NUMBER THEORY

SUBMITTED BY

STEBIN.A.S

Reg No. 170021032436

KISHORE.M

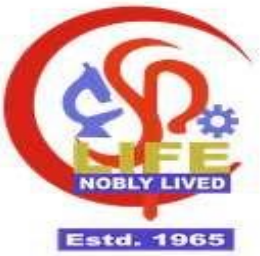
Reg No. 170021032417

GREEN MARY.K.J

Reg No. 170021032412

IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE
BACHELOR DEGREE OF SCIENCE IN MATHEMATICS

2017-2020



ST. PAUL'S COLLEGE, KALAMASSERY
(AFFILIATED TO M.G.UNIVERSITY, KOTTAYAM)

CERTIFICATE

This is to certify that the project report title "NUMBER THEORY" submitted by STEBIN.A.S(Reg No.170021032436), KISHORE.M(Reg No.170021032417), GREEN MARY.K.J(Reg No.170021032412)towards partial fulfilment of the requirements for the award of degree of Bachelor of Science in Mathematics is a bonafide work carried out by them during the academic year 2017-2020

Project Supervisor

Mr. ARAVIND KRISHNAN.R

Department of Mathematics

Head of the Department

Dr.SAVITHA. K.S

Assistant Professor

Department of Mathematics

DECLARATION

We, STEBIN.A.S, KISHORE.M, GREEN MARY.K.J hereby declare that this project entitled "NUMBER THEORY" is an original work done by us under the supervision and guidance of Mr. ARAVIND KRISHNAN R , Department of Mathematics, St. Paul's college Kalamassery in partial fulfilment for the award of The Degree of Bachelor of Science in Mathematics under Mahatma Gandhi University. I further declare that this project is not partly or wholly submitted for any other purpose and the data included in the project is collected from various sources and are true to the best of my knowledge.

STEBIN.A.S

Place: KALAMASSERY KISHORE.M

GREEN MARY.K.J

ACKNOWLEDGEMENT

We express our heartfelt gratitude to our project supervisor Mr. ARAVIND KRISHNAN R, Department of Mathematics, for providing us necessary stimulus for the preparation of this project.

We would like to acknowledge our deep sense of gratitude to Dr.SAVITHA. K.S, Head of the Department of Mathematics and all other teachers of the department and classmates for their help at all stages.

We also express our sincere gratitude to Ms.VALENTINE D'CRUZ, Principal of St. Paul's College, Kalamassery for the support and inspiration rendered to us in this project.

CONTENTS

Chapter 1: Introduction and Prleminaries	6
Chapter 2: The Theory of Congruences	10
Chapter 3: Number Theoretic functions	22
Chapter 4: Some Applications of Number Theory	33
Conclusion	39
References	40

CHAPTER-1
INTRODUCTION AND PRELIMINARIES

1.1 INTRODUCTION

The Theory of numbers is one of the oldest branches of mathematics; an enthusiast, by stretching a point here and there, could extend its roots back to surprisingly remote date. Although it seems probable that the Greeks were largely indebted to the Babylonians and ancient Egyptians for a core of information about the properties of the natural numbers, the rudiments of an actual theory are generally credited to Pythagoras and his disciples.

Another approach to divisibility question is through the arithmetic of remainders, or the theory of congruence's as it's now commonly known. The concept and the notation that makesit such a powerful tool, was first introduced by the German mathematician *Carl Friedrich Gauss*(1777-1855)in his 'Disquisitions Arithmetical', this monumental work, which appeared in 1801 when Gauss was 24 year old, laid the foundations of modern number theory. "It's really astonishing", said Kronecker, "to think that a single man of such young years was able to bring to light such a wealth of results, and above all to present such a profound and well-organized treatment of an entirely new discipline".

Gauss was the last complete mathematician, and it is no exaggeration to say that he was in some degree connected with nearly every aspect of the subject. His contemporaries regarded him as Princeps Mathematicorum(Prince of Mathematics), on a par with Archimedes and Isaac Newton.

Although Gauss adrned every branch of Mathematics, he always held Number Theory in high esteem and affection. He insisted that, "Mathematics is the Queen of the science, and the theory of numbers is the Queen of Mathematics".

1.2 PRELIMINARIES

1.2.1 Basic Properties of Congruence

In the chapter of Disquisitione Arithmetical, Gauss introduces the concept of congruence and the notation that makes it such a powerful technique [He explains that he was induced to adopt the symbol '≡' because of the analogue with algebraic equality]. According to Gauss, "If a number 'n' measures the differences between two numbers 'a' and 'b', then 'a' and 'b' are said to be congruent with respect to n; If not, incongruent". Putting this into the form of a definition.

Definition 1.1

Let n be a fixed positive integer. Two integers 'a' and 'b' are said to be congruent modulo n, symbolized by,

$$a \equiv b \ (mod\ n)$$

If n divides the difference a-b; that is, provided that, $a - b = kn$ for some integer k.

For example, consider n=7, it's routine to check that $3 \equiv 24(mod\ 7)$

$$-31 \equiv 11(mod\ 7)$$

$$-15 \equiv -64(mod\ 7)$$

Because $3 - 24 = (-3)7$, $-31 - 11 = (-6)7$ and $-15 - (-64) = 7 \times 7$

When $n \nmid (a - b)$, we say that a is incongruent to b modulo n, and in this case we write $a \not\equiv b \ (mod\ n)$. for example, $25 \not\equiv 12(mod\ 7)$, because 7 fails to divide $25 - 12 = 13$.

It's to be noted that any two integers are congruent modulo 1, whereas two integers are congruent modulo 2 when they are both even or both odd.

Given an integer a, let q and r be its quotient and remainder upon division by n, so that

$$A = qn + r \text{ since } 0 \leq r \leq n$$

that is; $a - r = qn$

Then by definition of congruence, $a \equiv r(mod\ n)$. Because, there are n choices for r, we see that every integer is congruent modulo n to exactly one of the values

0,1,2,……n-1; In particular, $a \equiv 0(mod\ n)$ if and only if $n \mid a$. The set of n integers 0,1,2,….n-1 is called the set of least non-negative resides modulo n.

Theorem-1.1

For arbitrary integers a and b, $a \equiv b(mod\ n)$ if and only if a and b leave the same non-negative remainder when divided by n.

Proof: First we take $a \equiv b(mod\ n)$ so that $a = kn + b$ for some integer k. Upon division by n, b leaves a certain remainder r; that is, $b = qn + r$ where $0 \leq r \leq n$.

Therefore, a$= b + kn = (qn + r) + kn = (q + k)n + r$

Which indicates that 'a' has the remainder as 'b'. On the other hand, suppose we can write $a = q_1 n + r\ and\ b = q_2 n + r$, with the same remainder r$(0 \leq r<n)$. Then $a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$

Hence $n/a - b$. In the language of congruence, we have $a \equiv b(mod\ n)$.

Theorem 1.2

Let $n > 1$ be fixed and a,b,c,d are arbitrary integers. Then the following properties hold:

a) $a \equiv a(mod\ n)$

b) If $a \equiv b(mod\ n)$, then $b \equiv a(mod\ n)$

c) If $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$, then $a \equiv c(mod\ n)$

d) If $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$, then $a + c \equiv b + d(mod\ n)$ and $ac \equiv bd(mod\ n)$

e) If $a \equiv b(mod\ n)$, then $a + c \equiv b + c(mod\ n)$ and $ac \equiv bc(mod\ n)$

f) If $a \equiv b(mod\ n)$, then $a^k \equiv b^k$(mod n) for any positive integer k.

Example 1.1:- Let us try to show that 41 divides $2^{20} - 1$.

We begin by noting that $2^5 \equiv -9(\text{mod } 41)$, when $(2^5)^4 \equiv (-9)(mod\ 41)^4$ by Theorem 1.2; in other words $2^{20} \equiv 81.81(\text{mod } 41)$. But 81$\equiv -1(\text{mod } 41)$, and so 81.81$\equiv 1(\text{mod } 41)$ using parts (b) and (e) of theorem 1.2, we final arrive at

2^{20}-1≡81.81-1≡1-1(mod 41)

Thus, $41/2^{20}$-1

Theorem 1.3:

If ca$\equiv$ cb$(\mathrm{mod}\ \mathrm{n})$, then a$\equiv$ b$\left(\mathrm{mod}\ \frac{\mathrm{n}}{2}\right)$, $where$ d=gcd(c,n)**.**

Proof:- By hypothesis, we can write

$c(a-b)-ca-cb=kn$ for some integer k knowing that $gcd(c,n)=d$, there exixt relatively prime integers r and s satisfying $c=dr$, $n=ds$. When thse values are substituted in the equation above and the common factor d cancelled, the net result is,

$$r(a-b)=ks$$

Hence, $s/r(a-b)$ and $gcd(r,s)=1$. Euclid's Lemma yields [*If a/bc with* $gcd(a,b)=1$*, then a/c*] s/a-b, which may be recast as a$\equiv$ b$(\mathrm{mod}\ \mathrm{s})$; in other words, a$\equiv$ b$\left(\mathrm{mod}\ \frac{\mathrm{n}}{\mathrm{d}}\right)$. Theorem 1.3 gets its maximum force when the requirement that $gcd(c,n)=1$ is added , for then the cancellation many be accomplished without a change in modules.

Corollary 1 :

If ca$\equiv$ cb$(\mathrm{mod}\ \mathrm{n})$ and gcd(c,n)=1 then a$\equiv$ b$(\mathrm{mod}\ \mathrm{n})$**.**

Corollary 2:

If ca$\equiv$ cb$(\mathrm{mod}\ \mathrm{p})$ and p$\times$c. Where, p is a prime number. Then a$\equiv$ b(mod p).

CHAPTER-2
THE THEORY OF CONGRUENCES

BINARY AND DECIMAL REPRESENTATIONS OF INTEGERS

One of the more interesting applications of congruence theory involves finding special criteria under which a given integer is divisible by another integer. These divisibility tests depend on the notational system used to assign 'names' to integers and, more particularly, to the fact that 10 is taken as the base for our number system. Therefore, let us start by showing that given an integer $b > 1$, any positive integer N can be written uniquely in terms of powers of b as

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

where the coefficients $'a_k'$ can take on the 'b' different values 0,1,2,...,b−1. For the Division Algorithm yields integers $'q_1'$ and $'a_0'$ satisfying

N = $q_1 b + a_0$, 0≤a_0< b

If q1 ≥b, we can divide once more, obtaining

$q_1 = q_2 b + a_1$, 0≤a_1< b

Now substitute for q_1 in the earlier equation to get;

$$N = (q_2 b + a_1) b + a_0 = q_2 b^2 + a_1 b + a_0$$

As long as q_2≥b, we can continue in the same fashion. Going one more step: $q_2 = q_3 b + a_2$, where $0 \leq a_2 < b$,

Hence

$$N = q_3 b^3 + a_2 b^2 + a_1 b + a_0$$

Because $N > q_1 > q_2 > \cdots \geq 0$ is a strictly decreasing sequence of integers, this process must eventually terminate, say, at the (m−1)th stage, where

q_{m-1}=q_mb+a_{m-1} ; 0≤a_{m-1}< b and 0≤q_m< b.

Setting a_m=q_m, we reach the representation

N = $a_m b^m$+$a_{m-1} b^{m-1}$ +……+$a_1 b + a_0$

which was our aim.

To show uniqueness, let us suppose that N has two distinct representations, say,

$N = a_m b^m + \cdots + a_1 b + a_0 = c_m b^m + \cdots + c_1 b + c_0$ with $0 \le a_i < b$ for each i and $0 \le c_j < b$ for each j (*we can use the same m by simply adding terms with coefficients a_i =0 or c_j =0, if necessary*). Subtracting the second representation from the first gives the equation $0 = d_m b^m + \cdots + d_1 b + d_0$

where $d_1 = a_1 - c_i$ for i =0,1,...,m. Because the two representations for N are assumed to be different, we must have $d_i \neq 0$ for some value of i. Take k to be the smallest subscript for which $d_k \neq 0$. Then

$0 = d_m b^m + \cdots + d_{k+1} b^{k+1} + d_k b^k$ and so, after dividing by b^k,

$d_k = -b(d_m b^{m-k-1} + \cdots + d_{k+1})$

This tells us that b/d_k. Now the inequalities $0 \le a_k \le b$ and $0 \le c_k < b$ lead us to $-b < a_k - c_k < b$, or $|d_k| < b$. The only way of reconciling the conditions b/d_k and $|d_k| < b$ is to have d_k=0, which is impossible. From this contradiction, we conclude that the representation of N is unique. Smaller values of 5

For example, base b=2, gives the result of numbers only with 0's and 1's,

For example:- $105 = 1\cdot 2^6 + 1\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2 + 1 = 2^6 + 2^5 + 2^3 + 1$ (sum of distinct powers of 2) in Abbreviated form,

$105 = (1101001)_2$

We shall frequently wish to calculate the value of $a^k \pmod n$ when k is large. Is there a more efficient way of obtaining the least positive residue than multiplying a by itself k times before reducing modulo n? One such procedure, called the binary exponential algorithm, relies on successive squaring, with a reduction modulo n after each squaring. More specifically, the exponent k is written in binary form, as $k = (a_m a_{m-1} \ldots a_2 a_1 a_0)2$, and the values $a^{2^j} \pmod n$ are calculated for the powers of 2, which correspond to the 1's in the binary representation. These partial results are multiplied together to get the final results.

Let's look an example of this;

Example:- To calculate 5^{110} (mod 131), first note that the exponent 110 can be expressed in binary form as 110=64+32+8+4+2=$(1101110)_2$

Thus, we obtain the powers 5^{2^j} (mod131) for $0 \leq j \leq 6$ by repeatedly squaring while at each stage reducing each result modulo 131:

$5^2 \equiv 25 \pmod{131}$ $5^{16} \equiv 27 \pmod{131}$

$5^4 \equiv 101 \pmod{131}$ $5^{32} \equiv 74 \pmod{131}$

$5^8 \equiv 114 \pmod{131}$ $5^{64} \equiv 105 \pmod{131}$

When the appropriate partial results-those corresponding to the 1's in the binary expansion of 110-are multiplied, we see that

$5^{110} = 5^{64+32+4+2}$

$= 5^{64}.5^{32}.5^8.5^4.5^2$

$= 105 \cdot 74 \cdot 114 \cdot 101 \cdot 25 \equiv 60 \ (mod 131)$

As a minor variation of the procedure, one might calculate, modulo131, the powers

$5, 5^2, 5^3, 5^6, 5^{12}, 5^{24}, 5^{48}, 5^{96}$ to arrive at

$5^{110} = 5^{96} \cdot 5^{12} \cdot 5^2 \equiv 41 \cdot 117 \cdot 25 \equiv 60 \pmod{131}$

which require two fewer multiplications.

We ordinarily record numbers in the decimal system of notation, where b =10, omitting the 10-subscript that specifies the base. For instance, the symbol 1492 stands for the more awkward expression

$1 \cdot 10^3 + 4 \cdot 10^2 + 9 \cdot 10 + 2$

The integers 1, 4, 9, and 2 are called the digits of the given number. 1 being the thousands digit, 4 the hundreds digit, 9 the tens digit, and 2 the units digit. In technical language we refer to the representation of the positive integers as sums of powers of 10, with coefficients at most 9, as their decimal representation (from the Latin decem, ten). We are about ready to derive criteria for determining whether an integer is divisible by 9 or 11, without performing the actual division. For this, we need a result having to do with congruences involving polynomials with integral coefficients.

Theorem 2.1

Let P(x)= $\sum_{k=0}^{n} c_k x^k$ be a polynomial function of x with integral coefficients c_k, If $a \equiv b \ (mod\ n)$, then $P(a) \equiv P(b) \ (mod\ n)$.

Proof :-

Because $a \equiv b \ (mod\ n)$, from part (f) of Theorem in 1st chapter,

(that is, if a≡b (mod n), then $a^k \equiv b^k (mod\ n)$for any positive integer k)

$a^k \equiv b^k (mod\ n)$ for k =0,1,...,m.

Therefore, $c_k a^k \equiv c_k b^k \ (mod\ n)$ for all such k.

Adding these $m + 1$ congruences, we conclude that

$\sum_{k=0}^{n} c_k a^k \equiv \sum_{k=0}^{n} c_k b^k \ (mod\ n)$

Or

$P(a) \equiv P(b) \ (mod\ n)$.

If P(a) is a polynomial with integral co-efficients, we say that *a* is a solution of the congruence $P(x) \equiv 0 (mod\ n)$, if $P(a) \equiv 0 (mod\ n)$

Corollary:

If a is a solution of $P(x) \equiv 0 (mod\ n)$ and $a \equiv b (mod\ n)$ then, b also is a solution.

Proof :-

By last Theorem, it's known that $P(a) \equiv P(b) \ (mod\ n)$. Hence if a is a solution of $P(x) \equiv 0 (mod\ n)$,

Then $P(b) \equiv P(a) \equiv 0 \ (mod\ n)$, making b a solution.

This is one of the divisibility test that we have a positive integer is divisible by 9 if and only if the sum of the digits in its decimal representation is divisible by 9.

Theorem 2.2:-

Let $N = a_m 10^m + a_{m-1}10^{m-1} + \ldots\ldots\ldots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$, and let S =a_0+a_1+⋯+a_m.

Then $9/N$ if and only if $9/S$.

Proof:-

Consider $P(x) = \sum_{k=0}^{n} a_k x^k$, a polynomial with integral coefficients. The key observation is that 10 ≡1 (mod 9), whence by Theorem 2.1, $P(10) \equiv P(1)\ (mod\ 9)$. But $P(10) = N$ and $P(1) = a_0 + a_1 + \cdots + a_m = S$, so that $N \equiv S\ (mod\ 9)$. It follows that $N \equiv 0\ (mod\ 9)$ if and only if $S \equiv 0\ (mod\ 9)$, which is what we wanted to prove.

Theorem2.1 also serves as the basis for a well-known test for divisibility by 11: an integer is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. We state this more precisely by Theorem 2.3.

Theorem 2.3

Let N =$a_m 10^m$+ $a_{m-1}10^{m-1}$+. . . . . +$a_1 10$ + $a_0$be the decimal expansion of the positive integer N,$0 \leq a_k < 10$, and let T =a_0-a_1+a_2⋯+(-1)$^m a_m$

Then $11/N$ if and only if $11/T$.

Proof:-

As in the proof of Theorem 4.5, put P(x)= $\sum_{k=0}^{m} a_k x^k$.Because

10≡− 1 (mod 11),

we get P(10)≡ P(−1) (mod 11). But P(10)= N,

whereas P(−1)= a_0-a_1+a_2⋯+(-1)$^m a_m$= T, so that N ≡ T (mod 11). The implication is that either both N and T are divisible by 11 or neither is divisible by 11.

Example: - To see the illustration of the last two results, consider the integer N =1,571,724. Because the sum 1+5+7+1+7+2+4=27 is divisible by 9,

Theorem 2.2 guarantees that 9 divides N. It also can be divided by 11; for, the alternating sum 4−2+7−1+7−5+1=11, is divisible by 11.

LINEAR CONGRUENCES AND THE CHINESE REMAINDER THEOREM

An equation of the form $ax \equiv b\ (mod\ n)$ is called a linear congruence and by a solution of such an equation, we mean an integer $x_0$for which a_{x0}≡b (mod n). By definition, $a_{x_0} \equiv b\ (mod\ n)$ if and only if $n/a_{x_0} - b$ or, what amounts to the same thing, if and only if a_{x0}-b =ny_0 for some integer y_0. Thus, the problem of finding all integers that will satisfy the linear congruence $ax \equiv b\ (mod\ n)$ is identical with that of obtaining all solutions of the linear Diophantine equation $ax - ny = b$. This allows us to bring the results of Divisibility Theory in integers.

It is convenient to treat two solutions of $ax \equiv b\ (mod\ n)$ that are congruent modulo n as being "equal" even though they are not equal in the usual sense. For instance, x =3 and x =−9 both satisfy the congruence $3x \equiv 9\ (mod\ 12)$; because $3 \equiv -9(mod\ 12)$, they are not counted as different solutions. In short, when we refer to the number of solutions of $ax \equiv b\ (mod\ n)$, we mean the number of incongruent integers satisfying this congruence.

Theorem 2.4:-

The linear congruence $ax \equiv b(mod\ n)$has a solution if and only if d/b, where $d = gcd(a, n)$. If d/b, then it has d mutually incongruent solutions modulo n.

Proof: - We already have observed that the given congruence is equivalent to the linear Diophantine equation $a_x - n_y$=b. It is known that the latter equation can be solved if and only if d/b, moreover if it is solvable and x_0, y_0 is one specific solution, then any other solution has the form

$$x = x_0 + (n/d)ty = y_0 + (a/d)t$$

for some choice of t.

Among the various integers satisfying the first of these formulas, consider those that occur when t takes on the successive values,

t =0,1,2,...,d −1;

x_0, x_0+ n/d,x_0 + (2n /d),...,x0 + (d −1)n/d

We claim that these integers are incongruent modulo n, and all other such integers x are congruent to some one of them. If it happened that,

x_0+ (n/2) $t_1 \equiv x_0$+ (n/2) $t_2(mod\ n)$

where 0≤ $t_1 < t_2 \leq$d −1, then we would have

(n/d) t_1≡(n/2) t_2 (mod n)

Now $gcd((n/d), n)$ and therefore by Theorem 1.3 the factor n/d could be cancelled to arrive at the congruence

t1 ≡t2 (mod d)

which is to say that d(t2 −t1). But this is impossible in view of the inequality 0 < t2 −t1 < d. It remains to argue that any other solution x_0+(n/d)t is congruent modulo n to one of the d integers listed above. The Division Algorithm permits us to write t as t =qd+r, where 0≤r ≤d −1. Hence

x_0+(n/d)t = x_0+(n/d)(qd+r)

= x_0+nq+(n/d)r

≡ x_0+(n/d)r (mod n)

with x_0+(n/d)rbeing one of our d selected solutions. Hence the proof.

The argument that we gave in the above theorem; brings out a point worth stating explicitly: Ifx_0 is any solution of $ax \equiv b(mod\ n)$ then the $d = gcd(a, n)$incongruent solutions are given by

x_0: x_0+(n/d)x_0+2(n/d),. . . . . .,x_0+(d-1)(n/d)

Corollary:

If $gcd(a, n) = 1$, then the linear congruence $ax \equiv b\ (mod\ n)$ has a unique solution modulo n.

Given relatively prime integers a and n, the congruence $ax \equiv 1\ (mod\ n)$ has a unique solution. This solution is sometimes called the (multiplicative) inverse of $a\ modulo\ n$.

Let's look at 2 different examples,

Example:-

First consider the linear congruence$18x \equiv 30(mod\ 42)$. Because $gcd(18,42) = 6$ and 6 surely divides 30.Theorem 2.4 guarantees the existence of exactly 6 solutions, which are incongruent modulo 42. By inspection, one solution is found to be x =4. Our analysis tells us that the 6 solutions are as follows:

x ≡4+(42/6)t ≡4+7t (mod 42) ; t=0,1,...,5

or

x ≡4,11,18,25,32,39(mod 42)

Example:-

Let us solve the linear congruence

$$9x \equiv 21 \ (mod\ 30).$$

At the outset, because

$gcd(9,30) = 3$ and $3/21$, we know that there must be three incongruent solutions.

One way to find these solutions is to divide the given congruence through by 3, thereby replacing it by the equivalent congruence $3x \equiv 7 \ (mod\ 10)$. The relative primeness of 3 and 10 implies that the latter congruence admits a unique solution modulo 10.

Although it is not the most efficient method, we could test the integers0, 1, 2,..., 9 in turn until the solution is obtained. A better way is that, multiply both sides of the congruence $3x \equiv 7 \ (mod\ 10)$ by 7 to get

$$21x \equiv 49 \ (mod\ 10)$$

Whichreduces to $x \equiv 9(mod 10)$.

Taking t =0, 1, 2, in the formula

$$x = 9 + 10t$$

we obtain 9, 19, 29, whence

$x \equiv 9 \ (mod\ 30)$,$x \equiv 19 \ (mod\ 30)$, $x \equiv 29 \ (mod\ 30)$ are the required 3 solutions of $9x \equiv 21 \ (mod\ 30)$.

Use the method in the proof of Theorem 2.4

$9x \equiv 21(mod\ 30)$ (Linear Diophantine Equation)

We begin by expressing $3 = gcd(9,30)$ as a linear combination of 9 and 30.It is for either by inspection or by using the Euclidean Algorithm, that 3=9(−3)+30·1, so that

$$21 = 7 \cdot 3 = 9(-21) - 30(-7)$$

Thus, x =−21

y =−7

satisfied the Diophantine solution

And now all solutions of the congruence has to be found

x =−21+(30/3)t =−21+10t

The integers

x =−21+10t

where t=0,1,2,are incongruent modulo 30(but all are congruent modulo 10); Thus, we end up with the incongruent solutions

x ≡−21 (mod 30) x ≡−11 (mod 30) x ≡−1 (mod 30) or, if one prefers positive numbers,

x ≡9,19,29 (mod 30).

Theorem 2.5:- Chinese Remainder Theorem

Letn_1, n_2 ,...,n_r bepositiveintegers such that gcd(n_i,n_j)=1 for $i \neq j$. Then the system of linear congruences,

$$x \equiv a_1(mod n_2)$$
$$x \equiv a_2\ (mod n_2)$$

.....

.....

.....

$$x \equiv a_r\ (mod n_r)$$

Has a simultaneous solution, which is unique modulo the integer $n_1 n_2 \cdots n_r$.

Proof:-

We start by forming the product

n =$n_1 n_2 \cdots n_r$.

For each $k = 1,2,\ldots,r$, let N_k= n/n_k=$n_1 \cdots n_{k-1} n_{k+1} \cdots n_r$

Where, $N_k$is the product of all the integers n_i with factor n_k. By hypothesis, the n_i are relatively prime in pairs, so that $gcd(N_k, n_k) = 1$.According to the theory of a

single linear congruence, it is possible to solve the congruence $N_k x \equiv 1 \pmod{n_k}$; call the unique solution x_k. Our aim is to prove that the integer

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

is a simultaneous solution of the given system.

First, observe that $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$, because n_k / N_i in this case. Theresult is,

$\bar{x} = a_1 N_1 x_1 + \cdots a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}$ But the integer x_k was chosen to satisfy the congruence $N_k x \equiv 1 \pmod{n_k}$ which forces

$\bar{x} \equiv a_k \cdot 1 \equiv a_k \pmod{nk}$

Hence, the solution to the given system of congruences exists. As for the uniqueness assertion, suppose that x' is any other integer that satisfies these congruences. Then, $\bar{x} \equiv a_k \equiv x' (mod\ n_k)$, k =1,2,...,r

and so $n_k / \bar{x} - x'$ for each value of k. Because $gcd(n_i, n_j) = 1$,

Now, $n_1 n_2 \ldots n_r / \bar{x} - x'$: hence

$x \equiv x\ (mod\ n)$.

Hence the proof.

Example:-

Let's take three congruences,

$$x \equiv 2\ (mod\ 3)$$

$$x \equiv 3\ (mod\ 5)$$

$$x \equiv 2\ (mod\ 7)$$

According to Theorem 2.5, we have

$n = 3 \cdot 5 \cdot 7 = 105$ and $N_1 = n/3 = 35$ $N_2 = n/5 = 21$ $N_3 = n/7 = 15$

Now, the linear congruences,

$35x \equiv 1\ (mod\ 3)$ $21x \equiv 1\ (mod\ 5)$ $15x \equiv 1\ (mod\ 7)$ are satisfied by x_1=2, x_2=1, x_3=1, respectively. Thus, a solution of the system is given by,

x=2·35·2+3·21·1+2·15·1=233

Modulo 105, we get the unique solution $x = 233 \equiv 23 \ (mod\ 105)$.

Theorem 2.6:-

The system of linear congruences

$$ax + by \equiv r \ (mod\ n)$$

$$cx + dy \equiv s \ (mod\ n)$$

has a unique solution modulo n whenever $gcd(ad - bc, n) = 1$.

Proof:-Let us multiply the first congruence of the system by d, the second congruence by b, and subtract the lower result from the upper. These calculations yield

$$(ad - bc)x \equiv dr - bs \ (mod\ n)$$

The assumption $gcd(ad - bc, n) = 1$sures that the congruence

$(ad - bc)z \equiv 1 \ (mod\ n)$ possess a unique solution; denote the solution by t. When congruence (1) is multiplied by t, we obtain

$$x \equiv t(dr - bs) \ (mod\ n)$$

A value for y is found by a similar elimination process. That is, multiply the first congruence of the system by c, the second one by a, and subtract to end up with $(ad - bc)y \equiv as - cr \ (mod\ n)$

Multiplication of this congruence by t leads to,

$y \equiv t(as - cr) \ (mod\ n)$

A solution of the system is now established.

We close this section with an example.

Example:-

Consider the system,

$$7x + 3y \equiv 10 \ (mod\ 16)$$

$$2x + 5y \equiv 9 \ (mod\ 16)$$

Since $gcd(7 \cdot 5 - 2 \cdot 3,16) = gcd(29,16) = 1$, a solution exists. It is obtained by the method developed in the proof of Theorem 4.9. Multiplying the first congruence by 5, the second one by 3, and subtracting, we arrive at,

$29x \equiv 5 \cdot 10 - 3 \cdot 9 \equiv 23 \ (mod\ 16)$

or, what is the same thing, $13x \equiv 7\ (mod\ 16)$. Multiplication of this congruence by 5 (noting that $5 \cdot 13 \equiv 1\ (mod\ 16)$) produces $x \equiv 35 \equiv 3\ (mod\ 16)$. When the variable x is eliminated from the system of congruences in a like manner, it is found that

$$29y \equiv 7 \cdot 9 - 2 \cdot 10 \equiv 43\ (mod\ 16)$$

But then $13y \equiv 11\ (mod\ 16)$, which upon multiplication by 5, results in

$y \equiv 55 \equiv 7\ (mod\ 16)$. The unique solution of our system turns out to be,

$$x \equiv 3\ (mod\ 16)\ , y \equiv 7\ (mod\ 16)$$

CHAPTER-3
NUMBER THEORETIC FUNCTIONS

THE SUM AND NUMBER OF DIVISORS

Certain functions are found to be of special importance in connection with the study of the divisors of an integer. Any function whose domain of definition is the set of positive integers is said to be a number-theoretic (or arithmetic) function. Although the value of a number-theoretic function is not required to be a positive integer or, for that matter, even an integer,most of the number-theoretic functions that we shall encounter are integer-valued. Among the easiest to handle, and the most natural, are the functions τ and σ.

Definition 3.1:-

Given a positive integer n, let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of these divisors.

For an example of these notations, consider n =12. Because 12 has the positive divisors 1, 2, 3, 4, 6, 12, we find that

$\tau(12) = 6$ and $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$

$\tau(n) = 2$ if and only if n is a prime number also, $\sigma(n) = n + 1$ if and only if n is a prime.

Before studying the functions τ and σ, we introduce notation that will clarify a number of situations later. It is customary to interpret the symbol

$$\sum_{d/n} f(d)$$

to mean, "*Sum the values f(d) as d runs over all the positive divisors of the positive integer n*".

For instance, we have

$\sum_{d/20} f(d)$ = f(1)+ f(2)+ f(4)+ f(5)+ f(10)+ f(20), τ and σ may be expressed in the form

$\tau(n) = \sum_{d/n} 1 \quad \sigma(n) = \sum_{d/n} d$

To illustrate: the integer 10 has the four positive divisors 1, 2, 5, 10.

$$\tau(10) = \sum_{d/10} 1 = 1 + 1 + 1 + 1 = 4$$

$$\sigma(10) = \sum_{d/10} d = 1 + 2 + 5 + 10 = 18$$

Theorem 3.1:-

If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of n are precisely those integers d of the form $d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ where $0 \le a_i \le k_i$ (i =1,2,...,r).

Proof:-

The divisor d =1 is obtained when $a_1 = a_2 = \cdots = a_r = 0$, and n itself occurs when

$a_1 = k_1$, $a_2 = k_2$,..., $a_r = k_r$. Suppose that d divides n trivially; say, n$n = dd'$, where $d > 1, d' > 1$. Express both d and d' as products of (not necessarily distinct) primes: $d = q_1 q_2 \dots\dots q_s \; d' = t_1 \, t_2 \dots\dots t_u$

with q_i , t_j prime. Then,

$$p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1 \dots \dots q_s t_1 \dots . t_u$$

are two prime factorizations of the positive integer n. By the uniqueness of the prime factorization, each prime q_i must be one of thep_j. Collecting the equal primes into a single integral power, we get

d = $q_1 q_2 \dots\dots\dots q_s = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ where the possibility that a_i=0 is allowed.

Conversely, every number d = $p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} (0 \le a_i \le k_i)$ turns out to be a divisor of n. For we can write

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

$$= \left(p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}\right)\left(p_1^{k_1 - a_1} p_2^{k_2 - a_2} \dots p_r^{k_r - a_r}\right)$$

$$= dd'$$

With $d' = p_1^{k_1-a_1}p_2^{k_2-a_2} \dots p_r^{k_r-a_r}$ and $k_i - a_i \geq 0$ for each i.

Then $d' > 0$ and d/n.

Theorem3.2:-

If $n = p_1^{k_1}p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of n>1, then

(a) $\gamma(n) = (k_1 + 1)(k_2 + 1) \dots\dots (k_r + 1)$ and

(b) $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1}\frac{p_2^{k_2+1}-1}{p_2-1} \dots \frac{p_r^{k_r+1}-1}{p_r-1}$

Proof:-

According to Theorem 3.1, the positive divisors of n are precisely those integers

$$d = p_1^{a_1}p_2^{a_2} \dots p_r^{a_r}$$

where $0 \leq a_i \leq k_i$.

There are $k_1 + 1$ choices for the exponent a_1 , $k_2 + 1$ choices for a_2 and $k_r + 1$ choices for a_r. Hence, there are

$$(k_1 + 1)(k_2 + 1)\dots(k_r + 1)$$

possible divisors of n.

To evaluate $\sigma(n)$, consider the product

$$\left(1 + p_1 + p_1^2 + \cdots + p_1^{k_1}\right)\left(1 + p_2 + p_2^2 + \cdots p_2^{k_2}\right) \dots (1 + p_r + p_r^2 + \cdots + p_r^{k_r})$$

Each positive divisor of n appears once and only once as a term in the expansion of this product, so that

$$\sigma(n) = \left(1 + p_1 + p_1^2 + \cdots + p_1^{k_1}\right) \dots (1 + p_r + p_r^2 + \cdots + p_r^{k_r})$$

Applying the formula for the sum of a finite geometric series to the i^{th} factor on the right-hand side, we get

$$1 + p_i + p_i^2 + \cdots + p_i^{k_i} = \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1}\frac{p_2^{k_2+1} - 1}{p_2 - 1} \dots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

If $n = p_1^{k_1}p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of n > 1, then

$$\gamma(n) = \prod_{1 \le i \le r} (k_i + 1)$$

And

$$\sigma(n) = \prod_{1 \le i \le r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

Example:-

The number 180 = $2^2.3^2.5$ has

$\gamma(180) = (2+1)(2+1)(1+1) = 18$ positive divisors.

These are the integers of the form

$$2^{a_1}3^{a_2}5^{a_3}$$

Where a_1=0,1,2 ,a_2=0,1,2 and a_3 = 0,1

We obtain 1,2,3,4,5,6,9,10,12,15,18,20,30,36,45,60,90,180.

The sum of the integers is

$$\sigma(180) = (2^3 - 1)/(2 - 1)\ (3^3 - 1)/(3 - 1)\ (5^2 - 1)/(5 - 1)$$
$$= (7/1)(26/2)(24/4)$$
$$= 7.13.6 = 546$$

Definition 3.2 :-

A number theoretic function f is said to be multiplicative if

$$f(mn) = f(m)f(n)$$

Whenever $gcd\ (m, n) = 1$ and if f is not identically zero.

Theorem3.3 :-

The function γ and σ are both multiplicative function

Proof:-

Let m and n be relatively prime integers. Because the result is trivially true if either m or n is equal to 1, we may assume that $m > I$ and $n > 1$.If

$$m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

and

$$n = q_1^{j_1} q_2^{j_2} \dots q_s^{j_s}$$

are the prime factorizations of m and n, then because $gcd(m,n) = 1$, no p_i can occur among the q_j. It follows that the prime factorization of the product mn is given by $mn = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} q_1^{j_1} q_2^{j_2} \dots q_s^{j_s}$

Applying theorem 3.2,we obtain

$$\gamma(m,n) = [(k_1 + 1) \dots (k_r + 1)][(j_1 + 1) \dots (j_s + 1)]$$
$$= \gamma(m)\gamma(n)$$

Similarly ,

$$\sigma(m,n) = [(p_1^{k_1+1} - 1)/(p_1 - 1) \dots . (p_r^{k_r+1} - 1)/(p_r - 1)][(q_1^{j_1+1} - 1)/(q_1 - 1) \dots . (q_s^{j_s+1} - 1)/(q_s - 1)]$$
$$= \sigma(m)\sigma(n)$$

Thus γ and σ are multiplicative functions.

Lemma:-

If $gcd(m,n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, where $d_1 | m, d_2 | n$ and $gcd(d_1, d_2) = 1$; furthermore, these products are all distinct.

Proof :- Assume that m>1 and n>1.

Let m= $p_1^{k1} p_2^{k2} \dots p_r^{kr}$ and n= $q_1^{j1} q_2^{j2} \dots q_s^{js}$ be their respective prime factorizations. The primes $p_1, p_2, \dots p_r, q_1, q_2, \dots q_s$ are all distinct, the prime factorization of mn is,

$$mn = p_1^{k1} \dots p_r^{kr} q_1^{j1} \dots q_s^{js}$$

Hence, any positive divisor d of mn will be uniquely representable in the form

d=$p_1^{k1} \dots p_r^{kr} q_1^{j1} \dots q_s^{js}$, $0 \le a_i \le k_i$, $0 \le b_i \le j_i$

This allows us to write d as $d = d_1 d_2$, where $d_1 = p_1^{a1} \dots p_r^{ar}$ divides m and $d_2 = q_1^{b1} \dots q_s^{bs}$ divides n. Because no p_i is equal to any q_j, we surely must have $gcd(d_1, d_2) = 1$.

Theorem3.4:-

If f is a multiplicative function and f is defined by

$$F(n) = \sum_{d|n} f(d)$$

then F is also multiplicative

Proof:- Let m and n be relatively prime positive integers. Then

$$F(mn) = \sum_{d|mn} f(d)$$

$$= \sum_{\substack{d|n \\ d|m}} f(d_1 d_2)$$

Because every divisor d of mn can be uniquely written as a product of a divisor d_1 of m and a divisor d_2 of n, where $gcd(d_1, d_2) = 1$. By the definition of a multiplicative function,

$$f(d_1 d_2) = f(d_1) f(d_2)$$

It follows that

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2)$$

$$= \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right)$$

Example :-

Let m= 8 and n = 3,

we have,

$\mathrm{F}(8.3) = \sum_{\mathrm{d}|24} \mathrm{f}(\mathrm{d})$

$= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24)$

$= f(1.1 + f(2.1) + f(1.3) + f(4.1) + f(2.3) + f(8.1) + f(4.3) + f(8.3)$

$= f(1)f(1) + f(2)f(1) + f(1)f(3) + f(4)f(1) + f(2)f(3) + f(8)f(1) + f(4)f(3) + f(8)f(3)$

$= [f(1) + f(2) + f(4) + f(8)][f(1) + f(3)]$

$= \sum_{d|8} f(d) . \sum_{d|3} f(d)$

$= F(8)F(3)$

By theorem3.4. , the conclusion that γ and σ are multiplicative.

Corollary:-

The functions γ and σ are multiplicative functions

Proof:-

The constant function $f(n) = 1$ is multiplicative, as is the identity function $f(n) = n$. Because γ and σ may be represented in the form

$\gamma(n) = \sum_{d|n} 1$ and $\sigma(n) = \sum_{d|n} d$

Hence it follows from theorem3.4

3.2 THE MÖBIUS INVERSION FORMULA

We introduce another naturally defined function on the positive integers, the Möbius μ-function.

Definition 3.3:- For a positive integer n, define μ by the rules

$$\mu(n) = \begin{cases} 1 & if\ n = 1 \\ 0 & if\ p^2|n\ for\ some\ prime\ p \\ (-1)^r & if\ n = p_1 p_2 \dots p_r, where\ p_i\ are\ distinct\ primes \end{cases}$$

It states that $\mu(n) = 0$ if n is not a square-free integer, whereas $\mu(n) = (-1)^{\mathrm{r}}$. If n is square-free with r prime factors.

For example: $\mu(30) = \mu(2.3.5) = (-1)^3 = -1$. The first few values of μ are

$$\mu(1) = 1\ \mu(2) = -1\ \mu(3) = -1\ \mu(4) = 0\ \mu(5) = -1\ \mu(6) = 1\ldots$$

If p is a prime number, it is clear that $\mu(\mathrm{p}) = -1$; In addition,

$\mu(p^{\mathrm{k}}) = 0\ for\ k \geq 2$.

Theorem3.5:-

The function μ is a multiplicative function.

Proof:-

We want to show that $\mu(mn) = \mu(m)\mu(n)$. Whenever m and n are relatively prime. If either $p^2|m$ or $p^2|n$, p a prime, then $p^2|mn$; Hence, $\mu(mn) = 0 = \mu(m)\mu(n)$, and the formula holds trivially. We therefore may assume that both m and n are square-free integers. Say, $m = p_1p_2\ldots p_{\mathrm{r}}$, $n = q_1q_2\ldots q_s$, with all the primes p_{i} and q_j being distinct. Then

$$\mu(mn) = \mu(p_1\ldots p_{\mathrm{r}}q_1\ldots q\ ) = (-1)$$
$$= (-1)^{\mathrm{r}}\,(-1)^{\mathrm{s}} = \mu(m)\mu(n)$$

which completes the proof.

If $\mu(d)$ is evaluated for all the positive divisors d of an integer and the results are added. In the case where n= 1,

$$\sum_{d|1} \mu(d) = \mu(1) = 1$$

Suppose that n>1 and put

$$F(n) = \sum_{d|n} \mu(d)$$

we first calculate F(n) for the power of a prime, say,

$n = p^{\mathrm{k}}$.

The positive divisors of p^k are just the k + 1 integers 1, p, p^2...p^k, so that

$$F(p^{\mathrm{k}}) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^{\mathrm{k}})$$

$$= \mu(1) + \mu(p) = 1 + (-1) = 0$$

Because μ is a multiplicative function, an appeal to Theorem 3.4 is legitimate; this result guarantees that F also is multiplicative. Thus, if the canonical factorization of n is n =$p_1^{k1}p_2^{k2}\ldots p_r^{kr}$,then F(n) is the product of the valuesassigned to F for the prime powers in this representation:

$$F(n) = F(p_1^{k1})F(p_2^{k2}) \ \ldots \ F(p_r^{kr}) = 0$$

Theorem3.6:-

For each positive integer n≥1,

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \ if \ n = 1 \\ 0 \ if \ n > 1 \end{cases}$$

Where d runs through the positive divisors of n.

For an illustration of this last theorem, consider n = 10. The positive divisors of 10 are 1, 2, 5, 10 and the desired sum is

$$\sum_{d|10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10)$$

$$= 1 + (-1) + (-1) + 1 = 0$$

Theorem 3.7:Möbius inversion formula

Let F and f be two number- theoretic functions related by the formula

$$F(n) = \sum_{d|n} f(d)$$

Then

$$f(n) = \sum_{d|n} \mu(d) \, F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$$

Proof:- The two sums mentioned in the conclusion of the theorem are seen to be the same upon replacing the dummy index d by $d' = n/d$; as d ranges over all positive divisors of n, s does d'.

Carrying out the required computation, we get

$$\sum_{d|n} \mu(d)\, F(n/d) = \sum_{d|n} \left(\mu(d) \sum_{c|(\frac{n}{d})} f(c) \right)$$

$$= \sum_{d|n} \left(\sum_{c|(\frac{n}{d})} \mu(d)\, f(c) \right)$$

It is easily verified that $d|n$ and

$c\,|(n/d)$ if and only if $c|n$ and $d|(n/c)$. Because of this, the last expression in Eq. (1) becomes

$$\sum_{d|n} \left(\sum_{c|(\frac{n}{d})} \mu(d)\, f(c) \right) = \sum_{c|n} \left(\sum_{d|(\frac{n}{c})} \mu(d)\, f(c) \right) = \sum_{c|n} \left(f(c) \sum_{d|(\frac{n}{c})} \mu(d) \right)$$

In compliance with Theorem 3.6, the sum $\sum_{d|(\frac{n}{c})} \mu(d)$ must vanish except when

$n|c = 1$ (that is, when n = c), in which case it is equal to 1; the upshot is that the right-hand side of Eq. (2) simplifies to

$$\sum_{c|n} \left(f(c) \sum_{d|(\frac{n}{c})} \mu(d) \right) = \sum_{c=n} f(c). = f(n)$$

Hence the result.

Theorem 3.8:-

If F is a multiplicative function and $F(n) = \sum_{d|n} f(d)$ then f is also multiplicative.

Proof:- Let m and n be relatively prime positive integers. Any divisor d of mn can be uniquely written as $d = d_1 d_2$, where $d^1|m$, $d_2|n$, and $gcd(d_1, d_2) = 1$.

Thus, using the inversion formula,

$$f(mn) = \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right)$$

$$= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right)$$

$$= f(m) f(n)$$

CHAPTER 4

SOME APPLICATIONS OF NUMBER THEORY

4.1 APPLICATIONS

Application to the calendar

The Gregorian calendar, goes back as far as the second half of the 16th century. The earlier 1 Julian calendar, introduced by Julius Caesar, was based on a year of 365 days, with a leap year 4 every fourth year. This was not a precise enough measure, because the length of a solar year the time required for the earth to complete an orbit about the sun-is apparently 365.2422 days. The small error meant that the Julian calendar receded a day from its astronomical norm every 128 years.

By the 16th century, the accumulating inaccuracy caused the vernal equinox (the first day of Spring) to fall on March 11 instead of its proper day, March 21.The calendar's inaccuracy naturally persisted throughout the year, but at this season it meant that the Easter festival was celebrated at the wrong astronomical time. Pope Gregory XIII rectified the discrepancy in a new calendar, imposed on the predominantly Catholic countries of Europe. He decreed that 10 days were to be omitted from the year 1582, by having October 15 of that year immediately follow October 4. At the same time, the Jesuit mathematician Christopher Clavius amended the scheme for leap years: these would be years divisible by 4, except for those marking centuries. Century years would be leap years only if they were divisible by 400. (For example, the century years 1600 and 2000 are leap years, but 1700, 1800,1900, and 2100 are not.)

Because the edict came from Rome, Protestant England and her possessions including the American colonies-resisted. They did not officially adopt the Gregorian calendar until 1752. By then it was necessary to drop 11 days in September from the Old Style, or Julian, calendar. So it happened that George Washington, who was born on February 11, 1732, celebrated his birthday as an adult on February 22 Other nations gradually adopted the reformed calendar: Russia in 1918, and China as late as 1949.

Our goal in the present section is to determine the day of the week for a given date after the year 1600 in the Gregorian calendar. Because the leap year day is added at the end of February, let us adopt the convenient fiction that each year ends at the end of February. According to this plan, in the Gregorian year Y March and April are counted as the first and second months. January and February of the Gregorian year Y+ l are, for convenience, counted as the eleventh and twelfth months of the year Y.

Another convenience is to designate the days of the week, Sunday through Saturday, by the numbers 0,1,...6:

Sun	Mon	Tue	Wed	Thu	Fri	Sat
0	1	2	3	4	5	6

The number of days in a common year is $365 \equiv 1\ (mod\ 7)$, whereas in leap years there are $366 \equiv 2\ (mod\ 7)$ days. Because February 28 is the 365th day of the year, and $365 \equiv 1\ (mod\ 7)$, February 28 always falls on the same weekday as the previous March 1. Thus if a particular March immediately follows February 28,its weekday number will be one more, modulo 7, than the weekday number of the previous March 1. But if it follows a leap year day, February 29, its weekday number will be increased by two.

For instance, it D_{1600} is the weekday number to March 1, 1600, then March 1 in the years 1601, 1602, and 1603 has numbers congruent modulo 7 to $D_{1600} + 1, D_{1600} + 2\ and\ D_{1600} + 3$ respectively; but the number corresponding to March 1,1604 is $D_{1600} + 5\ (mod\ 7)$

We can summarize this: the weekday number DY for March 1 of any year Y> 1600 will satisfy the congruence

$$DY \equiv D^{1600} + (\ Y\ -\ 1600\ ) + L\ (mod 7) \ldots\ldots\ldots\ldots\ldots\ldots . (1)$$

where L is the number of leap year days between March 1,1600, and March 1 of the year Y.

Let us first find L, the number of leap year days between 1600 and the year Y. To do this, we count the number of these years that are divisible by 4, deduct the number of century years, and then add back the number of century years divisible by 400. [x − a] = [x] − a whenever a is an integer. Hence the number of years n in the interval 1600 < n ≤ Y that are divisible by 4 is given by

$$([Y - 1600)/(100)] = [(Y/4) - 400] = [Y/4] - 400$$

Likewise , the number of elapsed century years is

$$[(Y - 1600)/4] = [(Y/100) - 16] = [(Y/100)] - 16$$

Whereas among those there are

$$[(Y - 1600)/400] = [Y/400] - 4$$

Century years that is divisible by 400. Taken together, these statements yields.

$$L = ([Y/4] - 400) - ([Y/100] - 16) + ([Y/400] - 4)$$

$$= [Y/4] - [Y/100] + [Y/400] - 388$$

Let us obtain, for a typical example, the number of leap years between 1600 and 1995. we compute.

$$L = [1995/4] - [1995/100] + [1995/400] - 388$$

$$= 498 - 19 + 4 - 388 = 95$$

Together with congruence (1), this allows us to find a value for D_{1600}. Days and dates of recent years can still be recalled; we can easily look up the weekday (Wednesday) for March 1, 1995. That is, D_{1995}=3. Then from (1).

$$3 \equiv D_{1600} + (1995\ 1600) + 95 \equiv D_{1600}\ (mod\ 7)$$

and so March 1, 1600, also occurred on a Wednesday. The congruence giving the day of the week for March 1 in any year Y may now be reformulated as

$$Dy \equiv 3 + (Y - 1600) + L\ (mod\ 7) \ldots\ldots\ldots\ldots\ldots (2)$$

An alternate formula for L comes from writing the year Y as

$$Y = 100c + y\ , 0 \leq y < 100$$

where c denotes the number of centuries and y the year number within the century. Upon substitution, the previous expression for L becomes

$$L = [25c + (y/4)] - [c + (y/100)] + [(c/4) + (y/400)] - 388$$

$$= 24c + [y/4] + [c/4] - 388$$

(Notice that y/100=0 and y/400 < y/4.) Then the congruence for Dy appears as

$$Dy \equiv 3 + (100c + y - 1600) + 24c + [y/4] + [c/4] - 388\ (mod\ 7)$$

Which reduces to $D_y \equiv 3 - 2c + y + \left[\frac{c}{4}\right] + \left[\frac{y}{4}\right] (mod 7)$.....(3)

Example:-

We can use the latest congruence to calculate the day of the week on which March 1, 1990, fell. For this year, c=19 and y=90 so that (3) gives

$$D_{1990} \equiv 3 - 38 + 90 + [19/4] \ + \ [190/4]$$

$\equiv 55 + 4 + 22 \equiv 4 \ (mod \ 7)$

March 1 was on a Thursday in 1990.

We move on to determining the day of the week on which the first of each month of the year would fall. Because $30 \equiv 2 \ (mod \ 7)$, a 30-day month advances by two the weekday on which the next month begins. A 31-day month increases it by 3. So, for example, the number of June 1 will always be $3 + 2 + 3 \equiv 1 \ (mod \ 7)$ greater than that of the preceding March 1 because March, April, and May are months of 31, 30, and 31 days, respectively. The table below gives the value that must be added to the day-number of March I to arrive at the number of the first day of each month in any year Y.

MARCH	0	SEPTEMBER	2
APRIL	3	OCTOBER	4
MAY	5	NOVEMBER	0
JUNE	1	DECEMBER	2
JULY	3	JANUARY	5
AUGUST	6	FEBRUARY	1

For m=1, 2,..., 12, the expression

$$[(2.6)m \ 0.2] \ - \ 2 \ (mod \ 7)$$

produces the same monthly increases as indicated by the table. Thus the number of the first day of the m^{th} month of the year Y is given by

$$Dy + [(2.6)m \ - \ 0.2] \ - \ 2 \ (mod \ 7)$$

Taking December 1, 1990, as an example, we have

$$D_{1990} + [(2.6)10 \ - \ 02] - 2 \ \equiv \ 4 + \ 25 \ - 2 \ \equiv \ 6(mod \ 7)$$

that is, the first of December in 1990 fell on a Saturday.

Finally, the number w of day d, month m,

year Y = 100c + y is determined

from congruence

$w \equiv (d-1) + Dy\ + [(2.6m\ 0.2] - 2\ (mod\ 7)$

We can use Eq. (3) to recast this:

$$w \equiv\ d + [2.6m - \ 0.2] - 2c + y + [c/4] + [y/4] + (mod\ 7)$$

We summarize the results of this section in the following theorem.

Theorem 4.1:-

The date with month m, day d, year $Y\ =\ 100c +\ y$ where c≥ 16 and 0<y < 100, has weekday number

$$w \equiv d +\ [2.6m - 0.2] - 2c + y + [c/4] + [y/4](mod\ 7)$$

provided that March is taken as the first month of the year and January and February are assumed to be the eleventh and twelfth months of the previous year. Let us give an example using the calendar formula.

Example:-

On what day of the week will January 14, 2020, occur?

In our convention, January of 2020 is treated as the eleventh month of the year 2019. The weekday number corresponding to its fourteenth day is computed as

$$w \equiv 14 + [(2.6)11\ -\ 0.2] - 40 +\ 19 +\ [20/4] + [19/4]$$

$$\equiv 14 + 28 - 40 + 19 + 5 + 4\ \equiv\ 2\ (mod\ 7)$$

We conclude that January 14, 2020, will take place on a Tuesday

Applications in Cryptography

Cryptography is one of the main applications of number theory. Classically the making and breaking of secret codes has usually been confined to diplomatic and military practices. With the growing quality of digital data stored and communicated by electronic data processing systems, organizations in both the public and commercial sectors have felt the need to protect information from unwanted intrusion. Their test has been a recent surge of interest by Mathematicians and computer scientists in cryptography (from the Greek Cryptos, meaning hidden and graphein meaning to write). The science of making communications unintelligible to all except authorized parties. Cryptography is the

only known practical means for protecting information transmitted through public communication networks, such as those using telephone lines, microwaves or satellites.

In the language of cryptography, where codes are called ciphers, the information to the concealed is called plain text. After transformation to secret form a message is called ciphers text. The process of converting from plaintext to cipher text is said to be encrypting (or enciphering), whereas the reverse process of changing from cipher text back to plaintext is called decrypting (or deciphering).

Applications of Chinese remainder theorem

The first application deals with polynomial congruence with composite moduli.

Theorem 4.2:-

Let f be a polynomial with integer coefficients, let $m_1, m_2, \dots, m_r$.

Then the congruence

$$f(x) \equiv 0(mod m)$$

Has a solution if and only if each of the congruence.

$$F(x) \equiv 0(mod m_i) \; i = 1,2, \dots, r$$

Has a solution. Moreover, If v(m) and v(m_i) denote the number of solution of (1) and (2) respectively, then

$V(m) = v(m_1)v(m_2) \dots v(m_r)$

The next application of the Chinese reminder theorem concerns the set of lattice points visible from the origin.

Theorem 4.3:-

The set of lattice points in the plane visible from the origin contains arbitrarily large square gaps. That is, do you want any integer k>0 there exists a lattice point (a,b) such that none of the lattice points

(a+r) ,b+s) , $0 < r \leq k$, $0 < s \leq k$

is visible from the origin.

CONCLUSION

Number theory (or arithmetic or higher arithmetic in older usage) is a branch of pure mathematics devoted primarily to the study of the integers and integer-valued functions. German mathematician Carl Friedrich Gauss (1777–1855) said, "Mathematics is the queen of the sciences—and number theory is the queen of mathematics."

Number theory has always fascinated amateurs as well as professional mathematicians. In contrast to other branches of mathematics, many of the problems and theorems of number theory can be understood by laypersons, although solutions to the problems and proofs of the theorems often require a sophisticated mathematical background.

Until the mid-20th century, number theory was considered the purest branch of mathematics, with no direct applications to the real world. The advent of digital computers and digital communications revealed that number theory could provide unexpected answers to real-world problems. At the same time, improvements in computer technology enabled number theorists to make remarkable advances in factoring large numbers, determining primes, testing conjectures, and solving numerical problems once considered out of reach. In 1974, Donald Knuth said "...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations". Elementary number theory is taught in discrete mathematics courses for computer scientists; on the other hand, number theory also has applications to the continuous in numerical analysis. As well as the well-known applications to cryptography, there are also applications to many other areas of mathematics.

REFERENCE

- David M.Burton, *Elementary Number Theory*-Seventh Edition, McGraw-Hill, Newyork, 2012.
- Adams.W and L.Goldstein, *Introduction to Number Theory ,* Englewood Cliffs , N.J Prentice-Hal,1976
- Nathanson , Melvyn . *Elementary Methods in Number Theory.* York:Springer-Verlag , New York.2000.
- Welsh, Dominic. *Codes and Cryptography,* Oxford University Press. New York,1988.