod_{i=1}^{r} \sigma(p_i^{e_i}) = \prod_{i=1}^{r} \frac{p_i^{e_i+1} - 1}{p_i - 1}, \quad \sigma(1) = 1.$$

Definition: (1) If $\sigma(n) < 2n$, then n is called a *deficit* number

(2) If $\sigma(n) = 2n$, then n is called a *perfect* number

(3) If $\sigma(n) > 2n$, then n is called an *abundant* number

Example 16.

$\sigma(1) = 1 < \times 1 \quad \therefore$ 1 is deficit

$\sigma(2) = 3 < 2 \times 2 \quad \therefore$ 2 is deficit

$\sigma(3) = 4 < 2 \times 3 \quad \therefore$ 3 is deficit

$\sigma(4) = 7 < 2 \times 4 \quad \therefore$ 4 is deficit

$\sigma(6) = 12 = 2 \times 6 \quad \therefore$ 6 is perfect

$\sigma(14) = 24 < 2 \times 14 \quad \therefore$ 14 is deficit

$\sigma(8) = 15 < 2 \times 8 \quad \therefore$ 8 is deficit

$\sigma(24) = 60 > 2 \times 24 \quad \therefore$ 24 is abundant

$\sigma(12) = 28 > 2 \times 12 \quad \therefore$ 12 is abundant

$\sigma(28) = 56 = 2 \times 28 \quad \therefore$ 28 is perfect

Example 17. Show that every prime power is deficit

Solution Suppose $n = p^k$ then $\sigma(p^k) = \dfrac{p^{k+1} - 1}{p - 1}$

Now $2p^k - 1 < p^k + 1$ since $p \geq 2$. It follows that $p^{k+1} - 1 < 2(p^{k+1} - p^k)$ $2p^k(p - 1)$,

so that $\dfrac{p^{k+1} - 1}{p - 1} < 2p^k = 2n.$

Hence $n = p^k$ is deficit.//

Example 18. Show that if n is an odd perfect number then n has at least three different prime divisors.

Solution: First suppose that $n = p^a$, where p is a prime and a is a positive integer. Then

$$\sigma(n) = \frac{p^{a+1}-1}{p-1} < \frac{p^{a+1}}{p-1} = \frac{np}{p-1} = \frac{n}{1-\frac{1}{p}} \leq \frac{n}{2/3} < \frac{3n}{2}$$ so that $\sigma(n) \neq 2n$ and n is not perfect.

Next suppose $n = p^a q^b$ where p and q are primes and a, b are positive integers. Then

$$\sigma(n) = \frac{p^{a+1}-1}{p-1}.\frac{q^{b+1}-1}{q-1} < \frac{p^{a+1}q^{b+1}}{(p-1)(q-1)} = \frac{npq}{(p-1)(q-1)}$$

$$= \frac{n}{\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)} \leq \frac{n}{\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)} = \frac{15n}{8} < 2n.$$

Hence $\sigma(n) \neq 2n$ and n is not perfect.

Theorem 4.8. If n is even and perfect then, $n = 2^{p-1}(2^p - 1)$, $2^p - 1$ and hence p is a prime (cf. Mersenne prime) and conversely.

Proof: n is even gives $n = 2^k.l$, where l is odd, $k \in \mathbb{N}$,

Obviously $(2^k, l) = 1$.

By definition, $2n = \sigma(n) = \sigma(2^k l)$

or $2^{k+1}.l = \sigma(2^k)\,\sigma(l)$

$$= \frac{2^{k+1}-1}{2-1} \times \sigma(l) = (2^{k+1}-1)\,\sigma(l) \quad \text{...(*}$$

or $2^{k+1}.l = (2^{k+1}-1)\,\sigma(l)$

or $2^{k+1} \mid (2^{k+1}-1)\,\sigma(l)$

or $2^{k+1} \mid \sigma(l)$ (since, $(2^k, 2^{k+1}-1) = 1$)

or $\sigma(l) = 2^{k+1}.t$, say $t \in \mathbb{N}$

$\therefore$ (*) becomes

$$2^{k+1}.l = (2^{k+1}-1).2k+1.t.$$

So $l = (2^{k+1}-1).t$ and $\sigma(l) = 2^{k+1}.t$

Now we find t

If $t \neq l$, then l has at least the divisors 1, l, t $2^{k+1}-1$

Now, $\sigma(l) \geq 1 + l + t + (2^{k+1}-1)$

[because of the fact that there may be some more divisors

$= 1 + t.2^{k+1} - t + t + 2^{k+1} - 1$

$= (t+1)2^{k+1} > t.2^{k+1}$

$= \sigma(l)$

$\therefore$ $\sigma(l) > \sigma(l)$ and is impossible.

$\therefore$ t is not greater than l, so, $t = l$

$\therefore \quad l = 2^{k+1} - 1, \ \sigma(l) = 2^{k+1}.$

If l is composite, the divisors of 1 are l, $2^{k+1} - 1$, some other divisors(s)

$\therefore \quad \sigma(l) = 1 + (2^{k+1} - 1) + \ldots > 1 + (2^{k+1} - 1)$

$= 2^k = \sigma(l)$ and is not possible.

$\therefore$ 1 is prime.

so, l is of the form $2p - 1$

i.e., $k + 1 = p$ [Ref: Mersenne prime]

$\therefore \quad k = p - 1$

$\therefore \quad n = 2k.1 = 2^{p-1}(2^p - 1)$

Converse: Let $n = 2^{p-1}(2^p - 1)$, $2^p - 1$ [and $\therefore$ p] is prime.

To prove that, n is a perfect number. (of course even)

i.e., to show that

$\sigma(n) = 2n$

Now $n = 2^{p-1}.p_1$, say $p_1 = 2^p - 1$ is a prime.

Obviously,

$(2^{p-1}, p_1) = 1$

or $\sigma(n) = \sigma(2^{p-1}.p_1) = \sigma(2^{p-1})\ \sigma(p_1)$

$$= \frac{2^{p-1+1} - 1}{2 - 1}(1 + p_1)$$

$= (2^p - 1)(1 + p_1)$

$= (2^p - 1)2^p$

$= 2.2^{p-1}(2^p - 1)$

$= 2n.$

Now the problem is to find all the positive integers $n > 1$ which are equal to the product of their proper divisors.,

or i.e., to find $n > 1$ such that $\prod_{d|n} d = n^2$

Theorem 4.9. If $n > 1$, $\prod_{d|n} d = n^2$ then $n = p^3$, p_1p_2, (p_1p_2, p's are primes)

Proof: Let $\prod_{d|n} d = n^2$, to prove that $n = p^3$ or p_1p_2

Remark: If d runs thro' the divisors of n so does $\frac{n}{d}$.

Now, $n^4 = n^2n^2 = \prod_{d|n} d \prod_{d|n} \frac{n}{d} = \prod_{d|n} n = n^{d(n)}$

or $n^4 = n^{d(n)}$

$\Rightarrow \quad d(n) = 4$

or $4 = d(n) = d\left(2^{a_1} p^{a_2} q^{a_3} \ldots\right)$ (where $n = 2^{a_1} p^{a_2} q^{a_3} \ldots$)

$= d\left(2^{a_1}\right) d\left(p^{a_2}\right) d\left(q^{a_3}\right) \ldots$

$= (a_1 + 1)(a_2 + 1)(a_3 + 1) \ldots (a_r + 1)$

$\therefore$ we get, $(a_1 + 1)(a_2 + 1)(a_3 + 1) \ldots (a_r + 1)$

$= 4$

Now, if $a_1 = 1$, any other of a's will be equal to 1 and the rest will be zero, i.e., all the a's but one (in particular say a_2) will be zero then $n = 2p$ (of the form $p'p''$)

(i) if $a_2 = 3$ then the rest of the a's will be zero and then $n = p^3$

(ii) if any a say $a_2 = 1$ then any other a say $a_3 = 1$ and the rest will be zero. Then $n = pq$, i.e. $n = p^3$ or $p_1 p_2$.

Example 19. If $\sigma(n)$ is odd then n is of the form k^2 or $2k^2$

Solution: Let $\sigma(n)$ be odd; to prove that $n = k^2$ or $2k^2$, $k \in \mathbb{N}$

Let $n = 2^a . p^l q^m \ldots$; $a \in \{0\} \cup \mathbb{N}$, $l, m \in \mathbb{N}$, p, q odd primes

or, $\sigma(n) = \sigma(2^a . p^l q^m \ldots) = \sigma(2^a)\, \sigma(p^l)\, \sigma(q^m)$ ...(1)

Since $\sigma(n)$ is odd, the right hand side is odd.

Now $\sigma(2^a) = 2^{a+1} - 1$ is always odd and

$$\sigma(p^l) = \frac{p^{i+1}}{p-1} = 1 + p + p^2 + p^3 + \ldots + p^l \text{ is odd}$$

if and only if $p + p^2 + p^3 + \ldots + p^l$ is even

if and only if l is even(say) $= 2k_1$, $k_1 \in \mathbb{N}$

Similarly, m is even(say) $= 2k_2$

Case I: Let a be even, say $2k$

or $n = 2^a . p^l q^m$

$= 2^{2k_0} . p^{2k_1} . q^{2k_2} \ldots$

$= \left(2^{k_0} . p^{k_1} . q^{k_2} \ldots\right)^2$

$= k^2$, say.

Remark: This is also true if $a = 0$,

Case II: Let a be odd, say $2k_0 + 1$;

Then $n = 2^a . p^l q^m$

$= 2.2^{2k_0} . p^{2k_1} . q^{2k_2} \ldots$

$= 2.\left(2^{k_0} . p^{k_1} . q^{k_2} \ldots\right)^2$

$= 2k^2$, say.

Conversely: Let $n = k^2$; to prove $\sigma(n)$ is odd

$$n = k^2 = \left(2^{k_0}.p^{k_1}.q^{k_2}\ldots\right)^2 = 2^{2k_0}.p^{2k_1}.q^{2k_2}\ldots$$

$$\sigma(n) = \sigma\left(2^{2k_0}\right)\sigma\left(p^{2k_1}\right)\sigma\left(q^{2k_2}\right)\ldots$$

$$= \left(2^{2k_0+1}-1\right)\times\frac{p^{2k_1+1}-1}{p-1}\times\frac{q^{2k_2+1}-1}{q-1}\times\ldots$$

$$= \left(2^{2k_0+1}-1\right)\times\left(1+p+p^2+\ldots+p^{2k_1}\right)\times\ldots$$

= and odd number (since each factor is odd).

Similarly, $n = 2k^2$, then $\sigma(n)$ is odd

Let $n = 2.\left(2^{k_0}.p^{k_1}.q^{k_2}\ldots\right)^2$

Then $n = 2^{2k_0+1}.p^{2k_1}.q^{2k_2}\ldots$

$\therefore$ $\sigma(n) = \sigma\left(2^{2k_0+1}\right)\sigma\left(p^{2k_1}\right)\sigma\left(q^{2k_2}\right)\ldots$

$$= \left(2^{2k_0+2}-1\right)\left(1+p+p^2+\ldots+p^{2k_1}\right)\times\ldots$$

$\therefore$ every factor is odd, so also $\sigma(n)$.

Example 20. Find the smallest positive integer with sum of all its divisors is 15.

Solution: Suppose $n = p^a.q^b \ldots r^c$

Then, $\sigma(n) = \sigma(p^a.q^b \ldots r^c) = \prod_p \frac{p^{a+1}-1}{p-1} = 15$

$$\frac{p^{a+1}-1}{p-1}\times\frac{q^{b+1}-1}{q-1} = 15 = 15.1$$

or $= 3.5$

or $p = 2$, $a = 3$; $q = 2$, $b = -1$ (not allowed) (other factors do not occur)

$\therefore$ the number is $n = 2^3 = 8$.

Example 21. Show that if m is prime then

$$\phi(m) + \sigma(m) = md(m)$$

Solution Suppose m is a prime.

Then, $\phi(m) = m - 1$, $\sigma(m) = m + 1$ and $d(m) = 2$

And the result is then obviously true.

Example 22. If m is an integer of the form p^k for some prime p and some integer k, then $\phi(m) + \sigma(a) \neq md(m)$

Solution:

Case 1 Suppose $p = 2$

Then, $\sigma(2^k) = 2^{k+1} - 1 < 2^{k+1} = 2.2^k$

Case II p is any odd prime

$$\sigma(p^k) = \frac{p^{k+1}-1}{p-1} = \frac{p^k - \frac{1}{p}}{1-\frac{1}{p}} < \frac{p^k}{1-\frac{1}{p}} \leq \frac{p^k}{1-\frac{1}{3}} = \frac{3}{2}\, p^k < p^k$$

Hence,

For $m = p^k \ (k \geq 2, p \geq 3)$

$$\phi(m) + \sigma(m) = \phi(p^k) + \sigma(p^k) < p^k + 2p^k = 3p^k = 3m \geq m\, d(m)$$

So, $\phi(m) + \sigma(m) \neq m\, d(m)$.

4.5 THE FUNCTION $\sigma_k(n)$

Definition: $\sigma_k(n) = \sum_{d|n} d^k$

$\therefore$ $\sigma_1(n) = \sum_{d|n} d$

$\sigma_4(6) = \sum_{d|6} d^4 = 1 + 2^4 + 3^4 + 6^4$

$\sigma_5(8) = \sum_{d|8} d^5 = \sum_{d|8} 1^5 + 2^5 + 4^5 + 8^5$

$\sigma_k(1) = 1, \forall k.$

Expression for $\sigma_k(n)$

$$\sigma_k(p^\alpha) = \sum_{d|p^\alpha} d^k = 1^k + p^k + p^{2k} \ldots + p^{\alpha k} = \frac{p^{(\alpha+1)k} - 1}{p^k - 1}.$$

The above result is sufficient to prove that

Theorem 4.10. $\sigma_k(n)$ is multiplicative.

Example 23. $\sigma_{-k}(n) = n^{-k}\, \sigma_k(n)$

Solution:

$$\sigma_{-k}(n) = \sum_{d|n} d^{-k} = \sum_{d|n} \left(\frac{n}{d}\right)^{-k}$$

$$= \sum_{d|n} n^{-k} d^k = n^{-k} \sum_{d|n} d^k.$$

4.6 THE MOBIUS FUNCTION $\mu(n)$

Definition: Mobius function $\mu(n)$ is defined by

$$\mu(n) = 1 \quad \text{if} \quad n = 1$$
$$= 0 \quad \text{if} \quad a^2 \mid n \quad \textit{for some } a > 1$$
$$= (-1)^r \text{ if } n = p_1 p_2 \ldots, p_r, p_1 \text{ are distinct primes}$$

Theorem 4.11. The function $\mu(n)$ is multiplicative

Proof: Suppose $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ and $n = q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$, $(m, n) = 1$

If any of α_i or β_j is greater than 1, then

$$\mu(mn) = 0 = \mu(m)\,\mu(n)$$

and if $\alpha_i = 0$ also $\beta_j = 0$ for all I and j, then

$$\mu(mn) = (-1)^{r+s} = \mu(m)\,\mu(n).$$

Thus the result follows.

Theorem 4.12. If n has k distinct prime factors an its divisors are arranged in an ascending order as $d_1, d_2, \ldots, d_m$ $(d_1 < d_2 < \ldots < d_m)$, then

(i) $\mu(d_1) + \mu(d_2) + \ldots + \mu(d_m) = 0$

(ii) $|\mu(d_1)| + |\mu(d_2)| + \ldots |\mu(d_m)| = 2^k$

Proof:

Case I: Suppose $n = p$, a prime. Then $k = 1$, $1 = d_1$, $p = d_2$ and has only two divisors.

$$\therefore \quad \mu(d_1) = 1, \mu(d_2) = -1$$

and hence $\mu(d_1) + \mu(d_2) = 0$

and $|\mu(d_1)| + |\mu(d_2)| = 2$

Case II: Suppose $n = p^\alpha$

Then the divisors are

$p, p^2, p^3, \ldots, p^\alpha$

And we note: $\mu(1) = 1, \mu(p) = -1, \mu(p^2) = \mu(p^3) = \ldots = \mu(p^\alpha) = 0$

$$\therefore \quad \mu(d_1) = 1, \mu(d_2) = -1, \mu(d_3) = \mu(d_4) = \ldots = \mu(d_m) = 0$$

Therefore, $\mu(d_1) + \mu(d_2) + \mu(d_3) + \ldots + \mu(d_m) = 0$

And, $|\mu(d_1)| + |\mu(d_2)| + \ldots + |\mu(d_m)| = 2 = 2^k$

Case III: Suppose $n = p_1 p_2 \ldots p_k$

Then the divisors of n are

$p_1, p_2 \ldots, p_k$;

$p_1p_2, p_1p_3, p_2p_3, \ldots, p_{k-1}p_k$;

$p_1p_2p_3, p_1p_2p_4, \ldots, p_{k-2}p_{k-1}p_k, \ldots, p_1p_2 \ldots, p_k$

Now

$$\mu(1) = 1$$

$$\mu(1) = \mu(1) = \ldots = \mu(1) = -1$$

$$\mu(p_1p_2) = \mu(p_1p_3) = \ldots = \mu(p_{k-1}p_k) = 1 \text{ and these are } {}^kC_2 \text{ in numbers}$$

$$\mu(p_1p_2p_3) = \mu(p_2p_3p_4) = \ldots = \mu(p_{k-2}p_{k-1}p_k) = 1 \text{ and these } {}^kC_3 \text{ in numbers}$$

.....

$$\mu(p_1p_2 \ldots p_r) = \ldots = (-1)^r \text{ and these are } {}^kC_r \text{ in numbers}$$

.....

$$\therefore \quad \mu(d_1) + \mu(d_2) + \ldots + \mu(d_m)$$

$$= \mu(1) + \sum_i \mu(p_i) + \sum_{i \neq j} \mu(p_ip_j) + \sum_{i \neq j \neq k} \mu(p_ip_jp_k) + \ldots$$

$$= 1 - k + {}^kC_2 - {}^kC_3 + \ldots$$

$$= (1-1)^k$$

$$= 0$$

And, $|\mu(d_1)| + |\mu(d_2)| + \ldots + |\mu(d_m)|$

$$= |\mu(1)| + \sum_i |\mu(p_i)| + \sum_{i \neq j} |\mu(p_ip_j)| + \ldots$$

$$= 1 + {}^kC_1 + \ldots = (1+1)^k = 2^k$$

4.7 THE FUNCTION $P(n) = \prod_{d|n} d$

Theorem 4.13. Prove that $P(n) = n^{\frac{d(n)}{2}}$

Clearly,

$$P(p) = p$$

Suppose $\{a_1, a_2, \ldots, a_{d(n)}\}$ is the set of all the positive divisors of n, Then,

$$\{a_2, a_2, \ldots, a_{d(n)}\} = \left\{\frac{n}{a_1}, \frac{n}{a_2}, \ldots, \frac{n}{a_{d(n)}}\right\}$$

$$\therefore \quad (P(n))^2 = \left(a_1 \cdot \frac{n}{a_1}\right)\left(a_2 \cdot \frac{n}{a_2}\right) \ldots \left(a_{d(n)} \cdot \frac{n}{d(n)}\right)$$

$$= \underbrace{n.n \ldots, n}_{d(n)\ times} = n^{d(n)}$$

or $$\underbrace{n.n \ldots . n}_{d(n)\ times} = n^{d(n)}$$

Therefore, $$P(n) = n^{\frac{d(n)}{2}}$$

We note the following table of

$\phi(n)$, $d(n)$, $\sigma(n)$, $P(n)$ for $1 \le n \le 10$

n	$\phi(n)$	$d(n)$	$\sigma(n)$	$P(n)$
1	1	1	1	1
2	1	2	3	2
3	2	2	4	3
4	2	3	7	8
5	4	2	6	5
6	2	4	12	36
7	6	2	8	7
8	4	4	15	64
9	6	3	13	27
10	4	4	18	100
11	10	2	12	
12	4	6	28	
13	12	2	14	
14	6	4	24	
15	8	4	24	
16	8	4	24	
16	8	5	31	
17	16	2	18	
18	6	6	39	
19	18	2	20	
20	8	6	42	

Theorem 4.14. If for positive integers m and n, $(m, n) = 1$ then,

$$P(mn) = P(m)^{d(n)}.P(n)^{d(m)}$$

Proof: Suppose m and n are positive integers such that $(m, n) = 1$

Since $d(n)$ is multiplicative

$$P(mn) = (mn)^{\frac{d(mn)}{2}} = (mn)^{\frac{d(m)\,d(n)}{2}} = m^{\frac{d(m)\,d(n)}{2}}\, n^{\frac{d(m)\,D(n)}{2}}$$

$$= \left(m^{\frac{d(m)}{2}}\right)^{d(n)} \cdot \left(n^{\frac{d(n)}{2}}\right)^{d(m)}$$

$$= P(m)^{d(n)}.P(n)^{d(m)}.$$

Note: $P(n)$, $d(n)$ $\sigma(n)$ are *not totally multiplicative*

For, $m = 525 = 3.5^2.7$, $n = 231 = 3.7.11$

$mn = 3^2.5^2.7^2.11$

$d(mn) = 54$, $\sigma(mn) = 275652$,

Here, $d(mn) \neq d(m)\, d(n)$, $\sigma(mn) \neq \sigma(m)n\sigma(n)$,

Moreover: $P(mn) \neq P(m)^{d(n)}.P(n)^{d(m)}$

And, $P(n)$ *is not even multiplicative:*

For $P(2) = 2$, $P(3) = 3$, but $p(6) = 36$

$\therefore$ $(2, 3) = 1$ and $P(2.3) = P(6) = 36 \neq 6 = 2.3 = P(2)P(3)$

$P(2.3) \neq P(6)$.

Example 24. Find all integers n such that $P(n) = 64$

Solution: $n = n^{\frac{d(n)}{2}} = 64 = 2^6$

$n^{d(n)} = 2^{12}$

Write $n = 2^{a_1}$,

Since, $d(n) = d(2^{a_1}) = a_1 + 1,\ 2^{a_1(a_1+1)}$

$= 2^{12}$ gives $a_1(a_1 + 1) = 12$

Thus, $n = 30$ or, $n = -4$. Hence $a = 2^3 = 8$.

Example 25. If $n > 2$, prove that between n and $n!$ there exists at least one prime number.

Solution: Suppose

$p_1, p_2, ..., p_k$ are primes not greater than n and $q = p_1 . p_2 . .., p_k$

Now q has a prime factor p different from p_i, thus

$p > n$ and $p < q < n! - 1 < n!$

4.8 SOME PROPERTIES OF ARITHMETIC FUNCTIONS

Remark: Many sums can be expressed as double sums.

Lemma 4.15. Let f and g be two arithmetic functions and $m, n \in \mathbb{N}$, then,

Then, $\sum_{d|m,\, D|n} f(d)\, g(D) = \sum_{j=1,2,..,s,\, k=1,2,..,t} f(d_j)\, g(D_k)$

$$
\begin{aligned}
& f(d_1)g(D_1) + f(d_1)\, g(D_2) + ... + f(d_1)g(D_t) \\
& f(d_2)g(D_1) + f(d_2)\, g(D_2) + ... + f(d_2)g(D_t) \\
= & f(d_3)g(D_1) + f(d_3)\, g(D_2) + ... + f(d_3)g(D_t) \\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
& f(d_s)g(D_1) + f(d_s)\, g(D_2) + ... + f(d_s)g(D_t) \\
= & [f(d_1) + f(d_2) + ... + f(d_s)][g(D_1) + g(D_2) + ... + g(D_t) \\
= & \sum_{1 \le j \le s} f(d_j) \times \sum_{1 \le k \le t} d(D_k) = \sum_{d|m} f(d) \times \sum_{D|n} g(D)
\end{aligned}
$$

Hence, $\sum_{d|m,\, D|n} f(d)\, g(D) = \sum_{d|m} f(d) \times \sum_{D|n} g(D)$.

Lemma 4.16. Let $S_1 = \{d_1, d_2, ..., d_k\}$ is the set of positive divisors of m

And $S_2 = \{e_1, e_2, ..., e_1\}$ is the set of positive divisors of n.

If $(m, n) = 1$, then, the set

$S = \{d_i e_j \mid d_i\ S_1,\ e_j\ S_2\}$ is the set of positive divisors of mn without repetition.

Proof: To prove this lemma we are to show

(i) $d_i e_j \mid mn\ \forall\ i, j$ ($d_i e_j$ are divisor)

(ii) If $d_r e_s = d_l e_m$ then $r = l$, $s = m$ (no repetition)

(iii) if $f \mid mn$ then $f = d_i e_j$ for some i, j(no other divisor)

(i) If $d_i \mid m$, $\forall i$, $e_j \mid n$, $\forall j$ then $d_i e_j \mid mn \quad \forall i, j$

(ii) If $d_i e_j = d_r e_s$ then $d_i \mid d_r e_s \quad \therefore \quad d_i \mid d_r$ [since, $(d_i, e_s) = 1$ for $(m, n) = 1$]

Similarly we can show that $d_r \mid d_i$

$\therefore \qquad d_i = d_r$ or, $i = r$

Similarly $j = s$.

(iii) $f \mid mn$

Let, $(f, m) = d$.

Then, $d \mid m$ or, $d = d_i$ for some i

Again $d \mid f$ gives $f = d \times$(some integer) $= d_i e$, say.

If we can show that this $e \in S_2$ i.e., $e \mid n$ then we are through.

Now $(f, m) = d$

or $\left(\frac{f}{d}, \frac{m}{d}\right) = 1$

or $(e, d_k) = 1$

And $f \mid mn$ gives $d_i e \mid mn$

or $e \mid \frac{m}{d} n = d_k n.$

$\therefore \quad e \mid d_k n$ and also, $(e, d_k) = 1$

$\therefore \quad e \mid n$ and so, $e = e_j$, for some $j \in \{1, 2, ..., s\}$.

$\therefore \quad f = d_i e_j$.

Theorem 4.17. If $f(n)$ is a multiplicative arithmetic function then so is also $\sum_{d \mid n} f(d)$

Proof: Let, $F(n) = \sum_{d \mid n} f(d)$.

We prove that $F(n)$ is multiplicative.

Let S_1, S_2, S be as in the lemma. 4.16.

We are to prove $F(m)\ F(m) = F(mn)$ if $(m, n) = 1$ and if $f(n)$ is multiplicative.

$$F(m)F(m) = \left(\sum_{d|m} f(d) \times \sum_{d|n} f(d)\right) = \left(\sum_{1\le i\le k} f(d_i) \times \sum_{1\le j\le l} f(e_j)\right)$$

$$= \sum_{1\le i\le k,\, 1\le j\le l} f(d_i)f(e_j) = \sum_{d_i \varepsilon S_1, e_j \varepsilon S_2} f(d_i e_j)$$

$$= \sum_{d_i e_j \varepsilon S} f(d_i e_j) = \sum_{D|mn} f(D)$$

$$\therefore \quad F(mn) = F(m)F(n).$$

Corollany 4.18. Prove that $\sigma(n)$ is multiplicative

$$\sigma(n) = \sum_{d|n} d, \text{ and } f(n) = n \text{ which is obviously multiplicative.}$$

$$\therefore \quad \sum_{d|n} f(d) = \sum_{d|n} d$$

is also multiplicative,

Thus $\sigma(n)$ is multiplicative.

Example 26. The identity function $e(n) = \left[\frac{1}{n}\right]$ is totally multiplicative.

Solution: Take any $m, n \in \mathbb{N}$

(i) If $m > 1$, $n > 1$

$$\text{then } e(mn) = \left[\frac{1}{mn}\right] = 0 = 0.0$$

$$= \left[\frac{1}{m}\right]\left[\frac{1}{n}\right]$$

$$= e(m)e(n)$$

(ii) If $m = 1$, $n > 1$

$$\text{then } e(mn) = \left[\frac{1}{mn}\right] = 0 = 1.0 = \left[\frac{1}{m}\right]\left[\frac{1}{n}\right]$$

(iii) If $m = n = 1$,

$$\text{then } e(mn) = \left[\frac{1}{mn}\right] = 1 = 1.1 = \left[\frac{1}{m}\right]\left[\frac{1}{n}\right] = e(m)\, e(n).$$

Note: It is already seen that $\phi(n)$, $\sigma(n)$ $d(n)$ are all multiplicative, but $P(n)$ is not. Moreover none of them is totally multiplicative.

Definition: If $f(n)$ and $g(n)$ are two arithmetic functions then their product and quotient are defined as follows:

$$(fg)(n) = f(n)\, g(n) \text{ and } \left(\frac{f}{g}\right)(n) = \frac{f(n)}{g(n)}$$

Example 27. $(fg)(n)$ and $\left(\frac{f}{g}\right)(n)$ are multiplicative as well as totally multiplicative if f and g both are so. (left as an exercise).

Theorem 4.19. If f is any arithmetic function such that f is multiplicative then $f(1) = 1$

Proof: (left as an exercise).

Theorem 4.20. f is an arithmetic function such that $f(1) = 1$;

Then

(i) f is multiplicative if and only if

$$f(p_1 \cdots p_r)^r = f\left(p_1^{a_1}\right) \cdots f(p_r^{a_r})$$

for all primes p_i and $a_i \geq 1$

(ii) If f is multiplicative, then f is completely (totally) multiplicative if and only if

$$f(p^\alpha) = f(p)^\alpha \text{ for all primes } p \text{ and all integers } a \geq 1$$

Proof (left as an exercise).

Definition: Let A denote the set of A.F's. then obviously $A \neq \Phi$

Let us define an operation * (called convolution) on A such that

$$f * g(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)$$

Properties 4.21. $f * g = g * f$. [* is commutative]

$$\begin{aligned} f * g(n) &= \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) \\ &= \sum_{d|n} f\left(\frac{n}{d}\right) g(d) \\ &= g * f(n) \end{aligned}$$

or $$f * g = g * f$$

Properties 4.22. If f and g are multiplicative arithmetic function then so is also $f * g$

Proof: [Remember the **Lemma 4.16:** Let $(m, n) = 1$ If $S_1 = \{d_1, d_2, d_3, \ldots, d_k\}$ and $S_2 = \{e_1, e_2, e_3, \ldots, e_l\}$ are the sets of divisors of m and n respectively, Then $S = \{d_i e_j \mid d_i \in S_1, e_j \in S_2\}$ is the set of divisors of mn without repetition.]

Then, $(f * g)(m) \times (f * g)(n)$

$$= \sum_{d|m} f(d)\, g\left(\frac{m}{d}\right) \times \sum_{e|n} f(e)\, g\left(\frac{n}{e}\right)$$

$$= \sum_{1 \leq i \leq k} f(d_i) g\left(\frac{m}{d_i}\right) \times \sum_{1 \leq j \leq l} f(e_j) g\left(\frac{n}{e_j}\right)$$

$$= \sum_{1 \le i \le k, 1 \le j \le l} f(d_i) g\left(\frac{m}{d_i}\right) f(e_j) g\left(\frac{n}{e_j}\right)$$

$$= \sum_{1 \le i \le k, 1 \le j \le l} f(d_i)(e_j) g\left(\frac{m}{d_i}\right) g\left(\frac{n}{e_j}\right)$$

$$= \sum_{1 \le i \le k, 1 \le j \le l} f(d_i\, e_j) g\left(\frac{mn}{d_i e_j}\right)$$

$$= \sum_{D \mid mn} f(D)\, G\left(\frac{mn}{D}\right)$$

$$= (f * g)(mn)$$

or $f * g$ is multiplicative

Properties 4.23. * is associative [i.e., $(f * g)*h = f* (g*h)$]

Proof: $((f * g) * h)(n) = \sum_{d \mid n} (f * g)(d)\, h\left(\frac{n}{d}\right)$

$$= \sum_{de = n} (f * g)(d) h(e)$$

$$= \sum_{de = n} h(e)(f * g)(d)$$

$$= \sum_{de = n} h(e) \sum_{k \mid d} f(k) g\left(\frac{d}{k}\right)$$

$$= \sum_{de = n} h(e) \times \sum_{d = kl} f(k) g(l)$$

$$= \sum_{de = n,\, kl = d} h(e) f(k) g(l)$$

$$= \sum_{n = kle} h(e) f(k) g(l)$$

$$= \sum_{km = n} f(k) \sum_{le = m} g(l) h(e)$$

$$= \sum_{km = n} f(k) \times \sum_{l \mid m} g(l) h\left(\frac{m}{l}\right)$$

$$= \sum_{km = n} f(k) . g * h(m)$$

$$= \sum_{k \mid n} f(k) . \left(g * h\left(\frac{n}{k}\right)\right)$$

$$= (f * g * h))(n)$$

or $(f * g) * h = f*(g * h)$.

Properties 4.24. Existence of identity:

If f is any arithmetic function and e is such that

$$e(n) = \begin{cases} 1 \text{ for } n = 1 \\ 0 \text{ for } n \neq 1 \end{cases}$$

$$\text{then } (f*e)(n) = \sum_{d|n} f(d)e\left(\frac{n}{d}\right)$$

$$= f(1)e(n) + f(d_1)e\left(\frac{n}{d_1}\right) + \ldots + f(n)e\left(\frac{n}{n}\right)$$

$$= f(1)0 + f(d_1).0 + \ldots + 0 + f(n).1$$

$$= \ldots$$

$$= 0 + f(n).1$$

$$= f(n)$$

$$= f(n)$$

or, $f * e = \text{If}$

Similarly we can show that $f = e * f$

Therefore, e is the identity with respect to $*$.

Note: $I(n) = 1 \ \forall \ n \in \mathbb{N}$, which is an arithmetic function

Then $$(f * 1)(n) = \sum_{d|n} f(d) I\left(\frac{n}{d}\right) = \sum_{d|n} f(d) = (I * f)(n)$$

Definition: If $f * g = e = g * f$ then g is said to be inverse of f and is written as $g = f^{-1}$

Remark: (1) For every arithmetic function its inverse may not exist

(2) A, the set of arithmetic functions is a commutative semi group under $*$

Note: If we define the operation addition as $(f \oplus g)(n) = f(n) + g(n)$, then A will be an *integral Domain* under $\oplus$ and $*$(proof is left as an exercise.)

Theorem 4.25. An arithmetic function f has a multiplicative inverse if ad only if $f(1) \neq 0$. If an inverse exists it is unique.

Proof: Suppose f has an inverse g.

Then $f * g = e$

And $f(1)g(1) = (f * g)(1) = e(1) = 1$ gives $f(1) \neq 0$

Conversely

Suppose, $f(1) \neq 0$ then from $f(1)g(1) = f * g(1) = 1$ we get $g(1)$

Now we calculate

$g(2)$ as follows:

$$0 = e(2) = (f * g)(2) = f(2)g(1) + f(1)g(2) \text{ gives } f(1)g(2) = -f(2)g(1) \text{ or, } g(2) = -\frac{f(2)g(1)}{f(1)}$$

This way we evaluate $g(j)$ (for $j = 1, 2, ..., n-1$)

Then we note: $0 = e(n) = (f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$

In the RHS expression $g(n)$ occurs only in one term viz. $f(1)g(n)$.

Hence the above equation can be solved uniquely for $g(n)$

Thus the result follows.

Note: the product * defined above is known as Dirichlet product.

The Dirichlet product of two totally multiplicative functions need not be totally multiplicative.

Theorem 4.26. If g and $f * g$ both are multiplicative, then f is also multiplicative.

[g and $f * g$ multiplicative $\Rightarrow f$ multiplicative]

Proof: Suppose f is not multiplicative and $h = f * g$

Since f is not multiplicative, we have two positive integers m, n with $(m, n) = 1$ such that $f(mn) \neq f(m)f(m)$

Consider $\{mn \mid m, n \in N, (m, n) = 1 \text{ and } f(mn) \neq f(m)f(m)\}$

And choose the smallest of this set, say mn

I. If $mn = 1$, then $f(1) \neq f(1)f(1)$ gives $f(1) \neq 1$.

Now $h(1) = f(1)g(1)$

or $1 = f(1)$ [since g and h are multiplicative,], a contradiction

Thus h is not multiplicative.

II. If $mn > 1$, then,

$f(ab) = f(a)f(b)$ for all positive integers a and b with $(a, b) = 1$ and $ab < mn$

$$h(mn) = \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(ab)g\left(\frac{mn}{ab}\right) + f(mn)g(1)$$

$$= \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(a)f(b)g\left(\frac{m}{n}\right)g\left(\frac{n}{b}\right) + f(mn)$$

$$= \sum_{a|m} f(a)g\left(\frac{m}{n}\right) \sum_{b|n} f(b)g\left(\frac{n}{b}\right) - f(m)f(n) + f(mn)$$

$$= h(m)h(n) - f(m)f(n) + f(mn)$$

$$\neq h(m)h(n) \quad \text{[Since } f(mn) \neq f(m)f(n) \text{ in general]}$$

And we meet a contradiction.

Hence, f is multiplicative.

Note: As for each f we have a g such that $f * g = e$ and if f is multiplicative, by what we have proved above g is also multiplicative. Thus we get the

Theorem 4.27. If f is multiplicative then so is its inverse f^{-1}.

Theorem 4.28. Given that f is a multiplicative arithmetic function.

f is totally multiplicative if and only if $f^{-1}(n) = \mu(n)f(n)$ for all $n \geq 1$

Proof: Assume that f is totally multiplicative and $h(n) = \mu(n)f(n)$

Now,

$$(h * f)(n) = \sum_{d|n} h(d) f\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} \mu(d) f(d) f\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} \mu(d) f\left(d \times \frac{n}{d}\right) \quad [f \text{ is totally multiplicative}]$$

$$= \sum_{d|n} \mu(d) f(n)$$

$$= f(n) \sum_{d|n} \mu(d)$$

$$= f(n)e(n)$$

$$= e(n) \qquad [\text{for } f(1) = 1,\ e(n) = 0 \text{ for } n > 1]$$

Hence, $h = f^{-1}$

Conversely,

Suppose $f^{-1}(n) = \mu(n)f(n)$

To show that f is totally multiplicative, it is sufficient to show that

$f(p^a) = f(p)^a$ [for prime powers].

Now $f^{-1}(n) = \mu(n)f(n)$

or $(f * f^{-1})(n) = e(n)$

or $$\sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0 \qquad [n > 1]$$

or $$\sum_{d|n} f\left(\frac{n}{d}\right) \mu(d) f(d) = 0$$

Now taking $n = p^a$, we have

$$\mu(1) f(1) f(p)^a + \mu(p) f(p) f(p^{a-1}) = 0$$

And this gives $f(p^a) = f(p)\, f(p^{a-1})$.

Hence, $f(p^a) = f(p)^a$

So, f is totally multiplicative.

4.9 MOBIUS INVERSION FORMULA (MIF)

Theorem 4.29. $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$

Proof: For $n = 1$ the result is trivial.

For $n > 1$ the proof will be by induction on different prime factors

I. Suppose $n = p^a$

Then, $$\sum_{d|p^a} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^a)$$
$$= 1 + (-1) + 0 + \ldots + 0$$
$$= 1 - 1 = 0$$

II. Assume that the result is true for integers with at most k distinct prime factors. i.e. suppose

$n = \alpha p^a$, where α is an integer with k distinct prime factors and $p \nmid \alpha$.

Now,

$$\sum_{d|n} \mu(d) = \sum_{d|\alpha} \mu(d) + \sum_{d|\alpha} \mu(pd) + \sum_{d|\alpha} \mu(p^2 d) + \ldots + \sum_{d|\alpha} \mu(p^a d)$$
$$= \sum_{d|\alpha} \mu(d) + \sum_{d|\alpha} \mu(p)\mu(d) + \sum_{d|\alpha} \mu(p^2)\mu(d) + \ldots + \sum_{d|\alpha} \mu(p^a)\mu(d)$$
$$= \sum_{d|\alpha} \mu(d) - \sum_{d|\alpha} \mu(d) = 0.$$

Theorem 4.30. Mobius inversion formula: $F(n) = \sum_{d|n} f(d)$ if and only if

$$f(n) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)F\left(\frac{n}{d}\right)$$

Proof: $(f * I)(n) = \sum_{d|n} f(d) I\left(\frac{n}{d}\right)$

$$= \sum_{d|n} f(d)$$

or $$F(n) = \sum_{d|n} f(d) = (f * I)(n),$$

so $$F = f * I.$$

Then, $$F * \mu = (f * I) * \mu = f * (I * \mu) \qquad [I * \mu = e]$$
$$= f * e = f$$

or $$f(n) = (F * \mu)(n)$$
$$= \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right)$$

Next, we have, $f(n) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right) = (F^* \mu)(n)$

or $f = F^* \mu.$

or $f^* I = (F^* \mu)^* I$

$= (F^* (\mu^* I)$

$= F^* e$

$= F$

or $F(n) = (f^* I)(n)$

$= \sum_{d|n} f(d) I\left(\frac{n}{d}\right)$

$= \sum_{d|n} f(d).$

Definition: If $f(n)$ and $g(n)$ are two arithmetic functions satisfying the condition $f(n) = \sum_{d|n} g(d)$, then we say that $\{f(n), g(n)\}$ is a Mobius pair.

Theorem 4.31. If one of the functions in the Mobius pair $\{f(n), g(n)\}$ is multiplicative, so is the other.

Proof: Suppose $g(n)$ is multiplicative, and assume

$(m, n) = 1$

since $(m, n) = 1$ and $e \mid m$, $h \mid n$, then $(e, h) = 1$

Then by Theorem 4.17 $f(n)$ is multiplicative

Suppose,

$f(n)$ is multiplicative. Now by MIF

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

$$\therefore \quad g(mn) = \sum_{d|mn} \mu(d) f\left(\frac{mn}{d}\right)$$

As above,

$$g(mn) = \sum_{e|m} \sum_{h|n} \mu(eh) f\left(\frac{mn}{eh}\right) = \sum_{e|m} \sum_{h|n} \mu(e)\mu(h) f\left(\frac{m}{e}\right) f\left(\frac{n}{h}\right)$$

[f is multiplicative]

$$= \sum_{e|m} \mu(e) f\left(\frac{m}{e}\right) \sum_{h|n} \mu(h) f\left(\frac{n}{h}\right)$$

$$= g(m)\, g(n).$$

Hence g is multiplicative.

Theorem 4.32. The pairs

$\{n, \varphi(n)\}$, $\{d(n), 1\}$ and $\{\sigma(n), n\}$ are all Mobius pairs.

Proof: We know that

$$n = \sum_{d|n} \phi(d) \text{ and } d(n) = \sum_{d|n} 1$$

and $$\sigma(n) = \sum_{d|n} d$$

Thus by definition of Mobius pair the given pairs are all Mobius pairs.

Example 28. Prove that if $f(n)$ is multiplicative, then

$$\sum_{d|n} \mu(d) f(d) = \prod_{p|n} \{1 - f(p)\}$$

Solution: As $f(n)$ and $\mu(n)$ are multiplicative, so is also their product $\mu(n).f(n)$

Now the pair $F(n)$ and $\mu(n).f(n)$ form a Mobius pair, where $F(n) = \sum_{d|n} \mu(d) f(d)$

We note that

If p is a prime then,

$$[F(p^a) = \sum_{d|p^a} \mu(d) f(d)$$

$$= \mu(1) f(1) + \mu(p) f(p) + \mu(p^2) f(p^2) + \ldots + \mu(p^a) f(p^a)$$

$$= f(1) - f(p) = 1 - f(p), \text{ for nonzero multiplicative function } f(1) = 1]$$

Now suppose,

$$n = p^a q^b \ldots r^c, \text{ then}$$

$$F(n) = F(p^a q^b \ldots r^c) = F(p^a).F(q^b) \ldots F(r^c) = \{1 - f(p)\}\{1 - f(q)\} \ldots \{1 - f(r)\}$$

$$= \prod_{p|n} \{1 - f(p)\}$$

Example 29. Prove that

$$n = \sum_{d|n} \mu(d) \sigma\left(\frac{n}{d}\right)$$

Solution By definition: $\sigma(n) = \sum_{d|n} d$

Applying MIF, we get,

$$n = \sum_{d|n} \mu(d) \sigma\left(\frac{n}{d}\right).$$

Example 30. Prove that $1 = \sum_{k|n} \mu(d) d\left(\frac{n}{k}\right)$

Solution: We have, $d(n) = \sum_{k|n}$, $(1 = k^0)$

or $$1 = \sum_{k|n} d(k)\mu\left(\frac{n}{k}\right) = \sum_{k|n} \mu(k) d\left(\frac{n}{k}\right).$$

Example 31. Prove that $\sum_{m|n} \mu(m)\left[\frac{n}{m}\right] = 1$ valid for all n.

Note: $\left[\frac{n}{m}\right]$ = the greatest integer ($\leq \frac{n}{m}$).

Solution: We have $\sum \mu(d) = \begin{matrix} 1 \text{ if } n = 1 \\ 0 \text{ if } n > 1 \end{matrix}$

or $$\sum_{d|1} \mu(d) + \sum_{d|2} \mu(d) + \ldots + \sum_{d|n} \mu(d) = 1 \qquad \ldots(*)$$

Now integers $\leq n$ and divisible by m, are m, $2m$, $3m$, ... $\left[\frac{m}{n}\right] m$

$\therefore$ when we break up (*)

$\mu(1)$ will occur $\left[\frac{n}{1}\right]$ times

$\mu(2)$ ..... $\left[\frac{n}{2}\right]$ .....

$\mu(3)$ ..... $\left[\frac{n}{3}\right]$ .....

$\mu(n)$ ..... $\left[\frac{n}{n}\right]$

Rearranging (*) we get,

$$\mu(1) \times \left[\frac{n}{1}\right] + \mu(2) \times \left[\frac{n}{2}\right] + \ldots + \mu(n) \times \left[\frac{n}{n}\right] = 1,$$

or $$\sum \mu(m) \times \left[\frac{n}{m}\right] = 1.$$

Example 32. Prove that $\sum_{d|n}(-1)^d \phi(d) = n - 2m$ [m is the largest odd divisor]

Solution:

Case I: Let n be odd.

$\therefore$ in this case $m = n$.

Since n is odd, each divisor d is also odd.

Then $\sum(-1)^d \Phi(d) = -\sum\Phi(d)$

$= -n$

$= n - 2n = n - 2m$, where $m = n$ is the largest odd divisor.

Case II: Let n be even and $n = 2^\alpha m$, where $2^\alpha \mid\mid n$

and

$\therefore$ m is odd

Now if d is an odd divisor of n(and this is a divisor of m) then

$$\sum_{d|n}(-1)^d \Phi(d) = \sum_{d|m}(-1)^d = \{(-1)^1 \Phi(1) + ... + (-1)^m \Phi(m)\}$$

And if d is an even divisor of n hen

$$\sum_{d|m}(-1)^d \Phi(d) = (-1)^2 \phi(2) + ... + (-1)^{2^\alpha . m} \Phi(2^\alpha m)$$

In general

$$\sum_{d|m}(-1)^d \Phi(d) = \{(-1)^1 \Phi(1) + ... + (-1)^m \Phi(m)\} + \{(-1)^2 \phi(2) + ... + (-1)^{2^\alpha . m} \Phi(2^\alpha m)$$

$$= -[\Phi(1) + ... + \Phi(m)] + [\Phi(2) + ... + \Phi(2^\alpha m)]$$

$$= [\Phi(1) + ... + \Phi(m) + \Phi(2) + ... + (2^\alpha m)] - 2[\Phi(1) + ... + \Phi(m)]$$

$$= \sum_{d|n}\phi(d) - 2\sum_{d|n}\phi(d)$$

$$= n - 2m.$$

Example 33. $\sum_{d|n}\phi(d) = n$, deduce that

$$\text{if } |x| < 1, \text{ then } \sum\phi(n)\frac{x^n}{1-x^n} = \frac{x}{(1-x)^2}$$

Solution:

$$\text{LHS} = \sum_{n=1}^{\infty}\frac{\phi(n)}{1-x^n}x^n$$

$$= \sum_{n=1}^{\infty}\phi(n)\,x^n(1-x^n)^{-1}$$

$$= \sum\Phi(n)x^n[1 + x^n + x^{2n} + x^{3n} + ...]$$

$$= \Phi(1)[x + x^2 + x^3 + ...] + \Phi(2)[x^2 + x^4 + x^6 + ...]$$
$$+ \Phi(3)[x^3 + x^6 + x^9 + ...] + ...$$
$$= \Phi(1).x^1 + [\Phi(1) + \Phi(2)]x^2 + [\Phi(1) + \Phi(3)]x^3$$
$$+ [\Phi(1) + \Phi(2) + \Phi(4)]x^4 + ...$$
$$= \sum_{d|1} \phi(d)x + \sum_{d|2} \phi(d)x^2 + \sum_{d|3} \phi(d)x^3 + ...$$
$$= x + 2x^2 + 3x^3 + 4x^4 + ...$$
$$= x[x + 2x + 3x^2 + ...]$$
$$= x(1 - x)^{-2}.$$

Example 34. We know that $n = \sum_{d|n} \phi(d) = \sum_{d|n} \phi\left(\frac{n}{d}\right)$ and $F(n) = \sum_{d|n} f(d)$ gives

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

Then, $$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d} m \frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}.$$

Example 35. Prove that $\frac{n}{\phi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}$

Solution: We know that $\mu(n)$ and $\phi(n)$ are multiplicative and $\phi(n) \neq 0$, $\frac{\mu^2(n)}{\phi(n)}$ is multiplicative and thus $\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = G(n)$ is also multiplicative (by Theorem 4.17)

So, If $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$, then

$$G(n) = G\left(p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}\right) = G\left(p_1^{\alpha_1}\right) G\left(p_2^{\alpha_2}\right) .... G\left(p_r^{\alpha_r}\right)$$

[**Note:** for a prime p and $\alpha \in \mathbb{N}$

$$G(p^\alpha) = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{\mu^2(1)}{\phi(1)} + \frac{\mu^2(p)}{\phi(p)} + ... + \frac{\mu^2(p^\alpha)}{g(p^\alpha)}$$
$$= 1 + \frac{(-1)^2}{p-1} + 0 + 0 ... + 0 = 1 + \frac{1}{p-1} = \frac{1}{1-\frac{1}{p}}]$$

$$\therefore \quad G(n) = \frac{1}{1-\frac{1}{p_1}} ... \frac{1}{1-\frac{1}{p_r}} = \frac{n}{n\left(1-\frac{1}{p_1}\right)...\left(1+\frac{1}{p_r}\right)} = \frac{n}{\phi(n)}$$

EXERCISES 4.1

1. Prove that the number of divisors of n is odd if and only if n is a perfect square. If the integer $k \geq 1$, prove that $\sigma_k(n)$ is odd if and only if n is a square or double a square.
2. Given an integer $n > 1$, prove that there are infinitely many integers x satisfying $d(x) = n$
3. Prove that if $(a, b) > 1$, then $\sigma_k(ab) < \sigma_k(a)\,\sigma_k(b)$ and $d(ab) < d(a)\,d(b)$
4. Prove that if n has r distinct prime factors, then $\varphi(n) \geq n^{2^{-r}}$. Prove that there are infinitely many integers for which $\varphi(n)$ is a perfect square.
5. Evaluate $\varphi(19)$, $\varphi(49)$, $\varphi(243)$ and $\varphi(1024)$,
6. Find the least positive integers n such that
   $(a)\ \varphi(n) \geq 100$, $(b)\ \varphi(n) \geq 1000$, $(c)\ \varphi(n) \geq 10000$, $(d)\ \varphi(n) \geq 100000$
7. Show that if m and n are positive integers with $m \mid n$ then, $\varphi(m) \mid \varphi(n)$.
8. Prove that $\sigma(n) \equiv d(m) \pmod 2$ where m is the largest odd factor of n
9. If $\sigma(n) = 2n$ then, n is a perfect number. Prove that if n is a perfect number, then
$$\sum_{d \mid n} \frac{1}{d} = 2$$
10. Evaluate $\sigma(210)$, $\varphi(100)$, and $\sigma(990)$
11. Evaluate $d(47)$, $d(63)$, and $d(150)$
12. Prove that for each integer n, there exist integers n_1 and n_2 such that
$$d(n_1) + d(n_2) = n.$$
13. Prove that there are infinitely many integers n for which $\varphi(n)$ is a multiple of 10.
[**Hint:** $\varphi(11^n) = 11^n - 11^{n-1} = 11^{n-1}.10$]
14. Prove that there are infinitely many integers n for which $\varphi(n)$ is a perfect square.
[**Hint:** $\varphi(2^{2n+1}) = 2^{2n+1} - 2^{2n} = 2^{2n}(2-1) = 2^{2n} = (2n)^2$]
15. Prove that $\dfrac{\sigma(n)}{d(n)} \geq \prod_{d \mid n} d^{\frac{1}{d(n)}}$ [Use arithmetic mean is greater than or equal to the geometric mean.]
16. If d is a positive divisor of a positive integer m, then prove that the number of integers in the complete residue system modulo m, which with m, have the greatest common divisor d, is $\phi\left(\dfrac{m}{a}\right)$
17. Show that $\sum_{d \mid n} \phi(d)\mu(d) = 0$ if and only if n is even.
18. If m is odd, find m.
$$\phi(m) = m \sum_{d \mid m} \frac{\mu(d)}{d} = \sum_{d \mid m} \mu\left(\frac{m}{d}\right) d$$

19. If $\phi(m)$ is odd, find m.

20. Show that there is no integer m such that $\phi(m) = 14$.

21. If m is a positive integer, prove that

$$\phi(2m) = \begin{matrix} \phi(m) & \textit{when } m \textit{ is odd} \\ 2\phi(m) & \textit{when } m \textit{ is even} \end{matrix}$$

22. Prove that the necessary and sufficient condition that a positive integer equals the product of all its positive divisors (excluding itself) is that this positive integer be a cube of a prime number or a product of two distinct primes.

23. Find all positive integers x, such that

$$x^{\phi(y)} = y$$

24. Prove that for any prime p and $n = 4,6,22$ the following congruence is satisfied $n\,\sigma(n) \equiv 2 (\text{mod } \phi(n))$

25. Find all positive integers m and prime numbers p such that $\phi(m) = \dfrac{m}{p}$

26. Prove that for any integer k, however large it may be, there exist infinitely many numbers a such that no one of

$$a + 1, \ldots, a + k - 1 \text{ is prime}$$

27. Find the six smallest even perfect numbers

28. Find the six smallest abundant positive integers.

29. Show that any multiple of an abundant or a perfect number, other than the perfect number itself, is abundant.

30. Two positive integers m and n are called an amicable pair if $\sigma(m) = \sigma(n) = m + n$. Show that each of the following pairs of integers are amicable pairs.

(a) 220, 284

(b) 1184, 1210

(c) 79750, 88730

31. Show that if $n = p^q m^2$ is an odd perfect number where p is prime, then $n \equiv p (\text{mod } 8)$

32. A positive integer is superfect of $\sigma(\sigma(n)) = 2n$

Show that

(i) 16 is superfect

(ii) If $n = 2^q$ where $2^{q+1} - 1$ is prime, then n is superfect.

(iii) Every even superfect number is of the form $n = 2^q$ where $2^{q+1} - 1$ is prime.

EXERCISES 4.2

1. If f is multiplicative then prove that

(i) $f^{-1}(n) = \mu(n) f(n)$ for every square free n.

(ii) $f^{-1}(p^2) = f(p)^2 - f(p^2)$ for every prime p.

2. Assume that f is multiplicative. Prove that f is totally multiplicative if and only if, $f^{-1}(p^a) = 0$ for all primes p and all integers $a \geq 2$.
3. If f is completely multiplicative, prove that
   $f(g * h) = (f . g)*h$, for all arithmetic functions g and h, where f.g denotes the ordinary product $(f.g)(n) = f(n)g(n)$
4. If f is multiplicative and if $f.(\mu^* \mu^{-1}) = (f.\mu)^* (f.\mu^{-1})$, then f is totally multiplicative.
5. If f is totally multiplicative, prove that
   $$(f.g)^{-1} = f.g^{-1}, \text{ for all arithmetic function } g \text{ with } g(1) \neq 0$$
6. If f is multiplicative and $(f.\mu^{-1})^{-1} = f.\mu$, then prove that f is totally multiplicative.
7. A multiplicative function is called *strongly multiplicative* if $f(p^k) = f(p)$ for every prime p

   Show that $f(n) = \dfrac{\phi(n)}{n}$ is strongly multiplicative.
8. Show that $\sum_{t|n} \dfrac{\mu(t)}{t} = \prod_p \dfrac{p-1}{p}$, where p runs over the prime divisors of n
9. Suppose $f(n)$ and $g(n)$ are multiplicative and that $f(p^r) = g(p^r)$ for each r and each prime p. Prove that $f(n) = g(n)$ for all n.
10. Prove that the following pairs
    $$\{n, \varphi(n)\}, \{d(n), 1\} \text{ and } \{\sigma(n), n\} \text{ are all Mobius pairs.}$$
11. Prove that if $f(n)$ is multiplicative, then
    $$\sum_{d|n} \mu(d) f(d) = \prod_{p|n} \{1 - f(p)\}$$

EXERCISES 4.3

1. Prove that $\sum_{d|n} \mu(d) \dfrac{n}{d} = n \prod_{p|n} \left(1 - \dfrac{1}{p}\right)$.
2. For each positive integer n, show that $\mu(n)\ \mu(n+1)\ \mu(n+2)\ \mu(n+3) = 0$
3. For any integer $n \geq 3$, show that $\sum_{k=1} \mu(k!) = 1$
4. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ be the prime factorization of the integer $n > 1$. If f is a multiplicative function that is not identically zero, prove that
   $$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)) \ldots (1 - f(p_r))$$
5. Let $S(n)$ denote the number of square free divisors of n. Establish that
   $$S(n) = \sum_{d|n} |\mu(d)| = 2^{\omega(n)}$$
   where $\omega(n)$ is the number of distinct prime divisors of n.

6. The function λ is defined such that

$\lambda(1) = 1$ and $\lambda(n) = (-1)^{k_1+k_2+\ +k_r}$, if the prime factorization of $n > 1$ is

$$n = p_1^{\alpha_1}\ p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

Prove that

(a) λ is multiplicative

(b) Given a positive integer n, verify that

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 \text{ if } n = m^2 \text{ for some integer } m \\ 0 \text{ otherwise} \end{cases}$$

[The function λ is known as the Liouville λ-function]

5

FAREY SEQUENCES, CONTINUED FRACTION, PELL'S EQUATIONS

5.1 FAREY SEQUENCE

Farey, a mineralogist, wrote down the following ordered pattern of non negative reduced fractions between 0 and 1, with denominators limited by a number n - called *the order of this chain of fractions known as the Farey Sequence* (F.S.).

$$F_1 : \frac{0}{1}, \frac{1}{1}$$

$$F_2 : \frac{0}{1}, \frac{1}{2}, \frac{1}{1}$$

$$F_3 : \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$$

$$F_4 : \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}$$

$$F_5 : \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}$$

$$F_6 : \frac{0}{1}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{1}{1}$$

etc.,

....

We have constructed the above table in the following way:

In the first row we write $\frac{0}{1}$

For $n = 2, 3, \ldots$

We use the following rule:

1. Form the n^{th} row by copying the $(n-1)^{st}$ in order, but insert the fraction $\frac{a+a'}{b+b'}$ between the consecutive fractions $\frac{a}{b}$ and $\frac{a}{b'}$ of the $(n-1)^{st}$ row if $b + b' \leq n$. Thus, since $1 + 1 \leq 2$ we insert $\frac{0+1}{1+1}$ between $\frac{0}{1}$ and $\frac{1}{1}$ and obtain $\frac{0}{1}, \frac{1}{2}, \frac{1}{1}$, for the 2^{nd} row. Similarly the 3^{rd} now.

2. To obtain the 4th row, we insert $\frac{0+1}{1+3}$ and $\frac{2+1}{3+1}$ but not $\frac{1+1}{3+2}$ and $\frac{1+2}{2+3}$ etc.

*all the fractions that appear are in reduced form

**all reduced fractions $\frac{a}{b}$ such that $0 \le \frac{a}{b} \le 1$ and $b \le n$ appear in the n^{th} row;

***if $\frac{a}{b}$ and $\frac{a}{b}$ are consecutive in the n^{th} row, then $ab' - a'b = 1$ and $b + b' > n$.

Definition: If $\frac{h}{k}$ and $\frac{l}{m}$ are two terms of an F.S. then $\frac{h+1}{k+m}$ is called the "mediant" between $\frac{h}{k}$ and $\frac{l}{m}$.

Theorem 5.1. No two consecutive terms of F_n have same denominator.

Proof: Case I If $k > 1$ and $\frac{h}{k}$ and $\frac{h'}{k}$ are two successive terms of F_n, having the same denominator then $h' > h$ (since, FS is an ordered sequence)

$\therefore \quad h + 1 \le h' \le k$

if $k \neq 1$

But then $$\frac{h}{k} < \frac{h}{k-1} < \frac{h+1}{k-1+1} = \frac{h+1}{k} \le \frac{h'}{k}$$

$\therefore$ $$\frac{h}{k} < \frac{h}{k-1} < \frac{h'}{k}$$

$\therefore$ the term $\frac{h}{k-1}$ comes between $\frac{h}{k}$ and $\frac{h'}{k}$

Since, $\frac{h}{k}$ and $\frac{h'}{k}$ are two consecutive terms, two consecutive terms cannot be with same denominators if $k > 1$.

Case II If $k = 1$, then 1st term $\frac{h}{k}$ will be $\frac{0}{1} = 0$, the next term is > 0,

$\therefore$ its numerator > 0

i.e., ≥ 1

and since, it is a proper fraction its denominator is ≤ 2

Therefore, *the two consecutive terms have different denominators.*

We state the following

Theorem 5.2. If $\frac{h}{k}$ and $\frac{h'}{k'}$ are two successive terms then $kh' - hk' = 1$

i.e., $$\begin{vmatrix} h & h' \\ k & k' \end{vmatrix} = -1$$

Theorem 5.3. If $\frac{h}{k}, \frac{h''}{k''}$ and $\frac{h'}{k'}$ are three successive terms of F_n, then $\frac{h''}{k''} = \frac{h+h'}{k+k'}$

The two theorems **5.2, 5.3** are equivalent

Theorem 5.4. Theorem 5.2 is true if and only if 5.3 is true.

Proof: (5.2)) ⇒ (5..3)

Assume Theorem **5.2.**

Therefore $\frac{h}{k}$ and $\frac{h'}{k'}$ being two consecutive terms

$$kh' - k'h = 1 \qquad \text{...(i)}$$

And $\frac{h''}{k''}, \frac{h'}{k'}$ being two consecutive terms

We get $k''h' - k'h'' = 1$ ...(ii)

Solving (i) and (ii) in terms of h'' and k''

we get $$\frac{h''}{k''} = \frac{h+h'}{k+k'}.$$

5.3 ⇒ 5.2

Proof: We assume that Theorem 5.3 is true.

[i.e., if $\frac{h}{k}, \frac{h''}{k''}, \frac{h'}{k'}$ are three consecutive terms in F.S., then $\frac{h''}{k''} = \frac{h+h'}{k+k'}$

We are to prove theorem 5.2. {i.e., if $\frac{h}{k}, \frac{h'}{k'}$ are two consecutive terms of an FS to prove

$$\begin{vmatrix} h & h' \\ k & k' \end{vmatrix} = -1$$

i.e., $h'k - hk' = 1$

Now $$F_1 = \frac{0}{1}, \frac{1}{1}$$

$\therefore$ $$\begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix} = -1,$$

$$F_2 = \frac{0}{1}, \frac{1}{2}, \frac{1}{1}$$

$\therefore$ $$\begin{vmatrix} 0 & 1 \\ 1 & 2 \end{vmatrix} = -1$$

$$\begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} = -1$$, i.e., the theorem 5.2 is true for $n = 1, 2$

Assume that the theorem is true for $n - 1$,

i.e., if $\frac{h}{k}, \frac{h'}{k'}$ are two consecutive terms of F_{n-1},

then $kh' - k'h = 1$ ...(i)

And to deduce that the theorem is true for n.

Let $\frac{h''}{k''}$ belongs to F_n but not to F_{n-1} and it lies in the interval $\left(\frac{h}{k}, \frac{h'}{k'}\right)$.

Obviously $k'' = n$, and both k, k' k''.

Since, the theorem 5.3 is true,

$\therefore$ $\frac{h''}{k''} = \frac{h}{k} + \frac{h'}{k'}$ and $\frac{h''}{k''}$ is irreducible

$\therefore$ $h + h' = \lambda h''$, $k + k' = \lambda k''$, $\lambda \in \mathbb{N}$

Now k and k' each less than k'' gives $k + k' < 2k''$ and $k + k' = \lambda k''$

$\therefore$ $\lambda = 1$

$\therefore$ $k + k' = k''$ and $h + h' = h''$.

Hence,

$$\begin{aligned} kh'' - k''h &= k(h + h') - h(k + k') \\ &= kh' - k'h \\ &= 1 \end{aligned}$$

Similarly $k''h' - k'h'' = 1$

Hence Theorem 5.2 is true for F_n.

Hence by method of induction, the theorem 5.2 is true for all $n \in \mathbb{N}$.

Theorem 5.5. Proof of theorem 5.2 and 5.3

Proof: As we may see easily that the theorems are true for F_1 and F_2

Assume that they are true for F_{n-1} and prove that they are true for F_n

Suppose that $\frac{h}{k}, \frac{h'}{k'}$ are two consecutive terms in F_{n-1} but separating $\frac{h''}{k''}$ in F_n.

$\therefore \frac{h}{k} < \frac{h''}{k''} < \frac{h'}{k'}$

From first inequality we get

$$k''h < h''k,$$

or $kh'' - k''h > 0$

or $kh'' - k''h = r > 0$

And similarly from the last inequality we get

$$h'k'' > h''k'$$

$$h'k'' - h''k' > 0$$

or $$h'k'' - h''k' = s > 0$$

consider $$\left.\begin{aligned} kh'' - k''h &= r \\ h'k'' - h''k' &= s \end{aligned}\right\} \ldots(\Psi)$$

Solving the equations (Ψ) in h'' and k'' and remembering that $hk' - h'k = -1$

$$h'' = sh + rh'$$

$$k'' = ks + rk'$$

$\therefore$ $(h'', k'') = 1$ gives $(r, s) = 1$

Let $$S = \left\{ \frac{h}{k} \mid \frac{h}{k} = \frac{\mu h + \lambda h'}{\mu k + \lambda k'}, \lambda, \mu \in N, (\lambda, \mu) = 1 \right\}$$

Now, $$\frac{h''}{k''} = \frac{sh + rh'}{sk + rk'} \in S \text{ for, } (r, s) = 1, r, s \in \mathbb{N}$$

And $$\frac{h}{k} < \frac{\mu h + \lambda h'}{\mu k + \lambda k'} < \frac{h'}{k'}$$

also $$\frac{\mu h + \lambda h'}{\mu k + \lambda k'} \text{ is in its lowest term,}$$

Because if $$d \mid \mu h + \lambda h', \mu k + \lambda k'$$

Then $$d \mid k(\mu h + \lambda h') - h(\mu k + \lambda k') = \lambda$$

Also, $$d \mid h'(\mu h + \lambda h') - k'(\mu k + \lambda k') = \mu$$

$\therefore$ $(\lambda, \mu) = d$, but $(\lambda, \mu) = 1$

$\therefore$ $d = 1$

Thus every fraction of S appears sooner or later in some F_q, $(q > n - 1)$ and plainly the first to make its appears is that for which k is least i.e., for which $\mu k + \lambda k'$ is least is for which $\lambda = 1 = \mu$

This fraction must be $\frac{h''}{k''}$ i.e., $\frac{h''}{k''} = \frac{h + h'}{k + k'}$ which is the theorem 5.3.

And by theorem 5.4, it follows that theorem 5.2 is also true.

Note: The mediant of $\frac{h}{k}$ and $\frac{h'}{k'}$ lies between $\left(\frac{h}{k}, \frac{h'}{k'}\right)$

Corollary 5.6. The denominators of two adjacent fractions of an F.S. of order n add up to at least $n + 1$,

i.e., If $\frac{h}{k}$ and $\frac{h'}{k'}$ are two consecutive terms of a Farey sequence of order n, then $k + k' > n$.

Proof: The mediant

$$\frac{h+h'}{k+k'} \text{ of } \frac{h}{k} \text{ and } \frac{h'}{k'} \text{ falls in the interval } \left(\frac{h}{k}, \frac{h'}{k'}\right)$$

If the theorem is not true

i.e., if $k + k' \leq n$

then, $\frac{h+h'}{k+k'}$ belongs to F_n

and will lie somewhere in the interval $\left(\frac{h}{k}, \frac{h'}{k'}\right)$,

which is a contradiction

Since $\frac{h}{k}$ and $\frac{h'}{k'}$ are two consecutive terms.

5.1.A: Application of Farey sequences:

Theorem 5.7. If $(a, b) = 1$, then Diophantine equation

$$ax + by = 1 \qquad \text{...(1) is solvable}$$

Proof: Assume without loss of generality $0 < a < b$ (if necessary $|a|, |b|$)

$\therefore$ $(a, b) = 1$, $\frac{a}{b}$ is a proper reduced fraction and consequently it appears in some Farey sequence (e.g., in F_b)

Let us now take an adjacent fraction $\frac{h}{k} < \frac{a}{b}$

$\therefore$ by theorem 5.2, $\begin{vmatrix} h & a \\ k & b \end{vmatrix} = -1$

or $$ak - bh = 1 \qquad \text{...(2)}$$

Comparing with (1)

we get $x = k$

and $y = -h$

is a solution of (1)

Hence (1) is solvable.

Euclid's Lemma 5.8. If $(a, b) = 1$, $a \mid bc$ then $a \mid c$

Proof: Consider the equation

$$ax + by = 1 \qquad \text{...(1)}$$

By theorem 5.7, (1) is solvable, say (x_0, y_0) is a solution of (1)

$\therefore$ $ax_0 + by_0 = 1$ and

So, $acx_0 + bcy_0 = c$

But, $a \mid bc$ gives $bc = ak,\ k \in \mathbb{Z}$

$\therefore$ $acx_0 + aky_0 = c$

or $a(cx_0 + ky_0) = c$

$\therefore$ $a \mid c.$

Corollary 5.9. If p is a prime then

$$p \mid a_1.a_2 \ldots a_n$$

Gives p divides at least one of ai.

Theorem 5.10. If $(a, b) = 1$, then the solution of $ax + by$ ...(1)

are given by $\left.\begin{aligned} x &= x_0 - bt \\ y &= y_0 - at \end{aligned}\right\}$ ...(2) where (x_0, y_0) is a solution of (1) and $t \in \mathbb{Z}$

Proof: Since by theorem 5.7, (1) is solvable $\exists\ x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = 1$ ...(3)

Now that (2) is a solution of (1) can be verified by putting the value of x and y

For, $\text{LHS} = ax + by$

$= a(x_0 - bt) + b(y_0 + at)$

$= ax_0 - abt + by_0 + bat$

$= ax_0 + by_0$

$= 1 = \text{RHS}.$

Again $ax + by = 1$ ...(1)

$ax_0 + by_0 = 1$ ...(3)

$\therefore$ $a(x - x_0) + b(y - y_0) = 0,$

or $a(x - x_0) = b(y - y_0)$ ...(4)

$\therefore$ $a \mid b(y - y_0)$

Now $(a, b) = 1,$

$\therefore$ By Euclids Lemma,

(4) gives $y - y_0 = at,\ t \in \mathbb{Z}$

and $a \mid y_0 - y$ gives $y - y_0 = at,\ t \in \mathbb{Z}.$

$\therefore$ $y = y_0 + at$

putting the value in (1)

$$x = x_0 - bt,$$

$\therefore$ $\left.\begin{aligned} x &= x_0 - bt \\ y &= y_0 - at \end{aligned}\right\}$, $t \in \mathbb{Z}$ where (x_0, y_0) is a solution of (1).

5.1.B Approximation of an irrational by rational

Let γ be an irrational number such that $0 < \gamma < 1$

We wish to find how closely we can approximate γ

by a rational number $\frac{h}{k}$ where $(h, k) = 1$

In the FS of order N (> 1), we know that we can find two consecutive terms

$$\frac{a}{b}, \frac{c}{d} \text{ such that } \frac{a}{b} < \gamma < \frac{c}{d}$$

Consider the mediant

$$\frac{a+c}{b+d}$$

then γ lies on one or the other side of

$$\frac{a+c}{b+d}$$

i.e., either case $\frac{a}{b} < \gamma < \frac{a+c}{b+d}$ ...(i)

or $\frac{a+c}{b+d} < \gamma < \frac{c}{d}$. ...(ii)

Since, the mediant is not present in F_n we have $b + d \geq + 1$

From (1)

$$0 < \gamma - \frac{a}{b} < \frac{a+c}{b+d} - \frac{a}{b} = \frac{ab + bc - ab - ad}{b(b+d)}$$

$$= \frac{bc - ad}{b(b+d)} = \frac{1}{b(b+d)} \leq \frac{1}{(N+1)b} \quad \text{...(iii)}$$

From (2),

$$0 < \frac{c}{d} - \gamma < \frac{c}{d} - \frac{a+c}{b+d} = \frac{bc + cd - ad - cd}{d(b+d)} = \frac{1}{d(b+d)} \leq \frac{1}{(N+1)d} \quad \text{...(iv)}$$

$\therefore$ (iii) and (iv) give.

Theorem 5.11. For an irrational γ and a positive integer N, there always exists a fraction $\frac{h}{k}$ with the denominator $k \leq \mathbb{N}$ such that

$$\left| \gamma - \frac{h}{k} \right| < \frac{1}{(N+1)k} \quad \text{...(v)}$$

Thus we can find γ in terms of h and k.

Remark: Our reasoning remains valid if γ is not irrational but is replaced by a reduced fraction $\frac{l}{m}$ with a denominator $m > N$, so that $\frac{l}{m}$ is not found in the FS of order N, then however it may happen that $\frac{l}{m} = \frac{a+c}{b+d}$ and this possibility will not allow us to state a strict inequality in (v).

We therefore obtain another.

Theorem 5.12. If $\frac{l}{m}$ is a reduced fraction of denominator $m \in \mathbb{N}$, then there always exists a fraction $\frac{h}{k}$ with denominator $k \leq \mathbb{N}$ such that $\left|\frac{l}{m} - \frac{h}{k}\right| \leq \frac{1}{(N+1)k}$ ...(vi)

Equality takes place here for $m = N + 1$

5.1.C: Better rational approximation of irrational number

If γ is irrational, and N is a given positive integer we have got the existence of a rational number $\frac{h}{k}$, $k \leq \mathbb{N}$ such that $\left|\gamma - \frac{h}{k}\right| \leq \frac{1}{(N+1)k}$

In particular we have $\left|\gamma - \frac{h}{k}\right| < \frac{1}{k^2}$.

Theorem 5.13. If γ is irrational, then there exist many fractions $\frac{h}{k}$ such that

$$\left|\gamma - \frac{h}{k}\right| < \frac{1}{2k^2} \quad (\textit{much stronger theorem})$$

Proof: Suppose that in F_N we have $\frac{a}{b} < \gamma < \frac{c}{d}$, we wish to show either

$$\gamma - \frac{a}{b} < \frac{1}{2b^2}$$

or $$\frac{c}{d} - \gamma < \frac{1}{2d^2}$$

If not, suppose

$$\gamma - \frac{a}{b} \geq \frac{1}{2b^2}$$

and $$\frac{c}{d} - \gamma \geq \frac{1}{2d^2}$$

then adding we get

$$\frac{c}{d} - \frac{a}{b} \geq \frac{1}{2b^2} + \frac{1}{2d^2} = \frac{b^2 + d^2}{2b^2d^2} \qquad \text{...(K)}$$

Again we have $\frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}$

Subtracting, $0 \geq \frac{b^2 + d^2 - 2bd(bc - bd)}{2b^2d^2} = \frac{(b-d)^2}{2b^2d^2}$

But this is possible only for $b = d$

and then in addition,

since, $bc - ad = 1$ we get from (K),

$d(c - a) = 1$

And these give $b = 1 = d$

But this is not the case (by a previous theorem) since $N > 1$ (because for $N = 1$, it may be true) Hence a contradiction.

Hence the theorem.

Remark Thus we are lead to the question whether many fractions $\frac{h}{k}$ exist with still better approximation $\left|\gamma - \frac{h}{k}\right| < \frac{1}{ck^2}$, with $c > 2$ and what the greatest value of c may be.

This equation was completely answered by A.Herwitz.

5.2 CONTINUED FRACTIONS

Observation

Note I: Suppose our task is to solve the equation

$$x^2 - 3x - 1 = 0 \qquad ...(1)$$

Now, $x^2 - 3x - 1 = 0$

gives
$$x = 3 + \frac{1}{x} = 3 + \frac{1}{3 + \frac{1}{x}} \qquad ...(2)$$

In this way if we go on putting

$3 + \frac{1}{x}$ in place of x it would continue for infinite times. And wilt give us to some definite value?

Let us view this from another anlge as follows:

The numbers we get from the equation (2) we write as

$$3, 3 + \frac{1}{3}, 3 + \frac{1}{3 + \frac{1}{3}}, 3 + \frac{1}{3 + \frac{1}{3 + \frac{1}{3}}} =, \ldots\ldots\ldots\ldots \text{ etc.}$$

And the above numbers thus we get are

$$3, \frac{10}{3} = 3.333 ..., \frac{33}{10} = 3.3, \frac{109}{33} = 3.30303, \ldots \text{ etc.}$$

It is interesting to note that the above numbers are approaching the positive value of the root of the given equation (1)

For we get from the given equation

$$x = \frac{3 + \sqrt{13}}{2} = 3.302775 \ldots @ 3.303$$

Therefore, we now come to know that

$$3 + \frac{1}{3 + \frac{1}{3 + \frac{1}{3 + \ldots\ldots}}} = \frac{3 + \sqrt{3}}{2}$$

and this type of fraction is called *a continued fraction.*

Definition: i.e. a fraction of the type

$$a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cfrac{b_3}{a_4 + \ldots\ldots}}}$$

is called a *continued fraction.*

Usually a_1, a_2, b_1, b_2, b_3 ... may be any real or complex numbers

However, our discussion would be only for the case where the continued fraction is of the type

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ldots\ldots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

which in short may be expressed as

$$[a_1, a_2, a_3, .., a_n]$$

or

$$a_1 + \frac{1}{a_2 +}\frac{1}{a_3 +}\ldots\frac{1}{a_n}$$

Now we note how a rational number can be expressed as a continued fraction [When some number a is expressed as a continued fraction, it would be called the expansion of the continued fraction]

$$\frac{67}{29} = 2 + \frac{9}{29} = 2 + \frac{1}{\frac{29}{9}} = 2 + \frac{1}{3 + \frac{2}{9}} = 2 + \frac{1}{3 + \frac{1}{\frac{9}{2}}} = 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{2}}}$$

$$= [2, 3, 4, 2]$$

Similarly

$$\frac{29}{67} = [0, 2, 3, 4, 2]$$

That finite continued fraction of above type denote a rational number is easy to follow. Now before going to prove that any rational number may be expressed as a finite continued fraction, we attempt to have a look at the usual division operation.

Note II: Let $u_0, u_1 \in \mathbb{N}$. then by Euclid algorithm (with usual notation)

$$\begin{aligned} u_0 &= u_1 a_0 + u_2, \quad 0 \le u_2 < u_1 \\ u_1 &= u_2 a_1 + u_3, \quad 0 \le u_3 < u_2 \\ u_2 &= u_3 a_2 + u_4, \quad 0 \le u_4 < u_3 \\ &\ldots\ldots \quad \ldots\ldots \quad \ldots\ldots \\ u_N &= u_{N+1}\, a_N + 0, \end{aligned}$$

Rewriting this we get

$$\alpha_0 = \frac{u_0}{u_1} = \alpha_0 + \frac{1}{\frac{u_1}{u_2}}$$

$$= \alpha_0 + \frac{1}{\alpha_1}$$

$$\alpha_1 = \frac{u_1}{u_2} = a_1 + \frac{1}{\frac{u_2}{u_3}}$$

$$= a_1 + \frac{1}{\alpha_2}$$

$$\alpha_2 = \frac{u_2}{u_3} = a_2 + \frac{u_4}{u_3} = a_2 + \frac{1}{\frac{u_3}{u_4}}$$

$$= a_2 + \frac{1}{\alpha_3}$$

$$\alpha_3 = \frac{u_3}{u_4} = a_3 + \frac{u_5}{u_4}$$

$$= a_3 + \frac{1}{\frac{u_4}{u_5}}$$

$$= a_3 + \frac{1}{\alpha_4}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$\alpha_N = a_N + 0$$

So,
$$\alpha_0 = a_0 + \frac{1}{\alpha_1}$$

$$= a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}}$$

$$= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\alpha_3}}}$$

so,
$$\alpha_0 = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} \ldots \frac{1}{a_N}$$

Definition: This is called *finite continued fraction* (*C.F*).

Note: Here $a_0 \in \{0, \mathbb{N})$ and all a_i's $\in \mathbb{N}$

C.F. is

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\cdots\cdots \cfrac{1}{a_{N-1} + \cfrac{1}{a_N}}}}}}}$$

$$= a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \frac{1}{a_4} \cdots \frac{1}{a_N}$$

$$= [a_0, a_1, a_2, a_3, \ldots, a_N]$$

Definition: a's are called Partial quotients of the C.F.

Observation:

(1) $[a_0, a_1, a_2, a_3, \ldots, a_N]$

$$= \left[a_0, a_1, a_2, a_3, \ldots . a_{N-2}, a_{N-2}, + \frac{1}{a_N}\right]$$

$$= [a_0, a_1, a_2, a_3, \ldots, a_{N-2}, [a_{N-1}, a_N]]$$

$$\ldots\ldots \quad \ldots\ldots\ldots \quad \ldots\ldots\ldots$$

$$\ldots\ldots \quad \ldots\ldots\ldots \quad \ldots\ldots\ldots$$

$$= [a_0, a_1, a_2, a_3, \ldots, a_i, [a_{i+1}, a_{i+2}, \ldots, a_N]$$

(2) Again if $a_N \geq 1$, then

$$[a_0, a_1, a_2, a_3, \ldots, a_{N-1}, a_N] = [a_0, a_1, a_2, a_3, \ldots, a_{N-1}, a_N - 1, 1]$$

Also, $[a_0, a_1, a_2, a_3, \ldots, a_{N-1}, a_N, 1] = [a_0, a_1, a_2, a_3, \ldots, a_{N-1}, a_N + 1]$

Definition: Such a C.F. is called a *normalized C.F.*

Remark: Given a rational number α, $\exists a$ finite (simple) Continued fraction $[a_0, a_1, a_2, a_3, \ldots a_{N-1}, a_N]$ with $a_i \in \mathbb{N}$, either $N = 0$, or $N > 0$ and $a_N > 1$

Remark: If $[a_0, a_1, a_2, a_3, \ldots, a_{N-1}, a_N]$ is not normalized, then

$$\alpha = [a_0, a_1, a_2, a_3, \ldots, a_{N-1}, a_N]$$

$$= \left[a_0, a_1, a_2, a_3, \ldots . a_{N-2}, a_{N-1}, + \frac{1}{a_N}\right]$$

Properties 5.14. If $N \geq 1$, $\alpha = [a_0, a_1, a_2, a_3, \ldots, a_{N-1}, a_N]$ is normalized then, $a_0 < \alpha < a_0 + 1$

Proof: Now, $\alpha = a_0 + \dfrac{1}{\alpha_1}$

$$\alpha = [a_0,a_1,a_2,a_3, \ldots, a_{N-1}, a_N] = [a_0,a_1]$$

$$= a_0 + \frac{1}{a_1},\ 0 < \alpha_1 = [a_2,a_2, \ldots, a_N]$$

$$= a_1 > 1 \text{ (since it is normalised)}$$

If $N > 1$, then $\alpha_1 = a_1 + \dfrac{1}{\alpha_2} > a_1 \geq 1$

$\therefore \quad \alpha_1 > 1$

$\therefore$ in any case, $\alpha_1 > 1$

$\therefore \dfrac{1}{\alpha_1}$ is a proper fraction

and

$\therefore a_0 + \dfrac{1}{\alpha_1} < a_0 + 1$ which gives

$$a_0 < \alpha < a_0 + 1.$$

Remark: $a_0 = \left[a_0 + \dfrac{1}{\alpha_1}\right] = [\alpha]$

Theorem 5.15. Every rational α has exactly one normalized continued fraction (NSCF).

Proof: Suppose α has two NSCF,

$$[a_0,a_1,a_2,a_3, \ldots, a_{N-1}, a_N] = \alpha = [b_0,b_1,b_2,b_3, \ldots, b_{M-1}, b_M]$$

Case (i)

Let $N = 0$ Then, $\alpha = a_0$ (an integer)

$M > 0$

$\therefore \quad b_0 < \alpha < b_0 + 1$

$\therefore \alpha$ is a fraction, a contradiction.

So $M \neq 0$, i.e., $M = 0$ and then $\alpha = 0$

$\therefore \quad a_0 = \alpha = b_0 = 1$

Hence, α has exactly one NSCF.

Case(ii) Let $N > 0$, $M > 0$,

Then, $[a_0,a_1,a_2,a_3, \ldots, a_{N-1}, a_N] = a_0 + \dfrac{1}{\alpha_1} = b_0 + \dfrac{1}{\beta_1}$ ...(1)

$$\left[a_0 + \frac{1}{\alpha_1}\right] = [\alpha] = \left[b_0 + \frac{1}{\beta_1}\right].$$

$\therefore \quad a_0 = [\alpha] = b0.$

or $\quad a_0 = b_0$

$\therefore$ From (1), $\quad \frac{1}{\alpha_1} = \frac{1}{\beta_1}$ gives

$$\alpha_1 = \beta_1$$

$\therefore \quad \alpha_1 = [a_1, a_2, a_3, \ldots, a_N],\ b_1 = [b_1, b_2, b_3, \ldots, b_M]$

Exactly in a similar argument, $a_1 = b_1$ and so on.

$\therefore \quad a_N = b_M$

Corollary 5.16. Every a has exactly two SCF. One being normalized and the other not normalized.

Proof Let $\alpha = [a_0, a_1, a_2, a_3, \ldots, a_{N-1}, a_N]$, an NSCF $(a_N > 1)$

and $\quad \alpha = [b_0, b_1, b_2, b_3, \ldots, b_M, 1]$

$\therefore \quad [b_0, b_1, b_2, b_3, \ldots, b_M, 1] = \alpha = [a_0, a_1, a_2, a_3, \ldots, a_{N-1}, a_{N-1}, 1]$

By the previous theorem we conclude that

$$a_0 = b_0$$
$$a_1 = b_1$$
$$a_2 = b_2$$
$$\ldots \ldots \ldots$$
$$a_{N-1} = b_M.$$

5.3 NOTION OF CONVERGENTS AND INFINITE CONTINUED FRACTIONS

Till now we have seen that continued fraction expansion of a rational number is simple and finite. On the contrary in case of an irrational number, continued fraction expansion is infinite, of course, simple.

We know that a number not possible of writing as the ratio of two integers is known as an irrational number.

$\sqrt{2}$ is an irrational number $\sqrt{2} > 1$ and 1 is the largest integer which is less than $\sqrt{2}$

Therefore, $\quad \sqrt{2} = 1 + \alpha,\ 0 < \alpha < 1$

Let $\quad \alpha = \frac{1}{x_2}$. Then $\sqrt{2} = 1 + \frac{1}{x_2}$ and then

$$x_2 = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1;$$

$\therefore \quad \sqrt{2} = 1 + \frac{1}{\sqrt{2} + 1}$. Here, $\sqrt{2} + 1 > 2$ (the largest integer).

$\therefore \quad x_2 = \sqrt{2} + 1 = 2 + \frac{1}{x_3}$

or $$x_3 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1 > 2$$

$\therefore$ $$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2}+1}}$$ and when we continue in this manner we get

$$\sqrt{2} = [1,2,2, \ldots], = [1, \overline{2}]$$

Now The equestion is : Does [1, 2, 2, ...] respesent $\sqrt{2}$?

Since, $$x = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ldots\ldots}}}$$

$$1$$

We get $$x = 1 + \cfrac{1}{2 + \left\{ \cfrac{1}{2 + \cfrac{1}{2 + \ldots\ldots}} \right\}}$$

$\therefore$ $$x = 1 + \frac{1}{2+(x-1)} = 1 + \frac{1}{x+1}$$

or $$x - 1 = \frac{1}{x+1}$$

or $$x^2 = 2 \text{ i.e., } x = \sqrt{2}.$$

Definition: An finite sequence $a_0,a_1,a_2, \ldots$ of integers, all positive except for a_0, determines an infinite simple continued fraction $[a_0,a_1,a_2, \ldots]$. The value of $[a_0,a_1,a_2, \ldots]$ is defined to be $\lim_{n \to \infty} [a_0,a_1, \ldots a_n]$

If $a_0,a_1, \ldots$ is an infinite sequence then

$$a_0 + \frac{1}{a_1 +} \cdot \frac{1}{a_2 +} \ldots = [a_0,a_1,a_2, \ldots, a_n, \ldots]$$

is called a simple infinite continued fraction.

Definition: $c_i = \frac{p_i}{q_i}$'s are called *successive convergents* to

$$\alpha = [a_0,a_1,a_2,a_3, \ldots, a_N]$$

Suppose $a_0, a_1, a_2, \ldots$ be an infinite sequence of integers, all positive except possibly a_0...

Then we define two sequences of integers

$$\{p_{-2}, p_{-1}, p_0, p_1, p_2, \ldots.\}$$

and $$\{q_{-2}, q_{-1}, q_0, q_1, q_2, \ldots.\}$$

inductively as follows:

$$\begin{aligned} p_{-2} &= 0 & q_{-2} &= 1 \\ p_{-1} &= 1 & q_{-1} &= 0 \\ p_0 &= a_0 p_{-1} + p_{-2} & q_0 &= a_0 q_{-1} + q_{-2} \\ p_1 &= a_1 p_0 + p_{-1} \quad \text{and} & q_1 &= a_1 q_0 + q_{-1} \\ p_2 &= a_2 p_1 + p_0 & q_2 &= a_1 q_1 + q_0 \\ &\cdots\cdots & &\cdots\cdots \\ p_{N-1} &= a_{N-1} p_{N-2} + p_{N-2} & q_{N-1} &= a_{N-1} q_{N-2} + q_{N-3} \\ p_N &= a_n p_{N-1} + p_{N-2} & q_N &= a_N q_{N-1} + q_{N-2} \end{aligned}$$

For the C.F.

$$\alpha = [a_0, a_1, a_2, a_3, \ldots, a_N]$$

The successive convergents are:

$$\frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots.$$

Now $$c_0 = \frac{p_0}{q_0} = [a_0] = \frac{a_0}{1},$$

$$c_1 = \frac{p_1}{q_1} = [a_0, a_1] = a_0 + \frac{1}{a_1}$$

$$= \frac{a_0 a_1 + 1}{a_1}$$

$$= \frac{a_1 p_0 + p_{-1}}{a_1 q_0 + q_{-1}}$$

Thus, $$c_1 = \frac{p_1}{q_1} = [a_0, a_1] = \frac{a_1 p_0 + p_{-1}}{a_1 q_0 + q_{-1}}$$

$$c_2 = \frac{p_2}{q_2} = [a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}}$$

$$= a_0 + \frac{a_2}{a_1 a_2 + 1} \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1}$$

$$= \frac{a_2 (a_0 a_1 + 1) + a_0}{a_2 a_1 + 1}$$

$$= \frac{a_2 p_1 + p_2}{a_2 q_1 + q_0}$$

Thus, $$c_2 = \frac{p_2}{q_2} = [a_0, a_1, a_2] = \frac{a_2 p_1 + p_0}{a_2 q_1 + q_0}$$

Similarly, $$c_2 = \frac{p_3}{q_3} = \frac{a_3 p_2 + p_1}{a_3 q_2 + q_1},$$

.....

$$c_i = \frac{p_i}{q_i} = \frac{a_i p_{i-1} + p_{i-2}}{a_i q_{i-1} + q_{i-2}}$$

Example 1. $\frac{61}{48} = [1,3,1,2,4]$

Solution:

$$\frac{p_0}{q_0} = \frac{1}{1},$$

$$\frac{p_1}{q_1} = \frac{3\times 1+1}{3\times 1+0} = \frac{4}{3},$$

$$\frac{p_2}{q_2} = \frac{1\times 4+1}{1\times 3+1} = \frac{5}{4}$$

$$\frac{p_3}{q_3} = \frac{2\times 5+4}{2\times 4+3} = \frac{14}{11},$$

$$\frac{p_4}{q_4} = \frac{4\times 14+5}{4\times 11+4} = \frac{61}{48}.$$

Theorem 5.17. $p_{i+1}\, q_i - q_{i+1}\, p_i = (-1)^i$ ...(*)

Proof: LHS $= \begin{bmatrix} p_{i+1} & p_i \\ q_{i+1} & q_i \end{bmatrix} = \begin{vmatrix} a_{i+1}p_i + p_{i-1} & p_i \\ a_{i+1}q_i + q_{i-1} & q_i \end{vmatrix} = \begin{vmatrix} a_{i+1}p_i & p_i \\ a_{i+1}q_i & q_i \end{vmatrix} + \begin{vmatrix} p_{i-1} & p_i \\ q_{i-1} & q_i \end{vmatrix}$

$$= a_{i+1}\begin{vmatrix} p_i & p_i \\ q_i & q_i \end{vmatrix} + \begin{vmatrix} p_{i-1} & p_i \\ q_{i-1} & q_i \end{vmatrix} = \begin{vmatrix} p_{i-1} & p_i \\ q_{i-1} & q_i \end{vmatrix} = (-1)\begin{vmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{vmatrix}$$

$$= (-1)^2 \begin{vmatrix} p_{i-1} & p_{i-2} \\ q_{i-1} & q_{i-2} \end{vmatrix}$$

$$= \ldots \quad \ldots\ldots \quad \ldots\ldots$$

$$= (-1)^{i+2}\begin{vmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{vmatrix} = (-1)^i \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = (-1)^i$$

Remark: (1) $(p_i, q_i) = 1\ \forall i$

Otherwise, if G.C.D $= d \neq 1$, $d \mid \pm 1$, impossible

Hence.

(2) It is obvious that $q_i \geq 0 (q_i = 0$ only when $i = -1)$

(3) Dividing (*) by $q_i q_{i+1}$ $(i \geq 0)$ we get

$$\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i} = \frac{(-1)^i}{q_i q_{i+1}} \qquad \text{...(a)}$$

Since RHS is positive if i is even, and negative if i is odd.

$$\therefore \qquad \frac{p_0}{q_0} < \frac{p_1}{q_1}, \quad \frac{p_1}{q_1} > \frac{p_2}{q_2}, \frac{p_3}{q_3} > \frac{p_2}{q_2}$$

i.e. $$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots$$

and $$\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \ldots$$

Theorem 5.18. $c_i = [a_0, a_1, a_2, a_3, \ldots, a_i] = \dfrac{p_i}{q_i}$ ...(i)

Proof: It is true when $i = 0$ for then $c_0 = a_0$

and $$\frac{p_0}{q_0} = \frac{a_0 p_{-1} + p_{-2}}{a_0 q_{-1} + q_{-2}} = \frac{a_0 q_{-1}}{q_{-2}} = \frac{a_0 . 1 + 0}{a_0 . 0 + 1} = a_0$$

Suppose, the theorem is true for i i.e., assume that

$$c_i = [a_0, a_1, a_2, a_3, \ldots, a_i] = \frac{p_i}{q_i} = \frac{a_i p_{i-1} + p_{i-2}}{a_i q_{i-1} + q_{i-2}}$$

Now, $$c_{i+1} = [a_0, a_1, a_2, a_3, \ldots, a_i, a_{i+1}]$$

$$= [a_0, a_1, a_2, a_3, \ldots, a_{i+1}, a_i + \frac{1}{a_{i+1}}]$$

$$= \frac{\left(a_i + \dfrac{1}{a_{i+1}}\right) p_{i-1} + p_{i-2}}{\left(a_i + \dfrac{1}{a_{i+1}}\right) q_{i-1} + q_{i-2}} = \frac{(a_i a_{i+1} + 1) p_{i-1} + a_{i+1} p_{i-2}}{(a_i a_{i+1} + 1) q_{i-1} + a_{i+1} q_{i-2}}$$

$$= \frac{a_{i+1}(a_i p_{i-1} + p_{i-2}) + p_{i-1}}{a_{i+1}(a_i q_{i-1} + q_{i-2}) + q_{i-1}} = \frac{a_{i+1} p_i + p_{i-1}}{a_{i+1} q_i + q_{i-1}} = \frac{p_{i-1}}{q_{i-1}}$$

Hence by method of induction the theorem is proved.

Theorem 5.19. If α is an irrational number then the corresponding continued fraction will be infinite.

Proof: Let $\alpha \in Q^c$ and $[\alpha] = a_0$

Since, $\alpha = a_0 + \alpha', 0 < \alpha' < 1$ and put, $\alpha' = \frac{1}{\alpha_1}$

Therefore, $\alpha_1 > 1$, and $\alpha_1 \varepsilon Q^c$

Similarly, $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, $\alpha_2 > 1$ and $\alpha_2 \varepsilon Q^c$

... ...

... ...

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}}, \alpha_{n+1} > 1 \text{ and } \alpha_{n+1} \varepsilon Q^c$$

Therefore,

$$\alpha = a_0 + \frac{1}{a_1 +}.\frac{1}{a_2 +} \ldots \frac{1}{a_n +}.\frac{1}{\alpha_{n+1}} \qquad \ldots(1)$$

Obviously, $\frac{p_0}{q_0} = a_0$, $a_0 \varepsilon \mathbb{Z}$, $a's \varepsilon \mathbb{N}$,

$$\frac{p_1}{q_1} = a_0 + \frac{1}{a_1}, \ldots$$

$$\alpha = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} \qquad \ldots(2)$$

$$\frac{p_n}{q_n} \rightarrow \text{ a limit as } n \rightarrow \infty$$

We claim that this limit is α

Now

$$\alpha - \frac{p_n}{q_n} = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{\alpha_{n+1} p_n q_n + p_{n-1} q_n - \alpha_{n+1} q_n p_n - p_n q_{n-1}}{q_n \left(\alpha_{n+1} q_n + q_{n-1}\right)}$$

$$= \frac{p_{n-1} q_n - p_n q_{n-1}}{q_n (\alpha_{n+1} q_n + q_{n-1})} = \frac{(-1)^n}{q_n (\alpha_{n+1} q_n + q_{n-1})} = \frac{\pm 1}{q_n (\alpha_{n+1} q_n + q_{n-1})}$$

Here denominator $> q_n q_{n+1}$

Since $q_{n+1} = a_{n+1} q_n + q_{n-1}$

$\alpha_{n+1} > a_{n+1}$, Because $\alpha_{n+1} = a_{n+1} + \frac{1}{\alpha_{n+2}}$

Therefore,

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}$$

Now q_n is increasing and when q_n increases indefinitely as $n \to \infty$

We get

$$\left| \alpha - \frac{p_n}{q_n} \right| \to 0, \text{ as } n \to \infty$$

Therefore,

$$\lim_{n \to \infty} \frac{p_n}{q_n} = \alpha$$

Note: The representation of an irrational number by an infinite continued fraction suggests a question: what is the meaning of $a_1, a_2, \ldots$?

Consider any sequence $a_0, a_1, a_2, \ldots$; $a_0 \in \mathbb{Z}$, $a_1, a_2, \ldots \in \mathbb{N}$

Can we attach a meaning to the infinite continued fraction?

If we can, will the resulting number be irrational? and will this continued fraction coincide with the one obtained by applying our former process to the number in question?

In fact if one forms a continued fraction from any infinite sequence of natural numbers $a_1, a_2, \ldots$ preceded by any integer a_0, then the corresponding sequence of convergence has a limit.

Consider $\frac{p_0}{q_0}, \frac{p_2}{q_2}, \frac{p_4}{q_4}, \ldots$ (the sequence of even convergence)

Now we have the sequence $\frac{p_{2n}}{q2_n}$ is increasing, bounded above and all of these $< \frac{p_1}{q_1}$

Therefore this sequence has a limit

Similarly the sequence formed by the odd convergence $\frac{p_{2n+1}}{q_{2n+1}}$ has a limit.

Since $\frac{p_m}{q_m} - \frac{p_{m-1}}{q_{m-1}} = \frac{(-1)^{m-1}}{q_m q_{m-1}}$, shows that the difference between two consecutive convergence has the limit zero as $m \to \infty$

Therefore, the limit of the sequence of convergence is the value of infinite continued fractions.

Theorem 5.20. The value of any infinite simple continued fraction $[a_0, a_1, a_2, \ldots]$ is irrational

Proof Let $\alpha = [a_0, a_1, a_2, \ldots]$

It is observed in the Note above that

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \frac{p_6}{q_6} < \ldots < \frac{p_7}{q_7} < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

And hence,

$$\frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}}$$

or $$0 < |\alpha - r_n| < |r_{n+1} - r_n| \qquad ...(*)$$

Also we know that

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_{n+1}q_n} \qquad ...(**)$$

Therefore multiplying (*) by q_n and using (**) we get

$$\left|\frac{p_{n+1}}{q_{n+1}}\right| = (q_n q_{n+1})^{-1}$$

and $$0 < |q_n\alpha - p_n| < \frac{1}{q_{n+1}} \qquad ...(***)$$

Suppose α were rational, say $\alpha = \frac{a}{b}$, with integers a and b, $b > 0$.

Then, (***) becomes

$$0 < |q_n a - p_n b| < \frac{b}{q_{n+1}}$$

Now it is possible to choose n sufficiently large so that $b < q_{n+1}$ (for the integers q_n increase with n) i.e. then,

$$0 < |q_n a - p_n b| < \frac{b}{q_{n+1}} < 1$$

or $0 < |q_n a - p_n b| < 1$ and this is not possible.

Thus the value of any infinite simple continued fraction is irrational.//

Now we look at the two different infinite simple continued fractions to see whether these converge to the same irrational number! The answer is negative and this becomes clear from the following.

First we prove the following.

Lemma 5.21. If $\alpha = [a_0, a_1, a_2, ...]$ is a simple continued fraction, then $[\alpha] = a_0$. And if $\alpha_1 = [a_1, a_2, a_3, ...]$, then $\alpha = a_0 + \frac{1}{a_1}$

Proof: As above we know that

$$\frac{p_0}{q_0} < \alpha < \frac{p_1}{q_1} \text{ i.e., } a_1 < \alpha < a_0 + \frac{1}{a_1}.$$

Now $a_1 \geq 1$ gives $a_0 < \alpha < a_0 + 1$ and hence $a_0 = [\alpha]$

Also, $$\alpha = \lim_{n\to\infty}[a_0,a_1,a_2, ..., a_n] = \lim_{n\to\infty}\left(a_0 + \frac{1}{[a_1, a_2, ..., a_n]}\right)$$

$$= a_0 + \frac{1}{\lim_{n\to\infty}[a_1, a_2, ..., a_n]} = a_0 + \frac{1}{\alpha_1}$$

Theorem 5.22. Two distinct infinite simple continued fractions converge to different values.

Proof: If possible let

$$[a_0,a_1,a_2, ...] = [b_0,b_1,b_2, ...] = \alpha$$

Then by lemma 5.3.5 $[\alpha] = a_0 = b_0$

and $$\alpha = a_0 + \frac{1}{[a_1,a_2,...]} = b_0 + \frac{1}{[b_1,b_2,...]}.:$$

Hence, $[a_1,a_2, ...] = [b_1,b_2, ...]$. Repeating in this way we finally get $a_n = b_n$ for all n (by mathematical induction)

5.4 APPLICATION TO EQUATIONS

Consider the equation $ax - by = 1$ ...(1)

Let $$\frac{a}{b} = a_0 + \frac{1}{a_1 +}\,\frac{1}{a_2 +} \cdots \frac{1}{a_{n-1} +}\,\frac{1}{a_n}$$

$$= [a_0,a_1,a_2, \ldots a_n]$$

Now, $c_n = \frac{p_n}{q_n} = \frac{a}{b}$, where $p_n = a$, $q_n = b$; $(a, b) = 1$, $(p_n, q_n) = 1$

and we have, $p_n\, q_{n-1} - q_n\, p_{n-1} = (-1)^{n-1}$

or $a\, q_{n-1} - b\, p_{n-1} = (-1)^{n-1}$ ...(2)

Hence, if we take

$$x = q_{n-1} \text{ and } y = p_{n-1}$$

we get, $\{q_{n-1}, p_{n-1}\}$ is a solution of

the equation $ax - by = (-1)^{n-1}$ ...(3)

If n is *odd*, (3) becomes $ax - by = 1$ and which is (1) and

Hence $x = q_{n-1}$

and $y = p_{n-1}$

is a solution.

If n is *even*, we can still find the solution by taking

$$x = b - q_{n-1}$$

$$y = a - p_{n-1}$$

Thus $a(b - q_{n-1}) - b(a - p_{n-1}) = -aq_{n-1} + bp_{n-1}$
$= -(aq_{n-1} - bp_{n-1})$
$= -(-1) = 1$

i.e. $a(b - q_{n-1}) - b(a - p_{n-1}) = 1$

Theorem 5.23. If $(a, b) = 1$ and

$$\frac{a}{b} = [a_0, a_1, a_2, \ldots, a_{n-1}, a_n],\ c_i = \frac{p_i}{q_i},\ i = 0, 1, 2, \ldots, n.$$

Then (i) (q_{n-1}, p_{n-1}) is a solution if n is odd
(ii) $(b - q_{n-1}, a - p_{n-1})$ is a solution if n is even.

Example 2. Solve $61x + 48y = 1$

Solution: The convergents are

$$\frac{1}{1}, \frac{5}{4}, \frac{4}{3}, \frac{14}{11}, \frac{61}{48};\ n = 4$$

Solution is $x = b - q_{n-1} = 48 - 11 = 37$
$y = a - p_{n-1} = 61 - 41 = 47$

i.e. $\left.\begin{matrix} x = 37 \\ y = 47 \end{matrix}\right\}$.

Example 3. Find out one solution of $51x - 71y = 1$

$$\frac{a}{b} = \frac{51}{71} = 0 + \frac{1}{\frac{71}{51}} = 0 + \frac{1}{1 + \frac{20}{51}} = 0 + \frac{1}{1 + \frac{1}{\frac{51}{20}}} = 0 + \frac{1}{1 + \frac{1}{2 + \frac{11}{20}}}$$

$$= 0 + \frac{1}{1 + \frac{1}{2 + \frac{1}{\frac{20}{11}}}} = 0 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{9}{11}}}}$$

$$= 0 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{11}{9}}}}} = 0 \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{2}{9}}}}}$$

$$= 0 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{9}{2}}}}}} = 0 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{4 + \frac{1}{2}}}}}}$$

$$\frac{a}{b} = \frac{51}{71} = [0, 1, 2, 1, 1, 4, 2]$$

$$\frac{p_0}{q_0} = 0 = \frac{0}{1}, \frac{p_1}{q_1} = \frac{1\times 0+1}{1\times 1+0} = \frac{1}{1}, \frac{p_2}{q_2} = \frac{2\times 1+0}{2\times 1+1} = \frac{2}{3},$$

$$\frac{p_3}{q_3} = \frac{1\times 2+1}{1\times 3+1} = \frac{3}{4}, \frac{p_4}{q_4} = \frac{1\times 3+2}{1\times 4+3} = \frac{5}{7},$$

$$\frac{p_5}{q_5} = \frac{4\times 5+3}{4\times 7+4} = \frac{23}{32}, \frac{p_6}{q_6} = \frac{2\times 23+5}{2\times 32+7} = \frac{51}{71}; \; n = 6$$

$\therefore$ $x = b - q_{n-1} = 71 - 32 = 39$

$y = a - p_{n-1} = 51 - 23 = 23$

$\therefore$ $\left.\begin{matrix} x = 39 \\ y = 23 \end{matrix}\right\}$.

Example 5 Find the integral solution of the indeterminate equation

$$205x - 93y = 1$$

Solution: Here, $205 = 5 \times 41$; $93 = 3 \times 31$ and these are relatively prime.

So the given equation has solution.

Now we consider the continued fraction $\frac{205}{93} = [2, 4, 1, 8, 2]$ and this has an odd number of partial quotients, but this can be replaced by

$\frac{205}{93} = [2, 4, 1, 8, 1, 1]$ the equivalent expansion with an even number of quotients.

The convergents are computed as follows:

i	-1	0	1	2	3	4	5	6
a_i			2	4	1	8	1	1
p_i	0	1	2	9	11	97	108	205
q_i	1	0	1	4	5	44	49	93
c_i			$\frac{2}{1}$	$\frac{9}{4}$	$\frac{11}{5}$	$\frac{97}{44}$	$\frac{108}{49}$	$\frac{205}{93}$

Here $n = 6$, $p_{n-1} = p_5 = 108 = y_0$, $q_{n-1} = q_5 = 49 = x_0$, and hence,

$205x - 93y = 1$

$\therefore$ $x = x_0 + tb = 49 + 93t$

$y = y_0 + ta = 108 + 205t$, $t = 0, \pm 1, \pm 2,$

As a check,

Let $t = 1$;

then $x = 142,$

$y = 313$

and $205(142) - 93(313) = 29110 - 29109 = 1.$

As a general check we have

$$205\,(49 + 93t) - 93(108 + 205t) = 1,$$

Since the terms involving t cancel.

Example 5. Find the general solution of the equation

$$205x - 93y = -1$$

Solution: Here the number 205 and 93 are relatively prime, hence the given equation has solution.

The continued fraction expansion of $\frac{205}{93}$ is

$$\frac{205}{93} = [2, 4, 1, 8, 2]$$

and has an odd number of partial quotients, so $(-1)^n = (-1)^5 = -1$ as required. To find the convergents we set up the table

i	-1	0	1	2	3	4	5
a_i			2	4	1	8	2
p_i	0	1	2	9	11	97	205
q_i	1	0	1	4	5	44	93
c_i			$\frac{2}{1}$	$\frac{9}{4}$	$\frac{11}{5}$	$\frac{97}{44}$	$\frac{205}{93}$

Now we see that

$$c_{n-1} = \frac{p_{n-1}}{q_{n-1}} = \frac{p_4}{q_4} = \frac{97}{44};$$

hence a particular solution of the given equation is $x_0 = q_4 = 44$ and $y_0 = p_4 = 97$. The general solution, therefore is

$$x = x_0 + tb = 44 + 93t$$

$$y = y_0 + ta = 97 + 205t,\ t = 0, \pm 1, \pm 2, \ldots$$

As a check take $t = -1$; then

$$(x, y) = (-49, -108),$$

and $205(-49) - 93(-108) = -10045 + 10044 = -1.$

Note: Equation of the type

$$ax + by = c,\ (a, b) = 1$$

Once we have learned to solve the indeterminate equation

$$ax + by = 1$$

where a and b are relatively prime integers, it is a simple matter to solve the equation

$$ax + by = c$$

where c is any integer.

For suppose that (x_0, y_0) is any particular solution of $ax + by = 1$

Then we have $ax_0 + by_0 = 1$

Multiplying by c we get

$$a(cx_0) + b(cy_0) = e$$

so that (cx_0, cy_0) is a particular solution of the given equation. Thus the general solution will be

$$x = cx_0 + bt$$
$$y = cy_0 + at,$$
$$t = 0, \pm 1, \pm 2, \ldots .$$

To find general solution of the type

$$ax + by = c$$

first we find a solution of

$$ax + by = 1, (a, b) = 1$$

To do this, expand $\frac{a}{b}$ as a simple continued fraction with an even number of partial quotients. From the table of convergent read off p_{n-1} and q_{n-1}.

Then $aq_{n-1} - bp_{n-1} = 1$ as before.

This trick now is to write the given equation as $ax + by = c$ in the form

$$ax + by = c.1 = c(aq_{n-1} - bp_{n-1})$$

Rearrange the terms to obtain

$$a(cq_{n-1} - x) = b(y + cp_{n-1}) \qquad \ldots(*)$$

So, $b \mid$ LHS but $(a, b) =$, and $b \nmid a$; so, $b \mid cq_{n-1} - x$

So that there is an integer t such that

$$cq_{n-1} - x = tb, \qquad \ldots(**)$$

or

$$x = cq_{n-1} - tb \qquad \ldots(***)$$

Substitute (**) into (*) to get

$$a(tb) = b(y + cp_{n-1}),$$

And solve for y to obtain

$$y = at - cp_{n-1}.(\&)$$

Conversely, for any integer t, a direct substitution of (***) and (&) into $ax + by$ gives

$$ax + by = a(cq_{n-1} - tb) + (at - cp_{n-1}) = \ldots = c$$

So the equation is satisfied. Thus the general solution of the equation $ax + by = c$ is

$$x = cq_{n-1} - tb$$
$$y = at - cp_{n-1}, \text{ where } t = 0, \pm 1, \pm 2, \ldots .$$

Note: We observe the following:

Consider the rational number of the type $\frac{p}{q}$, $(q > 0)$

we get $\frac{p}{q} = a_1 + \frac{r_1}{q}, \quad 0 \le r_1 < q$

If $r_1 = 0$,then $\frac{p}{q} = [a_1]$

If $r_1 \neq 0$, then $\frac{p}{q} = a_1 + \frac{r_1}{q} = a_1 + \frac{1}{\frac{q}{r_1}}, r_1 > 0$

As before, $\frac{q}{r_1} = a_2 + \frac{r_2}{r_1}, 0 \le r_2 < r_1$

If $r_2 = 0$, then $\frac{p}{q} = [a_1, a_2]$

if $r_2 \neq 0$ then $\frac{q}{r_1} = a_2 + \frac{1}{\frac{r_1}{r_2}}, 0 < r_2 < r_1 < q,$

Proceeding this way we get a sequence of positive integers viz.

$$r_1 > r_2 > r_3 > r_4 > \ldots$$

And such a sequence cannot be infinite.

Suppose $r_n = 0$ and then,

$$\frac{p}{q} = [a_1, a_2, a_3, \ldots, a_n]$$

In above $a_1, a_2, a_3, \ldots, a_n$ are called partial quotients.

$$c_1 = a_1$$

$$c_2 = a_1 + \frac{1}{a_2},$$

$$c_3 = a_1 + \frac{1}{a_2 + \frac{1}{a_3}}, \ldots \text{ etc. are convergents.}$$

Example 6. A farmer bought a number of goats and swine with rupees 80.00 per goat and rupees 50.00 per swine and in total he had to pay a sum of rupees 810.00.

How many goats and swine the farmer bought?

Solution: Suppose the number of goats is x and the number of swine is y

Then we get

$$80x + 50y = 810$$

or

$$8x + 5y = 81 \qquad \ldots(1)$$

[As the value of x and y will be only the positive integers, from the above equation, by trial end error, we get the solution as follows;

we go on putting the values

$$x = 0, 1, 2, 3, ..., 10$$

and the corresponding values of y will be those where $81 - 8x$ would be multiple of 5 and therefore $y = 13$ and 5

Thus, the required solution would be

$$(2, 13), (7, 5).$$

It is observed that the procedure is not a suitable one.

Now we take help of continued fraction as follows:

Our first step is now to solve the equation

$$8x + 5y = 81$$

We first note that $(8, 5) = 1$

And we take continued fraction expansion of this number as follows:

$$\frac{8}{5} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}} = [1,1,1,2]$$

Here, there are 4 convergents.

viz. $c_1 = 1, c_2 = 2, c_3 = \frac{3}{2}, c_4 = \frac{8}{5}$

It is seen that from $c_3 = \frac{3}{2}$ we get a pair (2, 3) and this pair is a solution to the equation

$$8x + 5y = 1$$

for, $8 \times 2 - 5 \times 3 = 1$

Now, $8x + 5y = 81$ gives,

$$8x + 5y = 81\ (8 \times 2 - 5 \times 3)$$

or $x = 162 + 5t$

$y = -243 - 8t$

and this true for $t = 0, \pm1, \pm2, \pm3, ...$

for $t = -32$ we get $x = 2, y = 13;$

$t = -31$ gives $x = 7, y = 5$ etc.

Example 7. *Sailors, coconut and monkeys problem:*

The following problem is of considerable age and, in one form or another, continues to appear from time to time.

Five sailors were cast away on an island. To provide food, they collected all the coconuts they could find. During the night one of the sailors awoke and decided to take his share of the coconuts. He divided the nuts into five equal piles and discovered that one nut was left over, so he threw this extra one to the monkeys. He then hid his share

and went back to sleep. A little later a second sailor awoke and had the same idea as the first,

He divided the remainder of the nuts into five equal piles, discovered also that one was left over, and threw it to the monkeys. Then he hid his share. In their turn the other three sailors did the same thing, each throwing a coconut to the monkeys. Then next morning the sailors, all-looking as innocent as possible, divided the remaining nuts into five equal piles, no nuts being left over this time. The problem is to find the smallest number coconuts in the original pile.

Solution: Suppose x is the original number of coconuts.

The first sailor took $\frac{1}{5}(x-1)$ Coconuts and left $\frac{4}{5}(x-1)$

Similarly the second sailor took

$\frac{1}{5}\left[\frac{4}{5}(x-1)-1\right] = \frac{4x-9}{25}$ Coconuts and left four times this number, or $\frac{16x-36}{25}$.

Similarly, we find that the third, fourth, and fifth sailors left, respectively,

$$\frac{64x-244}{125}, \frac{256x-1476}{625}, \frac{1024x-8404}{3125} \text{ Nuts.}$$

Now the number of nuts in the last pile must be a multiple of 5, since it was divided into five piles with no nuts left over.

Hence $$\frac{1024x-8404}{3125} = 5y,$$

where y is some integer. Multiplying both sides by 3125 we obtain the indeterminate equation

$$1024x - 15625y = 8404 \qquad \ldots(*)$$

As $(1024, 15625) = 1$ the equation has solutions.

We seek a particular solution (x_1, y_1) of the equation

$$1024x - 15625y = 1 \qquad \ldots(**)$$

To this end, the convergent of the continued fraction

$$\frac{1024}{15625} = [0, 15, 3, 1, 6, 2, 1, 3, 2, 1]$$

are calculated

i	-1	0	1	2	3	4	5	6	7	8	9	10
a_i			0	15	3	1	6	2	1	3	2	1
p_i	0	1	0	1	3	4	27	58	85	313	711	1024
q_i	1	0	1	15	46	61	412	885	1297	4776	10849	15625
c_i											$\frac{711}{10849}$	

The convergent c_9 yields the particular solution $x_1 = q_9 = 10849$, $y_1 = p_9 = 711$ of equation (**).

Hence $x_0 = 8404x_1 = 91174996,$

$y_0 = 840y_1 = 5975244$ will be a particular solution of equation(*).

The general solution is

$$x = 91174996 + 15625t$$

$$y = 5975244 + 1024t, t = 0, 1, 2, ...$$

Keeping in note that the values are positive, the possible value of t will be –5835 and we finally obtain

$$x = 91174996 - 91171875 = 3121$$

$y = 5975244 - 5975040 = 204$, which means that the original number of coconuts was 3121 and each sailor received 204 in the final distribution.

5.5 QUADRATIC IRRATIONALS

Definition: A number of the form $\frac{P \pm \sqrt{D}}{Q}$, where P, D, Q are integers, and where D is a positive integer but not a perfect square, is called *a quadratic irrational, or a quadratic surd.* It is the root of the quadratic equation

$$Q^2x^2 - 2PQx + (P^2 - D) = 0$$

There are irrational numbers, which are not quadratic. The number $\pi = 3.14159 ...$ is one example. The irrational number $\sqrt{2}$ is the solution of the algebraic equation $x^2 - 2 = 0$ and is therefore called an algebraic number. Thus

Definition: An algebraic number is a number x, which satisfies an equation of the type $a_0x^n + a_1x^{n-1} ... + a_n = 0$, where a_0, a_0, ... are integers, not all zero.

A number, which is not algebraic, is called a transcendental number. The irrational number π is transcendental.

We note the ICFs for $\sqrt{2}, \sqrt{3}, \sqrt{5}$ ... etc., .

ICF for $\sqrt{2}$

$$[\sqrt{2}] = 1$$

$$\therefore \quad \sqrt{2} = 1 + \alpha', 0 < \alpha' < 1, \alpha' \in Q^c$$

$$= 1 + \frac{1}{\alpha_1}, \alpha_1 > 1, \alpha_1 \in Q^c$$

or $$\frac{1}{\alpha_1} = \sqrt{2} - 1,$$

or $$\alpha_1 = \sqrt{2} + 1,$$

or $$\alpha_1 = 2 + \alpha'', \alpha' \in Q^c$$

$$= 2 + \frac{1}{\alpha_2}, \alpha_2 \in Q^c.$$

or $$\alpha_2 = \frac{1}{\alpha_1 - 2} = \frac{1}{\sqrt{2}+1-2} = \frac{1}{\sqrt{2}-1} = \sqrt{2} + 1$$

$\therefore$ $$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + ...}}}$$

$$= [1, 2, 2, 2, ...]$$

$$= [1, \overline{2}]$$

ICF for $\sqrt{3}$

$$[\sqrt{3}] = 1, \sqrt{3} = 1 + \frac{1}{\alpha_1}, \alpha_1 > 1, \quad \alpha_1 \in Q^c$$

or $$\alpha_1 = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}$$

or $$[\alpha_1] = 1, \alpha_1 = 1 + \frac{1}{\alpha_2}, \quad \alpha_2 > 1, \quad \alpha_2 \in Q^c$$

or $$\alpha_2 = \frac{1}{\alpha_1 - 1} = \frac{1}{\frac{\sqrt{3}+1}{2}} = \frac{2}{\sqrt{3}-1} = \frac{2(\sqrt{3}+1)}{2} = \sqrt{3} + 1$$

$$[\alpha_2] = 2, \alpha_2 = 2 + \frac{1}{\alpha_3}, \alpha_3 > 1, \alpha_3 \varepsilon Q^c$$

or $$\alpha_3 = \frac{1}{\alpha_2 - 2} = \frac{1}{\sqrt{3}+1-2} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} = \alpha_1$$

or $$\sqrt{3} = 1 + \frac{1}{1+}.\frac{1}{2+}.\frac{1}{1+}.\frac{1}{2+}...$$

$$= [1, 1, 2, 1, 2, ...] = \left[1, \overline{1, 2}\right]$$

I.C.F for $\sqrt{5}$ $[\sqrt{5}] = 2,$

$$\sqrt{5} = 2 + \frac{1}{\alpha_1},$$

$$\alpha_1 = \sqrt{5} + 2 = 4 + \frac{1}{\alpha_2},$$

$$\alpha_2 = \frac{1}{\alpha_1 - 4} = \frac{1}{\sqrt{5}-2} = \sqrt{5} + 2 = \alpha_1$$

Therefore, $$\sqrt{5} = 2 + \cfrac{1}{4 + \cfrac{1}{4 + ...}} = [2, \overline{4}].$$

Definition: The type of infinite continued fraction in which partial quotients are repeated after certain term is called a *periodic continued fraction.*

Definition: If an ICF is periodic from the very beginning, it is said to be purely *periodic.*

A purely periodic ICF is of the form $[\overline{a_0, a_1, a_2, ..., a_n}]$

Example 8. $\sqrt{2} = [1, \overline{2}]$ is periodic

For, $$\sqrt{2} = 1 + \frac{1}{2+}.\frac{1}{1+}.\frac{1}{2+}...$$

$$\sqrt{2} + 1 = 1 + 1 + \frac{1}{2+}.\frac{1}{1+}.\frac{1}{2+}... = [2, 2, \therefore] = [\overline{2}] \text{ is purely periodic}$$

$$\sqrt{6} = 2 + \frac{1}{2+}.\frac{1}{4+}.\frac{1}{2+}.\frac{1}{4+}... = [2, \overline{2,4}] \text{ is periodic}$$

$$\sqrt{6} + 2 = 2 + 2 + \frac{1}{2+}.\frac{1}{4+}.\frac{1}{2+}.\frac{1}{4+} ... = [\overline{4,2}] \text{ is purely periodic.}$$

Some result.

Note: We note the numerators p_n and the denominators q_n of the convergents $c_n = \frac{p_n}{q_n}$ of the infinite continued fraction

$$[a_0, a_1, ..., a_n, ...]$$

satisfy the result $$p_n q_{n-1} - p_{n-1} q_n = (-1)^n$$

and this gives, $$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$$ and this gives

Theorem: 5.24. $c_n - c_{n-1} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$, $n \geq 2$

Theorem 5.25. $c_n - c_{n-2} = \frac{a_n (-1)^n}{q_n q_{n-2}}$, $n \geq 3$

Proof: $$c_n - c_{n-2} = \frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{p_n q_{n-2} - p_{n-2} q_n}{q_n q_{n-2}}$$

Putting $p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$, we get

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) \\ &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \; a_n (-1)^{n-1} \end{aligned}$$

and therefore we get finally,

$$\begin{aligned} c_n - c_{n-2} &= \frac{a_n (-1)^{n-2}}{q_n q_{n-2}} \\ &= \frac{(-1)^n a_n}{q_n q_{n-2}} \end{aligned}$$

Note: If α is a periodic infinite continued fraction then α is a root of some equation of the type

$$ax^2 + bx + c = 0 \qquad ...(1)$$

$$a, b, c \in \mathbb{Z}$$

$$a > 0$$

$$b^2 - 4ac > 0, \text{ and is not a perfect square.}$$

Obviously $\alpha \in Q^c$

Example 9. Let $\alpha = 4 + \frac{1}{1+}.\frac{1}{3+}.\frac{1}{4+}\frac{1}{1+}\frac{1}{3+}.\frac{1}{4+}....$

$$= 4 + \frac{1}{1+}.\frac{1}{3+}.\frac{1}{\alpha} \text{ (is periodic)}$$

or $$\alpha = \frac{19\alpha + 5}{4\alpha + 1}$$

or $$4\alpha^2 - 18\alpha - 5 = 0.$$

or α is a root of $4x^2 - 18x - 5 = 0$,

and, α is *a quadratic surd*

Theorem 5.26. If α is a purely periodic infinite continued fraction then α is a root of some equation of the type

$$ax^2 + bx + c = 0 \qquad ...(1)$$

$$a, b, c \in \mathbb{Z},$$

$$a > 0$$

$$b^2 - 4ac > 0$$

and is not a perfect square.

Proof: *Suppose* $\alpha = \overline{[a_0, a_1, a_2, ..., a_n]}$

$$= [a_0, a_1, a_2, ..., a_n, \alpha]$$

$$= \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}} \text{ [a purely periodic ICF]}$$

or $$\alpha^2 q_n + \alpha q_{n-1} - \alpha p_n - p_{n-1} = 0$$

Therefore, α is a root of the equation

$$q_n x^2 + (q_{n-1} - p_n)\, x - p_{n-1} = 0 \qquad ...(*).$$

Thus α is either a quadratic irrational number or a rational number, but the later is ruled out by what we have already proved that the value of any infinite simple continued fraction is irrational.

Next $$\alpha = a_0 + \frac{1}{\alpha_1} > a_0 \geq 1 \text{ gives, } \alpha > 0$$

Now suppose a periodic ICF is

$$\beta = [b_0,b_1,b_2, ..., b_j, \overline{a_0,a_1,a_2,..., a_n}] = [b_0,b_1,b_2, ..., b_j, \alpha]$$

$$= \frac{\alpha m + m'}{\alpha q + q'}$$

where $\frac{m'}{q'}$ and $\frac{m}{q}$ are the last two convergents to $[b_0,b_1,b_2, ..., b_j]$

But α is of the form $\frac{a+\sqrt{b}}{c}$, and hence β is of similar form because, as with α, the possibility of α being rational can be ruled out.

Definition: (1) has two roots α and α', say ($\alpha \neq \alpha'$)

They are called conjugate of each other

Theorem 5.27. Let $\alpha = [a_0,a_1,a_2, ..., a_n]$ is purely periodic,

Then (1) $\alpha > 1$

(2) $-1 < \alpha' < 0$ (i.e., α is reduced)

Proof:

(1) $a_0 = a_n + 1 \geq 1 \Rightarrow a_0 \geq 1$

Theorem 5.28. If α and α' are the two roots of the equation (1)

And α is purely periodic, then

$$\alpha = a_0 + \frac{1}{\alpha_1} > a_0 \geq 1 \Rightarrow \alpha > 1.$$

(ii) $$\alpha = [a_0,a_1,a_2, ..., a_n] = [a_0,a_1,a_2, ..., a_n, \alpha]$$

$$= \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}}$$

or $$\alpha^2 q_n + \alpha q_{n-1} - \alpha p_n - p_{n-1} = 0$$

Therefore, α is a root of the equation

$$f(x) = q_n x^2 + (q_{n-1} - p_n)\, x - p_{n-1} = 0 \qquad ...(*)$$

The other root is α'

It is enough to show that $f(0) < 0$ and, $f(-1) > 0$

Now $f(0) = -p_{n-1} < 0$

And $f(-1) = q_n - (q_{n-1} - p_n) - p_{n-1}$

$= q_n - q_{n-1} + p_n - p_{n-1} \geq 0$

But $f(-1) = 0$ gives $\alpha \in Q$, a contradiction.

Therefore, $f(-1) > 0$.

Definition: A quadratic surd is said to be *reduced*

If (1) $\alpha > 1$

(2) $-1 < \alpha' < 0$

Now is a root of

$$ax^2 + bx + c = 0 \qquad \ldots(1)$$

$$a > 0$$

$$b, c \in \mathbb{Z}$$

$$b^2 - 4ac > 0$$

and α is not a perfect square.

$$\therefore \quad \alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$= \frac{P \pm \sqrt{D}}{Q}, \quad \text{say } P = -b, D = b^2 - 4ac, Q = 2a,$$

where $Q > 0$ and $P, Q, D \in \mathbb{Z}$, $D > 0$

$$\alpha = \frac{-b + \sqrt{b^2 - 4ac}}{2a},$$

$$\alpha' = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \ (\alpha > \alpha')$$

The above supposition gives that

(i) $P < \sqrt{D}$, $0 < P < \sqrt{D}$

(ii) $P > 0$. $\alpha' < 0 \Rightarrow 0 < P < \sqrt{D}$

Now, $\alpha > 1, -1 < \alpha' \Rightarrow \alpha + \alpha' > 0$

or $2(P/Q) > 0$ or $P > 0$

$\alpha > 1$ gives $\dfrac{P + \sqrt{D}}{Q} > 1$ or $Q < P + \sqrt{D}$,

Again, $\dfrac{P^2 - D}{Q} = \dfrac{b^2 - (b^2 - 4ac)}{Q} = \dfrac{4ac}{2a} = 2c \in Z$

$\therefore \quad Q \mid P^2 - D$

$\therefore$ (ii) $0 < Q < 2\sqrt{D}$

(iiii) $Q \mid P^2 - D$

Hence we get.

Lemma 5.29. (i) $0 < P < \sqrt{D}$

(ii) $0 < Q < 2\sqrt{D}$

(iii) $Q \mid P^2 - D$.

Lemma 5.30. Let $\alpha = \dfrac{P + \sqrt{D}}{Q}$ be reduced with $Q \mid P^2 - D$ and $a_0 = [\alpha]$, $\alpha = a_0 + \dfrac{1}{\alpha_1}$

Then α_1 is reduced and we can write

$$\alpha_1 = \frac{P_1 + \sqrt{D}}{Q_1}, \text{ where } P_1, Q_1, D \in Q^c; Q_1 \mid P^2{}_1 - D$$

Proof: $\dfrac{1}{\alpha_1} = \alpha - a_0$

Gives $$\alpha_1 = \frac{1}{\alpha - a_0} = \frac{P^* + R^* \sqrt{D}}{Q^*}, P^*, Q^*, R^* \in \mathbb{Z}$$

Since α_1', the conjugate of α_1 is obtained from α_1 by changing the sign of $\sqrt{D}$,

$\therefore$ $$\frac{1}{\alpha_1'} = \alpha_1 - a_0, \text{ since, } \alpha > 1, a_0 \geq 1$$

So $$\frac{1}{\alpha_1'} < -1, \text{ (since, } \alpha' < 0)$$

We have $$\alpha = \frac{P + \sqrt{D}}{Q} \text{ and } \alpha = a_0 + \frac{1}{\alpha_1}$$

or $$\frac{1}{\alpha_1} = \alpha - a_0 = \frac{P - a_0 Q + \sqrt{D}}{Q}$$

or $$\alpha_1 = \frac{Q}{P - a_0 Q + \sqrt{D}} = \frac{Q(\sqrt{D} - (P - a_0 Q))}{D - (P - a_0 Q)^2}$$

$$\text{Denominator} = D - P^2 + 2a_0 PQ - a_0{}^2 Q^2$$
$$= Q\,(Q' + 2a_0 P - a_0{}^2 Q) = QQ_1 \text{(say)}, Q_1 \in \mathbb{Z}$$

Now $Q \mid P^2 - D$ gives $Q \mid D - P^2$

or $$D - P^2 = QQ' \text{ (say)}, Q' \in \mathbb{Z}$$

$\therefore$ $$\alpha_1 = \frac{P_1 + \sqrt{D}}{Q_1}, P_1, Q_1 \in \mathbb{Z}$$

and $$D - P_1{}^2 = QQ_1$$

gives $Q_1 \mid D - P_1{}^2$ or $Q_1 \mid P_1{}^2 - D$.

Lemma 5.31. Let $\alpha = [a_0, a_1, \ldots, a_n]$

Then α_n is reduced and $\alpha_n = \dfrac{P_n + \sqrt{D}}{Q_n}$ $P_n, Q_n \in \mathbb{Z}$, $Q_n \mid D - P_n$

Proof: Applying the Lemma 5.30 times we get the result.

Lemma 5.32. The CF for $\alpha \in Q^c$ is periodic

Proof: Let $\alpha = [a_0, a_1, \ldots a_n, \alpha_{n+1}]$.

It is enough to show that

$$\exists i, j \hat{I} \mathbb{N},\ i < j, \text{ such that } \alpha_i = \alpha_j$$

By lemma 3, $\alpha_n = \dfrac{P_n + \sqrt{D}}{Q_n}$, where α_n is reduced and $P_n, Q_n, D \in \mathbb{Z}$.

Again we have, $0 < P_n < \sqrt{D}$

$$0 < Q_n < 2\sqrt{D}$$

$\therefore$ $\exists$

only finitely many integers (P_n, Q_n) since, P_n, Q_n, are bounded.

Since the choice of n is infinite ($n \in \mathbb{N}$), (P_n, Q_n) must coincide for some different values. i.e., $\exists$

$i < j$ such that $(P_i, Q_i) = (P_j, Q_j)$ (does not mean the GCD)

i.e., $\alpha_i = \alpha_j \qquad \left[\alpha_n = \dfrac{P_n}{Q_n} \ldots\right]$

Lemma 5.33. The α_i of the last lemma can be chosen to be α_0 $(=a_0)$ so that CF for α is purely periodic.

Proof: by the last lemma we have, $\alpha_i = \alpha_j$, $i < j$.

Suppose $i > 0$ (if $i = 0$, there is nothing to prove)

We know that $a_n = a_n + \dfrac{1}{\alpha_{n+1}}$ and α's are reduced.

The same relation must connect their conjugate

i.e., $\alpha_n' = a_n + \dfrac{1}{\alpha'_{n+1}}, \ 0 > \alpha'_n > -1$

$\therefore$ $-\dfrac{1}{\alpha'_{n+1}} = a_n - \alpha'_n$

and so, $\left[-\dfrac{1}{\alpha'_{n+1}}\right] = a_n$ ...(i)

Now, $\alpha_{i-1} = a_{i-1} + \dfrac{1}{\alpha_i}$

and, $\alpha_{j-1} = a_{j-1} + \dfrac{1}{\alpha_j}$, ...(ii)

and $a_{i-1} = \left[-\dfrac{1}{\alpha'_i}\right]$ [by (i)]

$$1 = \left[-\frac{1}{\alpha'_j}\right] = a_{j-1} \text{ gives } a_{i-1} = a_{j-1} \text{ also, } \alpha_j = \alpha_j$$

gives $$\frac{1}{\alpha_i} = \frac{1}{\alpha_j}, \qquad \text{...(iii)}$$

using (iii), (ii) gives

$$\alpha_{i-1} = \alpha_{j-1}$$

Applying this i times, we get

$$\alpha_0 (= a_0) = \alpha_{j-1} = \alpha_k \text{ (say)}$$

$$\therefore \quad \alpha = a_0 + \frac{1}{a_1 +}\cdot\frac{1}{a_2 +} \cdots \frac{1}{a_{k-1} +}\cdot\frac{1}{\alpha_k}$$

$$= a_0 + \frac{1}{a_1 +}\cdot\frac{1}{a_2 +} \cdots \frac{1}{a_{k-1} +}\cdot\frac{1}{a_0} \cdots$$

$$= [\overline{a_1 . a_2 \ldots, a_{k-1}}].$$

Consider $N \in \mathbb{N}$, $N \neq$ a perfect square.

Now CF for $\sqrt{N}$ cannot certainly be purely periodic, because the conjugate of $\sqrt{N}$ is $-\sqrt{N}$ and this does not lie between -1 and 0

Let $[\sqrt{N}] = a_0$ and consider $\sqrt{N} + a_0$.

Conjugate of this number is $-\sqrt{N} + a_0$ which does lie between -1 and 0

Hence CF for $\sqrt{N} + a_0$ is purely periodic.

If $$\sqrt{N} = a_0 + \frac{1}{a_1 +}\frac{1}{a_2 +} \cdots \frac{1}{a_{n-1} +}\frac{1}{a +} \cdots$$

Then, $$\sqrt{N} + a_0 = 2a_0 + \frac{1}{a_1 +}\frac{1}{a_2 +} \cdots \frac{1}{a_n +}\frac{1}{2a_0 +}\frac{1}{a_1 +} \cdots$$

Consequently, the expansion for $\sqrt{N}$ is

$$\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, 2a_0}],$$

where the period starts after the first term and ends with the term $2a_0$

e.g., $$\sqrt{2} = 1 + \frac{1}{2+}\frac{1}{2+} \ldots \text{ and } [\sqrt{2}] = 1, \sqrt{2} = [1, \overline{2}]$$

$$\sqrt{2} + 1 = 2 + \frac{1}{2+}\frac{1}{2+} \ldots \text{ ---- ---- } \ldots = [\overline{2}]$$

$$\sqrt{6} = [2,2,4], [\sqrt{6}] = 2, \sqrt{6} + 2 = [\overline{4,2}]$$

Example 10. Evaluate the infinite continued fraction [1, 1, 1, ...]

Solution: Let $m = [1, 1, 1, \ldots]$.

Then $m = m + 1/m$

And this gives

$$m^2 - m + 1 = 0$$

Therefore, $$m = \frac{1+\sqrt{1+4}}{2} = \frac{1+\sqrt{5}}{2}.$$

5.6 PELL'S EQUATION

$$x^2 - Ny^2 = 1 \qquad ...(1)$$

$$N \in \mathbb{N}$$

$$x, y \in \mathbb{Z}$$

Case I: N = a perfect square, say n^2, then (1) becomes $x^2 - (ny)^2 = 1$

$$\therefore \quad (x + ny)(x - ny) = 1$$

or $$x = \pm 1$$

$$y = 0$$

are the only solution; so we are not interested in this case.

Case II: $N \neq$ a perfect square

Let $$[\sqrt{N}] = a_0$$

Therefore, $$\sqrt{N} + a_0 = 2a_0 + \frac{1}{a_1 +}\frac{1}{a_2 +} \cdots \frac{1}{a_n + 2a_0}$$

so $$\sqrt{N} = a_0 + \frac{1}{a_1 +}\frac{1}{a_2 +} \cdots \frac{1}{a_n + 2a_0} \cdots$$

Now let,

$\frac{p_{n-1}}{q_{n-1}}$ and $\frac{p_n}{q_n}$ be the two convergents coming immediately before the term $2a_0$

i.e., $$\frac{p_{n-1}}{q_{n-1}} = a_0 + \frac{1}{a_1 +}\frac{1}{a_2 +} \cdots \frac{1}{a_{n-1}}$$

$$\frac{p_n}{q_n} = a_0 + \frac{1}{a_1 +}\frac{1}{a_2 +} \cdots \frac{1}{a_n}$$

By a former formula we get

$$\sqrt{N} = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} \qquad ...(i)$$

where α_{n+1} is the complete quotient after a_n

i.e., $$\sqrt{N} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots\ldots a_n + \cfrac{1}{\alpha_{n+1}}}}}$$

$\therefore \quad \alpha_{n+1} = \sqrt{N} + a_0$

Substituting this value for α_{n+1} in (i) we get

$$\sqrt{N}(\sqrt{N} + a_0)q_n + \sqrt{N}\, q_{n-1} = (\sqrt{N} + a_0)\, p_n + p_{n-1}$$

Here $\sqrt{N} \in Q^c$ and all others $\in \mathbb{N}$

This gives

$$Nq_n = a_0 p_n + p_{n-1}$$

$$a_0 q_n + q_{n-1} = p_n$$

Therefore,

$$p_{n-1} = Nq_n - a_0 p_n$$

$$q_{n-1} = p_n - a_0 q_n$$

Substituting this in $p_n q_{n-1} - p_{n-1}\, q_n = (-1)^{n-1}$, we get

$$p_n(p_n - a_0 q_n) - (Nq_n - a_0 p_n)\, q_n = (-1)^{n-1}$$

or $$p_n^2 - Nq_n^2 = (-1)^{n-1} \qquad \ldots(*)$$

If n is odd, (p_n, q_n) is a solution of Pell's equation $x^2 - Ny^2 = 1$

If n is every, we take two consecutive convergents at the end of the next period etc.,

i.e., $$\sqrt{N} + a_0 = 2a_0 + \frac{1}{a_1 +}\frac{1}{a_2 +}\ldots\frac{1}{a_n +}\frac{1}{2a_0 +}\frac{1}{a_1 +}\frac{1}{a_2 +}\ldots\frac{1}{a_n +}\ldots \text{ --- ---}$$

Since the term a_n when it occurs for the 2nd time would be a_{2n+1} if the terms were numbered consecutively and therefore to consider the new convergents, we have to change n in (*) into $2n + 1$ giving

$$p_{2n+1}^2 - Nq_{2n+1}^2 = (-1)^{2n+1}$$

and therefore,

Theorem 5.34. (p_{2n+1}, q_{2n+1}) is a solution of Pell's equation in terms of convergents.

Example 11. Find a solution of $x^2 - 21y^2 = 1$

Solution: Here, $N = 21$,

$$\sqrt{21} = 4 + \frac{1}{\alpha_1},\ \alpha_1 = \frac{1}{\sqrt{21} - 4} = \frac{\sqrt{21} + 4}{5}\ 1 + \frac{1}{\alpha_2}$$

or, $$\alpha_1 = 1 + \frac{1}{\alpha_2}$$

$$\therefore \quad \alpha_2 = \frac{1}{\alpha_1 - 1} = \frac{1}{\frac{\sqrt{21}+4}{5} - 1} = \frac{5}{\sqrt{21}-1} = \frac{5(\sqrt{21}+1)}{20} = \frac{\sqrt{21}+1}{4}$$

or, $$\alpha_2 = 1 + \frac{1}{\alpha_3};$$

$$\therefore \quad \alpha_3 = \frac{1}{\alpha_2 - 1} = \frac{4}{\sqrt{21}+1-4} = \frac{1}{3}(\sqrt{21}+3)$$

or, $$\alpha_3 = 2 + \frac{1}{\alpha_4}$$

$$\therefore \quad \alpha_4 = \frac{1}{\alpha_3 - 2} = \frac{3}{\sqrt{21}+3-6} = \frac{3}{\sqrt{21}-3} = \frac{\sqrt{21}+3}{4}$$

or, $$\alpha_4 = 1 + \frac{1}{\alpha_5}$$

$$\therefore \quad \alpha_5 = \frac{1}{\alpha_4 - 1} = 0 = \frac{1}{5}(\sqrt{21}+1)$$

or, $$\alpha_5 = 1 + \frac{1}{\alpha_6},$$

$$\therefore \quad \alpha_6 = \frac{1}{\alpha_5 - 1} = \frac{5}{\sqrt{21}-4} = \sqrt{21}+4$$

or, $$\alpha_6 = 8 + \frac{1}{\alpha_7}$$

$$\therefore \quad \alpha_7 = \frac{1}{\alpha_6 - 8} = \frac{1}{\sqrt{21}+4-8} = \frac{\sqrt{21}+4}{5} = \alpha_1$$

$$\therefore \quad \sqrt{21} = 4 + \frac{1}{1+}\frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{1+}\frac{1}{8+}\frac{1}{1+}\ldots = [4, \overline{1,1,2,1,1,8}]$$

$\therefore$ $\sqrt{21} + 4$ is purely periodic.

Here $n = 5$

$\therefore$ the convergents are:

$$\frac{p_0}{q_0} = \frac{4}{1}$$

$$\frac{p_1}{q_1} = \frac{5}{1}$$

$$\frac{p_2}{q_2} = \frac{9}{2}$$

$$\frac{p_3}{q_3} = \frac{23}{5}$$

$$\frac{p_4}{q_4} = \frac{32}{7}$$

$$\frac{p_5}{q_5} = \frac{55}{12}$$

$$\therefore \quad \left.\begin{matrix} x = 55 \\ y = 12 \end{matrix}\right\}.$$

Example 12. *Solve:* $x^2 - 29y^2 = 1$

Solution: $\sqrt{29} = [5, \overline{2,1,1,2,10}]$

so $\sqrt{29} + 5 = \left[\overline{10,2,1,1,2}\right]$

Here $n = 4$.

then $x = p_{2n+1} = p_9$

$y = q_{2n+1} = q_9$

Convergence are

$$\frac{5}{1}, \frac{11}{2}, \frac{16}{3}, \frac{27}{5}, \frac{70}{13}, \frac{727}{135}, \frac{1524}{283}, \frac{2251}{418}, \frac{3775}{418}, \frac{3775}{701}, \frac{9801}{1820}$$

$$\therefore \quad \left.\begin{matrix} x = 9801 \\ y = 1820 \end{matrix}\right\}.$$

Example 13. Find a particular solution of he equation $x^2 - 21y^2 = 1$

Solution: Here $N = 21$, and the continued fraction expansion of $\sqrt{21}$ is

$$\sqrt{21} = [4, \overline{1,1,2,1,1,8}] = [a_1, \overline{a_2, a_3, a_4, a_5, a_6, 2a_1}]$$

and this shows that $n = 6$, an even number. A calculation shows that $n = 6$, an even number. A calculation show that

$$c_6 = \frac{55}{12}$$

so that $x_1 = p_6 = 55$

$y_1 = q_6 = 12,$

and $x_1^2 - 21y_1^2 = 55^2 - 21.12^2 = 3025 - 3024 = 1$

Hence, $\left.\begin{matrix} x_1 = 55 \\ y_1 = 12 \end{matrix}\right\}$ is a particular solution of the given equation.

[Partial quotients begins from a_1]

Theorem 5.35. If (x_1, y_1) is the least positive solution of $x^2 - Ny^2 = 1$, then all the other positive solutions (x_n, y_n) can be obtained from the equation

$$x_n + y_n \sqrt{N} = (x_1 + y_1 \sqrt{N})^n \qquad ...(\&)$$

by setting $n = 1, 2, 3, ...$

Proof: The values of x_n and y_n are obtained from

$x_n + y_n \sqrt{N} = (x_1 + y_1\sqrt{N})n$ by expanding the term

$(x_1 + y_1 \sqrt{N})^n$ by binomial theorem and equating the rational and purely irrational parts of the resulting equation.

For, if (x_1, y_1) is the least positive solution of $x^2 - N y^2 = 1$,

then the solution (x_2, y_2) can be found by taking $n = 2$ in (&).

This gives

$$\begin{aligned} x_2 + y_2 \sqrt{N} &= (x_1 + y_1 \sqrt{N})^2 \\ &= (x_1^2 - Ny_1^2) + (2x_1y_1) \sqrt{N} \end{aligned}$$

So that $x_2 = x_1^2 + Ny_1^2$

and $y^2 = 2x_1y_1$.

Using these values, a direct calculation shows that

$$\begin{aligned} x_2^2 - Ny_2^2 &= (x_1^2 + N y_1^2) - N(2x_1y_1)^2 \\ &= x_1^4 + 2 N x_1^2y_1^2 + N^2 y_1^2 - 4N x_1^2 y_1^2 \\ &= x_1^4 - 2 N x_1^2y_1^2 + N^2y_1^4 \\ &= (x_1^2 - N y_1^2)^2 \\ &= 1 \end{aligned}$$

It can be easily shown that

$$x_n^2 - Ny_n^2 = (x_1^2 - Ny_1^2)^n = 1$$

Thus, x_n and y_n are solutions of the equation $x^2 - Ny^2 = 1$.

Example 14. Find a second solution of the equation $x^2 - 21y^2 = 1$

Solution: A second solution (x_2, y_2) can be obtained by setting $n = 2$ in

$$x_n + y_n \sqrt{N} = (x_1 + y_1\sqrt{N})^n$$

where $N = 21$

$x_1 = 55$

and $y_1 = 12$

this gives

$$\begin{aligned} x_2 + y_2 \sqrt{21} &= (55 + 12\sqrt{21})^2 \\ &= 3025 + 1320\sqrt{21} + 3024 \\ &= 6049 + 1320\sqrt{21} \end{aligned}$$

and this gives that

$$x_2 = 6049$$
$$y_2 = 1320.$$

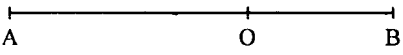
These values satisfy the equation $x^2 - 21y^2 = 1$,

Since

$$(6049)^2 - 21(1320)^2 = 6590401 - 46590400 = 1.$$

Note: In general, the solutions of Pell's equation becomes large very fast.

5.7 FIBBONACI NUMBERS



The line segment AB is divided at O in two parts so that

$$AB: AO = AO: OB \qquad \text{...(i)}$$

Suppose

$AO = x$ and $OB = 1$ then we get

$$\frac{x+1}{x} = \frac{x}{1} \text{ or } x^2 - x - 1 = 0 \qquad \text{...(ii)}$$

Since the root of this equation should be only positive,

so $$x = \frac{-1+\sqrt{5}}{2}$$

This value of x is usually denoted by the latter ϕ and is called the Golden Ratio.

From (ii) we get

$$x^2 = x + 1 \text{ or, } x = 1 + \frac{1}{x}$$

and putting $\frac{1}{x}$ in place of x we get the following infinite continued fraction:

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ldots}}}} = [1, 1, 1, 1, \ldots]$$

And the corresponding convergents are here,

$$C_1 = 1,$$

$$C_2 = 1 + \frac{1}{1} = \frac{2}{1},$$

$$C_3 = 1 + \cfrac{1}{1 + \cfrac{1}{1}} = \frac{3}{2},$$

$$C_4 = \frac{5}{3}, C_5 = \frac{8}{5}, C_6 = \frac{13}{8}, \ldots \text{ etc.}$$

The numbers we observe in the above convergents are

$$1, 1, 2, 3, 5, 8, 13, \ldots \text{ etc}$$

and these are given in the following formula:

$$F_1 = 1,\ F_2 = 1,\ F_n = F_{n-1} + F_{n-2},\ n \geq 3$$

Sometimes the sequence is assumed to start from 0 and then we write in the following form:

$$F_0 = 0,\ F_1 = 1,\ F_{n+1} = F_n + F_{n-1},\ n \geq 1$$

And this is called the *Fibonaci sequence.*

Fibonacci sequence is named after Fibonacci, an Italian mathematician of the thirteenth century who used this sequence to solve a problem about rabbit populations.

Example 15. $F_1 = 1,\ F_2 = 1,\ F_n = F_{n-1} + F_{n-2},\ n \geq 3$ is given as the Fibonacci sequence:

Prove that

$$F_1 + F_2 + F_3 + \ldots + F_n = F_{n+2} - 1$$

Solution: Since, $1 = F_1 = 2 - 1 = F_3 - 1$, the formula is true for $n = 1$.

Assume that the result is true for 1, 2, 3, ... k

Now

$$\begin{aligned} F_1 + F_2 + \ldots + F_{k+1} &= (F_1 + F_2 + \ldots + F_k) + F_{k+1} \\ &= (F_{k+2} - 1) + F_{k+1} \\ &= (F_{k+2} + F_{k+1}) - 1 \\ &= F_{k+3} - 1. \end{aligned}$$

Example 16. Prove that $F_{n+1}^2 - F_n F_{n+2} = (-1)^n$

Solution: As before, $F_2^2 - F_1 F_3 = 1 - 1.2 = -1 = (-1)^1$

Hence the result is true for $n = 1$

Assume that the same is true for 1, 2, ..., k

Now $$\begin{aligned} F_{k+2}^2 - F_{k+1} F_{k+3} &= F_{k+2}(F_{k+1} + F_k) - F_{k+1}(F_{k+2} + F_{k+1}) \\ &= F_{k+2} F_k - F_{k+1}^2 \\ &= -(F_{k+1}^2 - F_k F_{k+2}) = -(-1)^k = (-1)^{k+1} \end{aligned}$$

And the result follows by induction.

The Fibonacci numbers satisfy many identities.

We note the following example:

Here the Fibonacci sequence is defined as follows:

$$f_1 = 1, f_2 = 1, f_n = f_{n-1} + f_{n-2} \text{ for } n \geq 3.$$

Now we note the following:

$$f_1 = 1,$$
$$f_1 + f_2 = 1 + 1 = 2,$$
$$f_1 + f_2 + f_3 = 1 + 1 + 2 = 4,$$
$$f_1 + f_2 + f_3 + f_4 = 1 + 1 + 2 + 3 = 7,$$
$$f_1 + f_2 + f_3 + f_4 + f_5 = 1 + 1 + 2 + 3 + 5 = 12$$

The very pattern of the above arrangement helps us to guess that

$$\sum_{j=1}^{n} f_j = f_{n+2} - 1$$

Example 17. Prove that in Fibonaci sequence

$$\sum_{j=1}^{n} f_j = f_{n+2} - 1$$

Solution: Proof will be by induction as follows:

We note that $\sum_{1}^{1} f_j = 1$ and this is same as $f_1 + 2 - 1 = f_3 - 1 = 2 - 1 = 1$. The inductive hypothesis is

$$\sum_{j=1}^{n} f_j = f_{n+2} - 1$$

Now we show that

$$\sum_{j=1}^{n+1} f_j = f_{n+3} - 1$$

Now

$$\sum_{j=1}^{n+1} f_j = \left[\sum_{j=1}^{n} f_j\right] + f_{n+1}$$
$$= (f_{n+2} - 1) + f_{n+1} = (f_{n+2} + f_{n+1}) - 1 = f_{n+3} - 1.$$

EXERCISES 5.1

1. Let $\frac{a}{b}$ and $\frac{a'}{b'}$ be the fractions immediately to the left and right of the fraction ½ in the Farey sequence of order n. Prove that $b = b' = 1 + 2\left[\frac{n-1}{2}\right]$, that is, b is the greatest odd integer $\leq n$. Also prove that $a + a' = b$.]

2. If $\frac{a}{b}, \frac{a'}{b'}, \frac{a''}{b''}$ are any three consecutive fractions in the Farey sequence of order n, then prove that $\frac{a'}{b'} = \frac{a + a''}{b + b''}$.

3. Given that $\frac{a}{b}$ and $\frac{a'}{b'}$ run through all pairs of adjacent fractions in the Farey sequence of order $n > 1$. Prove that

   Prove that

$$\min\left(\frac{a'}{b'}, \frac{a}{b}\right) = \frac{1}{n(n-1)} \text{ and } \max\left(\frac{a'}{b'}, \frac{a}{b}\right) = \frac{1}{n}.$$

4. $\frac{a}{b}$ and $\frac{c}{d}$ are two rational numbers such that $ad - bc = 1$, $b > 0$, $d > 0$; $n = \max(b, d)$. Prove that $\frac{a}{b}$ and $\frac{c}{d}$ are adjacent fractions in the Farey sequence of order n.
5. Prove that in the Farey sequence of order $n + 1$ the above-mentioned two fractions need not be adjacent.

EXERCISES 5.2

1. Expand the rational fractions 14/5, –63/25, 101/201 into finite simple continued fractions.
2. Convert the following expansion of continued fractions into rational fractions:

   [5, 1, 2], [0, 5, 1, 2], [8].

3. Let $a_0, a_1, ..., a_n$ and $b_0, b_1, b_2, ..., b_{n+1}$ be positive integers. Prove the necessary and sufficient condition that $[a_0, a_1, ..., a_n] < b_0, b_1, ..., b_{n+1}]$ are that
   (i) $a_j = b_j$ for $0 \le j \le n$, then n must be even.
   (ii) if $r = \text{Min}(j)$ such that $a_j \ne b_j$ and $r \le n - 1$, then we require $a_r < b_r$, but for r odd, $a_r > b_r$.
   (iii) in case $r = n$, then for n even we require $a_n < b_n$, but for n odd we require $a_n > 1 + b_n$, or $a_n = 1 + b_n$ with $b_{n+1} > 1$.
4. Let $a_1, a_2, ..., a_n$ and c be positive real numbers. Prove that

$$[a_0, a_1, ..., a_n] > [a_0, a_1, ..., a_n + c]$$

   holds if n is odd, but is false if n is even.
5. Evaluate the infinite continued fraction [2, 1, 1, ...] and [2, 3, 1, 1, 1, ...]
6. Evaluate the infinite continued fractions:
   (i) [2, 2, 2, ...],
   (ii) [1, 2, 1, 2, ...]
   (iii) [2, 1, 2, 1, ...]
   (iv) [1, 3, 1, 2, 1, 2, ...]
7. If two irrational numbers have identical convergents $\frac{p_0}{q_0}, \frac{p_1}{q_1}$, upto $\frac{p_n}{q_n}$, prove that their continued fraction expansions are identical upto a_n.

8. α, β, γ are irrational numbers with $\alpha < \beta < \gamma$. If α and γ have identical convergents $\frac{p_0}{q_0}, \frac{p_1}{q_1}$, upto $\frac{p_n}{q_n}$, prove that β also has these same convergents upto $\frac{p_n}{q_n}$
9. Find the general integral solutions of the following equations. Check each answer.
   (i) $13x - 17y = 1$
   (ii) $65x - 56y = 1$
   (iii) $56x - 65y = 1$
   (iv) $13x - 17y = -1$.
   (v) $65x - 56y = -1$.
   (vi) $13x - 17y = 5$
   (vii) $56x - 65y = -3$
10. Two of these six equations do not have integral solutions. Find the general solutions in integers of the others.
   (i) $183x + 147y = 9$
   (ii) $34x - 49y = 5$
   (iii) $183x - 174y = 9$
   (iv) $77x + 63y = 40$
   (v) $34x + 49y = 5$
   (vi) $56x - 20y = 11$

EXERCISES 5.3

1. Prove that $F_n (< 7/4)^n$ where F_n is the n^{th} term of Fibonacci Sequence
2. Prove that $F_2 + F_4 + F_6 + \ldots + F_{2n} = F_{2n+1} - 1$
3. $F_1F_2 + F_2F_3 + F_3F_4 + \ldots + F_{2n-1}F_{2n} = F_{2n}^2$
4. $F_1F_2 + F_2F_3 + F_3F_4 + \ldots + F_{2n}F_{2n+1} = F_{2n+1}^2 - 1$
5. The *Lucas number* L_n are defined by the equations
   $$L_1 = 1, \text{ and } L_n = F_{n+1} + F_{n-1} \text{ for each } n \geq 2.$$
   Prove that $L_n = L_{n-1} + L_{n-2} (n \geq 3)$
   Prove that $F_{2n} = F_n L_n$
6. Prove that
   $$L_1 + 2L_2 + 4L_3 + 8L_4 + \ldots + 2^{n-1}L_n = 2^n F_{n+1} - 1$$
7. Write down the first ten terms of the Fibonacci series. Prove in general that any two consecutive terms are relatively prime.
8. Prove that the Fibonacci numbers satisfy the inequalities
   $$\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} < F_{n+1} < \left(\frac{1+\sqrt{5}}{2}\right)^n, \text{ if } n > 1.$$

9. Prove that $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$ for any positive integers m and n. Then prove that $F_m \mid F_n$ if $m \mid n$

(Take $n = mq$ and use induction on q)

10. Prove that for $n \geq 2$.

$$F_n = \sum_{r=1}^{j} {}^{n-r}C_{r-1}$$

such that $2j \leq n + 1$ [use the fact that ${}^{m}C_r = {}^{m-1}C_{r-1} + {}^{m-1}C_r$]

11. Find the following Fibonaci numbers (f_n denotes the n^{th} Fibonacci numbers)

(a) f_{10} (b) f_{15} (c) f_{20} (d) f_{13} (e) f_{18} (f) f_{25}

12. Use the fact that $f_k = f_{k+2} - f_{k+1}$ for every positive integer k to find $\sum_{k=1}^{n} f_k$

13. Determine a formula for $\sum f_{2j-1} = f_1 + f_3 + \ldots + f_{2n-1}$ where n is a positive integer by examining the value of this sum for all small positive integers. Prove this formula using mathematical induction.

14. Prove that $\sum_{j=1}^{n} f_j^2 = f_1^2 + f_2^2 + \ldots + f_n^2 = f_nf_{n+1}$ for every positive integer n.

15. Prove that $f_{n+1}f_{n-1} - f_n^2 = (-1)^n$ for every positive integer n

16. Prove that $f_{n+1}f_n - f_{n-1}f_{n-2} = f_{2n-1}$ for every positive integer n, $n > 2$.

17. Prove that $f_1f_2 + f_2f_3 + \ldots + f_{2n-1}f_{2n} = f_{2n}^2$ if n is a positive integer.

18. Let $F = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. Show that $F^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}$ when $n \in Z+$

By taking determinants of both sides of the result above prove exercise (15)

19. Show that $x_1 = 8$, $y_1 = 3$ is a solution of the equation

$x^2 - 7y^2 = 1$

20. Show that $x_1 = 18$, $y_1 = 5$ is a solution of the equation

$x^2 - 13y^2 = -1$, and proceed to the next period to find a solution of the equation $x^2 - 13y^2 = 1$

21. Show that $x_1 = 17$, $y_1 = 4$ is the minimal solution of the equation

$x^2 - 18y^2 = 1$.

Find the next two solutions.

22. Show that $x_1 = 3$, $y_1 = 1$ is the minimal solution of the equation

$$x^2 - 10y^2 = -1.$$

Find a second solution by setting $n = 3$.

6

QUADRATIC RESIDUES, LEGENDER'S SYMBOLS, JACOBI'S SYMBOLS

6.1 QUADRATIC RESIDUES

Consider the general quadratic congruence

$$ax^2 + bx + c \equiv 0(\text{mod } m),\ a \not\equiv 0(\text{mod } m) \qquad ...(1)$$

Note: (1) is a particular case of general congruence of n^{th} degree. There we have reduced the problem of (mod m) to a series of problems mod p, a prime and the solutions mod p were to be found by trial of all residue classes.

This is feasible for small p but impracticable for large p

It is that defect which we propose to remain the case of quadratic congruence in the sense of proving another way of deciding whether another solution exists.

Definition: If $b \equiv 0(\text{mod } m)$ in (1), then (1) is called a *pure quadratic congruence* (*pure Q.C.*)

i.e., $ax^2 + c \equiv 0(\text{mod } m),\ a \not\equiv 0(\text{mod } m)$ is a pure quadratic congruence

Theorem 6.1. Let p be an odd prime [for $p = 2$ it is trivial]

And if $a \not\equiv 0(\text{mod } p)$ then,

$$ax^2 + bx + c \equiv 0(\text{mod } p) \qquad ...(1')$$

is equivalent to the chain of the following congruences

$$u^2 \equiv b^2 - 4ac(\text{moc } p)$$
$$2ax \equiv u - b(\text{mod } p)$$

Proof: By hypothesis $(4a, p) = 1$. Therefore (1') is equivalent to

$$4a^2x^2 + 4abx + 4ac \equiv 0(p)$$

or $$(2ax + b)^2 \equiv b^2 - 4ac(\text{mod } p)$$

or $$u^2 \equiv b^2 - 4ac(\text{mod } p), \text{ where } u \equiv 2ax + b(\text{mod } p)$$

i.e., $$2ax \equiv u - b(\text{mod } p).$$

Note: If there is no u satisfying $u^2 \equiv b^2 - 4ac(\text{mod } p)$ then there is no x satisfying the given congruence (1') and if there is a u satisfying

$u^2 \equiv b^2 - 4ac(\text{mod } p)$, then because $(2a, p) = 1$ there is an x satisfying $2ax \equiv u - b(\text{mod } p)$ and satisfying the given congruence.

Remark: The solution of the general quadratic congruence mod m reduces finally to solutions of pure Q.C. modulo a prime.

Hence we may consider a congruence of the form

$$x^2 \equiv a(\text{mod } p),\ (a, p) = 1,\ p \text{ an odd prime.}$$

Remark: The case $a \equiv 0(\text{mod } p)$ i.e., $(a, p) \neq 1)$ is trivial having the unique solution $x \equiv 0(\text{mod } p)$.

Definition: If the congruence $x^2 \equiv a(\text{mod } m)$ has a solution, then a is said to be *a quadratic residue (q.r.) (R) mod m.*

If there is no solution then a is said to be *a Quadratic non-residue (q.n.r.) (N) mod m*

e.g., $x^2 \equiv a(\text{mod } 13)$

Congruence	Solution	R or N
$x^2 \equiv 1(\text{mod } 13)$	$x \equiv 1$	1 is an R
$x^2 \equiv 1(\text{mod } 13)$	No solution	2 is an N
$x^2 \equiv 1(\text{mod } 13)$	$x \equiv 3$	3 is an R
$x^2 \equiv 1(\text{mod } 13)$	$x \equiv 4$	4 is an R
$x^2 \equiv 1(\text{mod } 13)$	No solution	5 is an N
$x^2 \equiv 1(\text{mod } 13)$	No solution	6 is an N
$x^2 \equiv 1(\text{mod } 13)$	No solution	7 is an N
$x^2 \equiv 1(\text{mod } 13)$	No solution	8 is an N
$x^2 \equiv 1(\text{mod } 13)$	$x \equiv 9$	9 is an R
$x^2 \equiv 1(\text{mod } 13)$	$x \equiv 10$	10 is an R
$x^2 \equiv 1(\text{mod } 13)$	No solution	11 is an N
$x^2 \equiv 1(\text{mod } 13)$	$x \equiv 12$	12 is an R

Thus 1, 3, 4, 9, 10, 12 are *R mod* 13

And 2, 5, 6, 7, 8, 11 are *N mod* 13

Euler's Criterion 6.2.

If $(a, p) = 1$, p is an odd prime then

a is a q.r. $(R)(\text{mod } p)$ if $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$

And is a q.n.r. (N) mod p if $a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$

Proof: $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = a^p - 1 \equiv 0 (\text{mod } p)$ (by Fermat Theorem) ...(1)

i.e., $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$ or, $a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$

Let a be a q.r. mod p.

Then $\exists x_0 \in \mathbb{Z}$ such that

$$x_0^2 \equiv a(\text{mod } p)$$

or $$a \equiv x_0^2(\text{mod } p)$$

$$\therefore \quad a^{\frac{p-1}{2}} \equiv \left(x_0^2\right)^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv x_0^{\Phi(p)} \equiv 1(\text{mod } p) \text{ by Fermat's theorem.}$$

Conversely, Let $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$

If g is a primitive root mod p, then,

$$g^{\Phi(p)} \equiv g^{p-1} \equiv 1(p) \text{ and } p-1 \text{ is the least such positive integer}$$

Now $$a^{\lambda} \equiv 1(p), \text{ where, } \lambda \text{ is of the order of a (mod } p)$$

Therefore, $\lambda \mid \frac{p-1}{2}$ gives $\lambda \mid p-1$

$$\therefore \quad p - 1 = \lambda t, \text{ for some } t \in \mathbb{N}.$$

or $$g^{\lambda t} = g^{p-1} \equiv 1 \equiv a^{\lambda}$$

$$\therefore \quad g^t \equiv a(p)$$

$\therefore \exists\ t \in \mathbb{N}$ such that

$$g^t \equiv a(\text{mod } p)$$

Then $$g^{t\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$$

Gives $$p - 1 \mid \frac{t}{2}(p-1)$$

or $$\frac{t}{2} \in \mathbb{N}$$

$$\therefore \quad \left(g^{\frac{t}{2}}\right)^2 \equiv g^t \equiv a(\text{mod } p)$$

$\therefore$ the solution $x^2 \equiv a(\text{mod } p)$

is $$x = g^{\frac{t}{2}}(\text{mod } p)$$

Hence a is an R

Thus,

a is R if $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$

a is N if $a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$.

Corollary 6.3. (1) If a is R and b is R, then ab is also R

Proof:

$\because$ a is R $\quad\therefore\quad a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$ and

$\because$ b is R $\quad\therefore\quad b^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$

$\therefore\quad (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}\, a^{\frac{p-1}{2}}\, b^{\frac{p-1}{2}} \equiv 1.\,1 \equiv 1(\text{mod } p)$

$\therefore$ ab is R.

(2) If a is N and b is R, then ab is N

Proof:

$\because$ a is N $\quad\therefore\quad a^{\frac{p-1}{2}} \equiv -1(p)$

And b is R gives $\quad b^{\frac{p-1}{2}} \equiv 1(p)$

$\therefore\quad (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}\, b^{\frac{p-1}{2}} \equiv -1.\,1 = \equiv -1(p)$

$\therefore$ ab is N.

(3) if a is N and b is N, then ab is R

Proof:

a is N $\therefore\quad a^{\frac{p-1}{2}} \equiv -1(p)$

and b is N $\therefore\quad b^{\frac{p-1}{2}} \equiv -(p)$

$\therefore\quad (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}\, b^{\frac{p-1}{2}} \equiv -1.\,-1 \equiv 1(p)$

$\therefore$ ab is R.

Remark: We have, $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = a^{p-1} - 1 \equiv 0(\text{mod } p)$ ...(i)

From (1) it clear that if $a^{\frac{p-1}{2}} \not\equiv 1(\text{mod } p)$, i.e., if $p \nmid a^{\frac{p-1}{2}} - 1$ (i.e., a is not R or a is N)

Then $P \mid a^{\frac{p-1}{2}} + 1$ i.e., $a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$.

Therefore, a is N if $a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$

Theorem 6.4. There is exactly $\frac{p-1}{2}$ quadratic residue and $\frac{p-1}{2}$ quadratic non residue mod p

Proof: Let R_0 = the number of q.r. (R)

N_0 = the number of q:n.r. (N)

Obviously $R_0 + N_0 = p - 1$ ...(1)

Now a is R gives $a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$ $\therefore$ a is solution of $x^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$

$$\therefore \quad R_0 \leq \frac{p-1}{2} \qquad \text{...(2)}$$

And a is N gives

$$a^{\frac{p-1}{2}} = -1 \text{ (mod P)}$$

$\therefore$ a is a solution of

$$x^{\frac{p-1}{2}} = -1 \text{ (mod } p)$$

$$\therefore \quad \text{No} \leq \frac{p-1}{2} \qquad \text{....(3)}$$

$\therefore$ (1), (2), (3) give $R_0 = \frac{p-1}{2} = N_0$.

Theorem 6.5. If a is R so is also b if $a \equiv b (\text{mod } p)$

Proof: $a \equiv b (\text{mod } p)$ gives $a = b + \lambda p$, $\lambda \varepsilon \mathbb{Z}$

And a is R gives $a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$

or $(b + \lambda p)^{(p-1)/2} \equiv 1 (\text{mod } p)$

or $b^{\frac{p-1}{2}} + \mu p \equiv 1 (\text{mod } p)$ $\mu \varepsilon \mathbb{Z}$

or $b^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$

$\therefore$ b is R.

Lemma 6.6. The congruence $x^{\Phi(p)} = x^{p-1} \equiv 1 (\text{mod } p)$ ...(*)

has $p - 1$ incongruent solutions mod p

viz., $1, 2, 3, \ldots, p - 1$

Proof: Because, this set is incongruent mod p and by Euler's theorem every one satisfies (*).

The set of solution can also be taken as

$$\pm 1^2, \pm 2^2 \pm 3^2 \ldots \pm (\frac{p-1}{2})^2 \qquad \text{...(2)}$$

Because

(i) they are $p - 1$ in number

(ii) they all satisfy (*) obviously.

(iii) they are incongruent mod p,

For if m^2 and n^2 are any two positive roots, $m > n$,

then $$1 \le n < m \le \frac{p-1}{2}$$

or $$0 < m - n < m + n < p - 1 < p$$

or $$m^2 - n^2 = (m + n)(m - n) \not\equiv 0(p) \quad \therefore \quad m^2 \not\equiv n^2(p)$$

Similarly, if m and n are negative, or one is positive, and the other is negative, we can prove the result.

The proof of the following lemma is left as an exercise.

Lemma 6.7. The incongruence roots of $x^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$ ...(Ψ)

are given by $$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

(i) they are $\frac{p-1}{2}$ in numbers

(ii) all of them satisfy (Ψ)

(iii) they are incongruent mod p

Theorem 6.8. $(p, a) = 1 \Rightarrow x^2 \equiv a(\text{mod } p)$ ... (1) has two solutions

Proof: (i) If $a^{\frac{p-1}{2}} \equiv 1(p)$, then a is a solution of $x^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$ ...(2)

Therefore, a is one of $\frac{p-1}{2}$ solutions of (Ψ) in lemma 6.7 So, a is one of

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Let $a = n^2$, $\quad 1 \le n \le \frac{p-1}{2}$

Then (1) has the two incongruent solutions, $x = n$ and $x = -n$

$(n \not\equiv p - n$, for $n \equiv p - n \Rightarrow 2n \equiv p(\text{mod } p) \Rightarrow p \mid n$, impossible

since . $$1 \le n \le \left(\frac{p-1}{2}\right)$$

(ii) Suppose $a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$

If not let $x \equiv c$ be a solution of (1)

$\therefore$ $$c^2 \equiv a(\text{mod } p)$$

or $a \equiv c^2 (\text{mod } p)$,

or $a^{\frac{p-1}{2}} \equiv (c^2)^{(p-1)/2}$
$\equiv c^{p-1} \equiv 1 (\text{mod } p)$, by Euler's theorem

i.e., $a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$ which is not the case, Hei. e.

Example 1. If prime $p \equiv 1 (\text{mod } 4)$ and a is a q.r. of p, show that

$p - a$ is also a q.r. of p

Hence show that

if a_i $(i = 1, 2, 3, ..., \frac{p-1}{2})$ are q.r. of p satisfying $0 < a_i < p$, then

$$\sum_{i=1}^{\frac{1}{2}(p-1)} a_i = \frac{1}{4} p(p-1)$$

Solution: If $x^2 \equiv a (\text{mod } p)$ has a solution, then a is a q.r. of p

If a is a q.r. of p, then

$a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$ and conversely.

Here $p \equiv 1 (\text{mod } 4)$ i.e., $p = 4k + 1$, $k \varepsilon \mathbb{Z}$.

$\therefore \quad \frac{p-1}{2} = 2k$

and therefore,

$a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$ which gives, $a^{2k} \equiv 1 (\text{mod } p)$ ...(i)

Now $(p-a)^{\frac{p-1}{2}} \equiv (p-a)^{2k}$
$\equiv p^{2k} - C_1 p^{2k-1} a + ... + (-)^{2k} a^{2k}$
$\equiv a^{2k} + \lambda p$
$\equiv a^{2k} (\text{mod } p)$
$\equiv 1 (\text{mod } p)$

$\therefore \quad (p-a)$ is a qr of p.

Let $S = a_1 + a_2 + ... + a_{2k}$

$\therefore \quad S = (p - a_1) + (p - a_2) + ... + (p - a_{2k})$

$\therefore \quad 2S = p + p + ...$ to $2k$ terms
$= 2kp$

$\therefore \quad S = kp = \frac{1}{4} p(p-1)$.

Example 2. Prove that if r is a quadratic residue modulo $m > 2$, then

$$r^{\frac{\phi(m)}{2}} \equiv 1 (\text{mod } m)$$

Solution: Since r is a quadratic residue mod m there is an a such that $r \equiv a^2 (\text{mod } m)$ Again $a^{\phi(m)} \equiv 1 (\text{mod } m)$ Therefore, $r^{\phi(m)} \equiv a^{2\phi(m)} \equiv 1 (\text{mod } m)$

$$\therefore \qquad r^{\frac{\phi(m)}{2}} \equiv 1 (\text{mod } m).$$

Example 3. Let p be an odd prime. If there is an integer x such that $p \mid (x^4 + 1)$ then $p \equiv 1 (\text{mod } 8)$.

Show that there are infinitely many primes of each of the forms

$$8n + 1,\ 8n + 3,\ 8n + 5,\ 8n + 7.$$

Solution: Left as exercise.

6.2 LEGENDRE'S SYMBOL

The Legendre symbol is the special symbol associated with quadratic residues named after Adrein–Marie-Legendre, the French mathematician.

Definition:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \\ 1 \\ -1 \end{cases} \begin{cases} \text{if } p \mid a \\ \text{if } a \text{ is } R, (a, p) = 1 \text{ [p – a prime]} \\ \text{if } a \text{ is } N \end{cases}$$

Theorem 6.9. **(I)** $f(a, p) = 1$, then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\text{mod } p)$$

Proof: $\left(\frac{a}{p}\right) \equiv \pm 1$, by definition

But $a^{\frac{p-1}{2}} \equiv \pm 1 (\text{mod } p)$ by Euler's criterion

Therefore, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\text{mod } p).$

(II) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

Proof:

(i) if a is R and b is R, then ab is also R and then

$$\left(\frac{a}{p}\right) = 1 = \left(\frac{b}{p}\right) \text{and} \left(\frac{ab}{p}\right) = 1$$

Therefore $\left(\frac{ab}{p}\right) = 1 = 1.1 = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(ii) a is R, b is N then ab is N

$$\therefore \quad \left(\frac{a}{p}\right) = 1, \left(\frac{b}{p}\right) = -1, \left(\frac{ab}{p}\right) = -1 = 1.(-1) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

(iii) a is N, b is N then ab is R

$$\therefore \quad \left(\frac{a}{p}\right) = -1, \left(\frac{b}{p}\right) = -1, \left(\frac{ab}{p}\right) = 1.1 = (-1)(-1) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

(III) $$a \equiv b(p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

Proof: If a is R or N so is also b and therefore, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(IV) $$\left(\frac{r^2}{p}\right) = 1,$$

since r^2 is always a q.r.

(V) $(r, p) = 1$ then $\left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right)$

Proof: $\left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{r^2}{p}\right) = \left(\frac{a}{p}\right).1 = \left(\frac{a}{p}\right)$

Example 4. If p is an odd prime, show that $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$

Solution: Out of 1, 2, 3, ..., $p - 1$, half is R and half is N

Therefore, for one half $\left(\frac{a}{p}\right) = 1$ and for other half $\left(\frac{a}{p}\right) = -1$

Therefore, $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$

Theorem 6.10. Let $(a, p) = 1$.

If $p \equiv 1 (\text{mod } 4)$, then $-a$ is R mod p if and only a is R

If $p \equiv 3 (\text{mod } 4)$ then $-a$ is N mod p if and only if a is R

Proof: $$\left(-\frac{a}{p}\right) \equiv (-a)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \left(\frac{a}{p}\right)$$

(i) If $p \equiv 1 (\text{mod } 4)$ then

$$p = 4k + 1 \text{ and therefore, } \frac{p-1}{2} = 2k, \text{ even}$$

And $$(-1)^{\frac{p-1}{2}} = (-1)2k = 1$$

Therefore, $\left(-\frac{a}{p}\right) \equiv \left(\frac{a}{p}\right)$

$\Rightarrow$ $\left(-\frac{a}{p}\right) = \left(\frac{a}{p}\right)$ Since, $\left(-\frac{a}{p}\right) = \pm 1, \left(\frac{a}{p}\right) = \pm 1$

$\therefore$ $\pm 1 \equiv \pm 1$ so, both + 1 or both – 1 (i.e., both are equal.)

$\therefore$ $-a$ is R iff a is R

(ii) If $p \equiv 3 (\text{mod } 4)$ then

$$p = 4m + 3 \text{ and so,}$$

$$\frac{p-1}{2} = 2m + 1 \text{ and is odd.}$$

So, $(-1)^{\frac{p-1}{2}} = (-1)^{2m+1} = -1$

Therefore, $\left(-\frac{a}{p}\right) \equiv \left(\frac{a}{p}\right) (\text{mod } p)$

$\Rightarrow$ $\left(-\frac{a}{p}\right) = -\left(\frac{a}{p}\right)$

Thus, $-a$ is N iff a is R.

Corollary 6.11. if $p \equiv 1 (\text{mod } 4)$ then -1 is R

and if $p \equiv 3 (\text{mod } 4) - 1$ is N

Guass' Lemma 6.12.

Let p be an odd prime and let $(a, p) = 1$, μ denote the number of integers in the sequence: $a, 2a, 3a, ..., \frac{p-1}{2}a$... ...(1), whose least positive remainder mod p are greater than $\frac{p}{2}$ (divisor less than p) then $\left(\frac{a}{p}\right) = (-1)^{\mu}$

Proof: Let $\alpha_1, \alpha_2, ..., \alpha_\mu$ be those among the least positive remainders of the numbers in ...(1) which are greater than $\frac{p}{2}$, then the remaining numbers are $\beta_1, \beta_2, ..., \beta_1$ such that $\lambda + \mu = \frac{p-1}{2}$.

$\therefore$ $\alpha_1.\alpha_2 ... \alpha_\mu.\beta_1.\beta_2 ... \beta_1 \equiv a.2a.3a .... \frac{p-1}{2}a (\text{mod } p)$

$$\equiv a^{\frac{p-1}{2}} . \frac{p-1}{2}! (\text{mod } p)$$

$$\equiv \left(\frac{a}{p}\right) \frac{p-1}{2}! (\text{mod } p) \quad \text{...(ii)}$$

Next the numbers $p - \alpha_1, p - \alpha_2, ..., p - \alpha_\mu\ \beta_1, \beta_2, ..., \beta_\lambda$ ...(iii),

all occur among $1, 2, 3, ... \frac{p-1}{2}$

Moreover, $p - a_i \not\equiv \beta_j(p)$,

for $p - \alpha_i \equiv \beta_j$

gives $\alpha_i + \beta_i \equiv 0(\text{mod}\, p)$

or $\alpha_i + pq_1 + \beta_j + pq_2 \equiv 0(\text{mod}\, p)$

or $as + at \equiv 0(\text{mod}\ p)\ (1 \le s, t \le \frac{p-1}{2},$

since α_i, β_j are remainder of the form ka are divisible by p]

or $p \mid a\ (s + t)$

$\therefore$ $p \mid s + t$ (since, $(a, p) = 1$)

which is impossible.

Thus the numbers $p - \alpha_1, p - \alpha_2, ..., p - \alpha_\mu\ \beta_1, \beta_2, ..., \beta_l$ are exactly the number $1, 2, 3, ... \frac{p-1}{2}$ in some order.

Therefore, $\frac{p-1}{2}! = 1.2.3. ... \frac{p-1}{2}$

$= (p - \alpha_1)(p - \alpha_2) ... (p - \alpha_\mu)\ \beta_1\ \beta_2 ... \beta_\lambda$

$\equiv (-\alpha_1)(-\alpha_2) ... (-\alpha_\mu)\ \beta_1\ \beta_2 ... \beta_l\ (\text{mod}\ p)$

$\equiv (-1)^\mu\ \alpha_1\alpha_2 ... \alpha_\mu\ \beta_1\beta_2 ... \beta_\lambda\ (\text{mod}\ p)$

putting in (ii) and cancelling α's and β's we get

$$\left(\frac{a}{p}\right) \equiv (-1)^\mu (\text{mod}\ p) \Rightarrow \left(\frac{a}{p}\right) = (-1)^\mu,$$

[since, $\left(\frac{a}{p}\right) = \pm 1 = (-1)\mu$ and both must be same otherwise $\not\equiv$ (mod p)]

Example 5. Show that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Solution: Consider the numbers $2.1, 2.2, 2.3, ..., 2.\frac{p-1}{2}$

i.e., $2, 4, 6, ..., p - 1$

Clearly μ = the number of $2x$ such that $\frac{p}{2} < 2x < p$

i.e., $\frac{p}{4} < x < \frac{p}{2}$ ...(*)

Let $p = 8k + r,\ r = 1, 3, 5, 7$

If $r = 1$; then (*), becomes

$$2k + \frac{1}{4} < x < 4k + \frac{1}{2}$$

i.e., $2k + 1 \le x \le 4k,$

$\therefore \quad \mu = 4k - (2k + 1) + 1 = 2k$

$\therefore \quad (-1)^{\mu} = (-1)^{2k} = 1.$

So, $$\left(\frac{2}{p}\right) = 1 = (-1)^{2k} = (-1)^{\frac{p^2-1}{8} - 8k^2} = (-1)^{\frac{p^2-1}{8}}$$

If $r = 3$ then (*) becomes

$2k + 1 \le x \le 4k + 1$; Therefore, $\mu = 2k + 1$, therefore,

$$\left(\frac{2}{p}\right) = (-1)^{(2k+1)} = (-1)^{\frac{p^2-1}{8}}$$

If $r = 5$ then (*) becomes

$(8k + 5)/4 < x < (8k + 5)/2$, or $2k + 2 \le x \le 4k + 2$

$\therefore \quad \mu = (4k + 2) - (2k + 2) + 1 = 2k + 1$

$\therefore \quad (-1)^{\mu} = (-1)^{2k+1}.$

So, $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8} - 8k - 8k^2 - 2} = (-1)^{\frac{p^2-1}{8}}.$$

Note: $p = 8k + r$, $\dfrac{p^2-1}{8} = 8k + 2kr + \dfrac{r^2-1}{8} \equiv \dfrac{r^2-1}{8} \pmod 2$

And, $$\frac{r^2-1}{8} = \begin{matrix} 0 \\ 1 \\ 3 \\ 6 \end{matrix} \Bigg\} \begin{matrix} \text{if } r = 1 \\ \text{if } r = 3 \\ \text{if } r = 5 \\ \text{if } r = 7 \end{matrix}$$

Hence $$(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{r^2-1}{8}} = \begin{matrix} 1 \\ -1 \end{matrix} \Bigg\} \begin{matrix} \text{if } r = 1,7 \text{ i.e., if } p \equiv \pm 1 (\text{mod } 8) \\ \text{if } r = 3,5 \text{ i.e., if } p \equiv \pm 3 (\text{mod } 8) \end{matrix}$$

Example 6. Show that if $p \equiv \pm 1(8)$ then 2 is R,

$p \equiv \pm 3(8)$ then 2 is N

or

Example 7. Determine the prime for which the integer 2 is R and those for which it is N

Example 8. Determine: $\left(\dfrac{3}{p}\right)$

Solution: Here we consider

$$3.1, 3.2, 3.3, ..., 3.\frac{p-1}{2} \qquad ...(1)$$

μ = the number of these among (1) which lies between $\dfrac{p}{2}$ and p = no. of x such that

$$\frac{p}{2} < 3x < p \text{ i.e., } \frac{p}{6} < x < \frac{p}{3}$$

Let us put $p = 2k + r$, $r = 1, 5, 7, 11$

(1) $r = 1$ gives $\quad 2k + \frac{1}{6} < x < 4k + \frac{1}{3}$

i.e., $\quad 2k + 1 \le x \le 4k$

$\therefore\ \mu = 2k$ and so $\quad (-1)^{\mu} = (-1)^{2k} = 1\ .\ \therefore\ \ (3/p) = 1$

(2) $r = 5$ gives $\quad 2k + \frac{5}{6} < x < 4k + 1 + \frac{2}{3}$

$$2k + 1 \le x \le 4k + 1$$

$\therefore \quad \mu = (4k+1) - (2k+1) + 1 = 2k + 1$

and so $\quad (-1)^{\mu} = (-1)^{2k+1} = -1. \quad \therefore \ \left(\frac{3}{p}\right) = -1$

(3) $r = 7$ gives $\quad 2k + 1 + \frac{1}{6} < x < 4k + 2 + \frac{1}{3}$

$$2k + 2 \le x \le 4k + 2$$

$\therefore \quad \mu = (4k+2) - (2k+2) + 1 = 2k + 1$

and so $\quad (-1)^{\mu} = (-1)^{2k+1} = -1. \ \therefore \left(\frac{3}{p}\right) = 1$

(4) $r = 11$ gives $\quad 2k + 1 + \frac{5}{6} < x < 4k + 3 + \frac{2}{3}$

or, $\quad 2k + 2 \le x \le 4k + 3$

$\therefore \quad \mu = (4k+3) - (2k+2) + 1 = 2k + 2$

so $\quad (-1)^{\mu} = (-1)^{2k+2} = 1 \quad \therefore \ \left(\frac{3}{p}\right) = 1$

$\therefore \quad (3/p) = \left.\begin{matrix} 1 \\ -1 \end{matrix}\right\} \begin{matrix} \text{if } r = 1, 11 \text{ i.e., if } p \equiv 1, 11 \pmod{12} \\ \text{if } r = -1 \text{ i.e., if } p \equiv 5, 7 \pmod{12} \end{matrix}$

$\therefore \quad 3$ is R for $p \equiv \pm 1 \pmod{12}$

3 is N for $p \equiv \pm 5 \pmod{12}$.

Theorem 6.13. If $(a, p) = 1$, where a is an odd positive integer, then

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{1}{2}} \left[\frac{ja}{p}\right]}$$

Proof: If we divide ja by p, we obtain $ja = pq + r$, where $0 < r < p$ and r is one of the numbers

$$\alpha_1, \alpha_2, \ldots, \alpha_{\mu}, \beta_1, \beta_2, \ldots, \beta_{\lambda}, \text{ with}$$

$$\lambda + \mu = \frac{p-1}{2} \text{ [as in the proof of Gauss' Lemma]}$$

Now $ja = pq + r$ gives

$$\left[\frac{ja}{p}\right] = \left[q + \frac{r}{p}\right] = q$$

Therefore, $$ja = \left[\frac{ja}{p}\right] p + r$$

Thus $$\sum_{j=1}^{\frac{1}{2}(p-1)} ja = \sum_{j=1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right] p + \sum_{i=1}^{\mu} \alpha_i + \sum_{k=1}^{\lambda} \beta_k \quad \ldots(1)$$

since, $$\sum_{j=1}^{\frac{1}{2}(p-1)} r = \sum_{1}^{\mu} \alpha_i + \sum_{1}^{\lambda} \beta_k$$

In the proof of Gauss' lemma, we established that the number

$$p - \alpha_1, p - \alpha_2, \ldots, p - \alpha_\mu\ \beta_1, \beta_2, \ldots, \beta_\lambda$$

are just the number

$$1, 2, 3, \ldots, \frac{p-1}{2} \text{ in some order}$$

Therefore $$\sum_{j=1}^{\frac{1}{2}(p-1)} j = 1 + 2 + \ldots + \frac{p-1}{2}$$

$$= (p - \alpha_1) + (p - \alpha_1) + \ldots + (p - \alpha_\mu) + \beta_1 + \beta_1 + \ldots + \beta_\lambda$$

$$= p\mu - \sum_{1}^{\mu} \alpha_i + \sum_{1}^{\lambda} \beta_k \quad \ldots(2)$$

(1) – (2) gives

$$(a-1) \sum_{j=1}^{\frac{1}{2}(p-1)} j = p \left\{ \sum_{1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right] - \mu \right\} + \sum_{1}^{\mu} \alpha_i$$

Now, $a \equiv 1 (\text{mod } 2) \Rightarrow a - 1 \equiv 0 (\text{mod } 2)$ and $p \equiv 1 \pmod 2$, $2 \equiv 0 (\text{mod } 2)$

Therefore (3) becomes

$$0 \equiv 1 \left\{ \sum_{1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right] - \mu \right\} + 0 (\text{mod } 2)$$

$$\therefore \quad \sum_{1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right] \equiv \mu (\text{mod } 2)$$

$$\therefore \quad \sum_{1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right] = \mu + 2l,\ l \varepsilon \mathbb{Z}$$

$$\therefore \qquad \left(\frac{a}{p}\right) = (-1)^{\mu} = (-1)^{\mu+2l} = (-1)^{\sum_{1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right]}.$$

Example 9. Determine $\left(\frac{5}{p}\right)$

Solution: Consider $5.1, 5.2, 5.3, \ldots, 5.\frac{p-1}{2}$

μ = no. of x above between, $\frac{p}{2} < 5x < p$, i.e., $\frac{p}{10} < x < \frac{p}{5}$

Let $p = 20k + r, \quad r = 1, 3, 7, 9, 11, 13, 17, 19$

(i) $r = 1$ gives

$$2k + \frac{1}{10} < x < 4k + \frac{1}{5}, \text{ or } 2k + 1 \le x \le 4k$$

$$\therefore \qquad \mu = 4k - (2k + 1) + 1 = 2k$$

$$\therefore \qquad (-1)^{\mu} = (-1)^{2k} = 1$$

Therefore, $\left(\frac{5}{p}\right) = 1$

(ii) $r = 3$ gives

$$2k + \frac{3}{10} < x < 4k + \frac{3}{5},$$

or $\qquad 2k + 1 \le x \le 4xk$

$$\therefore \qquad \mu = 4k - (2k + 1) + 1 = 2k,$$

$$\therefore \qquad (-1)^{\mu} = (-1)^{2k} = 1$$

Therefore, $\left(\frac{5}{p}\right) = 1$

(iii) $r = 7$ gives

$$2k + \frac{7}{10} < x < 4k + 1 + \frac{2}{5},$$

or $\qquad 2k + 1 \le x \le 4k + 1$

$$\therefore \qquad \mu = (4k + 1) - (2k + 1) + 1 = 2k + 1,$$

$$\therefore \qquad (-1)^{\mu} = (-1)^{2k+1} = -1$$

Therefore, $\left(\frac{5}{p}\right) = -1$

(iv) $r = 9$ gives $2k + \frac{9}{10} < x < 4k + 1 + \frac{4}{5}$,

or, $\qquad 2k + 1 \le x \le 4k + 1$

$\therefore \quad \mu = 2k + 1,$

$\therefore \quad (-1)^{\mu} = (-1)^{2k+1} = -1$

Therefore, $\left(\frac{5}{p}\right) = -1$

(v) $r = 11$ gives $2k + 1 + \frac{1}{10} < x < 4k + 2 + \frac{1}{5}$,

or, $2k + 2 \leq x \leq 4k + 2$

$\therefore \quad \mu = (4k + 2) - (2k + 2) + 1 = 2k + 1,$

$\therefore \quad (-1)^{\mu} = (-1)^{2k+1} = -1$

$\therefore \quad \left(\frac{5}{p}\right) = -1$

(vi) $r = 13$ gives $2k + 1 + \frac{3}{10} < x < 4k + 2 + \frac{3}{5}$,

or, $2k + 2 \leq x \leq 4k + 2$

$\therefore \quad \mu = (4k + 2) - (2k + 2) + 1 = 2k + 1$

$\therefore \quad \left(\frac{5}{p}\right) = -1$

(vii) $r = 17$ gives $2k + \frac{17}{10} < x < 4k + 3 + \frac{2}{5}$

or, $2k + 2 \leq x \leq 4k + 3$

$\therefore \quad \mu = (4k + 3) - (2k + 2) + 1 = 2k + 2 = 2(k + 1)$

$(-1)^{\mu} = (-1)^{2(k+1)} = 1$

$\therefore \quad \left(\frac{5}{p}\right) = 1$

(viii) $r = 19$, $2k + 2 \leq x \leq 4k + 3$

$\mu = 2k + 2$

Therefore, $(-1)^{\mu} = 1$

$\therefore \quad \left(\frac{5}{p}\right) = 1$

$\therefore$ 5 is R is $p \equiv \pm 1, 3 \pmod{20}$

and 5 is N if $p \equiv \pm 7, 9 \pmod{20}$.

6.3 QUADRATIC RECIPROCITY LAW

The quadratic reciprocity Law is one of the jewels in the crown of '*The Queen of Mathematics*' the theory of numbers.

Quadratic reciprocity law deals with the solvability of quadratic congruences.

Theorem 6.14. If p and q are odd prime numbers, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)} \qquad \ldots(*)$$

[Eisenstein Geometric proof of Quadratic Reciprocity Law.]

Proof: we have

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{1}^{\frac{1}{2}(q-1)}\left[\frac{jp}{q}\right]}$$

$$\therefore \quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{1}^{\frac{1}{2}(q-1)}\left[\frac{jp}{q}\right]+\sum_{1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]} \qquad \ldots(Y)$$

Comparing (*) and (Y) we have to show that

$$\sum_{1}^{\frac{1}{2}(q-1)}\left[\frac{jp}{q}\right]+\sum_{1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right] = \frac{1}{2}(p-1)\frac{1}{2}(q-1)$$

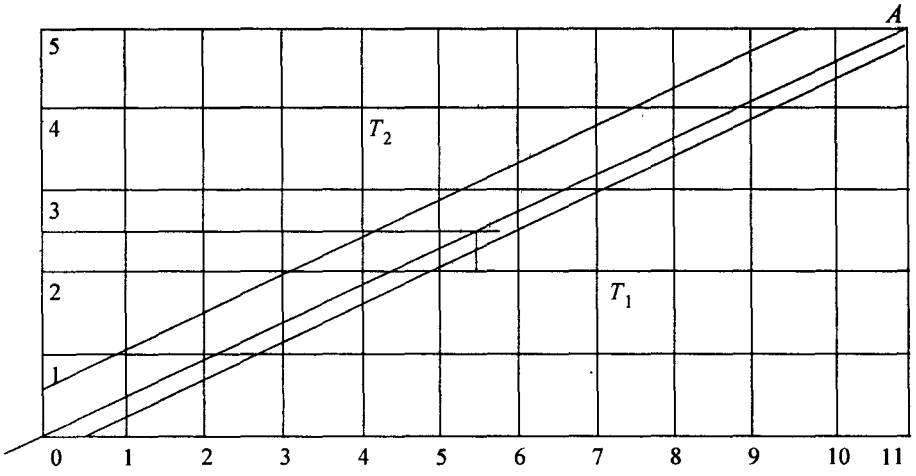
The method will be to count the lattice points in a portion of the xy plane in two different ways.

Consider the rectangle in xy plane bounded by

$$x = 0, x = \frac{p}{2}$$

$$y = 0, y = \frac{q}{2}$$

The diagonal of this rectangle is $y = \frac{q}{p}x$



Let T_1 be the portion of the rectangle below the line OA and T_2 be the portion of the rectangle above the line OA.

Since p and q are primes, $\frac{p}{q}$ is a fraction, therefore, none of the lattice points interior to the rectangle lies on the line $y = \frac{q}{p} . x$ (or, OA)

Hence the lattice points, all lie in T_1 or T_2. To count the lattice points interior to T_1 we observe that if $1 \leq j \leq p/2$

The number of lattice points in T_1 that are directly above the point $(j, 0)$ is $\left[\frac{jq}{p}\right]$.

Since the equation of the diagonal is $y = x . \frac{q}{p}$

Thus the number of lattice points in T_1 is $\sum_{1}^{\frac{1}{2}(p-1)} \left[\frac{kq}{p}\right]$

In similar way the number of lattice points in T_2 is $\sum_{1}^{\frac{1}{2}(q-1)} \left[\frac{jp}{q}\right]$

Thus the number of lattice points within the rectangle is

$\sum_{1}^{\frac{1}{2}(q-1)} \left[\frac{jp}{q}\right] + \sum_{1}^{\frac{1}{2}(p-1)} \left[\frac{kq}{p}\right]$ and it is obvious that the rectangle contains a total of

$\frac{1}{2}(p-1)\frac{1}{2}(q-1)$ lattice points ...(ii)

$\therefore$ From (i) and (ii) the result follows.

Following are different forms of quadratic reciprocity law:

Form I: If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}$$

Since, $\left(\frac{p}{q}\right)$ is + 1 or − 1, we have

$$\left(\frac{p}{q}\right)^2 = +1$$

$$\therefore \quad \left(\frac{p}{q}\right)^2\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}$$

Form II: $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}$

[This law is stated in this form also]

Form III: $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ unless both p and q are of the form $4m - 1$ in which case $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Since $\frac{p-1}{2}.\frac{q-1}{2}$ is odd for $p \equiv q \equiv 3 \pmod 4$ i.e., p and q are of the form $4m + 3$ and is even if one of these numbers is of the form $4m + 1$, the above law can be formulated as follows:

Form IV: $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$

i.e., one of p and q is of the form $4m + 1$

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) \text{ if } p \equiv q \equiv 3 \pmod 4$$

i.e., if both numbers p and q are of the form $4m + 3$

Form V: The congruences

$$x^2 \equiv p \pmod q, y^2 \equiv q \pmod p$$

are both solvable or both unsolvable unless $p \equiv q \equiv 3 \pmod 4$, if $p \equiv q \equiv 3 \pmod 4$, then one is solvable and the other unsolvable.

Corollary 6.15. Let $(p, q) = 1$,

(i) if $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$, then p is R mod q if q is N mod p

(ii) if $p \equiv 1 \pmod 4$, $q \equiv 3 \text{(or } 1) \pmod 4$, then p is R mod q if q is R mod p

Proof: (i) Since $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$

Then, $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)} = (-1)^{(2k_1+1)(2k_2+1)} = -1$$

Therefore, $$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

This means that p is Rmod q iff q is N mod p

(ii) Since $p \equiv 1 \pmod 4$, $q \equiv 3 \text{(or } 1) \pmod 4$, then,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)} = 1$$

($\frac{1}{2}(p - 1)$ is always even as $p = 4k_1 + 1$)

$$\therefore \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

So, p is Rmod q if q is R mod p.

Example 10. Find $\left(\frac{10}{17}\right)$

Solution: $\left(\frac{10}{17}\right) = \left(\frac{5\times 2}{17}\right) = \left(\frac{2}{17}\right)\times\left(\frac{5}{17}\right)$

Now $\left(\frac{2}{17}\right) \equiv 2^{\frac{1}{2}(17-1)} \pmod{17} \equiv 256 \pmod{17}$

Now, $+1 \equiv 256 \pmod{17}$,

Therefore, $\left(\frac{2}{17}\right) = +1$ (i.e., 2 is R mod 17)

$\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right)$ [since $17 \equiv 2(5)$ and $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b\ (p)$]

$\equiv 2^{\frac{1}{2}(5-1)} \pmod{5} \equiv 4 \pmod{5}$

Therefore,

$\left(\frac{2}{5}\right) \equiv 4 \pmod{5}$

But $-1 \equiv 4 \pmod{5}$,

Therefore, $\left(\frac{2}{5}\right) = -1$.

So, $\left(\frac{10}{17}\right) = 1(-1) = -1$.

Example 11. Determine $\left(\frac{-42}{31}\right)$

Solution: $\left(-\frac{42}{31}\right) = \left(\frac{-1\times 2\times 3\times 7}{31}\right)$

$= \left(\frac{-1}{31}\right)\times\left(\frac{2}{31}\right)\times\left(\frac{3}{31}\right)\times\left(\frac{7}{31}\right)$

Now, $\left(\frac{-1}{31}\right) \equiv (-1)^{\frac{1}{2}(31-1)} \pmod{31} \equiv (-1)^{15} \pmod{31} \equiv -1 \pmod{31}$

And, $\left(\frac{3}{31}\right) = (-1)^{\frac{1}{2}(31-1)\frac{1}{2}(3-1)}\left(\frac{31}{3}\right)$

$= (-1)^{15.1}\left(\frac{31}{3}\right) = -1\left(\frac{31}{3}\right) = -\left(\frac{1}{3}\right) = -1$ [for, $31 \equiv 1(3)$]

Therefore, $\left(\frac{3}{31}\right) = -1$

$$\left(\frac{2}{31}\right) = 1[31 \equiv -1(\text{mod } 8)],$$

$$\left(\frac{7}{31}\right) - (-1)^{15\times 3}\left(\frac{31}{7}\right) = -\left(\frac{31}{7}\right) = -\left(\frac{3}{7}\right) = +\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$$

Therefore, $\left(-\frac{42}{31}\right) = (-1).(-1).(1).(1) = 1.$

Example 12. $(2/p) = 1$ if $p \equiv \pm 1(8)$
$= -1$ if $p \equiv \pm 3(8)$

Solution: [Left as exercise]

Example 13. Find all primes p for which -3 is a q.r.

Solution:
$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$$

$$= (-1)^{\frac{1}{2}(p-1)}\,(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(3-1)}\left(\frac{p}{3}\right)$$

$$= \left(\frac{p}{3}\right) = \left(\frac{r}{3}\right), [r = 1 \text{ or } 2,\ p \equiv r(3),\ r = 1,2]$$

If $r = 1$, then $\left(\frac{-3}{p}\right) = \left(\frac{1}{3}\right) = +1$ therefore; -3 is R if $p \equiv 1(\text{mod } 3)$

If $r = 2$, then $\left(\frac{-3}{p}\right) = \left(\frac{2}{3}\right) \equiv 2^{(3-1)/2}(3) \equiv 2(\text{mod } 3)$; -3 is N if $p \equiv 2(\text{mod } 3)$.

Example 14. Find all primes for which 5 is a q.r.

Solution:
$$\left(\frac{5}{p}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(5-1)}\left(\frac{p}{5}\right)$$

$$= (-1)^{\frac{1}{2}(p-1).2}\left(\frac{p}{5}\right)$$

$$= \left(\frac{p}{5}\right) = \left(\frac{r}{5}\right)\ [p \equiv r(5)]$$

If $r = 1$ then $\left(\frac{5}{p}\right) = \left(\frac{1}{5}\right) = 1$ therefore, 5 is R if $p \equiv 1(\text{mod } 5)$

If $r = 2$ then $\left(\frac{5}{p}\right) = \left(\frac{2}{5}\right) = 2^{\frac{1}{2}(5-1)} (\text{mod } 5) \equiv 2^2(\text{mod } 5) \equiv 4(\text{mod } 5)$

or $\left(\frac{5}{p}\right) = -1.$

$\therefore$ 5 is N if $p \equiv 2(\text{mod } 5)$

If $r = 3 \Rightarrow$ then $\left(\frac{5}{p}\right) = \left(\frac{3}{5}\right) = (-1)^{\frac{1}{2}(5-1)\frac{1}{2}(3-1)}\left(\frac{5}{3}\right) = \left(\frac{5}{3}\right)$

$= \left(\frac{2}{3}\right) = -1$ [since $5 \equiv 2(\text{mod } 3)$, $3 \equiv 3(\text{mod } 8)$]

$\therefore$ $\left(\frac{5}{p}\right) = -1$, i.e., 5 is N if $p \equiv 3(\text{mod } 5)$

If $r = 4$ then $\left(\frac{5}{p}\right) = \left(\frac{4}{p}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{5}\right) = \left(\frac{2^2}{5}\right) = 1$ [2 is always R]

$\therefore$ 5 is r if $p \equiv 1, 4, (\text{mod } 5)$ i.e., $p \equiv \pm 1(\text{mod } 5)$.

6.4 QUADRATIC RESIDUE FOR COMPOSITE MODULES: JACOBI'S SYMBOL

The Jacobi symbol, named after the German mathematician Carl Jacobi who introduced this symbol. The Jacobi symbol is a generalization of the Legendre symbol. Jacobi symbol is useful in the evaluation of Legendre symbols and in the definition of a type of Pseudoprime.

Let $(P, Q) = 1$ and Q is an odd positive integer with prime decomposition

$$Q = \prod_{i=1}^{r} p_i^{\alpha_i}$$

Then Jacobi's Symbol $\left(\frac{P}{Q}\right)$ is defined as follows

(i) $\left(\frac{P}{1}\right) = 1 \ \forall P \in \mathbb{Z}$

(ii) $\left(\frac{P}{Q}\right) = \left(\frac{P}{p_1}\right)^{\alpha_1} \cdot \left(\frac{P}{p_2}\right)^{\alpha_2} \cdots \left(\frac{P}{p_r}\right)^{\alpha_r}$,

where $\left(\frac{P}{p_i}\right)$ is Legender's symbol

Remark $\left(\frac{P}{Q}\right) = 0$ if $(P, Q) \neq 1$

Proof If $(P, Q) \neq 1$ let q be a common factor of P and Q

$\therefore$ $\left(\frac{P}{q}\right) = 0$ by definition of Legender's symbol. And is a factor of $\left(\frac{P}{Q}\right)$.

Hence $\left(\frac{P}{Q}\right) = 0$

Proposition 6.16.

(i) $\left(\frac{P}{Q}\right)$ has always the value 1 or -1

Proof: Follows from the definition

(ii) $(P, Q) = 1$ and P is a q.r. of Q then $\left(\frac{P}{Q}\right) = 1$

Proof: If $x^2 \equiv P(\text{mod } Q)$ has a root for each $i = 1, 2, 3, \ldots$ then the algebraic congruence $x^2 \equiv P(\text{mod } p_i)$ has a root. Consequently $\left(\frac{P}{p_i}\right) = 1$ for $i = 1, 2, 3 \ldots r$ [by Legender symbol, since p is a R mod pi]

$$\therefore \qquad \left(\frac{P}{Q}\right) = 1$$

Remark: *Converse* of (ii) is not true i.e., (If $\left(\frac{P}{Q}\right) = 1$, P need not be a q.r.)

Theorem 6.17. If Q, P_1, P_2 are odd positive integers, then

(i) $\left(\frac{P_1}{Q}\right)\left(\frac{P_2}{Q}\right) = \left(\frac{P_1 P_2}{Q}\right)$

(ii) $\left(\frac{P}{Q_1}\right)\left(\frac{P}{Q_2}\right) = \left(\frac{P}{Q_1 Q_2}\right)$

(iii) $P_1 \equiv P_2 = (\text{mod } Q) \Rightarrow \left(\frac{P_1}{Q}\right) = \left(\frac{P_2}{Q}\right)$

(iv) $(R, Q) = 1 \Rightarrow \left(\frac{PR^2}{Q}\right) = \left(\frac{P}{Q}\right)$

(v) $\left(\frac{-1}{Q}\right) = (-1)^{\frac{1}{2}(Q-1)}$

(vi) $\left(\frac{2}{Q}\right) = (-1)^{\frac{1}{8}(Q^2-1)}$

(vii) $(P, Q) = 1$, and P is also an odd positive integer,

Then $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{1}{2}(P-1)\frac{1}{2}(Q-1)}$ [Reciprocity Law]

Proof: Proofs of (i) to (iv) directly follow from definition.

(v) $\left(\frac{-1}{Q}\right) = (-1)^{\frac{1}{2}(Q-1)}$

(v) is true for $Q = 1$.

Suppose $Q > 1$.

Suppose $Q = p_1 p_2 p_3 \ldots p_r$, where p_i are odd primes not necessarily distinct

Therefore, $$\left(\frac{-1}{Q}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\ldots\left(\frac{-1}{p_r}\right)$$

$$= \prod_{i=1}^{r}\left(\frac{-1}{p_i}\right) = (-1)^{\frac{1}{2}(p_1-1)}(-1)^{\frac{1}{2}(p_2-1)} \ldots (-1)^{\frac{1}{2}(p_r-1)}$$

$$= (-1)^{\sum_1^r \frac{1}{2}(p_i-1)}$$

The result will be proved if we can show that

$$\sum_1^r \frac{1}{2}(p_i - 1) \equiv \frac{1}{2}(Q-1) \equiv \frac{1}{2}(p_1 p_2 \ldots p_r - 1) \pmod 2 \qquad \ldots(*)$$

(*) will be proved by induction

The result is true for $r = 1$

Suppose (*) is true for $r - 1$

i.e., $$\sum_1^{r-1}\left(\frac{p_i-1}{2}\right) \equiv \left(\frac{p_1 p_2 \cdots p_{r-1}-1}{2}\right) \pmod 2 \qquad \ldots(**)$$

Again, $$\sum_1^r\left(\frac{p_i-1}{2}\right) = \sum_1^{r-1}\left(\frac{p_i-1}{2}\right) + \frac{p_r-1}{2}$$

Using (**) we get

$$\sum_1^r\left(\frac{p_i-1}{2}\right) \equiv \left(\frac{p_1 p_2 \cdots p_{r-1}-1}{2}\right) + \frac{p_r-1}{2} \pmod 2 \qquad \ldots(\Psi)$$

Now p_i are odd primes

Therefore $(p_1 p_2 p_3 \ldots p_{r-1} - 1)(p_r - 1) \equiv 0 \pmod 4$

Therefore, $p_1 p_2 p_3 \ldots p_{r-1} p_r - p_1 p_2 p_3 \ldots p_{r-1} - p_r + 1 \equiv 0 \pmod 4$

$\Rightarrow$ $(p_1 p_2 p_2 \ldots p_{r-1} - 1) - (p_1 p_2 p_3 \ldots p_r - 1) + (p_r - 1) \equiv 0 \pmod 4$

or $$\left(\frac{p_1 p_2 \cdots p_{r-1}-1}{2}\right) - \left(\frac{p_1 p_2 \cdots p_r - 1}{2}\right) + \frac{p_r-1}{2} \equiv 0 \pmod 4$$

or, $$\left(\frac{p_1 p_2 \cdots p_{r-1}-1}{2}\right) + \frac{p_r-1}{2} \equiv \left(\frac{p_1 p_2 \cdots p_r - 1}{2}\right) \pmod 2$$

Therefore, Ψ becomes

$$\sum_1^r\left(\frac{p_i-1}{2}\right) \equiv \left(\frac{p_1 p_2 \cdots p_r - 1}{2}\right)((\text{mod } 2)$$

$$\equiv \left(\frac{1}{2}\right)(Q-1)(\text{mod } 2)$$

Hence the result follows by induction.

(vi) $\left(\frac{2}{Q}\right) = (-1)^{\frac{1}{2}(Q-1)}$

Proof: $\left(\frac{2}{Q}\right) = \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_r}\right) = (-1)^{\frac{p_1^2-1}{8}}(-1)^{\frac{p_2^2-1}{8}}\cdots(-1)^{\frac{p_r^2-1}{8}} = (-1)^{\Sigma\left(\frac{p_i^2-1}{8}\right)}$

The theorem will be proved by the method of induction

The theorem will be proved if we show that

$$\sum_1^r\left(\frac{p_i^2-1}{8}\right) \equiv \left(\frac{Q^2-1}{8}\right) \equiv \left(\frac{p_1^2 p_2^2 \cdots p_r^2 - 1}{8}\right)(\text{mod } 8) \qquad \ldots(*)$$

The result is true for $r = 1$

Assume that it is true for $r-1$, i.e.,

$$\sum_1^{r-1}\frac{1}{8}(p_i^2-1) \equiv \frac{1}{8}\left(p_1^2\, p_2^2 \cdots p_{r-1}^2 - 1\right)(\text{mod } 8) \qquad \ldots(**)$$

$$\therefore \quad \sum_1^r\frac{1}{8}(p_i^2-1) \equiv \sum_1^{r-1}\frac{1}{8}(p_i^2-1) + \frac{1}{8}(p_r^2-1)\,(\text{mod } 8) \ldots(\Psi) \text{ (using (**))}$$

Now if a is any odd integer then

$$a^2 \equiv 1(8) \text{ gives } a^2 - 1 \equiv 0(\text{mod } 8)$$

Consequently

$$\left(p_1^2\, p_2^2 \cdots p_{r-1}^2 - 1\right)\left(p_r^2 - 1^2\right) \equiv 0(\text{mod } 64)$$

or $$p_1^2 p_2^2 \cdots p_{r-1}^2 p_r^2 - p_r^2 - p_1^2 p_2^2 \cdots p_{r-1}^2 + 1 \equiv 0 \text{ (mod } 64)$$

or $$p_1^2 p_2^2 \cdots p_{r-1}^2 - p_1^2 p_2^2 \cdots p_r^2 + p_r^2 - 1 \equiv 0(\text{mod } 64)$$

or $$\left(p_1^2 p_2^2 \cdots p_{r-1}^2 - 1\right) - \left(p_1^2 p_2^2 \cdots p_r^2 - 1\right) + \left(p_r^2 + 1\right) \equiv 0(\text{mod } 64)$$

or $$\left(\frac{p_1^2 p_2^2 \cdots p_{r-1}^2 - 1}{8}\right) - \left(\frac{p_1^2 p_2^2 \cdots p_r^2 - 1}{8}\right) + \frac{1}{8}\left(p_r^2 - 1\right) \equiv 0(\text{mod } 8)$$

or $$\left(\frac{p_1^2 p_2^2 \cdots p_{r-1}^2 - 1}{8}\right) + \frac{1}{8}\left(p_r^2 - 1\right) \equiv \frac{1}{8}\left(p_1^2 p_2^2 \cdots p_r^2 - 1\right)(\text{mod } 8)$$

Then, Ψ gives,

$$\sum_1^r\frac{1}{8}\left(p_1^2 - 1\right) \equiv \frac{1}{8}\left(p_1^2\, p_2^2 \cdots p_r^2 - 1\right)(\text{mod } 8)$$

Therefore, * follows by induction.

(vii) $(P, Q) = 1$ and P is also a positive odd, then

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{1}{2}(P-1)\frac{1}{2}(Q-1)}$$

Proof: If P or Q equals 1, then the result is immediate (since both sides equal to + 1)

Let $P = q_1 q_2 \dots q_s$,

$Q = p_1 p_2 \dots p_r \quad \because (P, Q) = 1 \therefore p_i \neq q_j$ for all i, j

Consequently $\left(\frac{p_i}{q_i}\right)$ and $\left(\frac{q_j}{p_i}\right)$ are non zero

$$\therefore \quad \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i=1}^{r}\left(\frac{P}{p_i}\right)\prod_{j=1}^{s}\left(\frac{Q}{q_j}\right) = \prod_{i=1}^{r}\left\{\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\right\}\prod_{j=1}^{s}\left\{\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right)\right\}$$

$$= \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right) = (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{1}{2}(q_j-1)\frac{1}{2}(p_i-1)}$$

$$= (-1)^{\sum_{j=1}^{r}\frac{1}{2}(q_j-1)\times\sum\frac{1}{2}(p_i-1)} \qquad \text{...(*)}$$

But from,

$$\Sigma\frac{1}{2}(p_i - 1) \equiv \frac{1}{2}(p_1 p_2 \dots p_r - 1) \pmod 2$$

And the corresponding result for

$P = q_1 q_2 \dots q_s$, the RHS of (*) is equal to $(-1)^{\frac{1}{2}(P-1)\frac{1}{2}(Q-1)}$.

Example 15. Show that the congruence $x^2 \equiv 15 \pmod{1093}$ has no solution;

[i.e., to show that 15 is $N \bmod 1093$; i.e., $\left(\frac{15}{1093}\right) = -1$]

Solution: We first note that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

and $$\left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}\left(\frac{q}{p}\right)$$

also, $$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ if } a \equiv b \pmod p$$

Now, $\left(\frac{15}{1093}\right) = \left(\frac{3}{1093}\right)\left(\frac{5}{1093}\right) = \left(\frac{1093}{3}\right)\left(\frac{1093}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{3}{5}\right)$

$= (+1)\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right)$

$= -1$ [2 is R if $p \equiv \pm 1(8)$
2 is in if $p \equiv \pm 3(8)$]

Therefore 15 is a q.n.r. mod 1093.

Example 16. Show that the congruence $x^2 + 3 \equiv 0(\text{mod } 59)$ has solution
[i.e., -23 is R mod 59. i.e., $(-23/59) = 1$]

Solution: $\left(-\frac{23}{59}\right)\left(\frac{-1}{59}\right)\left(\frac{23}{59}\right) = (-1)\,(-1)^{\frac{1}{2}\times 22\frac{1}{2}\times 58}\left(\frac{59}{23}\right)$

$= (-1)(-1) = \left(\frac{13}{23}\right)$

$= (-1)^{\frac{1}{2}\times 12\frac{1}{2}\times 22}\left(\frac{23}{13}\right) = \left(\frac{10}{13}\right)$

[since, $23 \equiv 10(\text{mod } 13)$] $= \left(\frac{2}{13}\right)\left(\frac{5}{13}\right)$

$= (-1)\,(-1)^{\frac{1}{2}\times 4\frac{1}{2}\times 12}\left(\frac{13}{5}\right)$

$= (-1)\left(\frac{3}{5}\right) = (-1)\left(\frac{5}{3}\right) = (-1)\left(\frac{2}{3}\right)$

$= (-1)(-1) = 1$

Therefore, -23 is R (mod 59)

Therefore, $x^2 + 23 \equiv 0(\text{mod } 59)$ has solution. $\left(\frac{-23}{59}\right)$

Example 17. Evaluate $\left(\frac{-23}{59}\right)$

Solution: $\left(\frac{-23}{59}\right) = \left(\frac{-1}{59}\right)\left(\frac{23}{59}\right) = (-1)\,(-1)^{\frac{1}{2}.22.\frac{1}{2}.58}\left(\frac{59}{23}\right)$

$= \left(\frac{13}{29}\right) = (-1)^{\frac{1}{2}.12.\frac{1}{2}.22}\left(\frac{23}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right)$

$= (-1).(-1)^{\frac{1}{2}.4.\frac{1}{2}.12}\left(\frac{13}{5}\right) = (-1)\left(\frac{3}{5}\right) = (-1)\left(\frac{5}{3}\right)$

$= (-1)\left(\frac{2}{3}\right) = (-1)(-1) = 1$

Therefore -23 is R mod 59

Therefore, $x^2 + 23 \equiv 0(\text{mod } 59)$ has solution.

EXERCISES 6.1

1. Let p be a prime, and let $(a, p) = (b, p)$. Prove that if $x^2 \equiv a(\text{mod } p)$ and $x^2 \equiv b(\text{mod } p)$ are not solvable then $x^2 \equiv ab(\text{mod } p)$ is solvable.
2. If p is an odd prime then prove that $x^2 \equiv 2(\text{mod } p)$ has solution if and only if $p \equiv 1$ or $7(\text{mod } 8)$.
3. Prove that the quadratic residues of 11 are 1, 3, 4, 5, 9 and list all solutions of each of the ten congruences $x^2 \equiv a(\text{mod } 11)$ and $x^2 \equiv a(\text{mod } 112)$ where $a = 1, 3, 4, 5, 9$.
4. Determine whether 7 is a quadratic residue of 17?
5. Use Wilson's Theorem to prove that the solutions of $x^2 + 1 \equiv 0(\text{mod } p)$; $p = 4m + 1$ are $x \equiv \pm(2m)!\ (\text{mod } p)$.
6. Assuming that the solutions exist, find the solutions of the congruence $x^2 \equiv a(\text{mod } p)$.
7. Show that the indeterminate equation $x^2 + 3y = 17$ has no solution.
8. Let p and q be both odd primes and $p = q + 4a$, show that
   (i) $(p/q) = (a/q)$
   (ii) $(a/p) = (a/q)$
9. If $(x, 3) = 1$, show that the odd prime factor p of $x^2 + 3$ is of the form $3k + 1$.
10. Prove that 3 is a quadratic residue of 13 but quadratic non residue of 7.
11. Solve $x^2 \equiv 5(\text{mod } 19)$ if the solutions exist
12. Solve $x^2 \equiv -2(\text{mod } 19)$.
13. Show that
    (i) $(3/11) = 1, (-2/11) = 1, (-1/13) = 1$
    (ii) $(2/13) = -1, (-2/13) = -1, (3/13) = 1$
    (iii) $(-2/17) = 1, (3/17) = -1, (2/17) = 1$
14. Solve
    (i) $x^2 \equiv 4(\text{mod } 7)$
    (ii) $x^2 \equiv 1(\text{mod } 7)$
    (iii) $x^2 \equiv 5(\text{mod } 11)$
15. Is 85 a quadratic residue of 97?
16. Find (171/173)
17. Is 105 a qr of 317?
18. Which of the following congruences are solvable?
    (i) $x^2 \equiv 2(\text{mod } 7)$
    (ii) $x^2 \equiv 11(\text{mod } 61)$
    (iii) $x^2 \equiv 42(\text{mod } 97)$
    (iv) $x^2 \equiv 137(\text{mod } 401)$
    (v) $x^2 = -43(\text{mod } 79)$

19. If p is an odd prime, prove that

$$(1/p) + (2/p) + (3/p) + \ldots + (p - 1/p) = 0$$

20. Let p be an odd prime. Prove that if there is an integer x such that

(i) $p \mid (x^2 + 1)$ then $p \equiv 1 (\text{mod } 4)$

(ii) $p \mid (x^2 - 2)$ then $p \equiv 1$ or $7 (\text{mod } 8)$

21. Evaluate

(i) (423/563)

(ii) (–1457/2389)

(iii) (365/1847)

22. Prove that $\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) = 0$, p an odd prime.

23. Use Wilson's theorem to prove that if p is a prime of the form $4n + 3$, then $1.2.3 \ldots p - 1/2 \equiv (-1)m \pmod{p}$, where m is the number of quadratic no residue among the factors on the left side.

24. For which primes p do their exist integers x and y with $(x, p) = 1$, $(y, p) = 1$, such that $x^2 + y^2 \equiv 0 (\text{mod } p)$. [$p = 2$, $p \equiv 1 (\text{mod } 4)$]

25. Prove that there are infinitely many primes of each of the form $3n = 1$ and $3n - 1$. [**Hit:** first determine primes p such that $(-3/p) = 1$]

26. Find all odd primes p such that 3 is a quadratic residue mod p. [$p \equiv \pm 1 (\text{mod } 12)$]

27. If p is an odd prime and $(a, p) = 1$, prove that
$ax^2 + bx + c \equiv 0 (\text{mod } p)$ has two, one, or no solutions according as $b^2 - 4ac$ is a quadratic residue, is congruent to zero, or is a quadratic non-residue modulo p.

28. If prime $p \equiv 1 (\text{mod } 4)$ and a is a quadratic residue of p show that $p - a$ is also a quadratic residue of p. Hence show that, if a_i ($i = 1, 2 \ldots \frac{1}{2}(p - 1)$) are the quadratic residue of p satisfying $0 < a_i < p$ then

$$\sum_{i=1}^{\frac{1}{2}(p-1)} a_i = \frac{1}{4} p(p - 1)$$

29. Prove that $\left(\frac{6}{p}\right) = \begin{matrix} 1 \\ -1 \end{matrix}\Bigg\} \begin{matrix} \text{if } p \equiv 1, -1, 5 \text{ or } -5 (\text{mod } 24) \\ \text{if } p \equiv 7, -7, 11 \text{ or } -11 (\text{mod } 24) \end{matrix}$

30. If $M = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \ldots + \left[\frac{p-1}{2} \cdot \frac{q}{p}\right]$, then prove that

$$m = M + \frac{(p^2 - 1)(q - 1)}{8} (\text{mod } 2),$$

where m is the number of the least positive residue of the set $q, 2q, 3q, \ldots, \frac{p-1}{2} q$.

7

HOMOGENEOUS QUADRATIC DIOPHANTINE EQUATION

Theorem 7.1. The Diophantine equation $x^2 + y^2 = z^2$ ...(*) has infinite solution.

For if (a, b, c) is a solution then (ka, kb, kc) is also a solution for $k \in \mathbb{Z}$

Remark: If (a, b, c) is a solution and $(a, b) = d$ then $(b, c) = (c, a) = d$

Proof: $\because$ $(a, b) = d \therefore d \mid a, d \mid b, d^2 \mid a^2, d^2 \mid b^2 \therefore d^2 \mid a^2 + b^2$

But $a^2 + b^2 = c^2$ gives $d^2 \mid c^2 \therefore d \mid c$

Now $d \mid b, d \mid c$; Claim $(b, c) = d$

If not, suppose

$(b, c) = d_1 > d$

Then, $d_1 \mid b, d_1 \mid c, d_1^2 \mid b^2, d_1^2 \mid c^2 \therefore d_1^2 \mid a^2$ (since $a^2 + b^2 = c^2$) $\therefore d_1 \mid a$

But $d_1 \mid b \therefore d_1 \mid (a, b) = d$ and is impossible

Therefore $d_1 = d$, Hence

Similarly $(c, a) = d$

Corollary 7.2. If $(x, y) = 1$ then $(y, z) = (z, x) = 1$

If (a, b, c) is a solution of (*) then the ordered triple is called a *Pythagorean triple* because there is a right angled triangle whose sides have corresponding lengths. This theorem in geometry goes after the name of Pythagoras.

We have seen above that if x, y, z is a triple then so is also kx, ky, kz for every integer k. And if for the Pythagorean triple (a, b, c) we have $(a, b, c) = 1$ then we say that it is primitive.

We confine only to primitive solutions of (*). [Observe: (3, 4, 5); (7, 24, 25); (8, 15, 17) etc. are primitive Pythagorean triples]

Now the question is how many solutions of (*) are which are relatively prime [or primitive]

Lemma 7.3. If (x, y, z) is a primitive solution of (*), then one of x and y is even and the other is odd. (called x and y are of *opposite parity* otherwise are of *same parity*.)

Proof: Since $(x, y) = 1 \therefore$ both of x and y cannot be even

If both of them are odd then x^2 and y^2 are also odd and $\therefore$ $x^2 + y^2$ is even.

$\therefore$ z^2 is even and so, z is even ...(*i*)

Now x is odd gives

$$x \equiv 1 \text{ or } 3 (\text{mod } 4)$$

or $$x^2 \equiv 1 (\text{mod } 4)$$

Similarly, y odd gives

$$y^2 \equiv 1 (\text{mod } 4)$$

Therefore $$z^2 = x^2 + y^2 = 1 + 1 = 2 (\text{mod } 4)$$ ...(i)

But z is even $\therefore$ (i) contradicts (ii)

$\therefore$ Both of x and y cannot be odd.

$\therefore$ One of them is odd and the other is even.

Remark: Let us assume that x is odd and y is even.

Lemma 7.4. 2 If x, y, z is a primitive solution of (*) then $\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$

Proof: If not let $\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = g \neq 1$

$\therefore$ $$g \mid \frac{z-x}{2}, \frac{z+x}{2}$$

or $$g \mid \frac{z-x}{2} + \frac{z+x}{2} \text{ and } \frac{z-x}{2} - \frac{z+x}{2}$$

i.e., $$g \mid z \text{ and } g \mid x$$

$\therefore$ $(z, x) \neq 1$, a contradiction [$\because$ x, y, z primitive solution] Hence.

Lemma 7.5. If $(x, y) = 1$ and $xy = d^2$, then x and y are also squares

Proof: Suppose $x = p_1 p_2 \ldots p_i$ (not necessarily distinct primes)

$$y = q_1 q_2 \ldots q_j \text{ (not necessarily distinct primes)}$$

Here no $$p_i = q_j \text{ (since } (x, y) = 1$$

Now $$xy = p_1 p_2 \ldots p_i q_1 q \ldots q_j = d^2$$

This is possible only when $p_1 p_2 \ldots p_i = d_1^{\,2}$ and $q_1 q_2 \ldots q_j = d_2^{\,2}$.

Theorem 7.6. (*) has a primitive solution if and only if $\exists$ $s, t \in \mathbb{N}$, $s > t$, $(s, t) = 1$ and one even the other odd such that

$$x = s^2 - t^2$$
$$y = 2st \quad \ldots(**)$$
$$z = s^2 + t^2$$

Proof: Let x, y, z be a primitive solution of (*).

Then $$x^2 + y^2 = z^2$$

or, $$y^2 = z^2 - x^2 = (z + x)(z - x)$$

$$\therefore \quad \left(\frac{y}{2}\right)^2 = \frac{z+x}{2}\frac{z-x}{2} \qquad \text{...(i)}$$

By Lemma 7.4

$$\left(\frac{z+x}{2}\frac{z-x}{2}\right) = 1$$

$\therefore$ By Lemma 7.5

$$\frac{z+x}{2} = s^2, \frac{z-x}{2} = t^2, \text{ Say } s, t \in \mathbb{N}, s > t$$

$\therefore$ Solving we get

$$z = s^2 + t^2$$
$$x = s^2 - t^2$$
$$y = (z^2 - x^2)^{\frac{1}{2}} = 2st$$

Now since s and t both are odd (even) z and x are both odd (even) And therefore $(z, x) \neq 1$, which is not the case. Therefore one of s and t is even and the other is odd.

Again if $(s, t) = g \neq 1$ then,

$$(s, t) = 1$$

Conversely, suppose (**) exists. Then $x^2 + y^2 = (s^2 - t^2)^2 + (2st)^2 = s^2 + t^2 = z^2$.

Note: Since there is infinity of choice for s and it, therefore there are infinite number of primitive solutions for (*)

Some Primitive Pythagorean Triples (with $s \leq 6$)

s	t	$x = s^2 - t^2$	$y = 2st$	$z = s^2 + t^2$
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61

Corollary 7.7. $x^2 + y^2 = z^4$ ...(1)

will have infinite number of solutions

Since it is same as

$$x^2 + y^2 = r^2 \qquad \text{...(2)}$$

where $r = z^2$ and $x = 3$, $y = 4$, $r = 5$ is a solution of (2) so, $x = 15$, $y = 20$, $z = 25$ is a solution of (2) and therefore $x = 15$, $y = 20$, $z = 5$ is a solution of (1)

Note: The above theorem can also be stated as given below:

The positive primitive solutions of $x^2 + y^2 = z^2$ with y even are

$$x = s^2 - t^2,\ y = 2st,\ z = s^2 + t^2,$$

where s and t are arbitrary integers of opposite parity with $s > t > 0$ and $(s, t) = 1$

Example 1. Find all primitive solutions of $x^2 + y^2 = z^2$ having $0 < z < 30$

Solution: Let $x = s^2 - t^2$, $y = 2st$, $z = s^2 + t^2$

(1) Since $s > t$, and s, t are of opposite parity, let us take $t = 1$, $s = 2$, then $x = 3$, $y = 4$, $z = 5$ which is a *primitive solution.*

(2) When $t = 1$, $s = 4$ then $x = 15$, $y = 8$, $z = 17$ which is a *primitive solution.*

(3) When $t = 1$, $s = 6$, then $z = 37 > 30$, hence we stop taking $t = 6$

(4) When $t = 2$, $s = 3$, then $x = 5$, $y = 12$, $z = 13$ which is a *primitive solution.*

(5) When $t = 2$, $s = 5$, $x = 21$, $y = 20$, $z = 29$, which is a *primitive solution.*

(6) When $t = 3$, $s = 4$, $x = 7$, $y = 24$, $z = 25$, which is a *primitive solution.*

(7) When we take $t = 4$, we get a value of $z > 30$. Hence we stop here.

Hence the primitive solutions are

t	s	x	y	z
1	2	3	4	5
1	4	15	8	17
2	3	5	12	13
2	5	21	20	29
3	4	7	24	25

since x and y are interchangeable, therefore other solutions are

t	s	x	y	z
1	2	4	3	5
1	4	8	15	17
2	3	12	5	13
2	5	20	21	29
3	4	24	7	25

(4, 3, 5), (8, 15, 17), (12, 5, 13), (20, 21, 29), (24, 7, 25).

Example 2. Prove that if $x^2 + y^2 = z^2$, then one of x, y is $\pm$ 1(mod 4) and the other is 0(mod 4)

Solution Since s and t are of opposite parity let t be even and s odd. Then

$$x = s^2 - t^2 = (\text{odd})^2 - (\text{even})^2 \equiv \text{odd}^2 \pmod 4$$

$$\equiv (2n + 1)^2 \pmod 4 \equiv 4n^2 + 4n + 1 \equiv 1 \pmod 4$$

When r is even, s is odd we get

$$x \equiv \pm 1 \pmod 4.$$

Now $y = 2rs = 2(\text{even number}).(\text{odd number}) \equiv 0 \pmod 4$

Example 3. Prove that the are of a right-angled triangle can never be a perfect square.

Solution: Suppose x and y are the lengths of the two sides of the triangle and z is the length of the hypotenuse, then $x^2 + y^2 = z^2$

Area of the right triangle is given by $\frac{1}{2}xy$.

We now show that $\frac{1}{2}xy$ is not a perfect square

Suppose the solution of the equation (*) is

$$x = a^2 - b^2,\ y = 2ab,\ z = a^2 + b^2$$

where a, b are of opposite parity and $(a, b) = 1$

Therefore, $\frac{1}{2}xy = (a^2 - b^2)\ ab.$

Now if b is even and a is odd, b^2 will contain 4 and b will contain 2.

Therefore (2) can never be a perfect square.

Example 4. Show that the positive integer solution of the equation $x^{-2} + y^{-2} = z^{-2}$, $(x, y, z) = 1$ is given by

$$x = a^4 - b^4,\ y = 2ab(a^2 + b^2),\ z = 2ab\ (a^2 - b^2),$$

where $a > b > 0$, $(a, b) = 1$, a, b cannot be of some parity.

Solution: First we show that the solution of $X^{-1} + Y^{-1} = Z^{-1}$, $(X, Y, Z) = 1$, has and must be of the form

$$X = A\ (A + B),\ Y = B\ (A + B),\ Z = AB$$

Proof: The first part is easy.

For the second part

If X, Y, Z is a solution of the given equation, $(X, Y) = C$, then

$$X = CA,\ Y = CB,\ (A, B) = 1. \text{ Then}$$

$$Z^{-1} = X^{-1} + Y^{-1} = \frac{A + B}{CAB},$$

thus $$Z = \frac{CAB}{A + B}$$

As $(A, B) = 1$, $(AB, A + B) = 1$; Hence $(A + B) \mid C$.

Write $C = C'(A + B)$

Then $Z = C'AB$. Since $(X, Y, Z) = 1$ we have

$$(CA, CB, C'AB) = (C(A, B), C'AB) = (C'(A + B), C'(AB) = C' = 1$$

i.e., $C = (A + B)$, $C' = 1$. Hence the must part holds.

Now we prove the main result:

We take here

$$x^2 = X,\ y^2 = Y \text{ and } z^2 = Z \qquad \because (x, y, z) = 1 \therefore (X, Y, Z) = 1 .$$

$\therefore$ from the above example we have

$$X = R(R + S),\ Y = S(R + S),\ Z = RS,$$

where $R, S > 0$ $(R, S) = 1$.

From $Z = RS$, we know that R, S are both square numbers.

And from $Z = R(R + S)$, we find $R + S$ is also a square number.

Putting $R = r_1^2$, $z = s_1^2$, $R + S = t_1^2$. We have

$$r_1^2 + s_1^2 = t_1^2,\ R, S > 0,\ (R, S) = 1$$

Then by above theorem, we obtain

$$r_1 = a^2 - b^2,\ s_1 = 2ab,\ t = a^2 + b^2,$$

Where $a, b > 0$, $(a, b) = 1$, a and b of opposite parity.

Therefore

$$x = r_1 t_1 = a^4 - b^4$$
$$y = s_1 t_1 = 2ab(a^2 + b^2)$$
$$z = r_1 s_1 = 2ab\ (a^2 - b^2).$$

Theorem 7.8. The Diophantine equation $x^4 + y^4 = z^2$ ...(*) has no positive solution

Proof: Suppose (*) has a solution (x_0, y_0, z_0). By an argument similar to that of previous section we may assume that x_0, y_0, z_0 are pair wise relatively prime.

x_0 is odd, y_0 is even (i.e., one is odd and another odd)

Now $$x_0^4 + y_0^4 = z_0^2$$

or $$(x_0^2)^2 + (y_0^2)^2 = z_0^2$$

Therefore, (x_0^2, y_0^2, z_0) is a solution of $x^2 + y^2 = z^2$ ...(Ψ)

Therefore by theorem 7.6 there exist $s, t \in \mathbb{N}$ $(s, t) = 1$, $s > 1$, one even other odd such that

$$x_0^2 = s^2 - t^2$$
$$y_0^2 = 2st \quad ...(1)$$
$$z_0 = s^2 + t^2$$

From $x_0^2 = s^2 - t^2$ i.e, $x_0^2 + t^2 = s^2$ we see that (x_0, t, s) is also a solution of (Ψ) with x_0 odd and t even. Using theorem 7.6 again we find that there exist $a, b \in \mathbb{N}$, $a > b$, $(a, b) = 1$ one odd, other even such that

$$x_0^2 = a^2 - b^2$$
$$s = a^2 + b^2 \qquad ...(2)$$
$$t = 2ab$$

On substituting this in $y_0^2 = 2st$, we get

$$y_0^2 = 2(a^2 + b^2)2ab$$

or $$\left(\frac{y_0}{2}\right)^2 = (a^2 + b^2)\, ab.$$

$\because$ $(a, b) = 1$,

$\therefore$ $a^2 + b^2$, a, b are pair wise relatively prime.

Applying Lemma 7.5, twice we find that a, b and $a^2 + b^2$ are squares say $a = a_0^2$, $b = b_0^2$ and $s = s^2 + b^2 = s_0^2$

Thus $s_0^2 = a^2 + b^2 = a_0^4 + b_0^4$

Here $s_0 \le s < s^2 + t^2 = z_0$

We see that if a positive solution (x_0, y_0, z_0) exists there must exist another positive solutions (a_0, b_0, s_0) where $s_0 < z_0$

It follows from the method of infinite descent that no positive solution can exist.

[Method of infinite descent Let there exist a positive integer n with a certain property, such that there exists a smaller positive integer that has the same property. Such an n cannot exist; because if it exists we obtain an infinite decreasing sequence of positive integers all having the same specific property which is clearly impossible]

Corollary 7.9. The equation $x^4 + y^4 = z^4$ has no positive solution

Proof: If it has solution, say (x_0, y_0, z_0) then

$$x_0^4 + y_0^4 = z_0^4,$$

or $$x_0^4 + y_0^4 = (z_0^2)2$$

$\therefore$ $(x_0, y_0$ and $z_0)$ is a solution of

$x^4 + y^4 = z^2$ which is not possible.

$\therefore$ $x^4 + y^4 = z^4$ has no positive solution.

7.1 HISTORICAL NOTE OF FERMAT'S LAST THEOREM

Unlike equations of degree at most four, there is comparatively little structure, which may be imposed on the solutions of general Diaphantine problems of degree five or greater. Some particular classes of problems admit effective analysis, but for typical problems of this type it is difficult to determine the entire solution set.

In the 17^{th} century, Pirre Fermat conjectured that the equation $x^n + y^n = z^n$ had no solution in non zero integers with n greater than 2 – known as Fermat's Last theorem. The problem has little direct impact on broad field of mathematics, but has precipitated considerable research of significant impact on number theory and algebraic geometry.

The Fermat problem attracted considerable attention, and in addition to substantial progress by mathematicians of note, also engendered many attempts of dubious quality by amateurs.

Fermat himself provided a proof for the case $n = 4$; indeed the proved by induction (popularly: by infinite descent") the slightly stronger result that no two fourth powers can ever sum to a perfect square. Fermat's more general conjecture was in fact no more than

a personal note discovered after his death; it does not appear to be the case that he ever claims publicly to have proven the conjecture true – had he indeed been convinced as a challenge problem to a other mathematicians and eventually to have shared a proof in his letters to others.

Euler proved the result for $n = 3$, and Dirichlet and Legender proved for $n = 5$

E, Kumar (1810 – 1893) made the greatest advances towards a solution. Instead of confining himself to the field of rational numbers he extended to his concept of number theory to include the algebraic numbers (those complex numbers which are roots of polynomials with rational coefficients) Dirchlet pointed out a flaw in the argument. Kumar had assumed the factorization into primes is unique in a certain sub ring of the algebraic numbers where, in fact this factorization is not unique. Because this assumption was essential, the proof was not valid.

Kumar returned to the problem and by using the theory of ideals, he was able to solve parts of his proof and to establish very general condition for the insolvability of Fermat's theorem. Most of the progress made on the problem was along the lines of Kumar's theory. With the advent of the high-speed electronic computer it had been possible to check Kumar's criteria for large exponents. Till 1967 it had been proved that the Diaphontaine equation $x^n + y^n = z^n$ has no solution if $3 < n < 25{,}000$. In subsequent years, many refinements increased the set of exponents n for which the result was known to be true, but no proof valid for all n has been completed along these lines.

By the 1980 attention had shifted from algebraic number theory to algebraic geometry as the appropriate tool for the problem. Gerd falting's work on the model conjecture implied in particular that for any n there were at most a finite number of solutions to the Fermat equation. Frey noticed in 1986 that a non trivial solution to the Fermat equation would be related to an anomalous situation in elliptic curves; Serre clarified the conjectured connection, and Ribet proved this in K A Ribet "on modular representation of Gal (Qbar/Q) arising from modular forms", Inventions Mathematics, Vol. 100 (1990) pp431-476. What Ribet proved is that given a nontrivial solution to the Fermat equation $a^n + b^n = c^n$ the elliptic curve described by a particular equation would be fairly well behaved but would also be a counter example to the Tanyama – Shimura conjecture (that all elliptic curves over the rational numbers are modular)

The Taniyama-shimura conjecture is of great interest in elliptic curves and was not completely proved by 1994. However, Wiles has a given a proof valid for most elliptic curves this proves: there are no nontrivial solutions to the Fermat equation. Wiles first announced his proof in 1993 but technical difficulties showed the proof to be incomplete; a year later he managed a complete proof (actually using slightly simpler ideas) with the collaboration of Taylor for the particular portion, which had invalidated his earlier attempt. The papers were published together, constituting one issue of the Annals of Mathematics. The citations are ANDREW WILES, "MODULAR ELLIPIC CURVES AND FERMAT'S LAST THEOREM" ANNALS OF MATHEMATICS, vol. 141 (1995) pp443-551

Richard Taylor and Andrew Wiles, "Ring –theoretic properties of certain Hecje algebras" annals of Mathematics, Vol. 141 (1995) pp53 572

Extensions of this work have already appeared. Casual enthusiasts of number theory should be warned that this proof of Fermat's Last theorem is unlikely to be comprehensible without the investment of several year's study of algebraic number theory and algebraic geometry.

7.2 TWO SQUARES PROBLEM

To find those positive integers which can be expressed as a sum of two squares.

Lemma 7.10. If a and b can be written as sum of two squares, then the product ab can also be written as a sum of two squares.

Proof: Let
$$a = p^2 + q^2$$
$$b = r^2 + s^2$$
$$ab = (p^2 + q^2)(r^2 + s^2)$$
$$= p^2r^2 + p^2s^2 + q^2r^2 + q^2s^2$$
$$= (pr + qs)^2 + (ps - qr)^2.$$

Lemma 7.11. If $(a, p) = 1$, then $x \equiv ay \pmod p$ has a solution x_0, y_0 such that
$$0 < |x_0| < \sqrt{p} \text{ and } 0 < |y_0| < \sqrt{p}$$

Proof Let $[\sqrt{p}] = m$

Consider the set of numbers

$1 + a$	$1 + 2a$	.....	.....	$1 + (m + 1)a$
$2 + a$	$2 + 2a$	.....	.....	$2 + (m + 1)a$
$3 + a$	$3 + 2a$	.....	.....	$3 + (m + 1)a$
.....	.....	.....	.....	.....
$(m + 1) + a$	$(m + 1) + a$	.....	.....	$(m + 1) + (m + 1)a$

This set contains $(m + 1)^2$ numbers (not necessarily distinct) Since
$$(m + 1)^2 > p \qquad (\because m + 1 > \sqrt{p})$$
at least two of the numbers, say $x_1 + y_1a$ and $x_2 + y_2a$ must lie in the same residue class (mod p) where $x_1 \neq x_2$ or $y_1 \neq y_2$

$\therefore$ $$(x_1 + y_1a) - (x_2 + y_2a) \equiv 0 \pmod p$$
or $$(x_1 - x_2) + a(y_1 - y_2) \equiv 0 \pmod p$$
$\Rightarrow$ $$(x_1 - x_2) \equiv (y_2 - y_1)a \qquad \text{...(I)}$$

Because one of the terms $(x_1 - x_2)$, $(y_1 - y_2)$ is not zero, it follows obviously that neither is zero.

$\because$ $$0 < x_1, x_2, y_1, y_2 \leq m + 1$$

$\therefore$ $$0 < |x_1 - x_2| \leq m < \sqrt{p}$$

Similarly $$0 < |y_1 - y_2| \leq m < \sqrt{p}$$

If we let $$x_0 = x_1 - x_2$$

$$y_0 = y_2 - y_1$$

We get from (1)

$$x_0 \equiv y_0 a (\text{mod } p), \text{ where } 0 < |x_0| < \sqrt{p},\ 0 < |y_0| < \sqrt{p}$$

and which is the lemma to be proved.

Theorem 7.12. The odd prime number p can be written as a sum of two squares if and only if $p \equiv 1 (\text{mod } 4)$ (i.e., p is of the form $4n + 1$)

Proof: Recall: -1 is q.r. mod p if and only if $p \equiv 1 (\text{mod } 4)$

Proof: -1 is q.n.r if and only if $p \equiv 3 \pmod 4$

$\therefore$ $p = a^2 + b^2$ (to prove $p \equiv 1 (\text{mod } 4)$)

$\because$ p is a prime, $b \neq 0$

Again $p \nmid b$, for if $p \mid b$, $p \mid a$ also

Moreover, $p \mid b$, $p \mid a$ give $p^2 \mid a^2$ and $p^2 \mid b^2$

$\therefore$ $p^2 \mid a^2 + b^2 = p$ or $p^2 \mid p$ and is impossible.

$\therefore$ $p \nmid b$

$\therefore$ $(p, b) = 1$

$\therefore$ $\exists x_0, y_0 \in \mathbb{Z}$ such that

$$px_0 + by_0 = 1$$

$\therefore$ $$by_0 = 1 - px_0$$

or $$by_0 \equiv 1 (\text{mod } p)$$

$\therefore$ $$(by_0)^2 \equiv 1 (\text{mod } p)$$

Thus $$y_0^2 p = y_0^2 (a^2 + b^2)$$
$$= (y_0 a)^2 + (y_0 b)^2$$
$$\equiv (y_0 a)^2 + 1 (\text{mod } p)$$

$\therefore$ $$y_0^2 p \equiv (y_0 a)^2 + 1 (\text{mod } p)$$

or $$(y_0 a)^2 + 1 \equiv 0 (\text{mod } p)$$

or $$(y_0 a)^2 \equiv -1 (\text{mod } p)$$

or -1 is q.r. mod p

$\therefore$ $$p \equiv 1 (\text{mod } 4).$$

Conversely suppose

$$p \equiv 1 (\text{mod } 4) \text{ i.e., } p = 4n + 1,\ n \in \mathbb{N}$$

(to prove that $p = a^2 + b^2$)

$\because$ $$p \equiv 1 (\text{mod } 4), -1 \text{ is q.r. } (\text{mod } p)$$

$\therefore$ $\exists a \in \mathbb{Z}$ such that

$$a^2 \equiv -1 (\text{mod } p) \text{ i.e., } a^2 + 1 \equiv 0 (\text{mod } p) \quad \ldots(*)$$

Now obviously $(a, p) = 1$ ($\because p \mid 1$ impossible)

$\therefore$ By lemma 7.11, $\exists x_0, y_0 \in \mathbb{Z}$ such that

$$0 < |x_0| < \sqrt{p},\ 0 < |y_0| < \sqrt{p}, \text{ where } x_0 \equiv a y_0 (\text{mod } p)$$

If we now multiply (*) by y_0^2

$$y_0^2(a^2 + 1) = y_0^2a^2 + y_0^2 \equiv 0(\text{mod } p)$$

or $$y_0^2a^2 + y_0^2 \equiv 0(\text{mod } p)$$

or $$x_0^2 + y_0^2 \equiv 0(\text{mod } p)$$

or $$x_0^2 + y_0^2 = kp,\ k \in \mathbb{N} \qquad ...(i)$$

But $$0 < |x_0| < \sqrt{p},\ 0 < |y_0| < \sqrt{p}$$

give $$0 < x_0^2 < p,\ 0 < y_0^2 < p$$

$\therefore$ $$x_0^2 + y_0^2 < 2p \qquad ...(ii)$$

So (i) and (ii) give $x_0^2 + y_0^2 = p$.

Theorem 7.13. Let N be a positive integer

Write N in the form $m^2.k$, where k is square free. Then N can be written as a sum of two squares if and only if k has no prime factors of the form $4n + 3$

Proof: If k has no prime factor of the form $4n + 3$ then, it has prime factors of the form $4n + 1$. By Theorem 7.12 and lemma 7.10, k can be written as a sum of two squares, say

$$k = a^2 + b^2$$

$\therefore$ $$N = m^2k = m^2(a^2 + b^2) = (ma)^2 + (mb)^2$$

Suppose $$m^2k = N = a^2 + b^2$$

(To prove that k does not contain a factor of the form $4n + 3$)

Let $(a, b) = d$

Then, $d \mid a$, $d \mid b$ so, $d^2 \mid a^2$, $d^2 \mid b^2$

$\therefore$ $d^2 \mid a^2 + b^2$

or $d^2 \mid N$

or $d^2 \mid m^2k$

$\therefore$ $d^2 \mid m^2$, $\because$ $d^2 \nmid k$, (k being square free) $\therefore$ $\dfrac{m^2}{d^2} = \lambda \in \mathbb{N}$

$\therefore$ $$\frac{N}{d^2} = \frac{m^2k}{d^2} = \lambda k \text{ and}$$

$\because$ $d \mid a$, and $d \mid b$ $\therefore$ $a = a'd$, $b = b'd$, $(a', b') = 1$

and $$\frac{N}{d^2} = \frac{a^2 + b^2}{d^2} = \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 = a'^2 + b'^2$$

Also from $\dfrac{N}{d^2} = \lambda k$ we get

$$k \mid \frac{N}{d^2} = a'^2 + b'^2 \therefore a'^2 + b'^2 \equiv 0(\text{mod } k) \qquad ...(*)$$

Let p be an odd prime factor of k

$\therefore \quad \frac{N}{d^2} = a^2 + b^2 \equiv 0 (\text{mod } p)$ ...(**) [$\because$ p is a factor of k]

$\because \quad (a', b') = 1$, one of a' and b', say a' is relatively prime to p

i.e., $(a', p) = 1 \therefore \exists c, c' \in \mathbb{Z}$ such that $ca' + c'p = 1$

or $ca' \equiv 1 (\text{mod } p) \therefore (ca')^2 \equiv 1 (\text{mod } p)$

From (*), (**)

$(ca')^2 + (cb')^2 \equiv 0 (\text{mod } p)$

$\Rightarrow \quad 1 + (cb')^2 \equiv 0 (\text{mod } p)$

$\Rightarrow \quad (cb') \equiv -1 (\text{mod } p)$

or $x^2 \equiv -1 (\text{mod } p)$ has a solution $x = cb'$ so -1 is a q.r. (mod p)

$\therefore \quad p \equiv 1 (\text{mod } 4)$

$\therefore$ any factor of k is of the form $4n + 1$.

Theorem 7.14. If $p^c \mid n, p^{c+1} \nmid n$ where p is a prime of the form $4k + 3$, and c is odd, then n has no representation as the sum of two squares.

Proof: Suppose that there is a proper representation of the form $n = x^2 + y^2$

Let $(x, y) = d$ so that

$x = Xd, y = Yd, (X, Y) = 1$

Let p^l be the highest power of p which divides d.

Then $n = d^2(X^2 + Y^2) = d^2N$(say)

Hence $N = X^2 + Y^2, (X, Y) = 1$

Since $p^c \mid n, p^2 \mid d^2$ Therefore, $p^{c-2} \mid N$

$c - 21$ is positive as c is odd an 21 is even.

Hence by the preceding result,

Since N is divisible by p of the form $4k + 3$, N has no representation as the sum of the two squares.

Hence n will also have no such proper representation.

Theorem 7.15. If p is a prime of the form $4k + 1$, there exists a solution in integers x, y, m of $x^2 + y^2 = mp$, with $0 < m < p$

Proof: Since $p = 4k + 1$, we have

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$$

Hence, there exists an integer y such that

$1 + y^2 \equiv 0 (\text{mod } p)$ as -1 is a q.r.

We can find $Y \equiv \pm y (\text{mod } p)$ and such that $|Y| < p/2$

Then $0 < mp = 1 + Y^2$

$$< 1 + \frac{p^2}{4} < p^2$$

Thus $0 < m < p$

Therefore, the integers, 1, Y and m satisfy the equation

$$x^2 + y^2 = mp.$$

Example 5. If p is a prime of the form $4k + 1$ and if $x^2 + y^2 = mp$ with $1 < m < p$, m-even, there exist integers x_1, y_1 and M such that

$$x_1^2 + y_1^2 = Mp \text{ With } 1 \le M < m$$

(**Hint:** take $X = \frac{x+y}{2}$, $Y = \frac{x-y}{2}$, $M = \frac{m}{2}$ and see $X^2 + Y^2 = Mp$).

Ex. The same result is true when m is odd also.

Definition: If $x^2 + y^2 = n$ is solvable, we write

$N(n) \equiv$ number of solution of $x^2 + y^2$ is n

$P(n) \equiv$ number of non-negative, primitive solutions of $x^2 + y^2$ is n

$Q(n) \equiv$ number of primitive solutions of $x^2 + y^2$ is n

Example 6. Show that for $x^2 + y^2 = 1$, $N(1) = Q(1) = 4$, $P(1) = 2$

Proof: Since $1 = (\pm 1)^2 + 0^2 = 0^2 + (\pm 1)^2$ and there are no other solutions, we have

$$x = 1, y = 0; x = -1, y = 0, x = 0, y = 1; x = 0, y = -1$$

Hence, $N(1) = 4$

$Q(1) = 0, P(1) = 2.$

Example 7. Show that for $x^2 + y^2 = n$, $n > 1$

(i) $Q(n) = 4P(n)$

(ii) $N(n) = \sum_{d^2 \mid n} Q\left(\frac{n}{d^2}\right)$

Solution: (i) If $n > 1$ and (x, y) is a non negative primitive solution then $n \ge 1, y \ge 1$ and $(\pm x, \pm y)$ is a primitive solution for all choice of the signs. From this it follows that $Q(n) = 4P(n)$

(ii) If x, y is any solution of

$$x^2 + y^2 = n \text{ and if } (x, y) = d$$

then $d^2 \mid (x^2 + y^2)$ i.e., $d^2 \mid n$; $\left(\frac{x}{d}, \frac{y}{d}\right) = 1$

and $$\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{n}{d^2} \qquad \ldots(1)$$

from (1) it is obvious that

$$N(n) = \sum_{d^2 \mid n} Q\left(\frac{n}{d^2}\right).$$

7.3| THREE SQUARE PROBLEM

Lemma 7.16. If a is a sum of three squares

b ... ...

Then ab may not be sum of three squares e.g.

$$3 = 1^2 + 1^2 + 1^2,\ 5 = 1^2 + 2^2 + 0^2$$
$$3.5 = 15 = 3^2 + 2^2 + 1^2 + 1^2$$

Note: Because of this fact the three square problem becomes more difficult.

Lemma 7.17. The number of the form $8k + 7$ is not representable as a sum of three squares.

Proof: Any number $n \equiv 0, 1, 2, 3, 4, 5, 6$ or $7 \pmod 8$

$\therefore$ $n^2 \equiv 0, 1, 4 \pmod 8$

Hence the sum of the three squares $\not\equiv 7 \pmod 8$,

Since it is impossible to build up 7 from three terms each of which is 0 or 1 or 4.

Lemma 7.18. A number of the form $4^1(8k + 7)$ is not representable as a sum of three squares.

Proof: A multiple of 4, say $4m$ can only be representable if m itself be representable.

Because if $4m = m_1^2 + m2^2 + m3^2$ then $4 \mid$ RHS but $a^2 \equiv 0, 1, \pmod 4$

since $a \equiv 0, 1, 2, 3 \pmod 4$

$\therefore$ $4 \mid m_1^2, m_2^2, m3^2$

$\therefore$ $2 \mid m_1, m_2, m_3$

or $m_1 = 2k_1, m_2 = 2k_2, m_3 = 2k_3$

$\therefore$ $4m = (2k_1)^2 + (2k_2)^2 + (2k_3)^2$

$= 4k_1^2 + k_2^2 + k_3^2)$

i.e., m is representable as sum of three squares.

But m is not representable.

Hence, number of the form $4.(8k + 7)$ is not representable as a sum of three squares since $8k + 7$ is not.

And similarly $4(4(8k + 7))$ i.e., $4^2(8k + 7)$ is not represent able as sum of three squares and so on.

$\therefore$ In general $4^1(8k + 7)$ is not representable as a sum of three squares

Note: Every number which is not of the form $4^1(8k + 7)$ is representable as a sum of three squares and the proof of this is very difficult; so it is left out.

Example 8. Show that if $p \equiv 5 \pmod{12}$ and $p > 17$; then p can be represented as a sum of three distinct squares

[**Hint:** Use the identity: $9(a^2 + b^2) = (2a - b)^2 + (2a + 2b)^2 + (2b - a)^2$]

7.4 THE FOUR SQUARE PROBLEM

Lemma 7.19. If a and b can be written as a sum of four squares, so can the product

Proof:
$$a = x_1^2 + x_2^2 + x_3^2 + x_4^2$$
$$b = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

Now
$$ab = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$
$$= (x_1y_1)^2 + (x_1y_2)^2 + (x_1y_3)^2 + (x_1y_4)^2 + (xy)^2 + (xy)^2 + (xy)^2 + (xy)^2$$
$$+ (xy)^2 + (xy)^2 + (xy)^2 + (xy)^2 + (xy)^2 + (xy)^2 + (xy)^2 + (xy)^2$$
$$= \ldots\ldots\ldots\ldots$$
$$= \ldots\ldots\ldots\ldots$$
$$= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_4 + x_3y_4 - x_4y_1)^2$$
$$+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - \ldots)^2.$$

Notation: We call $(a, b) \equiv (c, d) \pmod m$ if $a \equiv c \pmod m$ and $b \equiv d \pmod m$

Lemma 7.20. A set of ordered pairs of integers containing more than m^2 elements must have two elements that are congruent mod m.

Proof: Each ordered pair of integers is congruent (mod m) to one of the following m^2 ordered pairs:

(1, 1)	(1, 2)	( )	( )	(1, m)
(2, 1)	(2, 2)	( )	( )	(2, m)
( )	( )	( )	( )	( )
( )	( )	( )	( )	( )
(m, 1)	(m, 2)	( )	( )	(m, m)

If a set contains more than m^2 ordered pairs, at least two of them must be congruent mod m to one of the ordered pairs in the above list. Obviously these two ordered pairs are congruent mod m.

Lemma 7.21. Let a, b, c, d be given integers

Let p be prime number

The system of congruences
$$ax + by - z \equiv 0 \pmod p$$
$$cx + dy - u \equiv 0 \pmod p$$

has non trivial solution, x_0, y_0, z_0, u_0 such that each number in the solution is less than $\sqrt{p}$ in absolute value

$$(\text{i.e., } |x_0| < |\sqrt{p}|, |y_0| < |\sqrt{p}| \ldots \text{ etc.}$$

Proof: Define
$$\alpha = \alpha(x, y, z, u) = ax + by - z$$
$$\beta = \beta(x, y, z, u) = cx + dy - u,$$

where x, y, z u vary over the domain

$$\{0, 1, 2, ..., m-1, m = [\sqrt{p}]$$

we obtain $(m+1)^4$ values of α (not necessarily distinct)

and $(m+1)^4$ values of β (not necessarily distinct)

Thus we have $(m+1)^4$ ordered pairs (α, β) with (α, β) corresponding to the some values of x, y, z, u.

$\because (m+1)^4 > p^2$, it follows from lemma 7.20 that at least two ordered (α_1, β_1) and (α_2, β_2) have corresponding components that are congruent mod p^2 and therefore congruent mod p

$$\alpha_1 \equiv ax_1 + by_1 - z_1 \equiv \alpha_2 \equiv ax_2 + by_2 - z_2 \pmod{p}$$
$$\beta_1 \equiv cx_1 + dy_1 - u_1 \equiv \beta_2 \equiv cx_2 + dy_2 - u_2 \pmod{p}$$

$\because$ (α_1, β_1) and (α_2, β_2) correspond to different values of x, y, z and u, then at least one of the numbers, $x_1 - x_2, y_1 - y_2, z_1 - z_2, u_1 - u_2$ is not zero.

If we recall the range of values for x, y, z, u we see that $x_1 - x_2, y_1 - y_2, z_1 - z_2, u_1 - u_2$ less than $\sqrt{p}$ in absolute values.

$$|x_1 - x_2|, |y_1 - y_2|, |z_1 - z_2|, |u_1 - u_2| \le m < \sqrt{p}$$

If we now let $x_0 = x_1 - x_2, y_0 = y_1 - y_2, z_0 = z_1 - z_2, u_0 = u_1 - u_2$

we get

$$ax_0 + by_0 - z_0 \equiv 0 (\mathrm{mod}\, p)$$
$$cx_0 + dy_0 - u_0 \equiv 0 (\mathrm{mod}\, p)$$

where $|x_0| < \sqrt{p}, |y_0| < \sqrt{p}, |z_0| < \sqrt{p}, |u_0| < \sqrt{p}$.

Lemma 7.22. If p is an odd prime then, there exist integers a, b such that

$$a^2 + b^2 \equiv -1 (\mathrm{mod}\, p)$$

Proof: Consider the following two sets

$$A = \{0^2, 1^2, 3^2, ... \left(\frac{p-1}{2}\right)^2\}$$

$$B = \{-0^2, -1, -1^2, -1, -3^2 - 1, ... -\left(\frac{p-1}{2}\right)^2 - 1\}$$

Obviously the element of A are incongruent mod p(i.e., $i^2 \not\equiv j^2 \pmod{p}$ for $i \neq j$ and also the elements of B.

$\because$ $A \cup B$ contains more than p elements, at least two numbers in the union are congruent mod to one another and one of these numbers say, a^2, must be in A and the other is in B

Theorem 7.23. Each prime number can be written as a sum of four squares

Proof: If $p = 2$, then $p = 1^2 + 1^2 + 0^2 + 0^2$

If $p = 3$ then $p = 1^2 + 1^2 + 1^2 + 0^2$

If $p \ge 5$

By Lemma 7.22

$$\exists a, b \in \mathbb{Z} \text{ such that } a^2 + b^2 \equiv -1 (\text{mod } p)$$

By Lemma 7.21

$\exists$ non trivial solution x_0, y_0, z_0, u_0, each of $|x_0|, |y_0|, |z_0|, |u_0| < \sqrt{p}$,

of

$$ax + by \equiv z (\text{mod } p)$$
$$bx - ay \equiv u (\text{mod } p)$$

Thus, $z_0^2 + u_0^2 \equiv (ax + by)^2 + (bx - ay)^2$

$$\equiv (a^2 + b^2)(x^2 + y^2) \equiv (x_0^2 + y_0^2) (\text{mod } p)$$

or $x_0^2 + y_0^2 + z_0^2 + u_0^2 \equiv 0 (\text{mod } p) \Rightarrow x_0^2 + y_0^2 + u_0^2 = \lambda p, \lambda \in \mathbb{N}$ ...(1)

Again $|x_0|, |y_0|, |z_0|, |u_0| < \sqrt{p}$

$\therefore$ $0 < x_0^2 + y_0^2 + z_0^2 + u_0^2 < 4p$ ...(2)

(1) and (2) suggest that

$$x_0^2 + y_0^2 + z_0^2 + u_0^2 = p, 2p, 3p$$

(2) **Case I** If $x_0^2 + y_0^2 + z_0^2 + u_0^2 = p$, then the theorem is proved.

Case II Let $x_0^2 + y_0^2 + z_0^2 + u_0^2 = 2p$

Then two of them must be even and the other two odd.

Expanding $\left(\frac{x_0 + y_0}{2}\right)^2 + \left(\frac{x_0 - y_0}{2}\right)^2 + \left(\frac{z_0 + u_0}{2}\right)^2 + \left(\frac{z_0 - u_0}{2}\right)^2$ we get

$$= \frac{1}{4}[2(x_0^2 + y_0^2 + z_0^2 + u_0^2)] = \frac{1}{4} \times 2 \times 2p = p.$$

i.e., $$p = \left(\frac{x_0 + y_0}{2}\right)^2 + \left(\frac{x_0 - y_0}{2}\right)^2 + \left(\frac{z_0 + u_0}{2}\right)^2 + \left(\frac{z_0 - u_0}{2}\right)^2$$

Case III Let $x_0^2 + y_0^2 + z_0^2 + u_0^2 = 3p$

Then exactly one of the numbers say, x_0 is divisible by 3

If we allow negative value for some of the other numbers, we may assume that $y_0 \equiv z_0 \equiv u_0 \pmod 3$

Now expanding

$$\left(\frac{y_0 + z_0 + u_0}{3}\right)^2 + \left(\frac{y_0 + z_0 - u_0}{3}\right)^2 + \left(\frac{x_0 - y_0 + u_0}{3}\right)^2 + \left(\frac{x_0 + y_0 - z_0}{3}\right)^2$$

$$= \frac{1}{9} \times [3(x_0^2 + y_0^2 + z_0^2 + u_0^2)] = \frac{1}{9} \times 3 \times 3p = p$$

$$\therefore p = \left(\frac{y_0 + z_0 + u_0}{3}\right)^2 + \left(\frac{y_0 + z_0 - u_0}{3}\right)^2 + \left(\frac{x_0 - y_0 + u_0}{3}\right)^2 + \left(\frac{x_0 + y_0 - z_0}{3}\right)^2.$$

Corolary 7.24. Each positive integer can be written as a sum of four squares (Lagrange's theorem)

Proof: Use Lemma 7.19 and above theorem

Let n be any positive integer

Then let

$$n = p_1 p_2 p_3 \ldots p_m,\ p\text{'s are primes not necessarily distinct}$$

$\because$ every prime number can be expressed as a sum of four squares and the product of two integers, each of which is expressible as sum of four squares, can be expressed as sum of four squares.

Hence a positive integer can be written as a sum of our squares.

7.5 WARING'S PROBLEM

Waring's problem is that of representation of positive integers as sum of a fixed numbers s of nonnegative k^{th} power i.e. whether,

for a given k, there is any fixed $s = s(k)$ such that

$$n = x_1^k + x_2^k + \ldots + x_s^k \qquad \ldots(1)$$

is solvable for any n. In his book, *Meditations Algebraicae* (1770), Edward Waring stated without proof that every number is the sum of four squares, nine cubes, of nineteen biquadrants, and so on. This assertion has been interpreted to mean the following: Can each positive integer be written as the sum of no more than a fixed number $g(k)$ of k^{th} powers, where $g(k)$ depends only on k, not the integer being represented? This can be stated in the following way also:

For a given k, a number $g(k)$ is sought such that every $n > 0$ can be represented in at least one way as

$$n = a_1^k + a_2^k + \ldots + a_{g(k)}^k,$$

where a_i are non negative integers, not necessarily distinct.

His language implies: he believed that the answer to our question is in the affirmative that (1) is solvable for each fixed k, any positive n, and an $s = s(k)$ depending only on k. It is very improbable that Waring had any sufficient grounds for his assertion, and it was not until more than hundred years later that Hilbert first proved true.

A number represented by $s - k^{th}$ powers there is a least value of s for which it is true. This least value of s is denoted by $g(k)$

Therefore, $g(2) = 4$

$g(3) = 9$

$g(4) = 19$

....

....

There is another number in some ways still more interesting than $g(k)$. Let us suppose at to fix our ideas that $k = 3$. It is known that $g(3) = 9$ i.e., every number is represent

able by 9 or fewer cubes.

$$23 = 2^3 + 2^3 + 1^3 + 1^3 + \ldots + 1^3 = 2.2^3 + 7.1^3 \ldots 9 \text{ cubes}$$
$$24 = \ldots. \qquad < 9 \text{ cubes}$$
$$239 = 2.4^3 + 4.3^3 + 3.1^3 \ldots 9 \text{ cubes}$$

and these numbers 23 and 239 cannot be represented by 8 cubes. It is also known that only a finite number of integers (positive require so many cubes as 9. That is that all sufficiently large numbers are represented by 8 or fewer cubes and it is highly probable that 23 and 239 are the only numbers for which 9 cubes are needed. The evidence indeed indicates that only 15 other numbers of which the largest is 8042, require so many cubes as 8 and that 7 suffices for 8043 on wards.

It is playing, if this be so, that 9 is not the numbers which is really most significant in the problem. The fact, if they be facts, that just two numbers 9 cubes ants just 15 more require 8. Most fundamental and most difficult problem is that of deciding, not how many cubes are required for the representation of all numbers, but how many are required for the representation of all large numbers i.e. of all numbers with some finite numbers of exception.

The existence of $g(k)$ for each value of k was resolved in the affirmative by Hilbert in 1909; unfortunately, his proof relies on heavy machinery (including a 25-fold integral at one stage) and is in no way constructive. We define $G(k)$ as the least value of s for which it is true that all sufficiently large numbers i.e, all numbers with at most a finite number of exception are represent able by $s - k^{th}$ power. Thus $G(3) \leq 8$. On the other hand it can be seen that $G(3) \geq 4$, there are infinitely many numbers not represent able by three cubes thus $G(3)$ is 4, 5, 6, 7, or 8. It is still not known which one. But it is playing that $G(k) \leq g(k)$ and the equality holds for $k = 2$, $G(2) = g(2) = 4$.

Some known values for the first few $g(k)$ and $G(k)$ are:

$g(2) = 2$	$G(2) = 2$
$g(3) = 9$	$4 \leq G(3) \leq 7$
$g(4) = 19$	$G(4) = 16$
$g(5) = 37$	$6 \leq G(5) \leq 17$
$g(6) = 73$	$9 \leq G(6) \leq 25$
$143 \leq g(7) \leq 3806$	$8 \leq G(7) \leq 33$
$279 \leq g(8) \leq 36119$	$32 \leq G(8) \leq 43$

EXERCISES 7.1

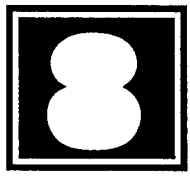
1. Find all primitive solutions of $x^2 + y^2 = z^2$ when $0 < z < 60$.
2. Find all integers $x > y > z > 0$ such that $x - y$, $y - z$, $x - z$ are all square numbers.
3. Prove that if $x^2 + y^2 = z^2$, then one of x, y is a multiple of 3 and one of x, y, z is a multiple of 5.

4. Find an integer x such that $x^2 - 60$ is a square number.
5. For what value of square integer t, $t - 5$ and $t + 5$ are both square numbers?
6. Prove that if n is any positive integer,
   $x^2 + y^2 = z^n$ always has positive integer solution.
   [**Hint:** If a, b, c be any solution of $x^2 + y^2 = z^2$ then $(a^{n-1})^2 + (bc^{n-1})^2 = (c^2)^n$]
7. For which integers n are there solutions to the equation $x^2 - y^2 = n$?
8. Prove that $x^4 + 4y^4 = z^2$ has no solutions with $xy \neq 0$
9. Prove that $x^4 - y^4 = z^2$ has no solutions with $yz \neq 0$
10. Prove that there are no positive integers a and b such that both $a^2 + b^2$ and $a^2 - b^2$ are perfect squares.
11. Establish that the equation $a^2 + b^2 + c^2 + a + b + c = 1$ has no solution in integers
    [**Hint:** The equation in question is equivalent to the equation $(2a + 1)^2 + (2b + 1)^2 + (2c + 1)^2 = 7$]
12. Verify the following:
    (i) Every positive odd integer is of the form $a^2 + b^2 + 2c^2$, where a, b, c are integers.
    [**Note:** With x, y odd, and z even, $4n + 2 = x^2 + y^2 + z^2$ and then
    $$2n + 1 = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + 2\left(\frac{z}{2}\right)^2$$
    ]
    (ii) Every positive integer is either of the form $a^2 + b^2 + c^2$ or $a^2 + b^2 + 2c^2$, where a, b, c are integers [**Note:** If $n > 0$, and cannot be written as a sum $a^2 + b^2 + c^2$, then it is of the form $4^m(8k + 7)$]
    (iii) Every positive integer is of the form $a^2 + b^2 - c^2$, where a, b, c are integers [**Note:** For $n > 0$, it is possible to choose a so that $n - a^2$ is positive odd and use that fact that a positive integer n can be represented as the difference of two squares if and only if n is not of the form $4k + 2$.]
13. Establish the following:
    (i) No integer of the form $9k + 4$ or $9k + 5$ can be the sum of three or fewer cubes.
    [**Note:** $a^3 \equiv 0, 1, 8 \pmod 9$]
    (ii) The only primes p which is represent able as the sum of two cubes is $p = 2$
    [**Note:** $a^3 + b^3 = (a + b)((a - b)^2 + ab)$.]
    (iii) Prove that a prime can be represented by the difference of two cubes if any only if it is of the form $p = 3k(k + 1) + 1$, for some k.
14. Show that for all positive integers n, the family

$$\{(x_n, y_n, z_n) \mid (x_n, y_n, z_n) = (1, 0, 1)\begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}^n\}$$ is a family of Pythagorean triples.

EXERCISES 7.2

1. Evaluate $N(n)$, $P(n)$, $Q(n)$ for $n = 100, 101, 102$ [[As Definition: 7.3.1]
2. Prove that if n is square free, $N(n) = Q(n)$
3. Prove that the number of representations of an integer $m > 1$ as a sum of two squares of positive relatively prime integers equals the number of solutions of the congruence $x^2 \equiv -1 (\text{mod } m)$
4. For a given positive integer K,
   Prove that there is an integer n such that
   (a)$N(n) = K$ if and only if $K \equiv 0(\text{mod } 4)$
   (b)$P(n) = K$ if and only if K has the form $2m$ with $m \geq 0$
   (c)$Q(n) = K$ if and only if K has the form $2m$ with $m \geq 2$.
5. Prove that if an integer n is divisible by a prime of the form $4k + 3$, then $Q(n) = 0$
6. q is a positive divisor of $a^2 + b^2$ with $(a, b) = 1$.
   Prove that q is expressible in the form $c^2 + d^2$ with $(c, d) = 1$
7. If p is a prime of the form $4k + 1$ and if $x^2 + y^2 = mp$ with $1 < m < p$, m-odd, then Show that there exist integers x_1, y_1 and M such that
   $$x_1^2 + y_1^2 = Mp \text{ with } 1 \leq M < m$$



SOME NUMBER THEORETIC PROBLEMS RELATED TO MATHEMATICS OLYMPIADS

Example 1. Compute $1^2 - 2^2 + 3^2 - 4^2 + ... - 1998^2 + 1999^2$

Solution: $1^2 - 2^2 + 3^2 - 4^2 + ... - 1998^2 + 1999^2$

$$= 1999^2 - 1998^2 ... - 4^2 + 3^2 + 2^2 + 1^2$$
$$= (1999^2 - 1998^2) + (1997^2 - 1996^2) + ... + (3^2 - 2^2) + 1^2$$
$$= 1999 + 1998 + ... + 3 + 2 + 1$$
$$= \frac{1999 \times 2000}{2} = 1{,}999{,}000.$$

Example 2. If the number $A3640548981270644B$ is divisible by 99, compute the ordered pair of digits (A, B).

Solution: $\because$ The number is divisible by 11, we have

$(A + 37) - (B + 34) = A - B + 3$ is a multiple of 11

i.e., $\therefore$ $A - B + 3$ is 0 or $\pm$ 11; ... (I)

Moreover the number is divisible by 9 also.

So, $A + B + 71$ is a multiple of 9 and so,

$A + B + 8$ is a multiple of 9. Thus $A + B = 1$ or 10 ...(II)

Thus we get from (I) and (II) the following equations

$A - B = -3$

$A - B = 8$

$A + B = 1$

$A + B = 10$

And only the valid pair is (9, 1).

Example 3. Compute the unit digit of $17^{1983} + 11^{1983} - 7^{1983}$

Solution: It is observed that the unit digits of 17^{1983} and 7^{1983} are same. And clearly the unit digit of 11^{1983} is 1

$\therefore$ the unit digit of the given number is 1.

Example 4. The sides of a right triangle are all integers. Two of these integers are primes that differ by 50. Compute the smallest possible value for the third side.

Solution: It is known that the sides form a Pythagorean triple and therefore

One of the sides must be even. Since, no such triple can contain the number 2, the given primes cannot both be legs.

Suppose the primes are p and q and the even leg is a.

$$\therefore \quad q^2 - p^2 = (q + p)(q - p) = 50(q + p)$$
$$= 50(2p + 50) = 100(p + 25)$$
$$= a^2$$

Thus, $p + 25$ must be a square; the smallest such p is 11,

So $a^2 = 100.36 = 3600$

And so $a = 60$.

Example 5. Find the smallest positive integer k such that the base 10 representations of 3^k have one hundred digits.

Solution: Suppose $N = 3^k$

Then $$k \log 3 = \log N \geq 99 \Rightarrow \geq \frac{99}{\log 3} = \frac{99}{.4771} = 207.5^+$$

$$\therefore \quad k = 208.$$

Example 6. Let $n = 1983$. Find the least positive integer k such that

$k.n^2 (n^2 - 1^2) (n^2 - 2^2) (n^2 - 3^2) .... (n^2 - (n - 1)^2) = r!$ for some integer r.

Solution: $k.n^2 (n^2 - 1^2) (n^2 - 2^2) (n^2 - 3^2) ... (n^2 - (n - 1)^2) = r!$

$$= kn(2n - 1) (2n - 2) ... (n + 2) (n + 1) n (n - 1) (n - 2) ... 2.1$$
$$= k.n. (2n - 1)!$$

Now it is seen that $k = 2$ does our job.

Example 7. A sequence of positive integers $a_1, a_2, a_3, ...$ is defined as follows:

$$a_{n+1} = a_n - S_n$$

where S_n is the sum of digits of a_n.

If $100 < a_1 < 1000$, show that the sequence must contain the number 63.

Solution: Observe that the sum of the digits of a three digit number (number lying in between 1 00 and 1000) < 30 (actually maximum is 27 = 9 + 9 + 9).

$\therefore$ [Note the sequence is of the type:

243,

$243 - (2 + 4 + 3) = 243 - 9 = 234,$

$234 - (2 + 3 + 4) = 234 - 9 = 225$

$225 - (2 + 2 + 5) = 225 - 9 = 216,$

$$216 - (2 + 1 + 6) = 216 - 9 = 207,$$
$$207 - (2 + 0 + 7) = 207 - 9 = 198,$$
$$198 - (1 + 9 + 8) = 198 - 18 = 180,$$
$$180 - (1 + 8 + 0) = 180 - 9 = 171,$$
$$171 - (1 + 7 + 1) = 171 - 9 = 162,$$
$$162 - (1 + 6 + 2) = 162 - 9 = 153,$$
$$153 - (1 + 5 + 3) = 153 - 9 = 144,$$
$$144 - (1 + 4 + 4) = 144 - 9 = 135,$$
$$135 - (1 + 3 + 5) = 135 - 9 = 126,$$
$$126 - (1 + 2 + 6) = 126 - 9 = 117,$$
$$117 - (1 + 1 + 7) = 117 - 9 = 108,$$
$$108 - (1 + 0 + 8) = 108 - 9 = 99,$$
$$99 - (9 + 9) = 99 - 18 = 81,$$
$$81 - (8 + 1) = 81 - 9 = 72,$$
$$72 - (7 + 2) = 72 - 9 = 63,$$
$$63 - (6 + 3) = 63 - 9 = 54,$$
$$54 - (5 + 4) = 54 - 9 = 45,$$
$$45 - (4 + 5) = 45 - 9 = 36,$$
$$36 - (3 + 6) = 36 - 9 = 27,$$
$$27 - (2 + 7) = 27 - 9 = 18,$$
$$18 - (1 + 8) = 18 - 9 = 9,$$
$$9 - 9 = 0]$$

$\therefore$ The sequence must eventually reach a number between 70 and 100. Also, since any number is congruent to the sum of its digits (mod 9), each member of the sequence after a1 is a multiple of 9. Thus the sequence must breach 99, 90, 81 or 72.

In any case, the sequence will shortly thereafter go to 63.

Example 8. A sequence of positive integers a_1, a_2, a_3, ... is defined as follows:

$$a_{n+1} = a_n + P_n$$

where P_n is the product of the digit of a_n.

The sequence ends if ever $a_{n+1} = a_n$.

Prove that, if $a_1 < 1000{,}000$, the sequence must end (if a_n consists of a single digit, then $P_n = a_n$).

Solution:

[Note: $a_1 = 23,$

$$a_2 = 23 + 2.3 = 23 + 6 = 29$$
$$a_3 = 29 + 2.9 = 29 + 18 = 47$$
$$a_4 = 47 + 4.7 = 47 + 28 = 75$$

$a_5 = 75 + 7.5 = 75 + 35 = 110$
$a_6 = 110 + 1.1.0 = 110 + 0 = 110$
$a_7 = a_6$
$a_8 = a_7 =$ ... etc.]

We shall prove that a term must eventually be reached that contains $a - 0$, so that all succeeding terms are identical to that one.

If (ever) 999 is reached, the next term is $999 + 9^3$

And we note: $1000 < 999 + 9^3 < 1100$ and this number jumps over from 1000 to 1100 (101 numbers)

So, the new term might not contain a zero. But if we reach 999 ... 9 (n-digits) and 9^n does not jump over the numbers from 100 ... 0 ($n + 1$ digits) to

1000 ... 0 ($n + 1$ digits), then we will certainly hit a number containing a zero as our next term. The interval contains 100 ... 0 (n digits), which is 10^{n-1} numbers. Thus, if ever $9^n < 10^{n-1}$, then the next term must contain a zero, and therefore be the maximum term of the sequence.

Example 9. Find all ordered triples (x, y, z) such that x, y, z are (positive) primes, and $x^y + 1 = z$

Solution: If y is odd, then $x^{\text{odd}} + 1$ would be divisible by $x + 1$ and would not be a prime. Thus y is even, and must be 2. Also, since z must be odd, x must be even; thus $x = 2$. Thus makes $z = 5$,
so the only answer is (2, 2, 5).

Example 10. The integers a, b, c are each greater than 20. One of them has an odd number of divisors; the other two each have three divisors. If $a + b = c$, compute the smallest possible value of c.

Solution: We note that [Student will try to prove that] only perfect square has an odd number of divisors and only the squares of primes have exactly 3 divisors. The quantities a, b, c must be r^2, p_1^2, and p_2^2 (in some order, with p_1, and p_2 primes) $a + b = c$ implies that r, p_1, p_2 must form a Pythagorean triple. Since one of these must then be even, r must be even; therefore r is a leg, so the hypotenuse is a prime. The smallest such hypotenuse is 13, so $c = 169$.

Example 11. Compute n if $(10^{12} + 25)^2 - (10^{12} - 25)^2 = 10^n$

Solution: LHS $= 4.10^{12}.25 = 2.\ 10^{12}\ .50 = 100.\ 10^{12} = 10^{14}$

And this gives $n = 14$.

Example 12. The integers x, y, z are each perfect squares, and $x > y > z > 0$. If x, y, z form an arithmetic progression, compute the smallest possible value of x.

Solution: Let $x = a^2$, $y = b^2$, $z = c^2$,

Then we have

$$c^2 - b^2 = b^2 - a^2; \text{ so } 2b^2 = a^2 + c^2.$$

Since b is at least 2, consider values of b from 2 on and find $2b^2$. The first such value that is the sum of two squares occurs when $b = 5$ ($a = 7$ and $c = 1$). Then $x = 49$.

Example 13. For each non-negative integer n we define a non-negative integer $\overline{n}$ as follows:

(a) $\overline{0} = 0, \quad \overline{1} = 2, \quad \overline{2} = 1$

(b) When n is represented in base three as

$$n = a_0 + a_1 3^1 + a_2 3^2 + \ldots + a_r 3^r, \text{ where } a_i \in \{0, 1, 2\}$$

Then $$\overline{n} = \overline{a_0} + \overline{a_1}.3^1 + \overline{a_2}.3^2 + \ldots + \overline{a_r}.3^r$$

For example, if $n = 46$ $(=1202_3)$, then $\overline{n} = 2102_3 = 65$

Thus $\overline{46} = 65$ (and $\overline{65} = 46$)

(1) If we make a table of value of n and $\overline{n}$, we see that $\overline{1} = 2$, $\overline{3} = 6$ and $\overline{4} = 8$

(a) Find the smallest n greater than 4 such that $\overline{n} = 2n$

(b) Describe any infinite set of numbers n for which $\overline{n} = 2n$, and justify your answer.

Solution: Let us consider a table of values of n and $\overline{n}$:

n	n in base 3	$\overline{n}$ in base 3	$\overline{n}$
0	0	0	0
1	1	2	2
2	2	1	1
3	10	20	6
4	11	22	8
5	12	21	7
6	20	10	3
7	21	12	5
8	22	11	4
9	100	200	18
10	101	202	20
11	102	201	19
12	110	220	24
13	111	222	26
14	112	221	25
15	120	210	21
16	121	212	23

(a) $n = 9$

(b) Powers of 3. Since they are of the form $100 \ldots 0_3$, the $\bar{n}$'s are of the form $2000 \ldots 0_3$, so $\bar{n} = 2n$. This will also hold for n's whose base 3 representation s consists only of 1's and 0's) e.g. n's of the form $3^k + 1$)

(2) Note that $\overline{1+3} = \bar{1} + \bar{3}$ and $\overline{2+3} = \bar{2} + \bar{3}$

(a) Find a pair of integers (a, b), with a and b each greater than 2, for which

$$\overline{a+b} = \bar{a} + \bar{b}.$$

(b) Describe any infinite set of pairs of integers (a, b) for which $\overline{a+b} = \bar{a} + \bar{b}$, and justify your answer.

Solution:

(a) $\overline{3+9} = \overline{12} = 24$, $\bar{3} + \bar{9} = 6 + 18 = 24$. Thus (3, 9) is an example. Other examples: (9, 3) and (6, 10).

(b) $(3^n, 1)$. Since 3^{n+1} is of the form $100 \ldots 01_3$, $\overline{3^n + 1} = 200 \ldots 02_3$, which is the same as $\overline{3^n} + \bar{1}$. More generally, we could use the set (a, b) where, when a "digit" of one is not 0(in base 3, of course), the corresponding digit (in terms of position) of the other is 0. Since any nonzero digit of $a + b$ will have to come from a or b itself, the corresponding digit of $\overline{a+b}$ will be same as that digit from $\bar{a}$ or $\bar{b}$

Thus $\overline{a+b} = \bar{a} + \bar{b}$.

For example $9 + 6 = 100_3 + 20_3$,

so $\overline{9+6} = 210_3$,

$\bar{9} + \bar{6} = 200_3 + 10_3 = 210_3$

(3) For each of the following find a number n such that

(a) $n - \bar{n} = 3$,

(b) $n - \bar{n} = -2$,

(c) $n - \bar{n} = 5$

Solution: From the table (extended) in the solution of equation (1), we find that the solutions are

(a) $n = 6$

(b) $n = 5$

(c) $n = 22$.

(4) If c is any positive integer, describe how to find an integer n for which $n - \bar{n} = c$.

Solution: We first express c in base 3: $c = a_0 + a_1 3^1 + a_2 3^2 + \ldots + a_r 3^r$

If any $a_i = 2$, replace a_i *by* -1 and add 1 to a_{i+1}. If a_{i+1} becomes 3, replace it with 0 and add 1 to a_{i+2}. Continue this way until all the digits are 0, 1 or -1. This is a new representation of c in base 3 using digits 0, 1 and -1 only. The integer n called

for in the problem will be the number in base 3 obtained by now replacing each –1 by 1 and each 1 by 2. Thus if $c = 19 = 201_3 = 1 - 101_3$.

Then n will be $2102^3 = 65$. Checking, we find that $\overline{65} = 1201_3 = 46$, and $65 - \overline{65} = 65 - 46 = 19$. Similarly, if $c = 11 = 102_3 = 11 - 1_3$, then will be $221_3 = 25$;

Thus $\quad n - \overline{n} = 25 - \overline{25} = 25 - 14 = 11.$

All this works because a 1 in c (base 3) eventually becomes a 2 in the representation of n (and a $\overline{2}$, or $\overline{1}$ in $\overline{n}$); thus, for that position $n - \overline{n} = -1$, which is the correct corresponding digit of c. Zeros remain in c, n and $\overline{n}$. Thus this formulation of n produces that called for value of c.

(5) notice that $2.\overline{2.3} = \overline{2}.\overline{3}$

(a) Find a pair of integers (a, b) with a and b each greater than 2, such that

$$2.\overline{a.b} = \overline{a}.\overline{b}$$

(b) Describe any infinite set of pairs of integers (a, b) for which $2.\overline{a.b} = \overline{a}.\overline{b}$, with $ab \neq 0$, and justify our answer.

Solution: (a) (9, 6). Note that $54 = 2000_3$, so $\overline{54} = 1000_3 = 27$. Then $\overline{9 \cdot 6} = \overline{54} = 2.27 = 54$ and also $\overline{9}.\overline{6} = 18.3 = 54$

(b) $(3^n, 6)$ or $(3^n, b)$ where b is a number whose base 3 representation has only o's and 2's for digits. Consider the base 3 representation of all numbers involved: since b has only 0's and 2's, $\overline{b}$ has only 0's, and 1's. Since 3^n is a 1 followed by n zeros, $\overline{3^n}$ is a 2 followed by n zeros. Thus $\overline{3^n}.\overline{b}$ is the same as b followed by n zeros, $\overline{3^n b}$ is $\overline{b}$ followed by n zeros, and $2.3^n b$ brings us back to b followed by n zeros.

Thus $\quad 2.\overline{3^n b} = \overline{3^n}.\overline{b}.$

(6) If either a or b is zero, then $\overline{a.b} = \overline{a}.\overline{b}$, then either a or b must be zero.

Solution: Consider the rightmost nonzero digit of a (in base 3 representation) and the rightmost nonzero digit of b, and forget about the zeros that follow.

The chart below shows the rightmost nonzero digit of various quantities:

a	b	ab	$\overline{a.b}$	$\overline{a}$	$\overline{b}$	$\overline{a}.\overline{b}$
1	1	1	2	2	2	4(becomes 1)
1	2	2	1	2	1	2
2	1	2	1	1	2	2
2	2	4(becomes 1)	2	1	1	1

Note that $\overline{a.b}$ never matches $\overline{a}.\overline{b}$. Thus $\overline{a.b} = \overline{a}.\overline{b}$, at least one of the numbers has only zeros for digits and hence is equal to zero.

Example 14. a, b and c are integers with $a \neq b$. If $(4^a + 1)(4^b + 1) = 3^c + 1$. Compute the numerical value of $a^b + b^a$

Solution: $a, b \geq 0 \Rightarrow 3^\circ + 1$ is an even integer, so $4^a + 1$ (for example) must be even, whereupon = 0. Then (noting that b may not also be 0),

$a^b + b^a = 0^b + b^0 = 1$. If a or b is negative, simple analysis will show that c must be negative and no solution is possible.

Example 15. Let x be the square of an integer. From x we subtract 1; from that result we subtract 3; from that result we subtract 5; and so on. (The quantities being subtracted continue to increase by 2). This continues until we reach a result that is the square of an integer other than zero. Compute the largest x less than 400 for which this occurs.

Solution: Let $x = c^2$. Note that $1 + 3 + 5 + = b^2$, at each stage. We want the largest c^2 less that 400 such that $c^2 - b^2 = a^2 \neq 0$. The largest $c < 20$ that is the hypotenuse of a Pythagorean triple is 17, so $x = c^2 = 289$.

Example 16. Find all positive integers $n(<17)$ for which $n!\ (n+1)! + (n+2)!$. Is an integral multiple of 49 ?

Solution: $n! + (n+1)! + (n+2)! = n![1 + (n+1) + (n+1)(n+2)]$

$= n!(n+2)^2$

Now $7^2\ (=49) \mid n!(n+2)^2 \Rightarrow 7^2 \mid n!$ or $7^2 \mid (n+2)^2$

$\Rightarrow 49 \mid n!$ or $7 \mid (n+2) \mid$

Therefore, $n = 5$, 12, 14, 15, or 16.

Example 17. How many two digit numbers have the property that when they are divide by the sum of their digits, the quotient is 7?

Solution: [Note: *A* two digit numbers cannot have 0 as its tens digit]

Let the number be $10t + u$. Then we should have

$$\frac{10t+u}{t+u} = 7. \text{ And this implies}$$

$$10t + u = 7t + 7u \Rightarrow t = 2u.$$

Thus the number are

21, 42, 63 and 48 and the answer is 4.

Note: Let N be the positive integer $A_nA_{n-1}\ldots\ldots A_2A_1$, where the A_i are digit. Thus $N = A_n10^n + A_{n-1}10^{n-1} + \ldots + A_2 10^2 + A_1.10 + A_0$, where $0 \leq A_i \leq 9$ and $A_n \neq 0$

For any integer r, we define the function

$$F(N, r) = A_0r^n + A_1r^{n-1} + \ldots + A_{n-1}.r + A_n$$

e.g. $F(253, 4) = 3.4^2 + 5.4 + 2 = 70$

$F(\underline{AB}, 5) = 5B + A$

(1) (a) Prove: If $\underline{AB}$ is a multiple of 7, so it $5B + A$ i.e. If $7 \mid \underline{AB}$, then $7 \mid F(\underline{AB}, 5)$

(b) Prove: If $7 \nmid \underline{AB}$, then $7 \nmid F(\underline{AB}, 5)$

(c) Prove: $7 \mid \underline{AB}\ \underline{C}$ if and only if $7 \mid F(\underline{AB}\ \underline{C}, 5)$

[Observation: A test for divisibility by 7 is $7 \mid N$ if and only if $7 \mid F(N, 5)$]

(d) Compute the smallest positive integer k such that, for any positive integer N, $19 \mid N$ if and only if $19 \mid F(N, k)$.

Solution:

(a) $7 + \underline{AB}$ i.e., $7 \mid 10A + B \Rightarrow 7 \mid 5\,(10A + B) \Rightarrow 7 \mid (49A + A + 5B) \Rightarrow 7 \mid (5B + A)$
$7 \mid F\,(\underline{AB}, 5)$.

(b) $7 \nmid \underline{AB} \Rightarrow 7 \nmid (10A + B) \Rightarrow 7 \nmid 5\,(10A + B)$
$7 \nmid (5B + A) \Rightarrow 7 \nmid F\,(\underline{AB}, 5)$.

(c) $7 \mid \underline{AB\,C} \Rightarrow 7 \mid 100A + 10B + C \Rightarrow 7 \mid 25\,(100A + 10B + C) \Rightarrow 7 \mid 25\,(2A + 3B + C)$
$\Rightarrow 7 \mid (50A + 75B + 25C) \Rightarrow 7 \mid (A + 5B + 25C)\ 7 \mid F\,(\underline{AB\,C}, 5)$.

Similarly the converse.

(c) The answer is 2.

In short: if $19 \mid A_n\,10^n + A_{n-1}\,10^{n-1} + \ldots + A_2 10^2 + A_1.\,10 + A_0$

Then, $19 \mid 2^n\,(A_n 10^n + A_n - 110^{n-1} + \ldots + A_2 10^2 + A_1.\,10 + A_0)$

$\Rightarrow$ $19 \mid (2^n A_0 + 2^{n-1} A_1 + 2^{n-2} A_2 + \ldots)$.

Example 18.

(a) Compute the smallest positive value of N such that $F(N, 1) = 18$ and (at the same time) $F(N, -1) = 0$

(b) Find all ordered pairs of digits (A, B) such that $19 \mid \underline{B111A111}$

(c) If N is a 3 digit number and $F(N, 5) = 67$, compute the remainder when N is divide by 7.

Solution: $F(N, 1) = A_0 + A_1 + \ldots + A_n = 18 \Rightarrow N$ is a multiple of 9;

$F(N, -1) = \pm A_0 \pm A_1 \pm A_2 \pm A_3 \pm \ldots = 0 \Rightarrow N$ is a multiple of 11; thus $N = 99$

(b) $19 \mid \underline{B111A111} \Rightarrow 19 + (2^7 + 2^6 + 2^5 + A2^4 + 2^3 + 2^2 + 2 + B2^0) \Rightarrow 19 + (238 + 16A + B) \Rightarrow B + 10 \equiv 3A \pmod{19}$

Trying values of A from 0 to 9 only leads to four pairs:

$$(0, 9), (4, 2), (5, 5), (6, 8).$$

(c) Let us consider a general solution.

Given N has $n + 1$ digits, $k \equiv 10^{p-2} \pmod{p}$ for prime $p > 5$, $Kk^n \equiv 1 \pmod{p}$ and $N \equiv G \pmod{p}$, where $0 \le G \le p$, Then considering everything (mod p):

$$K^n G \equiv K^n N \equiv F(N, k) \Rightarrow Kk^n G \equiv G \equiv K.F(N, k)$$

Thus, $N \equiv K.F(N, k) \pmod{p}$. For $n = 2$, $p = 7$, and $k = 5$

$$5^2 K \equiv 1 \pmod 7$$

$\Rightarrow$ $K \equiv 2 \pmod 7$

$\Rightarrow$ $N \equiv K.F(N, 5) \equiv 2.67 \equiv 2.4 \equiv 8 \equiv 1 \pmod 7$. The remainder is 1.

Example 19. The integer A has 198,519,851,985 digits, and is not a multiple of 3. The sum of the digits of A is B. The sum of the digits of B is C. The sum of the digits of C is D. Compute the possible values of D.

Solution: Suppose A has one 8 and the rest 9's as digits, Then the corresponding B is 1,786,678,667,864.

A smaller A can produce a B whose digital sum is larger,

The B with the greatest possible digital sum (while not being a multiple of 3) would be 999,999,999,998. The corresponding C is 107, but a further reduction in the original A could produce a reduction in B to get a C with the highest digital sum, that C is 98. This gives a maximum D of 17.

Example 20. Compute the smallest positive integer n, greater than 2, such that $2 \mid n$, $3 \mid n+1$, $4 \mid n+2$, ..., $10 \mid n+8$

Solution: Suppose $n = x + 2$. Then $2 \mid x+2$, $3 \mid x+3$, ... etc. This implies that $2 \mid x$, $3 \mid x$.. etc. The least possible x would be the least common multiple of the integers from 2 through 10, which is 2520. Thus $n = 2522$.

Example 21. If $f(n+1) = (-1)^{n+1}.n - 2f(n)$, for integral n, and $f(1) = f(1986)$, compute $f(1) + f(2) + f(3) + ... + f(1985)$

Solution:
$$f(2) = 1 - 2f(1), f(3) = -2 - 2f(2), f(4) = 3 - 2f(3), ...,$$
$$f(1985) = -1984 - 2f(1984), f(1986) = 1985 - 2f(1985).$$

Adding and replacing $f(1986)$ on the left side by $f(1)$.

We get $$\sum_{i=1}^{1985} f(i) = 1 - 2 + 3 - 4 + ... - 1984 + 1985 - 2\sum_{i=1}^{1985} f(i)$$

So, $$3\sum_{i=1}^{1985} f(i) = -\frac{1984}{2} + 1985 = 993 \text{ and } \sum_{i=1}^{1985} f(i) = 331.$$

Example 22. The smallest integer with exactly 8 divisors (including 1 and the number itself as divisors) is 24. Find the next higher with exactly 8 divisors.

Solution: The number of divisors of $N = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$, where the p_i are distinct primes, is $(\alpha_1 + 1)(\alpha_2 + 1)$. ... $(\alpha_n + 1)$. A number with 8 divisors must be one of the following forms: p^7, or p^1q^3 or $p^1q^1r^1$. The smallest N is $3^1.2^3 = 24$; the next higher is $2^1.3^1.5^1 = 30$.

Example 23. If the product $(2^{51} + 1)(2^{51} - 1)$ is expressed in base 2, compute the number of 0's in the result.

Solution: $(2^{n+1} + 1)(2^n - 1) = 2^{n+1}(2^n - 1) + (2^n - 1)$. In base 2, $2^n - 1$ is a series of n consecutive 1's; multiplying by $2^n + 1$ appends $(n + 1)$ 0's to the 1's. Now adding $2^n - 1$ to it changes the final n 0's into 1's. There will be 1 zero left in the middle.

Example 24. If $f(x)$ is defined for $x \geq 0$,
$$f(a + b) = f(a) + f(b) = 2f(ab), \text{ and } f(1) = 1$$
compute $f(1986)$.

Solution: We show that $f(\text{even}) = 0$ and $f(\text{odd}) = f(1) = 1$

And so, $f(1986) = 0$.

$[a = b = 0 \Rightarrow f(0) = 0; a = b = \Rightarrow f(2) = f(1) + f(1) - 2f(1) = 0$

(2) Assume that $f(n) = 0$, for even n such that $0 \leq n \leq 2k$ and $f(n) = f(1)$ for odd n such that $0 \leq n \leq 2k - 1$

Then $f(2k+1) = f(1) + f(2k) - 2f(2k) = f(1)$

and $f(2k+2) = f(1) + f(2k+1) - f(2k+1)$

$= f(1) + f(1) - 2f(1) = 0.$

Example 25. How many 2 digit numbers, neither of whose digits is 0, are such that the product of their digits is a square.

Solution: From 11 through 99 are 9 numbers, each with identical digits; if each digit is a square, we have 14, 41, 19, 91, 49 and 94 for 6 more numbers; finally we have 28 and 82 for 2 more numbers; total is 17.

Let the positive integer

$$N = \underline{a_n a_{n-1} a_{n-2}} \ldots \underline{a_2 a_1 a_0} \text{ where } ai \text{ are digits.}$$

Thus $N = a_n\, 10^n + a_{n-1} 10^{n-1} + \ldots + a_2 10^2 + a_1 10 + a_0$

where $0 \le a_i \le 9$ and $a_n \neq 0$.

We define the function

$$T(N) = (a_n + 1)\,(a_{n-1} + 1) \ldots (a_2 + 1)\,(a_1 + 1)\,(a_0 + 1)$$

Now

Example 26. $T(3079) = 4.1.8.10 = 320$

Also we define; $T^{-1}(X)$ = the smallest N for which $T(N) = X$

(I) (a) Find all $N < 300$ such that $T(N) = N + 1$

(b) Find all $N < 100$ such that $T(N) = N$

(c) Find all $N < 100$ such that $T(N) = N - 20$

(d) Find all $N < 100$ such that $T(N) = 7N/8$

(e) Find $T^{-1}(54)$

(f) Find $T^{-1}(720)$

(g) For what positive integers X does $T^{-1}(X)$ not exist?

(II) (a) Prove that $T(10A + B) = [T(A)][B + 1]$, where A and B are integers with $A \ge 1$ and $0 \le B \le 9$.

(b) Prove that $T(N) \le N + 1$ for all positive integer N.

III (a) Prove that for all positive integers N, $T(N) = N$ has only the solution(s) found in part I(b) above.

(b) Prove that for all positive integers N,
$T(N) = N - 20$ has only the solution(s) found in part I(c) above.

(c) We define $T(0) = 1$.
Prove that $T(0) + T(1) + T(2) + T(3) + \ldots + T(10^k - 1) = 55^k$
For all positive integer k.

Solution: The answers are

(I) (a) 1, 2, 3, 4, 5, 7, 7, 8, 9, 19, 29, 39, 49, 59, 69, 79, 89, 99, 199, 299 [it obviously works for one digit number. If $N = 10A + B$, we have $(A + 1)(B + 1) = 10A + B + 1$, leading to $B = 9$. If $N = 100A + 10B + C$, brief analysis for $A = 1$ and for $A = 2$ lead to the answers]

(c) The only solution is 18. [This cannot work for a one digit number. If $N = 10A + B$, then $(A + 1)(B + 1) = 10A + B - 20$ leads to $AB - 9A = -21$. Thus $A \mid 21$, so we need only consider $A = 1$, 3, or 7, getting the corresponding B's and checking lead to the solution]

(d) The only solution is 16. [For a one digit number, we get $N + 1 = 7N/2$, which leads to an impossibility

If $N = 10A + B$, we get $8(A + 1)(B + 1)$; Thus, $7 \mid (A + 1)$ or $(B + 1)$, leading to $A = 6$ or $B = 6$. Solving for the other variable leads to the only solution.]

(e) Searching for a two digit solution, we get two factors of 54 where one factor is as small as possible (of course, no factor may be greater than 100. This leads to 6, 9; the answer is 58.

(f) We search for three factors of 720, each number greater than 10, with one as small as possible. Clearly this factor must be greater than 7, so we use 8, 9, 10. This leads to the answer 789.

(g) $T^{-1}(1)$ does not exist. For X greater than 1, $T^{-1}(X)$ will exist so long as X can be expressed as a produced of factors, none of which is greater than 10. If X has any prime factor greater than 7, this factorization cannot be done. Thus the answer to the question is 1, and any positive integer having a prime divisor greater than 7.

II (a) If $A = \sum_{i=1}^{n} a_i .10^i$, then $T(A) = \prod_{i=0}^{n} (a_i + 1)$ $10A + B = \left[\sum_{i=1}^{n} a_i .10^{i+1} \right] + B,$

so, $$T(10A + B) = [\prod_{i=0}^{n} (a_i + 1)][B + 1] = [T(A)]\,[B + 1]$$

(b) This clearly holds for all single digit numbers. Assume it holds for all single digit numbers ≥ 1. Let N have $k + 1$ digits. Then if

$$N = 10A + B, \text{ [where } A \text{ has } k\text{-digits and } 0 \leq B \leq 9],$$
$$T(N) = [T(A)]\,[B + 1] \leq [A + 1]\,[B + 1]$$
$$= AB + A + B + 1$$
$$= [B + 1]\,A + B + 1 \leq 10A + B + 1 = N + 1.$$

By induction, therefore, the statements holds for all N.

III (a) Let $N = 10A + B$, where $A > 0$ and $0 \leq B \leq 9$

[note that for $A = 0$, $T(B) = B + 1$, not B],

$$T(10A + B] = [T(A)]\,[B + 1] = 10A + B, \text{ so}$$
$$(B + 1) \mid (10A + B) \Rightarrow (B + 1) \mid (10A + B + 1 - 1)$$
$$\Rightarrow (B + 1) \mid (10A - 1),$$

so B is even. But

$$10A + B = [T(A)]\,[B + 1] \leq [A + 1]\,[B + 1]$$
$$= AB + A + B + 1 \Rightarrow 9A \leq AB + 1,$$

so $$A(9 - B) \leq 1 \Rightarrow B = 9.$$

[Impossible, since B is even] or $A = 1$, $B = 8$. Thus 18 is the only answer.

(b) Since $T(N) > 0$, $N \geq 21$.

Let $N = 10A + B$,

where $A \geq 2$ and $0 \leq B \leq 9$. Then

$$T(10A + B) = [T(A)]\,[B + 1] = 10A + B - 20$$

$\Rightarrow$ $(B + 1) \mid (10A + B - 20)$

$\Rightarrow$ $(B + 1) \mid [10A + (B + 1) - 21]$

$\Rightarrow$ $(B + 1) \mid (10A - 21)$

$\Rightarrow$ $(B + 1) \mid [10(A - 22) - 1]$,

so $B + 1$ is odd, making B even and ≤ 9. Therefore

$$B = 0, 2, 4, 6, 8.$$

Also $[T(A)]\,[B + 1] \leq [A + 1]\,[B + 1]$,

so $10A + B - 20 \leq (A + 1)\,(B + 1) = AB + A + B + 1$

$$\Rightarrow \quad A \leq \frac{21}{9 - B}$$

Let us now consider the cases:

If $B = 0$, $A \leq 21/9 \Rightarrow A = 2$ and $N = 20$ (impossible, since $N \leq 21$]

No solution for $B = 0$.

If $B = 2$, $A \leq 21/7 = 3 \Rightarrow A = 2$ or 3,

$T(32) = 32 - 20$, but $T(22) \neq 22 - 20$.

Hence, only solution is $N = 32$.

If $B = 4$, $(B + 1) \mid [10(A - 2) - 1] \Rightarrow 5 \mid [10(A - 2) - 1]$,

which is not possible, since $5X - 1$.

If $B = 6$, $(B + 1) \mid [10(A - 2) - 2] \Rightarrow 7 \mid [10(A - 2) - 1]$

$\Rightarrow 7 \mid 3\,A \Rightarrow 7 \mid A$; then

$A \leq 21/3 \Rightarrow A = 7$. $T(76) = 76 - 20$.

Hence another solution is $N = 76$.

If $B = 8$, $(B + 1) \mid [10(A - 2) - 1] \Rightarrow 9 \mid [10(A - 2) - 1]$

$\Rightarrow 9 \mid (A - 3)$; then

$A \leq 21 \Rightarrow A = 3, 12, 21$.

$T(38) \neq 38 - 20$; $T(128) = 128 - 20$; $T(218) \neq 218 - 20$.

Thus the only solution is 32 and 76.

(c) The proof is by induction. Let us first illustrate this for $k = 1, 2, 3$. For $k = 1$,

$$T(0) + T(1) + \ldots + T(9) = 1 + 2 + \ldots + 10 = 55^1,$$

or $k = 2$,

$$\begin{aligned} &T(0) + T(1) + \ldots + T(99) \\ &= [T(0) + T(10 + T(20) + \ldots + T(99)] + [T(1) + T(11) + T(21) + \ldots + T(91) \\ &\quad + \ldots + (T(9) + T(19) + T(29) + \ldots + T(99) \text{ [using II(A)]} \\ &= [1 + T(1).\,1 + T(2).\,1 + \ldots + T(9).\,1\} + [2 + T(1).2 + T(2).2 + \ldots + T(9).\,2] \\ &\quad + \ldots + [10 + T(1).\,10 + T(2).10 + \ldots + T(9).\,10] = [1 + 2 + \ldots + 10] \end{aligned}$$

$$[T(0) + T(10 + \ldots + T(9)] = 55.55^1 = 55^2$$

For $k = 3$,

$$\begin{aligned} T(0) + T(1) + \ldots + T(999) &= [T(0) + T(10) + T(20) + \ldots + T(90) + T(100) + T(110) + \ldots + T(990)] \\ &\quad + [T(1) + T(11) + \ldots + T(991)] + \ldots + [T(9) + T(19) + \ldots + T(999) \\ &= [1 + T(1).1 + T(2).1 + \ldots + T(9).\ 1 + T(10).1 + T(11).\ 1 + \ldots + T(99).\ 1] \\ &\quad + 2 + T(1).\ 2 + \ldots + T(99).2] \ldots + [10 + T(1)\ 10 + \ldots + T999).10] \\ &= [\sum_{i=1}^{10} i]\,[\mathrm{i} \sum_{i=0}^{10^2-1} T(i)] = 55.55^2 = 55^3 \end{aligned}$$

Assume $\sum_{i=1}^{10^n-1} T(i) = 55^n$. Then

$$\begin{aligned} \sum_{i=1}^{10^{n+1}-1} T(i) &= [1 + T(1).1 + T(2).1 + \ldots + T(10^n - 1).1] + [2 + T(1).2 + \ldots \\ &\quad + T(10n - 1).2] + \ldots + [10 + T(1)\ 10 + \ldots + T(10n - 1).10] \\ &= [\sum_{i=1}^{10} i] \end{aligned}$$

$$[\sum_{i=1}^{10^n-1} T(i) = 55.55^n = 55^{n+1};$$

thus satisfying the induction hypothesis.

[**Note:** It can be shown that $[T(0)^2 + T(1)^2 + \ldots + [T(10^k - 1)]^2 = 385^k$, and in general

$$\left[\sum_{i=1}^{10^k-1} T(i)\right]^R = \sum_{i=0}^{9} \left([T(i)]^R\right)^k .$$

Thus function has many fascinating properties, including the fact that when N is written in base p (a prime) and $T(N)$ is suitably defined, then $T(N)$ is the number of terms in the N^{th} row of Pascal's triangle which are not divisible by p].

Example 27. The positive integer N has exactly 12 distinct (positive) divisors including itself and 1, but only 3 distinct prime factors. If the sum of these prime factors is 20, compute the smallest possible value of N.

Solution: If p, q and r are the prime factors, their sum is 20, so one must be even. Let $p = 2$. Then

$$(q, r) = (5, 13) \text{ or } (7, 11).$$

Let $N = 2^a.5^b.13^c$ or $2^a.7^b.11^c$

where $a \geq b \geq c$, $(a + 1)\ (b + 1)\ (c + 1) = 12$

and $a, b, c \geq 0 \Rightarrow a = 2, b = 1, c = 1$. Then

$$N = 2^2.5^1.13^1 = 260 \text{ or } N = 2^2.7^1.11^1 = 308.$$

Example 28. For all ordered pairs of positive integers (x, y), we define $f(x, y)$ as follows:

(a) $f(x, 1) = x$

(b) $f(x, y) = 0$ if $y > x$

(c) $f(x + 1, y) = y[f(x, y) + f(x, y - 1)]$

Compute $f(5, 5)$

Solution:

$$f(1,1) = 1$$

$$f(2,2) = 2\,[f(1,2) + f(1,1)]$$
$$= 2.1;$$

$$f(3,3) = 3[f(2,3) + f(2,2)]$$
$$= 3.2.1$$

and so on.

$$f(5,5) = 5! = 120.$$

Example 29. Compute the smallest positive integer N such that $\dfrac{N!}{12^{12}}$ is an integer.

Solution: It is necessary that 2^{24} and 3^{12} each divide $N!$. If $\left[\dfrac{N}{3}\right] = 8$, then

$$\left[\frac{N}{3^2}\right] = 2 \text{ and } \left[\frac{N}{3^3}\right] = 0$$

so $3^{10} \mid N!$ (not enough). If $\left[\dfrac{N}{3}\right] = 9$, then

$$\left[\frac{N}{3^2}\right] = 3 \text{ and } \left[\frac{N}{3^3}\right] = 1.$$

Therefore $\left[\dfrac{N}{3}\right] \geq 9$ and $N \geq 27$.

Now $$\left[\frac{27}{2}\right] + \left[\frac{27}{2^2}\right] + \left[\frac{27}{2^3}\right] + \left[\frac{27}{2^4}\right] = 13 + 6 + 3 + 1 = 23,$$

so $2^{23} \mid N!$ (not enough). But $N = 28$ works for both 2 and 3.

Example 30. If $a^{\frac{1}{2}} + b^{\frac{1}{2}} = 6$, compute the number of ordered pairs of positive integers (a, b) that satisfy the equation.

Solution: If the sum of two positive number is t then the first can be any one integer from 1 through $t - 1$. This gives $t - 1$ ordered pairs, so that answer is 5. For example,

$4 + 2 = 6$, so a can be 16 and b would be 4; $a^{\frac{1}{2}}$ ranges from 1 through 5.

Example 31. How many 5 digit numbers have all of the following properties?

(a) All 5 digits are different.

(b) The first digit is from 2 through 6 inclusive.

(c) The last digit is from 3 through 7 inclusive.

(d) The middle digit is odd.

Solution: Consider four cases: where the first and last digits are respectively even/odd, odd/even, odd/odd, even/even. For the first three cases: count the number of choices for the first digit, then the last digit, then the middle digit, then the remaining digits, for the last case: consider the final digit, then the first, then the middle, then the others.

Numbers of choices:

$$\underline{3}\ \underline{7}\ \underline{4}\ \underline{6}\ \underline{3} = 1512$$
$$\underline{2}\ \underline{7}\ \underline{4}\ \underline{6}\ \underline{2} = 672$$
$$\underline{2}\ \underline{7}\ \underline{3}\ \underline{6}\ \underline{2} = 504$$
$$\underline{2}\ \underline{7}\ \underline{5}\ \underline{6}\ \underline{2} = 840$$
$$\text{Total} = 3528$$

Example 32. Find the smallest 3 digit number such that both of the following are true:

(a) The number formed by any two of its digits (in either order) is a prime.

(b) The number formed by its three digits, in any order, is a prime.

Solution: Only 1, 3, 5, 9 are possible digits.

(a) If no digits are the same, they must be 1, 3, 7 (since 931 and 93 are composites), but 7 divides 371.

(b) If two digits are the same, they must be 1, 31. Then only 113 works (91 and 117 are composites) (**Note:** 131 and 311 are primes).

Example 33. The numbers x and y are positive integers with the following properties:

(a) The sum of their squares is L

(b) The sum of their cubes is K times the sum of the number themselves.

(c) $L - K = 28$.

Compute all possible ordered pairs (x, y) with $x < y$.

Solution:

$$x^2 + y^2 - \frac{x^3 + y^3}{x + y} = 28$$

$$\Rightarrow \quad x^2 + y^2 - (x^2 - xy + y^2) = 28$$

$$\Rightarrow \quad xy = 28,$$

producing (1, 28), (2, 14), (4, 7) all three pairs required.

Example 34. Compute the remainder when $3^{33^{32}}$ is divided by 7.

[**Note:** The answer must be an integer from 0 through 6]

Solution: $3 \mid 33 \Rightarrow 33^{32} = 3k$; where k is odd.

$$3^{3k} = 2^{7k} = (7a - 1)^k = 7b - 1 \qquad \text{[since } k \text{ is odd]}$$
$$= 7c + 6$$

So the remainder is 6. [The solution is shorter if "congruence" notation is used which is as follows:

$$3^3 \equiv -1 (\text{mod } 7)$$
$$\Rightarrow \quad 3^{33^{32}} \equiv 3^k$$
$$\equiv (-1)^k (\text{mod } 7)$$
$$\equiv -1 (\text{mod } 7) \qquad \text{where } k = (331, 1132) \text{ is odd}$$
$$\equiv 6 (\text{mod } 7).$$

Example 35. When represented in base k, where k is a positive integer, the number x is 29_k, and the number x^2 is 769_k. Compute k (expressing your answer as a base 10 numeral)

Solution: $7k^2 + 6k + 9 = (2k + 9)^2 \Rightarrow k = 12$.

Example 36. If the integer A is reduced by the sum of its digits, the result is B. If B is increased by the sum of its (B's) digits, the result is A. Compute the largest 3 digit number A with this property.

Solution: Since a number and the sum of its digits are "congruent Mod 9", B is a multiple of 9[that is, A-sum of its digits) must be divisible by 9]; since this means that the sum of B's digits is also a multiple of 9, then B + (sum of its digits) = A is also a multiple of 9. Now try 999[999 – 27 = 972, which does not have a digital sum of 27]; try 990[990 – 18 = 972; which also has a digital sum of 18], which works.

Example 37. [**Note:** $1^2 + 2^2 + 3^2 + ... + 1986^2 + 1987^2 = 1987.9994.1325$]

If $1.1987 + 2.1986 + ... + 1987.1 = 1987.994x$, compute the integer x.

Solution: If $S = 1.1987 + 2.1986 + ... + 1987.1$ and

$$K = 1987.1987 + 1986.1986 + ... + 1.1,$$

$$S + K = 1988(1987 + 1986 + ... + 1) = 1988 \cdot \frac{1987.1988}{2}$$

$$= 1987.994x + 1987.994.1325;$$

Simplifying both sides leads to $x + 1325 = 1988$, so $x = 663$. It can be shown that

$$(1)(n) + (2)(n - 1) + (3)(n - 2) + ... + (n)(1) = \frac{n(n+1)(n+2)}{6}.$$

Example 38. If $\frac{32}{p} + \frac{32}{q} = \frac{32}{p} \cdot \frac{32}{q}$, where p and q are primes and $3 < p < q$, compute the ordered pair (p, q).

Solution: $32(p + q) = 32.32$ implies $p + q = 32$. Trying prime values of p larger than 3 only produces $p = 13$, $q = 19$.

So the answer is (13, 19).

Example 39. Find all four ordered pairs of positive integers (x, z) such that

$$x^2 = z^2 + 120$$

Solution:

$$(x - z)(x + z) = ab$$

$$a < b \Rightarrow x = \frac{b+a}{2}, z = \frac{b-a}{2}.$$

Note that a and b must have the same parity. We have $120 = a.b = 1$.

$120 = 2 \times 60 = 3 \times 40 = 4 \times 30 = 5 \times 24 = 6 \times 20 = 8 \times 15 = 10 \times 12$, only the second fourth, sixth and eighth factorings are satisfactory. For example, 2×60 leads to $(x, z) = \left(\frac{60+2}{2}, \frac{60-2}{2}\right)$.

Answer: (31, 29), (17, 13), (13, 7), (11, 1).

Example 40. Find all four ordered pair of integers (x, z) such that $x^3 = z^3 + 721$.

Solution: $x^3 - z^3 = (x - z)(x^2 + xz + z^2)$. For integral x, z the second factor is clearly never negative. So both factors will be positive (since their product is 721) Thus we need only consider "positive" factorization:

$$(x - z)(x^2 + xz + z^2) = 1 \times 721 = 7 \times 103 = 721 \times 1 = 103 \times 7$$

Letting $x = 1 + z$ leads to $z = 15$ or -16, letting $x = 7 + z$ leads to $z = 20r - 9$; the other two factorizations lead to imaginary x and z.

Answer: (16, 15), (–15, – 16), (9, 2), (–2, –9).

Example 41. Consider the equation $x^2 + y^2 = z^2 + 18$, where x, y and z are positive integers.

(i) Prove that z must be even

(ii) There are infinite number of solutions where $z = y + 1$.

Solution: If x and y are both even or both odd, $z^2 = x^2 + y^2 - 18$ is even, so z is even. If x and y have opposite parities, let $x = 2p$, $y = 2q + 1$; then

$$z^2 = 4p^2 + 4q^2 + 1 - 18 = 4k + 3.$$

But no square can be 3 more than a multiple of 4, so this is impossible and z must be even. [note: If x and y are even, $4 \mid (x^2 + y^2)$, but $4 \nmid (x^2 + y^2 - 18)$; thus z would be even, but not divisible by 4.

This is impossible, so actually x and y both must be odd].

Example 42. In the equation $x^2 + y^2 = z^2 + 18$, where x, y and z are positive integers, prove that

(i) there are an infinite number of solutions where $z = y + 1$

(ii) there are no solutions where $z = y + 5$

Solution:

(i) $z = y + 1$

$\Rightarrow \quad x^2 = 2y + 19$

$\Rightarrow \quad y = \dfrac{x^2 - 19}{2}$.

For $y = 2k + 1$ (odd) we get

$y = 2k^2 + 2k - 9$, and then

$z = 2k^2 = 2k - 8$ for each $k > 1$.

Thus for each $k > 1$ we a solution.

(ii) $z = y + 5$

$\Rightarrow \quad x^2 = 10y + 43 = 10k + 3;$

but no square ends in a 3.

Example 43. In the equation $x^2 + y^2 = z^2 + 18$, where x, y and z are positive integers, prove that

(i) there are no solutions where x, y and z are in arithmetic progression

(ii) there are no solutions where x, y and z are in geometric progression.

Solution: (i) Suppose the numbers are $(x=)\ y - d, y, y + d(=z)$

Then $y^2 = 4dy + 18.$

Now the right side is a multiple of 2 but not a multiple of 4, so y^2 is divisible by 2 but not divisible by 4 and is not possible.

Also since x is odd and z is even, $x + z$ is odd, so $y = \dfrac{x + z}{2}$ is not integral.

(ii) Suppose the numbers are x, $\sqrt{(xz)}$, z

Then $x^2 + xz - z^2 - 18 = 0 \Rightarrow x = \dfrac{-z + \sqrt{5z^2 + 72}}{2}$.

Now $5z^2 + 72$ $[=5k + 2]$ would have to be 2 more than a multiple of 5 and this is not possible.

For a simpler solution note that odd x and even z makes y $[=\sqrt{(xz)}]$ even and is not possible.

Example 44. In the equation $x^2 + y^2 = z^2 + 18$, where x, y and z are positive integers

(i) Find a numerical solution where $x = y$

(ii) Prove that there are an infinite number of solutions where $x = y$

Solution: Suppose $x = y = 2k + 1$ and $z = 2r$. then

$$8k^2 + 8k + 2 = 4r^2 + 18 \Rightarrow 12k^2 + 2k = r^2 + 4. \text{ Let } r = 2p. \text{ Then}$$

$$k^2 + k = 2p^2 + 2 \Rightarrow \frac{k(k+1)}{2} = p^2 + 1$$

$\Rightarrow \qquad 1 + 2 + \ldots + k = p^2 + 1.$

Adding successive positive integers quickly produces $k = 4$, $p = 3$.

[leading to $x = y = 9$, $z = 12$]

Thus one solution is (9, 9, 12). [several others are indicated in the answer to the next part of the question]

(ii) Suppose $(x, z) = (u, v)$ is a specific solution to our equation $x^2 + x^2 = z^2 + 18$.

In an attempt to find other solutions, let us try some "linear combinations" of the u and v and see if it works; Let

$$x = au + bv,$$

and $$z = cu + dv,$$

where a, b, c and d are positive integers. Then we have

$$2\,(au + bv)^2 = (cu + dv)^2 + 18$$

$$\Rightarrow \qquad 2a^2u^2 + 4abuv + 2b^2v^2 = c^2u^2 + 2cduv + d^2v^2 + 18.$$

We can make the "uv" terms equal by setting $\underline{cd = 2ab}$. Then

$$2u^2.(a^2 - c^2/2) = v^2.(d^2 - 2b^2) + 18$$

Since (u, v) is a solution we have

$$2u^2 = v^2 + 18. \text{ We set } \underline{a^2 - c^2/2 = 1} \text{ and } \underline{d^2 - 2b^2 = 1}$$

Claim: The three underlined equations will lead to specific values for a, b, c, d. Now $2a^2 - c^2 = 2$ gives c is even; let $c = 2k$. Then $a^2 - 2k^2 = 1$, leading to one easy solution $a = 3$, $k = 2$ [so $c = 4$] Now the first underlined equation, using these values for a and c, gives $d = 3b/2$; substituting this into the third underlined equation leads to $b = 2$ and $d = 3$. Thus we have $x = au + bv = 3u + 2v$ and $z = cu + dv = 4u + 3v$. These produce an infinite number of positive solution, each based on a previous solution. For example, starting with $(x, z) = (u, v) = (9, 12)$ [from part IIel above] we get $(x, z) = (3u + 2v, 4u + 3v) = (51, 72)$ as a solution. This in turn leads to (297, 420) as a solution; and so on.

Example 45. The number N, when expressed in base 3, is $.11111\ldots_{(3)}$ and when expressed in base 10, N is the fraction a/b. Compute the ordered pair (a, b) where a and b are relatively prime positive integers.

Solution:

$$.11111\ldots_{(3)} = \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \ldots = \frac{\frac{1}{3}}{1 - \frac{1}{3}} = \frac{1}{2}, \text{ so } (a, b) = (1, 2).$$

Example 46. Compute the number of integers from 1 through 100 inclusive that are of the form kn^2 where k and n are positive integers and $n > 1$

Solution: From 1 through 100, there are 25 multiples of 4, 11 multiples of 9, 4 multiples of 25 and 2 multiples of 49. That totals 42 multiples of squares. But we are counting twice the 2 multiples of (4)(9) and the 1 multiple of (4)(25), so the final answer is $42 - 3 = 39$.

Example 47. If $(1 + 3 + 5 + ... + p) + (1 + 3 + 5 + ... + q) = (1 + 3 + 5 + ... + r)$, where each set of parenthesis contains the sum of consecutive odd integers as shown, Compute the smallest possible value for the sum $p + q + r$, if $p > 7$.

Solution: If the parentheses contains a, b, c addends respectively, then $a^2 + b^2 = c^2$. Note that $p > 7 \Rightarrow a > 4$; this eliminates the Pythagorean triple 3, 4, 5. The triple with the next smallest sum is in each pair of parentheses, so $(p, q, r) = (11, 15, 19)$, for a sum of 45.

Example 48. In decimal representation, the positive integer x has 11 digits and the positive integer y has k digits. The product xy is a 24-digit number. Compute the maximum possible value of k.

Solution: $10^{10} \le x \le 10^{11}$ and $10^{23} \le xy \le 10^{24}$. Minimum x implies maximum y, so $10^{23}/10^{10} \le y \le 10^{24}/10^{10} \Rightarrow 10^{13} \le y \le 10^{14} \Rightarrow k = 14$.

Example 49. Given $N = \underbrace{999...9999}_{220\ times}$. Compute the sum of the digits of N^2

Solution: $N = 10^{220} - 1$, so $N^2 = 10^{440} - 2.10^{220} + 1$

The positive terms result in a 1 followed by 439 zeros, followed by a 1. The negative term is a 2 followed by 220 zeros. Then subtraction leaves a 1 in the units position, preceded by 219 zeros, then an 8, then 219 nines. The sum of the digits of N^2 is therefore $220(9) = 1980$.

Example 50. A B and C are distinct, non zero digits. Compute the smallest three digit number ABC with the property that the mean of the numbers

$\underline{ABC}$, $\underline{ACB}$, $\underline{BCA}$, $\underline{BAC}$, $\underline{CAB}$ and $\underline{CBA}$ has 5 as its unit digit.

Solution: If $A + B + C = S$, then $6 \le S \le 24$ and $2(100S + 10S + S)$, which equals $37S$, ends in the digit 5. Therefore S ends in a 5, so $S = 15$. Letting $A = 1$, $B + C = 14$ the smallest satisfactory number is 159.

Example 51. The number N is a multiple of 7. If the base 2 representation of N is $10110101010101\,\underline{ABC}\,110$.

Compute the ordered triple of digits (A, B, C).

Solution: A number in base 10 is divisible by 9 iff the sum of its digits is divisible by 9. Similarly a number in base b is divisible by $(b - 1)$ iff the sum of its digits is divisible by $(b - 1)$. Change N to base 8[this is easily done by grouping the binary digits in blocks of three and evaluating each block, effectively producing the base 8 representation]; we get

$$N = 10/110/101/010/101/ABC/110_2 = 26525 - 6_8$$

For the sum of these digits to be divisible by 7, the missing number must be 2. In base 2, that is 010, so the answer is (010).

Example 52. Prove that the number

$$0.12345679810111213141516...$$

obtained by writing all numbers in order after the decimal point is a non-recurring non terminating decimal number.

Solution: Suppose it is recurring and it consists of m-non-recurring digits repeated again and again; so that it is of the form

$$a_1a_2a_3 \ldots a_mb_1b_2b_3 \ldots b_nb_1b_1b_2b_3 \ldots b_n \ldots$$

As we go on writing natural numbers, the number 111...1 with n 'ones' will occur and this will imply, if the period is n, that

$$b_1b_2 \ldots b_n = 11 \ldots 1$$

Similarly at some later stage, the number 222....2 with 2 occurring n-times will come and if the period is n, this would imply $b_1b_2 \ldots b_n = 22....2$

This leads to a contradiction. As such, the given number is a non-recurring non-terminating decimal number and is thus an irrational number.

Example 53. Show that the product of digits of any natural numbers containing more than two digits is less than the number itself.

Solution: Let $a_0, a_1, \ldots a_n$ be the digits of the number starting from the unit place, then the number is given by

$$N = a_0 + 10a_1 + 10^2a_2 + \ldots + 10^na_n$$

Now $a_0 < 10$, $a_1 < 10$,..., $a_{n-1} < 10$, $a_n < 10$ so that $a_0a_1a_2a_3 \ldots a_n < 10^na_n < N$

Thus the product of digits of n, is less than the number n.

Example 54. Delete 100 digits from the number 123456 ... 5960 in such a way that the remaining number is as small as possible.

Solution: The number of digits in the given number is $9 + 2.51 = 111$ After deleting 100 digits we shall get a number of 11 digits and we want it to be as small as we possible.

Starting from the left we want to retain as many zeros as possible. We retain zeros 10, 20, 30, 40, 50 so that from the first 50 numbers, we get five zeros. We have to get six more digits. From 51 we keep 1, from 52 we keep 2 from 53 we keep 3, from 54 we keep 4, from 55 we keep 5. This gives us 10 digits. The last digit we retain is the 0 of 60. Thus we get the number 00000123450.

Example 55. In how many zeros does the product of the first hundred natural numbers end?

Solution: In numbers 1 to 100, there are 50 multiples of 2, 20 multiples of 5 and 4 multiples of 25.

Thus there are 16 numbers which are multiples of 5, but not of 25. When these are multipled by 16 of the even numbers, we get one zero each time so that their product gives 16 zeros. Again there are 4 numbers which are multiples of 25. When these are multiplied by two even numbers each, we get 2 zeros each time so that we get 8 additional zeros. We can choose different even multiples in the 20 cases.

Thus the total number of zeros is 24.

Example 56. A certain natural number has 3000 one's and the rest of digits are zeros. The one's are not necessarily in the first 3000 places. Can it be a perfect square?

Solution: The sum of the digits is 3000. As such the number is divisible by 3, but it is not divisible by 9, so that it cannot be a perfect square.

Example 57. Find the greatest common divisor of

$$a. = 1111, 1111, 1111 (12 \text{ one's})$$
$$b = 1111, 1111, ..., 1111 (100 \text{ one's})$$

Solution: .
$$b = a \times 10^{88} + a \times 10^{76} + a \times 10^{64} + ... + a \times 10^4 + 1111$$
$$a = 1111 \times 10^8 + 1111 \times 10^4 + 1111$$

so that a and b are both divisible by 1111, which is the required greatest common divisor.

Example 58. Prove that there are no natural numbers which are solutions of $15x^2 - 7y^2 = 9$

Solution: Since $15x^2 - 9 = 7y^2$, y is a multiple of 3.

Let $y = 3z$, so that $5x^2 - 3 = 21y^2 \Rightarrow 5x^2 = 3 + 21y^2$, so that $5x^2$ is a multiple of 3, so that x is a multiple of 3.

Let $x = 3u$, so that

$$15u^2 - 6y^2 = 1 + y^2$$

$\therefore$ $1 + y^2$ has to be a multiple of 3. Now the number y can be written as $9a + b$, where $b < 9$.

$\therefore$ $1 + y^2 = 1 + (9a + b)^2 = (1 + b^2)$ + a multiple of 9, then $1 + b^2$ has also to be a multiple of 3, where $b = 0, 1, 2, 3, 4, 5, 6, 7, 8$, but for none of these values, $1 + b^2$ is a multiple of 3. Thus $1 + y^2$ is not a multiple of 3 for any integral values of y which is a contradiction. Hence our result follows.

Example 59. All the natural numbers are written in order starting with 1. Find the digits in the 5,00,001th place.

Solution:

(The number is of the type $\overbrace{123..91011..99100101..9991000...}^{500001}$)

There are 9 one digit numbers (1, 2,..., 9); number of digits they take = 9

90 two – digit numbers (10, 11, ... 99); number of digits they take = 180

900 three digits numbers (100,101, ... 999); number of digits they take = 2700

9000 four digit numbers (1000,1001 ... 9999); number of digits they take = 36000

90,000 five digit numbers (10000, 10001, .. 99999); number of digits they take 450,000

Thus the total number of digits required to write all numbers of 1, 2, 3, 4 and 5 digits = 9 + 180 + 2700 + 36000 + 450000 = 488889

We have to fill in 500001 – 488889 = 11112 places with 6 digit numbers.

Therefore, number of six digits numbers is $\frac{11112}{6} = 1852$. As such we require 1852 six digit numbers

Numbers with six digits begin with 100000, 100001, .. and therefore, the last number will be 101851 and so the digits in the $5,00,001^{th}$ place unity.

Example 60. Find the digits x and y so that $N = 30x0y03$ is divisible by 13.

Solution:

$$N = 3000003 + 10{,}000x + 100y = 6 + 3x - 4y + \text{a multiple of } 13$$

$\therefore$ N will be divisible by 13 if $3x - 4y + 6$ is divisible by 13

We have to try out values 0 to 9 for x and y. We get the solutions:

x :	8	2	6	0	5	9	3
y :	1	3	6	8	2	5	7

As such the solutions are

3080103, 3020313, 3060603, 3000803, 3050203, 3090503, 3030703.

Example 61. Show that the number 2178 has the property that

(i) When it is multiplied by 4, we get a number with the same digits in the reverse order.

(ii) Show that the result remains same if any number of 9's are inserted between 21 and 78.

(iii) Find more numbers with the property that when the number is multiplied by 4, we get a number with the same digits in the reverse order.

Solution: (i) It is easy to verify that $8712 = 2178.4$ so that

$$(8700 + 12) = 4.(2100 + 78)$$

(ii) Now let x 9's be inserted between 21 and 8 so that the L.H.S and R.H.S numbers are: $87\ \underbrace{99\ldots99}_{x\text{-times}}\ 12$ and $21\underbrace{99\ldots99}_{x\text{-times}}\ 78$

The insertion of x 9's increases the larger number by

$$8700.10^x - 8700 + 10^{x+2} - 10^2$$
$$= 8700\,(10^x - 1) + 10^2(10^x - 1)$$
$$= 8800.(10^x - 1)$$

Similarly insertion of x 9's increase the smaller number by

$$2100.10^x - 2100 + 10^{x+2} - 10^2$$
$$= 2100.(10^x - 1) + 100.(10^x - 1)$$
$$= 2200.(10^x - 1)$$

So that whatever be the value of x, the increase in the larger number is 4 times the increase in the smaller number; but the original larger number 8712 was 4 times the original smaller number 2178, so that the new larger number will be 4 times the new smaller number.

We thus get an infinity of number pairs, so that when the smaller number is multiplied by 4, we get a number with same digits in the reverse order.

However these are not the only number with this property.

(iii) We can get more numbers by combining these numbers, e.g.,

$$219782178217821978$$

if we multiply it y 4, we get

$$879128712871287912.$$

So that if $A_1, A_2, A_3, A_4, \ldots$ denote the smaller numbers formed in part (*ii*), we can take numbers of the type

$$A_i A_j A_k A_j A_i.$$

Example 62. Find the final digits of the millionth number of the sequence,

$$7, 77, 7^{7^7}, 7^{7^{7^7}}, \ldots$$

Solution: Suppose Nk is for the k^{th} term of the given sequence.

Then $N_k = N^7{}_{k-1}$, $N_1 = 7$

Keeping track of the final digit only, we find the final digits as:

$7^1 \to 7$, $7^2 \to 9$, $7^3 \to 3$, $7^4 \to 1$, $7^5 \to 7$, $7^6 \to 9$, $7^7 \to 3$, ... etc

Thus we get the final digit of N_1 is 7,

N_2 ... 3, Now $3^1 \to 3$, $3^2 \to 9$, $3^3 \to 7$, $3^4 \to 1$, $3^5 \to 3$, $3^6 \to 9$, $3^7 \to 7$

Thus the final digit of N_3 is 7.

Therefore, the final digit of N_4 is 3 and final digit of N_5 is 7.

In general, the final digit of N_{2k} is 3 and the final digit of N_{2k+1} is 7.

As a particular case, the final digit of $N_{100,0000}$ is 3.

Example 63. Prove that if one of the numbers $2^n - 1$, $2^n + 1$ is prime, when $n > 2$, then the other is composite.

Solution: As 2^n is not divisible by 3, when 2^n is divided by 3 the remainder would be 1 or 2. In other words 2^n is of the type $3k + 1$ or $3k - 2$, where k is an any integer.

In the first case $2^n - 1$ is divisible by 3 and in the second case $2^n + 1$ is divisible by 3. As such either $2^n - 1$ or $2^n + 1$ is a composite number. Since 3 is not a composite number, we leave out the case $n = 2$.

Example 64. Prove that 10001, 100010001, 1000100010001,

(With three zeros between two one's) are composite numbers?

Solution: Since

$$x^{k+1} - 1 = (x-1)(1 + x + \ldots + x^k)$$

We have, $10^{4k+4} - 1 = (10^4 - 1)(1 + 10^4 + \ldots + 10^{4k})$

$$10^{2k+2} - 1 = (10^2 - 1)(1 + 102 + \ldots + 10^{2k})$$

Dividing

$$(10^{2k+2} + 1)(1 + 10^2 + ... + 10^{2k}) = 101 \times (1 + 10^4 + ... + 10^{4k})$$

Since 101 is a prime number, it must divide either of the numbers

$$10^{2k+2} = 1 \text{ or } 1 + 10^2 + ... + 10^{2k}$$

And if $k > 1$, the quotient will be > 1.

This shows that when $k > 1$, $1 + 10^4 + ... + 10^{4k}$ is always a composite number.

The number 10001 is easily verified to be composite ($10001 = 73 \times 137$).

Example 65. Show that $2^{2n} - 1$ and $2^{2n-1} + 1$ are both divisible by 3, for all positive integral values of n.

Solution: Since $a^k + b^k$ is divisible by $a + b$, if k is an odd integer, we find that $2^{2n} - 1 + 1$ is divisible by $2 + 1 = 3$. Also $2^{2n} - 1 = 2.(2^{2n-1} + 1) - 3$ so that $2^{2n} - 1$ is also divisible by 3.

Example 66. Prove that no number in the sequence

$$11,111,1111,11111, ... \text{ is the square of an integer.}$$

Solution: Any number of the sequence is of the form $11 + 10m = 4(25m + 2) + 3$ and so leaves a remainder 3 after division by 4. However every square number is either the square of an even number (and so is divisible by 4) or the square of an odd number (which is of the type $4n^2 + 4n + 1$ and leaves 1 as remainder after being divided by 4) Thus no square member can be of the form $4k + 3$ and as such no member of the given sequence can be a perfect square.

Example 67. Determine all three digit numbers N having the property that N is divisible by 11, and $N/11$ is equal to the sum of the squares of the digits of N

Solution: Let $N = 100\,h + 10t + u$

The digits h, t, u are to be determined so that

$$N = 11(h^2 + t^2 + u^2) \qquad ...(*)$$

We note first that N can be written as a sum of two terms,

$$N = (99h + 11t) + (h - t + u) \qquad ...(**)$$

The first term is always divisible by 11, so N is divisible by 11 if and only if $h - t + u$ is. Since neither h, t, u exceeds 9, the combination $h - t + u$ is divisible by 11 only if it is 0 or 11.

Case I $h - t + u = 0$

Then $h + u = t$ and from (*) and (**) we get

$$(99h + 11t) + (h - t + u) = 11\,(h^2 + t^2 + u^2)$$

which gives,

$$9h + (h + u) = h^2 + (h + u)^2 + u^2$$

or

$$10h + u = 2(h^2 + uh + u^2)$$

So u must be even. We rewrite the last equation as a quadratic in h:

$$2h^2 + (2u - 10)h + 2u^2 - u = 0$$

Since h is an integer, the discriminant

$$(2u - 10)^2 - 8(2u^2 - u) = 4(25 - 8u - 3u^2)$$

must be a perfect square. But this is true only if $u = 0$[In fact $25 - 8u - 3u^2 < 0$ for $u \geq 2$]

The equation for h now reads $2h^2 - 10h = 0$

So $h = 5$, $t = h + u + 5 = 0 = 5$, and $N = 550$

Case II $h - t + u = 11$; so $t = h + u - 11$. Now relation (*), (**) yield

$$9h + (h + u - 11) + 1 = h^2 + (h + u - 11)^2 + u^2$$

or $$10h + u - 10 = 2[h^2 + uh + u^2 - 11(h + u)] = 121$$

So u must be odd. Again we rewrite the last equation in the form

$$2h^2 + (2u - 32)\, h + 2u^2 - 23u - 131 = 0$$

and require that its discriminant,

$$(2u - 32)^2 - 8(2u^2 - 23u + 132) = 4[-3u^2 + 14u - 6]$$

be a perfect square.

Since u is odd, we test 1 (which does not yield a perfect square). 3, which yields the perfect square 36, and find that all larger odd u yield a negative discriminant. If $u = 33$ our quadratic in h becomes

$$2h^2 - 26h + 80 = 0$$

or $$h^2 - 13h + 40 = (h - 5)\,(h - 8) = 0$$

when $h = 5$, $t = 5 + 3 - 11 = -3$, not admissible

when $h = 8$, $t = 8 + 3 - 11 = 0$, so $N = 803$

Thus, the only numbers satisfying the conditions of the problem are therefore 550 and 803.

Example 68. Find the smallest natural number n which has the following properties:

(a) Its decimal representation has 6 as the last digit.

(b) If the last digit 6 is erased and placed in front of the remaining digits, the resulting number is four times as large as the original number n.

Solution: Suppose the desired number has $(k + 1)$ digits, and write it in the form $10N + 6$; then the transformed number is $6.10^k + N$. The problem requires that

$$6.10^k + N = 4(10N + 6)$$

Which when simplified becomes

(1) $2.10^k - 8 = 13N$

(2) This equation tells us that the number on the left, which has digits 199....2(where there are $((k - 1)$ 9's) is divisible by 13.

(3) We divide it by 13 to determine the quotient N; $13\overline{)19999...2}$ $\quad 15384$

Thus the smallest possible value of N is 15384 and the desired number is 153846.

If there were a smaller number with the required properties, we would have found a smaller exact quotient in the above division.

We could also have determined the number $k-1$ of 9's in $13N = 199....2$ as follows:

From (1) we obtain

$$2.10^k \equiv 8(\text{mod } 13)$$
$$10^k \equiv 4(\text{mod } 13)$$
$$10^{k+1} \equiv 40 \equiv 1(\text{mod } 13)$$

The task is to find the smallest power $k+1$ such that

$10^{k+1} \equiv 1(\text{mod } 13)$. We find that

$k+1 = 6$, whence $k-1 = 4$ and $13N = 199992$.

The desired result can also be obtained by successive multiplication since the original number ends in 6. The new number ends in 4, the old number must have ended in 46. Now successive multiplication gives in succession, the remaining digits of the original number.

The process as follows":

Original number	New number
.....6 × 4	= 6.....4
....46 × 4	= 6.....84
.....846 × 4	= 6.....384
.....3846 × 4	= 6.....5384
.....53846 × 4	= 6.....15384
.....153846 × 4	= 615384.

Example 69. Find all positive integers n for which $(2^n - 1)$ is divisible by 7.

Solution: We note

$2^1 \equiv 2(\text{mod } 7)$ and so,

$2^2 \equiv 4(\text{mod } 7) \Rightarrow 2^3 \equiv 1(\text{mod } 7)$ for any natural number k we have

$2^{3k} \equiv (2^3)^k \equiv 1^k \equiv 1(\text{mod } 7)$. Thus $2^{3k} - 1 \equiv 0(\text{mod } 7)$

So it is clear that if the number n is a multiple of 3 then the result is true.

Now the case arises if n is of the form $3k+1$ or $3k+2$

$$2^{3k} \equiv 1(\text{mod } 7) \Rightarrow$$

(i) $$2^{3k+1} \equiv 2.23k(\text{mod } 7) \Rightarrow 2^{3k+1} \equiv 2(\text{mod } 7)$$
$$2^{3k+2} \equiv 4.2^{3k} \equiv 4(\text{mod } 7)$$

from which it follows that multiples of 3 are the only exponents n such that $2^n - 1$ is divisible by 7.

Example 70. Prove that there is no positive integer n for which $2^n + 1$ is divisible by 7.

Solution: As above,

$$2^{3k} \equiv 1(\text{mod } 7) \Rightarrow 2^{3k+1} + 1 \equiv 3(\text{mod } 7),\ 2^{3k+2} + 1 \equiv 5(\text{mod } 7),$$

Moreover, $2^{3k} + 1 \equiv 2(\text{mod } 7)$

Thus $2^n + 1$ leaves a remainder of 2, 3 or 5 when divided by 7, and hence is not divisible by 7.

Example 71. k, m, n are natural numbers such that $m + n + k$ is a prime number greater than $n + 1$. Let $C_s = s(s + 1)$.

Prove that the product $(C_{m+1} - C_k)(C_{m+2} - C_k) \ldots (C_{m+n} - C_k)$ is divisible by the product $C_1 C_2 \ldots C_n$ respectively

Solution: By definition of C_s, we have

$$C_a - C_b = a(a + 1) - b(b + 1) = a^2 - b^2 + a - b = (a - b)(a + b + 1)$$

Hence, the factors of the first product are

$$C_{m+1} - C_k = (m + 1 - k)(m + k + 2)$$
$$C_{m+2} - C_k = (m + 2 - k)(m + k + 1)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$C_{m+n} - C_k = (m + n - k)(m + k + n + 1)$$

Their product is

$$[(m-k+1)(m-k+2) \ldots (m-k+n)]\,[(m+k+2)(m+k+3) \ldots (m+k+n+1)]$$

Which we write as $A.B$, where A is a product of n consecutive integers starting with $m - k + 1$, and B is a product of n consecutive integers starting with $m + k + 2$. Now the factors in the product $C_1 C_2 \ldots C_n$ are

$$C_1 = 1.2,\ C_2 = 2.3,\ \ldots,\ C_n = n(n + 1)$$

And their product is $n!(n + 1)!$

We shall solve the problem by showing that A is divisible by $n!$, and B is divisible by $(n + 1)!$

We know that the product of any n-consecutive integers is divisible by $n!$ And so it follows at once that A is divisible by $n!$ It also follows that the product $(m + k + 1)$ B of $(n + 1)$ consecutive is divisible by $(n + 1)!$ But we are told that $(m + k + 1)$ is a prime greater than $(n + 1)$, so it is relatively prime to $(n + 1)!$ Hence B is divisible by $(n + 1)!$ as was to be shown.

Example 72. Find all natural numbers x such that the product of their digits (in decimal notation) is equal to $x^2 - 10x - 22$.

Solution: Suppose the number x has n digits.

Then $$x = a_0 + a_1 10 + a_2 10^2 + \ldots + a_{n-1} 10^{n-1},\ a_i \le 9$$

Let $$P(x) = a_0 . a_1 . a_2 \ldots a_{n-1} = x^2 - 10x - 22.$$

But $$P(x) = (a_0 . a_1 . a_2 \ldots a_{n-2})\, a_{n-1}$$
$$\le 9^{n-1} a_{n-1} < 10^{n-1} a_{n-1} \le x$$

So $$x^2 - 10x - 22 < x, \text{ i.e., } x^2 - 11x < 22$$

Now, $$x^2 - 11x + 121/4 = (x - 11/2)^2 < 22 + 121/4 = 209/4$$

So $$x - 11/2 < \sqrt{209}/2 < 15/2.$$

It follows that $x < 13$. That is, x is either has one digit, or $x = 10$, 11 or 12.

If x has one digit, then

$$x = a_0,$$

and $$P(x) = a_0 = x = x^2 - 10x - 22, \text{ so } x^2 - 11x - 22 \Rightarrow 0.$$

But this equation has no integral solutions. If x has two digits, we can easily test all three possibilities:

(i) If $x = 10$, $P(x) = 0$, $x^2 - 10x - 22 = -22 \neq 0$, so the given condition is not met.

(ii) If $x = 11$, $P(x) = 1$, $x^2 - 10x - 22 = -11 \neq 1$, and again the given condition is violated.

(iii) If $x = 12$, $P(x) = 2$, $x^2 - 10x - 22 = 2$, so $x = 12$ is the only solution.

Instead of testing the three conditions, we could have found all two digit solutions by setting $x = a_0 + 10$.

Then $$x^2 - 10x - 22 = a_0^2 + 20a_0 + 100 - 10a_0 - 100 - 22$$
$$= P(x) = a_0$$

Hence $$a_0^2 + 9a_0 - 22 = (a_0 + 11)(a_0 - 2) = 0$$

Which implies that $$a_0 = 2 \text{ i.e., } x = 12.$$

Example 73. Prove that there are infinite many natural numbers 'a' with the property that: the number $z = n^4 + a$ is not prime for any natural number n.

Solution: We look for natural numbers 'a' of a form that allows us to factor $n^4 + a$. We claim that $a = 4k^4$, $k = 2, 3, \ldots$, has this property; for adding and subtracting $4n^2k^2$ enables us to write $n^4 + a$ as a difference of two squares, and this can always be factored. Thus

$$z = n^4 + 4k^4 = n^4 + 4n^2k^2 + 4k^4 - 4n^2k^2$$
$$= (n^2 + 2k^2)^2 - (2nk)^2$$
$$= (n^2 + 2k^2 + 2nk)(n^2 + 2k^2 - 2nk)$$

It remains to show that for all $n \geq 1$, both factors exceeds 1 if $k \geq 2$. Observe that $n^2 + 2k^2 + 2nk \geq n^2 + 2k^2 - 2nk = (n - k)^2 + k^2 \geq k^2 \geq 4$. We conclude that each factor in the expression for z is, in fact, at least 4 for infinitely many k, hence for infinitely many $a = 4k^4$, and so z has the required property.

Example 74. Find the set of all positive integers n with the property that the set $\{n, n + 1, n + 2, n + 3, n + 4, n + 5\}$ can be partitioned into two sets such that the product of the numbers in one set equals the product of the numbers in the other set.

Solution: Let $S = \{n, n + 1, n + 2, n + 3, n + 4, n + 5\} = S_1 \cup S_2$

Such that $S_1 \cap S_2 = \phi$ with $\prod_{s \in S_1} s = \prod_{s \in S_2} s$

So (a prime) $p \mid s$ for some $s \in S_1$ then the $p \mid t$ for some $t \in S_2$. However, if $p \mid a, b$ where $a, b \in S$ then $\mid a - b \mid = pk \leq 5$, so the only candidates for p are 2, 3, 5. A set of six consecutive integers contains at least one divisible by 5, and by the above argument, 5 must contain two such elements; these must be n and $n + 5$. The remaining elements $n + 1$, $n + 2$, $n + 3$ and $n + 4$ can have only 2 and 3 as prime factors, so that they are of the form $2^{\alpha}3^{\beta}$. Two of them are odd and two of them are even, so the odd ones are

of the form 3^{γ} and 3^{δ} where $\gamma, \delta > 0$. But they are consecutive odd numbers, so their difference is only 2, while the closest powers $3^{\beta} > 1$ has a difference of 2. Thus we see that there is no integers n with the prescribed property.

Example 75. Prove that the set of integers of the form $2^k - 3$ ($k = 2, 3, ...$) contains an infinite subset in which every two members are relatively prime.

Solution: Suppose we have n relatively prime members

$$a_1 = 2^{k1} - 3$$
$$a_2 = 2^{k2} - 3, ..., a_n = 2^{kn} - 3$$

Let $S = (2^{k1} - 3)(2^{k2} - 3) ... (2^{kn} - 3)$ and this being a product of odd numbers this is also odd.

Now among the numbers

$$2^0, 2^1, 2^2, ..., 2^S$$

we have at least two, say, 2^{α} and 2^{β} where $2^{\alpha} \equiv 2^{\beta} (\text{mod } S)$ or, $2^{\beta}(2^{\alpha} - \beta - 1) = mS$, m an integer

The odd number S does not divide 2^{β}, so it must divide $2^{\alpha - \beta} - 1$;

Hence $2^{\alpha - \beta} - 1 = 1s$, 1 an integer

Since $2^{\alpha - \beta} - 1$ is divisible by S, and since s is odd, $2^{\alpha - \beta} - 3$ is relatively prime to S. Therefore it can be adjoined as a new member to the desired set. Repeated application of this construction leads to an infinite subset of relatively prime integers.

Example 76. Prove that from a set of ten distinct two digit numbers (in the decimal system) it is possible to select two disjoint subsets whose members have the same sum.

Solution: Suppose $S = \{a_1, a_2, ..., a_{10}\}$ Now the number of subsets of S is $2^{10} = 1024$.

Again for any $a \in S \Rightarrow a \leq 99$. Hence the sum of the numbers in any subset of S is $\leq 10.99 = 990$. So the pigeon –hole principle, gives that at least two different subsets say, S_1 and S_2 must have the same sum. If S_1 and S_2 are disjoint, the problem is solved. If not, we remove all elements common to S_1 and S_2 from both, obtaining non-intersecting subsets S_1' and S_2' of S. The sum of the numbers in S_1' is equal to the sum of the numbers in S_2'.

Example 77. Prove that for any non-negative integers m and n the number $\dfrac{(2m)!(2n)!}{m!n!(m+n)!}$ is an integer.

Solution: We write $f(m, n) = \dfrac{(2m)!(2n)!}{m!n!(m+n)!}$ and note that $f(m, 0) = \binom{2m}{m}$ which is an integer for all m.

Also we note that

$$f(m, n) = 4f(m, n-1) - f(m+1, n-1)$$

Now it is easy to prove the result by induction.

Example 78. When $(4444)^{4444}$ is written in decimal notation, the sum of its digits is A. Let B be the sum of the digits of A. Find the sum of the digits of B (A and B are written in decimal notation)

Solution: We know that every integer written in decimal notation is congruent to the sum of its digits modulo 9.

Suppose $N = d_1 + 10d_2 + 10^2d_3 + ... + 10^kd_{k+1}$. Then

$$N = d_1 + d_2 + 9d_3 + d_3 + 99d_3 + ... + d_{k+1} + (10^k - 1)d_{k+1}$$
$$\equiv d_1 + d_2 + d_3 + ... + d_{k+1} (\text{mod } 9)$$

Since 9 is a divisor of every number of the form $(10^m - 1)$

We write $X = (4444)^{4444}$

Then we see that

$$4444 \equiv 16 \equiv 7(\text{mod } 9), \text{ hence } 4444^3 \equiv 7^3 \equiv 1(\text{mod } 9)$$

And since $4444 = 3(1481) + 1$

$$X = 4444^{4444} = 4444^{3(1481)}.4444 \equiv 1.7 \equiv 7(\text{mod } 9)$$

Thus $x \equiv A \equiv B \equiv$ sum of the digits of $B \equiv 7(\text{mod } 9)$

On the other hand, if $\log x$ is the common logarithm of x, then

$$\log x = 4444 \log 4444 < 4444 \log 10^4$$
$$= 4444.4 \text{ i.e., } \log x < 17776$$

Therefore x has at most 177776 digits, and even if all of them were 9, the sum of the digits of x would be

$$9.1776 = 159984$$

Therefore $A \leq 159984$

Among all natural numbers less than or equal to 159984, the one whose sum of digits is a maximum is 99999. It follows that $B \leq 45$; and among all natural numbers less than or equal to 45,39 has the largest sum of digits, namely 12. So the sum of the digits of B is at most 12. But the only natural numbers no exceeding 12 and congruent o 7 mod 9 is 7. Thus 7 is the solution to the problem.

Example 79. a and b are positive integers. When $a^2 + b^2$ is divided by $a + b$, the quotient is q and the remainder is r. Find all pairs (a, b) such that $q^2 + r = 1977$

Solution: As given

$$a^2 + b^2 = q(a + b) + r \quad ...(1)$$

with $0 \leq r < a + b$

And $$q^2 + r = 1977 \quad ...(2)$$

These imply

$$q^2 \leq 1977 = q^2 + r < q^2 + a + b \quad ...(3)$$

and $$a^2 + b^2 < (q + 1)(a + b) \quad ...(4)$$

Since, $2ab \leq a^2 + b^2$, (4) also implies that

$$2ab < (q + 1)(a + b) \quad ...(5)$$

Adding (4) and (5), we get

$$(a + b)^2 < 2(q + 1)(a + b)$$

and this gives

$$a + b < 2(q + 1) = 2q + 2$$

and we get

$$a + b \leq 2q + 1$$

Replacing $a + b$ in (3) by $2q + 1$ yields

$$q^2 \leq 1977 \leq q^2 + 2q + 1 = (q + 1)^2$$

The only integer q satisfying these inequalities is $q = 44$, because

$$44^2 = 1936 \text{ and } 45^2 = 2025$$

Thus $q = 44$ and so $r = 41$ from (2) above substituting these values into the (1), we get

$$a^2 + b^2 = 44a + 44b + 41$$

or $$(a - 22)^2 + (b - 22)^2 = 1009$$

By listing all squares up to 505 and their difference from 1009 (remembering that a square ends in 0, 1, 4, 9, 6, 5), we find that the only representation of 1009 as sum two squares is

$$(15)^2 + (28)^2 = 1009$$

Therefore the sets $\{|a - 22|, |b - 22|\}$ and $\{15, 28\}$ must be the same. We conclude that

$$(a, b) = (50, 37), (37, 50), (50, 7) \text{ or } (7, 50).$$

ANSWERS

EXERCISES 1.2

5. $d = 9$, $m = 22$, $n = -15$

6. (a) $m = -11$, $n = 9$;

(b) $m = 31$, $n = 44$;

(c) $m = 7$, $n = 8$

7. (i) 9, (ii) 11

13. (i) F, $a = 2$, $b = 5$;

(ii) T

(iii) T

(iv) F, $p = 3$, $a = 3$, $b = 2$

19. (a) 77, (b) 1, (c) 7 (d) 1

20. $g = 17$, $x = 71$, $y = -36$

21. (a) $x = 9$, $y = -11$

(b) $x = 31$, $y = 44$

(c) $x = 3$, $y = -2$

(d) $x = 7$, $y = 8$

(e) $x = 1$, $y = 1$, $z = -1$

35. $(1, n(n + 1))$

40. $<a, b>$

42. 200,340

43. $2^r - r - 1$

EXERCISES 1.3

1. $(5554)_7, (2112)_{10}$

3. $(175)_{10}, (1111100111)_2$

6. $(10010110110)_2$

8. $(10110001101)_2$

16. $(B705736)_{16}$

EXERCISES 1.4

3. (a) $2^8.3^5.11^3$;

(b) $2^2.3^3.5^2.7^3.11^2.17.23.37$

8. p, p^2; p, p^2, p^3; p^2, p^3

9. p^3, p

EXERCISES 2.4

1. (i) $x = -3 + 7t$
$y = 5 - 8t$;
(ii) $x = 4 - 9t_1 - 10t_2$
$y = 2 - 4t_1 - 5t_2$
$z = 2 - t_2$
(iii) $x = -18 - 54c + 21b + 5a$
$y = 6 + 18c - 7b - 2a$
$z = 1 + 3c - b$, $t = 3 - c$

2. $y = 2 + t$,
$z = 1 + 2t$,
$x = 3 - 8t$

3. 22 integers which all contain 2 digits and form an arithmetic progression whose sum is 1210

4.

Cock	0	4	8	12
Hen	25	18	11	4
Chicken	75	78	81	84

5. 156

6. 1, 5; 2, 1

7. 11, 31, 51, 71, 91

8. 2, 3, 5

EXERCISES 2.5

A. **1.** no, **2.** no, **3.** 5 **4.** 5 **5.** 1

B. **1.** 81 **2.** 200, 751, 1302, 1853, 2404 **3.** 42

EXERCISES 2.7

1. 58(mod 60) **2.** 23, 128

EXERCISES 2.8

1. 106(mod 105) **2.** 33(mod 84) **3.** 27(mod 140)

EXERCISES 2.9

1. $x \equiv 6$, 103 and 194
2. $x \equiv 74$, 153 mod 158
3. no solution
4. $x \equiv 6$, 14, 22 mod 24

EXERCISES 2.10

1. $x \equiv 31 (\text{mod } 77)$
3. $x \equiv 619 (\text{mod } 1092)$
9. $x \equiv 31 (\text{mod } 60$

EXERCISES 2.11

1. There are three solutions mod (24, 26)
2. 23
3. No solution
4. All integers congruent to 7 modulom 13
5. All integers congruent to 4 modulo 7

EXERCISES 3.1

1. (i) $x \equiv 0, 1, \pm 2 (\text{mod } 5)$;
   (ii) $x \equiv 1, -2, \pm 3, (\text{mod } 7)$,
   (iii) $x \equiv \pm 2, \pm 18 (\text{mod } 41)$
4. (i) $22 (\text{mod } 27)$,
   (ii) no,
   (iii) $1, 7 (\text{mod } 25)$,
   (iv) $2, 5, 11, 17, 20, 26 (\text{mod } 30)$,
   (v) $1, 4, 11, 14 (\text{mod } 15)$,
   (vi) $93 (\text{mod } 125)$
5. (i) $x \equiv -1 (\text{mod } 5)$,
   (ii) $x \equiv -3, -4 (\text{mod } 11)$,
   (iii) none.
6. (i) $x^4 - 3\text{Ix} + 1 \equiv (x + 1)(x^3 - x^2 + x + 1) (\text{mod } 5)$,
   (ii) $x^5 + 3x^3 - x + 2 \equiv (x + 3)(x + 4)(x^3 + 4x^2 + 2) (\text{mod } 11)$
7. (i) $x \equiv 1, 2, 6 (\text{mod } 9)$
   (ii) $x \equiv 1, 3 (\text{mod } 5)$
   (iii) $x \equiv 1, 6, 11, 28, 33, 38 (\text{mod } 45)$
   (iv) No solution

EXERCISES 3.2

2. 5, 7, 10, 11, 14, 15, 17, 19, 20, 21;
5, 11, 23, 29, 41, 47;

4. (i) 33 mod 7
(ii) 59, 11, 39 mod 109
(iii) no solution

5. 4.

7. $p - 1$, 0.

EXERCISES 4.1

27. [6, 28, 496, 81828, 33550336, 8589869056

28. [12, 18, 20, 24, 30, 36]

EXERCISE 5.2

1. [2, 1, 4], [–3, 2, 12], [0, 1, 1, 100]

2. [17/3, 3/17, 8/1]

6. $\frac{3+\sqrt{5}}{2}, \frac{22-\sqrt{5}}{10}$

7. (i) $[1 + \sqrt{2}$

(ii) $\frac{1+\sqrt{3}}{2}$

(iii) $1 + \sqrt{3}$

(iv) $3 - \sqrt{3}$

9. (i) $13/1 - [3,1,3,4]$, $n = 4$, $x_0 = q_3 = 4$, $y_0 = p_3 = 3$, $x = x_0 + tb = 4 + 17t$, $y = y_0 + ta = 3 + 13t$

(ii) $65/56 = [1,6,4,2] = n = 4$, $x_0 = q_3 = 25$, $y_0 = p_3 = 29$, $x = 25 + 56t$, $y = 29 + 65t$

(iii) $56/65 = [0, 1, 6, 4, 1, 1]$, $n = 6$, $x_0 = q_5 = 36$, $y_0 = p_5 = 31$, $x = 36 + 65t$, $y = 31 + 56t$

(iv) $13/17 = [0, 1, 3, 3, 1]$, $n = 5$, $x_0 = q_4 = 13$, $y_0 = p_4 = 10$,
$x = x0 + tb + 13 + 17t$,
$y = y0 + ta = 10 + 13t$

(v) $65/56 = [1, 6, 4, 1, 1]$, $n = 5$,
$x_0 = q_4 = 31$, $y_0 = p_4 = 36$,
$x = 31 + 56t$,
$y = 36 + 65t$

(vi) $x_0 = 4, y_0 = 3, c = 5,$
$x = cx_0 + bt = 20 + 17t,$
$y = cy_0 + at = 15 + 13t$

(vii) $x_0 = 29, y_0 = 25,$ is a particular solution of $56x - 65y = -1, c = 3,$
$x = cx_0 + bt = 87 + 65t,$
$y = cy_0 + at = 75 + 56t$

10. (i) $x = 117 - 58t, y = 61t - 123,$

(ii) $x = 65 + 49t, y = 123 + 61t$

(iii) $x = 117 + 58t, y = 123 + 61t$

(iv) Unsolvable

(v) $x = 65 - 49t, y = 34t - 45$

(vi) No integral solution

EXERCISES 5.3

11. (a) 55, (b) 610, (c), 6765, (d) 233, (e) 2584, (f) 75025

13. $\sum_{j=1}^{n} f_{2j-1} = f_1 + f_3 + \ldots + f_{2n-1} = f_{2n}$

21. 577,136

22. 19, 6

EXERCISES 6.1

3. $x \equiv \pm 1 (\text{mod } 11), x \equiv \pm 5 (\text{mod } 11), x \equiv \pm 2 (\text{mod } 11), x \equiv \pm 4 (\text{mod } 11), x \equiv \pm 3 (\text{mod } 11);$
$x \equiv \pm 1 (\text{mod } 11^2), x \equiv \pm 27 (\text{mod } 11^2), x \equiv \pm 2 (\text{mod } 11^2),$
$x \equiv \pm 48 (\text{mod } 11^2), x \equiv \pm 3 (\text{mod } 11^2).$

4. Non-residue.

6. $p = 4m + 3$

11. $x \equiv 9, 10 (\text{mod } 19)]$

12. $x \equiv 13, 6 (\text{mod } 19)].$

15. (i) 2, 5 (ii) 6, 1 (iii) 4, 7

16. yes

19. (i) yes, (ii) no, (ii) no (iii) no,
(iv) yes

22. (i) 1 (ii) -1 (iii) 1

EXERCISES 7.1

(1) 3, 4, 5; 15,8,17; 35,12,37; 5,12,13; 21,20,29; 45,28,53; 7,24,25; 9,40,41

(2) for given values of $\sqrt{x-y}$ and $\sqrt{y-z}$ we ca find the values of x, y, z.

(1) $x = 8$

(2) Such t does not exist

(7) $N \equiv 0, 1, 3 \pmod 4$

EXERCISES 7.2

[12,0,0]; [8,2,8]; [0,0,0]

❑❑❑