Number theory ①

Symbols and Notations

N	Natural Numbers
Z, I	Integers
Q	Rational Numbers
R	Real Numbers
C	Complex Numbers
p	prime number
$a \mid b$	a divides b
$a \nmid b$	a doesnot divide b
$a^k \mid b$ but $a^{k+1} \nmid b$	$a^k \| b$
$[x]$	Integer part (greatest integer $\leq x$)
$\{x\} = x - [x]$	Fractional part
$\lvert x \rvert$	Absolute value of x
ϕ	Euler ϕ-function
μ	Mobius μ-function
τ, d	* Numbers of positive divisors • divisor function
σ	Sum of positive divisors
$\pi(x)$	Number of primes $\leq x$
WOP	well ordering principle
WLOG	without loss of generality
(a, b)	gcd of a, b
$[a, b]$	LCM of a, b
$(a_1, a_2, \ldots, a_n)$	GCD of a_i

Section-I

Number Theory is The Queen of Mathematics

Numbers theory may briefly be defined as the study of the properties of integers. We shall find it convenient to classify the set of integers into the following subsets

positive integers	$1, 2, 3, \ldots$
Negative integers	$-1, -2, -3, \ldots$
Non Negative	$0, 1, 2, 3, \ldots$
nonzero integers	$\pm 1, \pm 2, \pm 3, \ldots$

★ Number Theory (Books) By

(1) Apostol
(2) Ivan Niven
(3) Andrew Adler
(4) Thomas Koshy
(5) S.B. Malik
(6) S.G. Telang
(7) David Burton
(8) W. J. Leveque
9) Harry Pollard
10) M.B. Nathanson
11) E.P. Armendariz

②

$[b_1, b_2, \dots b_n]$	LCM of a_i
$N(\alpha)$	Norm of α
F_n	nth Fermat number
M_n	n^{th} Mersenne numbers
p_n	nth prime
$a \equiv b \pmod m$	a congruent to b modulo m
$a \not\equiv b \pmod m$	a not congruent to b modulo m
$\det A$	determinant of a square matrix
$Q[x]$	set of polynomials in x with rational coefficients
$Z[x]$	set of polynomials in x with integral coefficients
$GL(n, F)$	General linear Group
$SL(n, F)$	Special linear Group
$\left(\frac{a}{p}\right)$ or (a/p)	Legendre Symbol
$\left(\frac{a}{b}\right)$ or (a/b)	Jacobi Symbal
$p(n)$	Number of partitions of n

(4)

★ If $d|n$ then n/d is called the divisor conjugate to d.

Remark (1) 0 is divisible by every integer b

because $0 = b \times 0$

(2) If b divides a then $-b$ also divides a

because $a = bq \Rightarrow a = (-b)(-q)$

It is therefore enough if we consider positive divisors of an integer only. Thus whenever we speak of divisors ~~in this book~~ we mean positive divisors unless stated otherwise.

Example (1) 1 and 29 are the only divisors of 29

(2) 1, 2, 3, 4, 6, 9, 12, 18, 36 are all divisors of 36

(S.G. Telang P84)

Theorem: If b divides a, then every divisor of b divides a ~~$b|a$ and $c|b \Rightarrow c|a$~~

Proof: b divides a. Therefore $a = bq_1$ for some integer q_1

Let c be divisor of b, Then $b = cq_2$ for some integer q_2

~~Then we have~~

It follows that $a = bq_1 = cq_1q_2 = c(q_1q_2)$

That shows c divides a

(S.G. Telang P84)

Theorem: Let a be positive integer. If an integer b divides a then b is not numerically greater than a.

Proof: b divides a Therefore $a = bq$ where $|q| \geq 1$

Hence $a = |a| = |b||q| \geq |b|$

(3)

Preliminaries

Well ordering Principle (WOP)

Every non empty subset S of non-negative integers contains a least or smallest element

i.e, S contains an integer n such that $n \leq x$ for all x in S

Archemedian property

For any two positive integers a and b there exists an integer n necessarily positive such that $na \geq b$

Definition (Multiple): Let a be any given integer and q an arbitrary integer. Then the number aq is called multiple of a

e.g $3 \times 4 = 12$ Therefore 12 is a multiple of 3

$(-7) \times (-5) = 35$ $\therefore$ 35 is a multiple of -7

Definition (Divisibility)

An integer a is said to be divisible by an integer $b \neq 0$ if $a = bq$ for some integer q.

The statement a is divisible by b can be written in any of the following alternate forms.

(1) b divides a

(2) b is divisor of a (5) b is factor of a

(3) $b \mid a$

(4) a is multiple of b

(5)

Tom M. Apostol Pg 14

Theorem Divisibility has the following properties:

(a) $a|a$ (Reflexive property)

(b) $a|b$ and $b|c$ implies $a|c$ (Transitive property)

(c) $d|a$ and $d|b$ implies $d|ax+by$ (Linearity property)

(d) $b|a$ implies $bd|ad$ (multiplication property)

(e) $bd|ad$ and $d \neq 0$ implies $b|a$ (Cancellation law)

(f) $1|a$ (1 divides every integer)

(g) $a|0$ (every integer divides 0)

(h) $b|a$ and $|a| \neq 0$ implies $|b| \leq |a|$ (Th) (Comparison property)

(i) $a|b$ and $b|a$ implies $|a| = |b|$ or $a = \pm b$

(j) $a|b$ and $c|d$ implies $ac|bd$

(k) $a|b_i$ for $i = 1, 2, \ldots, n$, then

$a|(b_1x_1 + b_2x_2 + \cdots + b_nx_n)$

for all integers $x_1, x_2, \ldots, x_n$

(6)

Proof (a) $a|a$ because $a = 1 \times a$

(b) Let $a|b$ and $b|c$ Then

$b = aq_1$ and $c = bq_2$

$\Rightarrow \quad c = aq_1q_2$

$\Rightarrow \quad a|c$

(c) $d|a$ and $d|b$

$a = rd$ and $b = sd$

$ax = rxd$ and $by = syd$

$ax + by = (rx + sy)d$

$d \mid ax + by$

(d) $b|a \Rightarrow a = bq$

$ad = (bd)q$

$\Rightarrow bd|ad$

(e) $a|b$ and $b|a$

$b = aq_1$ and $a = bq_2$

$b = aq_1$

$b = bq_1q_2$

$q_1q_2 = 1 \Rightarrow$ either $q_1 = q_2 = 1$ or $q_1 = q_2 = -1$

$\rightarrow a = \pm b$

(7)

(j) $a|b$ and $c|d$

$b = aq_1$, $d = cq_2$

$bd = ac(q_1 q_2)$

$ac|bd$

(k) $a|b_i$

$b_i = aq_i$

$b_1 = aq_1$ $\quad b_1 x_1 = a x_1 q_1$

$b_2 = aq_2$ $\quad b_2 x_2 = a x_2 q_2$

$\cdots$ $\quad \cdots$

$b_n = aq_n$ $\quad b_n x_n = a x_n q_n$

$b_1 x_1 + \cdots + b_n x_n = a(x_1 q_1 + \cdots + x_n q_n)$

$a \mid (b_1 x_1 + \cdots + b_n x_n)$

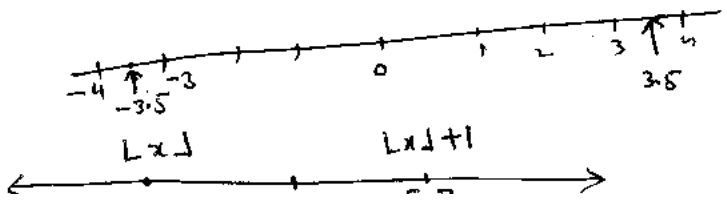
$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{otherwise} \end{cases}$$

The Floor function of a real number x, denoted by $\lfloor x \rfloor$, is the greatest integer $\leq x$. * Also called greatest integer function

The ceiling function of a real number x, denoted by $\lceil x \rceil$, is the least integer $\geq x$. * Also called least integer function

$\lfloor \pi \rfloor = 3$ $\quad \lfloor -3.5 \rfloor = -4$

$\lfloor 3.5 \rfloor = 3$



(8)

The Division Algorithm (Thomas Koshy Pg 65)

The division algorithm is a fine application of the well-ordering principle and is often employed to check the correctness of a division problem.

Suppose an integer a is divided by a positive integer b. Then we get a unique quotient q and a unique remainder r, where the remainder satisfies the condition $0 \le r < b$; a is the dividend and b the divisor.

$$b \overline{)a} \quad \begin{matrix} q \\ bq \\ \hline r \end{matrix}$$

$$\text{dividend} \quad a = bq + r \quad \text{remainder}$$

divisor, quotient

~~where $0 \le r < b$~~

Theorem (The division algorithm)

Let a be any integer and b a positive integer. Then there exist unique integers q and r such that

$$a = bq + r \quad \text{where} \quad 0 \le r < b$$

Proof: The proof consists of two parts. First, we must establish the existence of the integers q and r; and then we must show they are indeed unique.

Part 1. (Existence)

consider the set $S = \{ a - bn \mid n \in \mathbb{Z} \text{ and } a - bn \ge 0 \}$

clearly $S \subseteq W$ (The set of whole numbers)

we shall show that S contains a least element

first we will show that S is non-empty subset of W

WLOG we can suppose that $b \in Z^+$

Case 1. Suppose $a \geq 0$. Then $a = a - b.0 \in S$. So S contains an element.

Case 2. Suppose $a < 0$. Then since $b \in Z^+$, $b \geq 1$

Then $ba \leq a$

$-ba \geq -a$

$a - ba \geq 0$ Consequently $a - ba \in S$

In both cases S contains at least one element, so S is non empty subset of W. Therefore, by the well-ordering principle, S contains a least element r.

Since $r \in S$, an integer q exists such that

$$r = a - bq, \text{ where } r \geq 0$$

To show that $r < b$

we will prove this by ~~induction~~ Contradiction. Assume $r \geq b$

Then $r - b \geq 0$ But $r - b = a - bq - b = a - b(q+1)$

Since $a - b(q+1)$ is of the form $a - bn$ and

$a - b(q+1) \geq 0$ so $a - b(q+1) \in S$

That is $r - b \in S$ since $b > 0$, $r - b < r$

Thus $r - b$ is smaller than r is in S. This contradiction our choice of r, so $r < b$

Thus there are two integers q and r such that

$$a = bq + r, \text{ where } 0 \leq r < b$$

(2) Uniqueness

Assume there are integers q, q', r, r' such that

$a = bq + r$ and $a = bq' + r'$ where $0 \leq r < b$ and $0 \leq r' < b$

Assume for convenience that $q \geq q'$. Then

$$r' - r = b(q - q')$$

Because $q \geq q' \Rightarrow q - q' \geq 0$ and hence $r' - r \geq 0$

But, because $r' < b$ and $r < b$, $r' - r < b$

(10)

Suppose $q > q'$; that is $q - q' > 1$. Then $b(q-q') > b$ that is $r' - r > b$

This is a contradiction because $r' - r < b$

Therefore $q \neq q'$; Thus $q = q'$ and hence $r = r'$

Thus the integers q and r are unique.

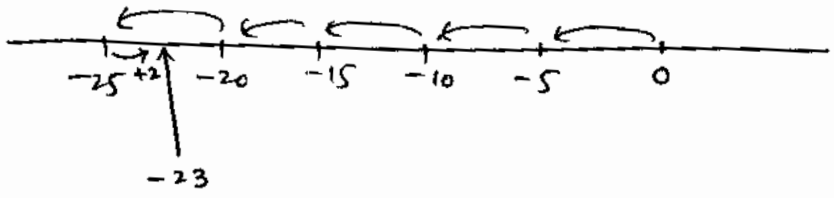
Example Find quotient and remainder when

① 207 is divided by 15

$207 = 15(13) + 12 \qquad q = 13, r = 12$

② -23 is divided by 5

$-23 = 5(-5) + 2 \quad , q = -5, r = 2$



Note: ① Although the above theorem has been traditionally called the division algorithm, it does present an algorithm for finding q and r. They can be found using the familiar long division method.

② The Equation $a = bq + r \; ; \quad 0 \leq r < b$

Can be written as

$$\frac{a}{b} = q + \frac{r}{b} \; ; \quad 0 \leq \frac{r}{b} < 1$$

Then $q = \lfloor a/b \rfloor$ and $r = a - bq = a - b\lfloor a/b \rfloor$

(11)

Div and mod operators Thomas Koshy Pg 67

a div b = quotient when a is divided by b

a mod b = remainder when a is divided by b

$\lfloor 23/5 \rfloor$

$23 \text{ div } 5 = 4 = q$

$23 \text{ mod } 5 = 3 = r$

$-23 \text{ div } 5 = \lfloor -23/5 \rfloor = -5$

$-23 \text{ mod } 5 = 2$

Thomas Koshy Pg 67

Theorem: Let a and b be any positive integers. Then the number of positive integers $\le a$ and divisible by b is $\lfloor a/b \rfloor$

Proof: Suppose there are k positive integers $\le a$ and divisible by b. We need to show that $k = \lfloor a/b \rfloor$.

The positive multiples of b less than or equal to a are

$$b, 2b, \ldots, kb$$

clearly $kb \le a$ and $(k+1)b > a$

$$\therefore \quad k \le \frac{a}{b} \quad \text{and} \quad k+1 > \frac{a}{b}$$

$$\therefore \quad \frac{a}{b} - 1 < k \le \frac{a}{b}$$

Thus k is the largest integer less than or equal to a/b

So $k = \lfloor a/b \rfloor$

(12)

Example: The positive integers ≤ 100 divisible by 13 are $\lfloor 100/13 \rfloor = \lfloor 7.69 \rfloor = 7$

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

Inclusion – Exclusion Principle Thomas Koshy [72]

Let $A_1, A_2, \ldots, A_n$ be n finite sets then

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k < n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} \left|\bigcap_{i=1}^{n} A_i\right|$$

Ex 2.3 Thomas Koshy [73]

Find the number of positive integers ≤ 2076, and divisible by neither 4 nor 5.

$A = \{x \in N \mid x \leq 2076 \text{ and divisible by } 4\}$

$B = \{x \in N \mid x \leq 2076 \text{ and divisible by } 5\}$

Then

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$= \lfloor 2076/4 \rfloor + \lfloor 2076/5 \rfloor - \lfloor 2076/20 \rfloor$$

$$= 519 + 415 - 103 = 831$$

$$|A \cup B|^c = 2076 - 831 = 1245$$

(13)

Example Thomas Koshy [73]

Find the number of positive integers ≤ 3000 and divisible by 3, 5 or 7

$A = \{x \in N \mid x \leq 300 \text{ and divisible by } 3\}$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

$$= \lfloor 3000/3 \rfloor + \lfloor 3000/5 \rfloor + \lfloor 3000/7 \rfloor - \lfloor 3000/3\times5 \rfloor$$

$$- \lfloor 3000/7\times5 \rfloor - \lfloor 3000/3\times7 \rfloor + \lfloor 3000/3\times5\times7 \rfloor$$

$$= 1000 + 600 + 428 - 200 - 85 - 142 + 28$$

$$= 1629$$

---

(14)

Basic Representation Theorem

Decimal expansion

Example $234 = 2.10^2 + 3.10^1 + 4.10^0$

$23.45 = 2.10^1 + 3.10^0 + 4.10^{-1} + 5.10^{-2}$

2	9
2	4 – 1
2	2 – 0
	1 – 0

Binary expansion

$(1001)_2 = 1.2^3 + 0.2^2 + 0.2^1 + 1.2^0 = 9$

Binary Base = 2
octal Base = 8
Decimal Base = 10
hexa decimal Base = 16

Theorem 2.9 Thomas koshy Pg 77 / SB Malik Pg 9

Let $b \geq 2$ be positive integer, Then every positive integer N can be expressed uniquely in the form

$$N = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$, where $a_0, a_1, \ldots, a_k$ are non negative integer less than b, $a_k \neq 0$, and $k \geq 0$

Proof: (Existence) case i) if $N < b$, Then $N \to$ representation $0 \leq N < b$ is the unique
case ii) $N = b$ Then $N = 1.b + 0$ is unique representation
case iii) $N > b$

Apply the division algorithm with N as dividend and b as divisor:

$$N = bq_0 + a_0 \; ; \quad 0 \leq a_0 < b$$

if $q_0 < b$ Then the representation is unique

if $q_0 \geq b$ Then by division algorithm

$$q_0 = bq_1 + a_1 \; ; \quad 0 \leq a_1 < b$$

Substitute for q_0:

$$N = b(bq_1 + a_1) + a_0 \; ;$$

$$N = q_1 b^2 + a_1 b + a_0 \; ; \quad 0 \leq a_0, a_1 < b$$

if $q_1 < b$ Then the representation is unique

(15)

If $q_1 \geq b$ then again by division algorithm

$$q_1 = bq_2 + a_2 \quad ; \quad 0 \leq a_2 < b$$

Substituting for q_1

$$N = (bq_2 + a_2)b^2 + a_1 b + a_0$$

$$N = q_2 b^3 + a_2 b^2 + a_1 b + a_0$$

and so on, consequently we have

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

or equivalently

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

where $0 \leq a_i < b$ for every i

Also $a_k \neq 0$ and $a_k = q_{k-1}$. Thus N has the desired expansion

(Uniqueness)

Suppose N has two expansions:

$$N = \sum_0^k a_i b^i = \sum_0^k c_i b^i \quad \text{where } 0 \leq a_i, c_i < b$$

(WOLG we can assume both expansions contain same numbers of terms, since we can always add enough zero coefficients to yield the same number of terms.)

Subtracting one expansion from the other

$$\sum_{i=0}^k (a_i - c_i) b^i = 0 \quad \text{let } d_i = a_i - c_i$$

$$\sum_{i=0}^k d_i b^i = 0 \quad \text{If } d_i = 0 \text{ then } a_i = c_i \text{ for every } i,$$

So the two expansions are the same

If the expansion are dist. (16) inct, There must be a smallest integer j, wh $0 \le j \le k$, such that $d_i \neq 0$. Then $\sum_{i=j}^{k} d_i b^i = 0$

Factor out b^j: $b^j\left(\sum_{i=j}^{k} d_i b^{i-j}\right) = 0$

Cancel b^j: $\left(\sum_{i=j}^{k} d_i b^{i-j}\right) = 0$

This yields $d_j + b\left(\sum_{i=j+1}^{k} d_i b^{i-j-1}\right) = 0$

$$b\left(\sum_{j+1}^{k} d_i b^{i-j-1}\right) = -d_j$$

Thus $b \mid d_j$. But, since $0 \le a_i, c_i < b$

That is $-b \le a_i - c_i < b$

$-b \le d < b$

$\therefore$, since $b \mid d_j$, $d_j = 0$, which contradiction our assumption that $d_j \neq 0$.

Thus Two expansions are the same, establishing the uniqueness of the expansion.

(17)

Greatest common divisors GCD

Let a and b be any two integers at least one of which is non-zero. Then their GCD is a positive integer d such that

(i) $d|a$ and $d|b$

(ii) If $c|a$ and $c|b$, then $d \geq c$

gcd of a, b is denoted by (a,b) or $\gcd(a,b)$

Ex 1) $\gcd(a,a) = a \; ; \; a \neq 0$

2) If $a|b$ then $(a,b) = a$

$(-8,36) = 4$

$(15,35) = 5$

Theorem: S B. Malik (17)

Proof:- Let a and b be any two integers at least one of which is non zero. Then (a,b) exists and is unique.

Existence: observe that $(a,b) = (|a|, |b|)$. Thus we can suppose that both a and b are positive. we also suppose $a \geq b$ (The case $a \leq b$ is symmetric) By division algorithm

(1) $\longrightarrow a = bq_1 + r_1 \; ; \; 0 \leq r_1 < b$

If $r_1 = 0$ Then $b|a$ and $(a,b) = b$ and we are done in this case

Suppose $r_1 \neq 0$ one again by division algorithm applied to b and r_1

(2) $\longrightarrow b = r_1 q_2 + r_2 \; ; \; 0 \leq r_2 < r_1$

If $r_2 = 0$, Then $r_1 | b$ and from (1)

$a = r_1 q_2 q_1 + r_1 \Rightarrow r_1 | a$

(18)

Let $s|a$ and $s|b$ then $s|r_1 = a - bq_1$

$\Rightarrow \quad r_1 = (a, b)$

Suppose $r_2 \neq 0$ we repeat the process. This process must terminate in finite numbers of steps, say n, thus we shall arrive at zero remainder after the nth step and have a sequence of integers r_i such that

$$b > r_1 > r_2 \ldots \geq 0, \quad r_{n-2} = r_{n-1} q_n + r_n \quad \forall\, n \geq 3$$

and $r_{n-1} = q_{n+1} r_n$.

This last expression gives $r_n | r_{n-1}$ therefore

$$r_n | r_{n-2}, \ldots \quad r_n | b \quad \text{and} \quad r_n | a$$

If 's' were a common divisor of a and b then

$s|a$ and $s|b \Rightarrow s|r_1$ by (1)

$$s|r_2, \ldots, s|r_n$$

Hence $r_n = (a, b)$ showing gcd of a and b exists

Uniqueness: If d_1 and d_2 are two gcds of a and b

Then by (2) of the definition

$$d_1 \geq d_2 \text{ and } d_2 \geq d_1 \Rightarrow d_1 = d_2$$

Example Find $(256, 1166)$

$1166 = 4 \cdot 256 + 142$

$256 = 1 \cdot 142 + 114$

$142 = 1 \cdot 114 + 28$

$114 = 4 \cdot 28 + 2$

$28 = 14 \cdot 2$

we have

$(256, 1162) = 2$

(19)

$$2 = (256, 116)$$
$$= 114 - 4.28$$
$$= 114 - 4.(142 - 1.114)$$
$$= 5(114) - 4(142)$$
$$= 5(256 - 1.42) - 4(142)$$
$$= 5.256 - 9(142)$$
$$= 5.256 - 9(1166 - 4.256)$$
$$= 14(256) - 9(1166)$$
$$2 = 256x + 116y$$
$$x = 41, \quad y = -9$$

2 is linear combination of 256 and 116

Remark: A prime number is usually denoted by p and the nth prime by p_n. e.g $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... and so on.

Def: A composite number is one which has atleast one divisor except 1 and the number itself.

TH: Let 'p' be a prime and 'a' be any given integer. Then either $(a,p) = 1$ or 'a' is a multiple of p (or p divides a).

PROOF: Since p is a prime it has two divisors 1 and p. It follows that $(a,p) = 1$ or $(a,p) = p$

If $(a,p) = 1$, then theorem is proved.

If $(a,p) = p$, then p obviously divides a which means a is a multiple of p. (or p divides a).

Alternative:

Case: If $p \mid a$ (or a is a multiple of p) Then there is nothing to prove.

Case: If $p \nmid a$. we will show $(a,p) = 1$

Suppose $(a,p) = d$ imply

$d \mid a$ and $d \mid p$.

Since p is prime, so either $d = 1$ or $d = p$

If $d = p$, then $p \mid a$ which is a contradiction to the fact that $p \nmid a$.

Hence $d = 1$. Thus $(a,p) = 1$ which complete the proof.

TH: The smallest divisor (other than 1) of a composite number is a prime.

PROOF: Let a be any given composite number then a has atleast one divisor other than 1 and 'a'. This implies that it has a smallest divisor. Let this be d. If d is composite then d has a divisor d_1 other than 1 and d. Hence d_1 is less than d and d_1 divides a. ($\because d_1 \mid d$ & $d \mid a$) This obviously contradicts our supposition that d is the smallest divisor of a. Hence d cannot be composite. This means d is a prime.

Corollary: Every integer $n > 1$ has a prime divisor

PROOF: If n is prime, then n is itself a prime divisor.

If n is composite. then it has a least positive divisor d which is prime. Suppose d is least composite divisor. Then $d = d_1 d_2$; $\because d_1, d_2 < d$ If $d \mid n$ this implies $d_1 \mid n$ & $d_1 < d$, a contradiction that d is the least divisor of n. Hence d is not composite. it is prime.

TH If P is a prime number and $P \mid ab$. Then either $P \mid a$ or $P \mid b$.

PROOF: If $P \mid a$, then nothing to prove.

If $P \nmid a$, then $(a, P) = 1$

Since $(a, P) = 1$, so there exist integers x and y s.t

$$ax + Py = 1$$

or $$abx + Pby = b. \quad \text{—(i)}$$

But $P \mid ab$ (given)

$$\Rightarrow P \mid abx \quad \text{—(ii)}$$

Also $P \mid Pb$

$$\Rightarrow P \mid Pby \quad \text{—(iii)}$$

(ii) & (iii) imply

$$P \mid abx + Pby = b \quad \text{using (i)}$$

$$\Rightarrow P \mid b$$

That is if $P \nmid a$, then $P \mid b$

Which complete the proof.

4

TH: If a prime p divides the product $a_1 \cdot a_2 \cdot a_3 \cdots a_k$. Then p divides atleast one of the integers $a_1, a_2, \cdots, a_k$.

PROOF: Let us assume that p does not divide any of the numbers $a_1, a_2, \cdots, a_k$. Then p is relatively prime to each of these numbers. That is

$$(p, a_1) = 1 \ , (p, a_2) = 1 \ , \cdots, (p, a_k) = 1$$

which clearly asserts,

$$(p, a_1 a_2 a_3 \cdots a_k) = 1$$

which is shows that $a_1 a_2 a_3 \cdots a_k$ is not a multiple of p. That is

$p \nmid a_1 a_2 \cdots a_k$. a contradiction to the fact that p divides $a_1 a_2 \cdots a_k$. Hence our supposition is untenable. this implies that p divides atleast one of $a_1, a_2, \cdots, a_k$.

Alternative: we prove this theorem by induction.

For $k = 2$. we know

If $p \mid a_1 a_2$. Then either $p \mid a$ or $p \mid b$

Thus statement is true.

Now Suppose that statement is true for $k = m$.

Now Let $p \mid a_1 \cdot a_2 \cdots a_m \cdot a_{m+1}$

then again

$$P \mid (a_1 \cdot a_2 \cdots a_m)(a_{m+1})$$

$\Rightarrow$ either $P \mid a_1 \cdot a_2 \cdots a_m$ or $P \mid a_{m+1}$

i.e $P \mid a_i$ for $1 \le i \le m+1$.

Hence by mathematical induction, it is true for all positive integers, which complete the proof.

Corollary 1: If a prime $P \mid a^K$, then $P \mid a$.

Corollary 2: If P is a prime and $P \mid P_1 \cdot P_2 \cdots P_K$ where $P_1, P_2, \cdots, P_K$ are all prime numbers. Then $P = P_i$ for some i ; $1 \le i \le K$.

Euclid's theorem: There exist infinitely many primes.

PROOF: Suppose that there exist only a finite number of primes namely $P_1, P_2, \cdots P_K$ in ascending order. Let $N = P_1 \cdot P_2 \cdot P_3 \cdots P_K + 1$ It is obvious $N > P_K$. If N is a prime then there is nothing to prove as $N > P_K$. on the other hand if N is composite then it is not divisible by $P_1, P_2, \cdots P_K$ because such a division leaves 1 as the remainder. Hence N being composite, must be divisible by a prime greater then P_K. Thus in either case there exist

a prime greater then P_k. But this contradicts our assumption that there are only a finite number of primes. Therefore our assumption is untenable. It follows that there are infinitely many primes. 6

Fundamental Theorem of Arithmatic (FTA)

STATEMENT: Every positive integer can be expressed as a product of primes. Apart from the order in which prime factors occur in the product, they are unique. i.e for an integer $n>1$, $n = P_1 P_2 \cdots P_r$ and $n = q_1 q_2 \cdots q_s$ then $r = s$ and after renaming $P_i = q_i \; \forall i$.

OR Every Composite number can be expressed as the product of prime factors in one way only.

PROOF: Let $n>1$ be an integer. If n is prime, we are done. Suppose n is not a prime. then n is ~~not~~ divisible by a prime say $P_1 \Rightarrow n = n_1 P_1$ for some integer n_1. If n_1 is a prime, we are done again, otherwise n_1 is divisible by a prime say P_2. $\Rightarrow n_1 = n_2 P_2$ for some integer n_2.

$$\Rightarrow n = n_1 P_1$$
$$\Rightarrow n = n_2 P_2 P_1$$

If n_2 is a prime, we are done. But if not

then we can continue this process. Since a given integer can have only finite number of divisors, in a finite number of steps and the smallest divisor of a number is a prime. We must get n as a product of primes. Next for uniqueness.

Suppose that $n = p_1 p_2 \cdots p_r$ and also $n = q_1 q_2 \cdots q_s$; $p_i, q_i, \forall i$ are primes.

Suppose (if possible) $r < s$.

Since $p_1 \mid n$ & $n = q_1 q_2 \cdots q_s$ imply there exist atleast one integer q_i for some i such that $p_1 \mid q_i$ but p_1 and q_i are both primes. Hence $p_1 = q_i$ we take $i = 1$ after rearranging the q_i's therefore $p_1 = q_1$. Then

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

$$\Rightarrow \quad p_2 \cdot p_3 \cdots p_r = q_2 \cdot q_3 \cdots q_s$$

We continue above process until all p_i's are cancelled as $r < s$. we must have

$$1 = q_{r+1} \cdot q_{r+2} \cdots q_s$$

which is a contradiction as all q_i's are primes (and their product can never be equal to one).

Hence $r \geq s$ — (1)

Similarly if we assume

$r > s$, we have after cancelation

$$p_{s+1} \cdot p_{s+2} \cdots p_r = 1$$

Again a contradiction as all p_i's are prime numbers.

Hence $r \not> s$

$\Rightarrow r \leq s$ — (2)

(1) & (2) imply

$r = s$ and

$\forall i \quad p_i = q_i$ which completes the uniqueness.

e.g $24 = 2 \times 12$

$= 2 \times 2 \times 6$

$= 2 \times 2 \times 2 \times 3$

$= 2^3 \times 3$

$= 3 \times 2^3$

Also $72 = 2^3 \times 3^2$

$= 3^2 \times 2^3$.

Remark: In last two examples ?

$$24 = 2^3 \times 3^1$$
$$72 = 2^3 \times 3^2$$

are called decomposition of 24 & 72.
Similarly if in the decomposition of any N (Integer) there is repetition of some or all of the prime divisors, we can write it in the form

$$N = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_K^{\alpha_K} \quad \text{——— (1)}$$

where $P_1 < P_2 \cdots < P_K$ and (1) is then also written in the form

$$N = \prod_{i=1}^{K} P_i^{\alpha_i}$$

The decomposition (1) is called the "Standard or Canonical decomposition of N."
Thus fundamental theorem of arithmatic can also be stated in the following alternate form.

Statement: Every integer $n > 1$ can be expressed uniquely in the form

$$n = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_K^{\alpha_K}$$ where $P_1, P_2 \cdots P_K$ are primes such that $P_1 < P_2 \cdots < P_K$ and $\alpha_1, \alpha_2 \cdots \alpha_K$ are positive integers. This theorem is also called the "Unique factorization theorem."

10

THEOREM: The representation of a composite number as a product of primes is unique.

PROOF: Let us assume that theorem is not true. This implies that there exist integers which have two representation or more. Let N be the smallest among them (i.e any integer less then N has unique representation). Then

$$N = p_1 \cdot p_2 \cdot p_3 \cdots p_K = q_1 \cdot q_2 \cdots q_s \quad \text{---} (1)$$

where the p's and q's are some primes such that $p_1 < p_2 < p_3 \cdots < p_K$

Obviously no p is equal to any q, otherwise we could cancel the common factor from both sides of (1). The result would be that a smaller integer than N could have two representations thus contradicting our assumption that N is the smallest among such integers. Therefore without loss of generality we may take $p_1 > q_1$.

Now, consider the integer

$$n = N - q_1 \cdot p_2 \cdot p_3 \cdots p_K \longrightarrow (2)$$

$$= p_1 \cdot p_2 \cdots p_K - q_1 \cdot p_2 \cdots p_K \quad \text{using (1)}$$

$$n = (p_1 - q_1)\, p_2 \cdot p_3 \cdots p_K \longrightarrow (3)$$

Obviously $P_1 - q_1 < P_1 < N$ 11

Hence $P_1 - q_1$ has only one representation

We may then write $P_1 - q_1$ uniquely as the product of primes as follows

$$P_1 - q_1 = t_1 \cdot t_2 \cdots t_m \; ; \; t_1, t_2, \cdots t_m \text{ are primes.}$$

Then from (3), we have

$$n = t_1 \cdot t_2 \cdots t_m \cdot P_2 \cdot P_3 \cdots P_K \longrightarrow (4)$$

Now $n < N$ as $t_1 \cdot t_2 \cdots t_m < P_1$

Therefore it has only one representation namely (4) above. But we know from (1) & (2) that q_1 is one of the primes $t_1, t_2, \cdots, t_m, P_2, P_3, \cdots, P_K$ (For (1) q_1 is not P_1 & $q_1 \mid N = P_1 \cdot P_2 \cdots P_K \Rightarrow q_1$ is $P_2, P_3, \cdots$ or P_K

For (2) $q_1 \mid N$ & $q_1 \mid q_1 P_2 \cdots P_K$.

i.e $q_1 \mid n = t_1 \cdot t_2 \cdots t_m \cdot P_2 \cdot P_3 \cdots P_K$.

Now if q_1 is not any of $P_2, P_3, \cdots, P_K$ then clearly it is one of the $t_1, t_2, \cdots t_n$

This however is impossible for the following reasons.

(i) We have already proved above that no P equals any q.

(ii) If q_1 equals any of the primes $t_1, t_2 \cdots$

then q_i would divide 12

$t_1 t_2 \cdots t_m = p_1 - q_1$, which is impossible.

therefor our assumption at the beginning of the proof is untenable. Hence theorem is true.

Remark: We can exclude 1 from set of prime numbers.

Let $p_1, p_2, \ldots, p_k$ be distinct prime factors of n and suppose that they occur $\alpha_1, \alpha_2, \ldots, \alpha_k$ times $\alpha_i \geq 1$

then $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ ——— (1)

If 1 is a prime number.

then (1) can be written as

$$n = 1^s p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
$$= 1^t p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
$$= 1^r p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad s \neq t \neq r.$$

which shows that factorization is not unique. Hence 1 is not prime.

Example 1: Let $E = \{2, 4, 6, \cdots\}$

Suppose an integer is a prime if it cannot be written as a product two or more even integers.

13

e.g 6, 10, 14, 18, ... are all primes of E. Now

$$60 = 10 \cdot 6 = 2 \cdot 30$$

& $$120 = 10 \cdot 6 \cdot 2 = 2^2 \cdot 30$$

Where 6, 10, 30 are primes on E.

Hence factorization is not unique.

Example: Let S be the set of all possitive integers of the form $3K+1$ i.e $S = \{1, 4, 7, 10, \dots\}$

Suppose an integer of S is prime if it cannot be written as a product of smaller integers. Thus 4, 7, 10, 13, ... all are primes of S.

Now $$3(333)+1 = 1000 = 4 \cdot 25 \cdot 10 = (10)^3$$

& $$3(33)+1 = 400 = 4 \cdot 10^2 = 4^2 \cdot 25$$

Which shows that factorization is not unique.

14

THEOREM:
Let N be not divisible by any prime $P \leq \sqrt{N}$.
then N is a prime number.

PROOF: Assume that N is not a prime then by its canonical decomposition

$$N = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_k^{\alpha_k} \geq P_1 \cdot P_2.$$

imply $P_1 \mid N$ & $P_2 \mid N$

Hence $P_1 > \sqrt{N}$ & $P_2 > \sqrt{N}$

because N is not divisible by any $P \leq \sqrt{N}$.

Hence $N \geq P_1 \cdot P_2$

$> \sqrt{N} \cdot \sqrt{N}$

$\Rightarrow N > N$ which is impossible.

It follows that N is a prime.

Corollary: If N is composite then the smallest prime divisor of N is $\leq \sqrt{N}$.

Proof: First we will show that smalles divisor of N is $\leq \sqrt{N}$.

If N is composite, it has a factor x with $1 < x < N$.

Hence $N = xy$ where both x & y are positive integers greater than 1.

15

Suppose $x \nleq \sqrt{N}$ & $y \nleq \sqrt{N}$

Then $x > \sqrt{N}$ & $y > \sqrt{N}$

$\Rightarrow N = xy > \sqrt{N} \cdot \sqrt{N} = N$

$\Rightarrow N > N$, impossible.

Hence either $x \leq \sqrt{N}$ or $y \leq \sqrt{N}$.

which shows that smallest positive divisor of N is $\leq \sqrt{N}$.

Next, we claim that it is prime. because it is either prime or by Fundamental theorem of arithmatic has a prime divisor. Thus in either case, N has a prime divisor less than or equal to $\sqrt{n}$.

Example: Find by trial whether 503 is a prime.

Sol The primes $\leq \sqrt{503}$ are 2, 3, 5, 7 11, 17 & 19. None of these primes divides 503. Hence 503 is a prime

Example Find by trial whether 101 is prime

primes $\leq \sqrt{101}$, 2, 3, 5 & 7. Hence 101 is a prime num.

16

Proposition:

For each positive integer n, there exist n consecutive numbers each one of which is composite.

PROOF:

Consider the sequence of consecutive integers

$(n+1)!+2, (n+1)!+3, \cdots, (n+1)!+(n+1)$

containing n integers. We claim that none of these integers is a prime.

Now for any K ; $2 \leq K \leq n+1$.

$$(n+1)! + K$$
$$= 1 \cdot 2 \cdot 3 \cdots K \cdot \overline{K+1} \cdots n \cdot \overline{n+1} + K$$
$$= K\left(1 \cdot 2 \cdot 3 \cdots \overline{K-1} \cdot \overline{K+1} \cdots n \cdot \overline{n+1} + 1\right)$$

Which is clearly composite.

Hence, above all n consecutive integers are composite.

Example put $n = 5$

$6!+2, 6!+3, 6!+4, 6!+5, 6!+6$

$722, 723, 724, 725, 726$

are five consecutive composite integers.

Exercise: 1

Show that non of the following $n-1$ consecutive numbers are prime.

Solution: $n!+2, \cdots, n!+n \quad n \neq 1$

We know that

$$n!+2 = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 + 2.$$
$$n!+3 = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 + 3$$
$$\vdots$$
$$n!+n = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 + n$$

Clearly, above all integers are divisible by $2, 3, 4, \cdots, n$ respectively. Which is a contradiction against the definition of prime number. Hence non of the given numbers is prime.

Remark

Let $f(n) = n^2+n+41 \; ; n = 0, 1, 2, \cdots, 3$ gives prime numbers.

But $f(40) = (41)^2$ & $f(41) = 41\cdot 43$ which are not prime. Notice that, we have no formula to have all prime numbers, mathematically. But there is a theoretical formula that will only give primes.

Sieve of Eratosthenes

18

First write down all integers from 2 to n. 2 is the first integer in the table, and is obviously a prime. we retain it and Strike out all larger multiples of 2. Next, we retain 3 and Strike out all larger multiples of 3. We continue this process of cancelling the multiple of primes except Prime itself until the largest prime q such that $q \leq \sqrt{n}$ The remaining integers will give the list of prime between 1 and n.

Example: List all primes ≤ 50.

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	
19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	
~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	
~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~	41	~~42~~	
43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~	

19

Twin Primes:

If n is composite and $n \pm 1$ are primes, then these are called twin primes.

e.g

n	$n-1$	$n+1$
4	3	5
6	5	7
12	11	13

Hence 3, 5 w.r.t 4
5, 7 w.r.t 6
11, 13 w.r.t 12 are twin primes.

Prime triplet: If P is a prime number and $P+2$, $P+4$ are primes, then $(P, P+2, P+4)$ is called prime triplet. The only prime triplet is $(3, 5, 7)$

Powerful integer:
An integer n is called powerful if whenever a prime $p \mid n$, then also $p^2 \mid n$.

e.g 4, 8, 9, ...

Square free integer: An integer is called square free if it is not divisible by any perfect square. e.g 2, 3, 5, 6, 7, 10, ...

20

REMARK:

① If P and $P+2$ are twin primes then
(i) $P(P+2)+1$ is a perfect square.
(ii) 12 divide $P+(P+2)$ whenever $P>3$.

② A prime number greater than 2 can be represented as $4n-1$ or $4n+1$.
(or $4n-1+4 = 4n+3$).

③ A prime number greater than 3 can be represented as $6n-1$ or $6n+1$
(OR $6n+5 = 6n-1+6$ or $6n+1$)

PROOF: ① → (ii)

Since $P>3$, P is either $6n-1$ or $6n+1$.

Now $P + P+2 = 6n-1+6n+1$
$= 12n$

Hence 12 divide $P+P+2$.

Lemma: If a & b are integers of the form $4n+1$. Then ab is also of the form $4n+1$.

Proof: Let $a = 4r+1$ & $b = 4s+1$; r,s are integers

then $ab = (4r+1)(4s+1)$
$= 4(4rs+r+s)+1$
$= 4m+1$, as required.

21

THEOREM:
There are infinitely many primes of the form $4K+1$

PROOF: Assume that there are only n primes of the form $4K+3$, namely $P_1, P_2, \cdots, P_n$, in ascending order. It follows that the remaining primes, if any, are of the form $4K+1$. Consider the integer

$$N = 4P_1 \cdot P_2 \cdots P_n - 1 \quad \text{——} (1)$$

~~Consider the integer~~
Obviously N is of the form $4K+3$ because $N = 4(P_1 \cdot P_2 \cdots P_n - 1) + 3$
Now if N is a prime then it is a prime greater than P_n, which complete the proof. On the otherhand if N is composite it cannot be the product of the form $4K+1$ because the product of two integers $4s+1$ & $4t+1$ is of the form $4K+1$. Hence N must have atleast one prime factor of the form $4K+3$. But this prime factor cannot be one of $P_1, P_2, \cdots, P_n$, because of 1 above. (because $P_1, P_2, \cdots P_n$ does not divide N). Therefore it must be a prime greater than P_n. Thus in either case there exi a prime of the form $4K+3$ greater than P_n. But this contradicts our assumption. Therefore the theorem is true.

THEOREM: There are infinitely many primes of the form $6k+5$ (Assignment) 29

THEOREM: $\sqrt{2}$ is not a rational number.

PROOF: Suppose $\sqrt{2}$ is a rational number and $\sqrt{2} = \frac{a}{b}$ where a, b are positive integers with $(a,b) = 1$. ——— (1*)

$$\sqrt{2} = \frac{a}{b} \quad \text{——} (1^{**})$$

$$\Rightarrow 2b^2 = a^2$$

$$\Rightarrow b \mid a^2 \quad \text{——} (1)$$

Let $b > 1$, then by FTA 'b' has a prime divisor, (say) P.

then $P \mid b$ & $b \mid a^2$ by (1)

$\Rightarrow P \mid a^2 = a \cdot a$

Since P is prime, so

$P \mid a$ (If $P \mid a^k$, then $P \mid a$)

Since $P \mid a$ & $P \mid b$

Therefore $(a,b) \geq P$

$\Rightarrow 1 \geq P$ using (1*)

a contradiction as P is prime.

Hence $b \neq 1$

only possibility $b = 1$ put in (1**)

23

$\frac{a}{1} = \sqrt{2}$

$a = \sqrt{2}$.

this is not possible since a is positive integer.

Hence our supposition ($\sqrt{2}$ is rational) is wrong. which complete the proof.

Problem:

A number n is composite iff there exist non-negative integers p & q such that $n = p^2 - q^2$; $p - q > 1$

Solution: Suppose $n = p^2 - q^2$; $p - q > 1$

To show that n is composite, it is sufficient to show that n is the product of integers greater than one.

now $n = (p^2 - q^2)$

$= (p-q)(p+q)$

since $p - q > 1$

therefore $p + q > 1$

Hence $n = (p-q) \cdot (p+q)$; $p \pm q > 1$

thus n is composite.

Conversely, suppose that n is composite

then $n = rs$; $r > 1$ & $s > 1$

(i) ~~If $r = s$, then n is a perfect square~~

~~so is composite~~ ~~$r \neq s \neq 1$~~

24

(ii) If $r \neq s$.

Then $n = rs$

$= \left(\frac{r+s}{2}\right)^2 - \left(\frac{r-s}{2}\right)^2$

Take $\frac{r+s}{2} = p$ & $\frac{r-s}{2} = q$.

Thus $n = p^2 - q^2$

Moreover

$p - q = \frac{r+s}{2} - \frac{r-s}{2}$

$p - q = \frac{2s}{2} = s > 1$

Hence $p - q > 1$, which is required.

Problem:

If a prime p divide $a^2 + b^2$ & p divide a, then p divide b.

Sol Since $p \mid a^2 + b^2$

$\Rightarrow a^2 + b^2 = rp$ —① for some integer

Also $p \mid a$

$\Rightarrow a = ps$ —② for some integer

put ② in ①

$p^2 s^2 + b^2 = rp$

$\Rightarrow b^2 = p(r - ps^2)$

$\Rightarrow p \mid b^2$

But p is prime

Hence $p \mid b$ which is required

85

Mersenn Number: (French 1588–1645)

The numbers of the form $M_n = 2^n - 1 ; n > 1$ are called Mersenne numbers. If M_n is prime for some n then it is called Mersenne prime. e.g

n:	2	3	4	5	6	7	8	9	10	11
$2^n - 1$:	3	7	15	31	63	127	255	511	1023	2047

Notice that Mersenne are always odd. Moreover if M_n is prime then n is prime. But converse may not be true.

e.g If $n = 11$ then $M_n = 2047$
$= 23 \times 89$.
which is composite.

THEOREM:
Let $f(n) = a^n - 1$, $n > 1$ then $f(n)$ is prime only if $a = 2$ and n is prime.

PROOF: Let $a^n - 1$ be prime.
If $a = 1$ then $a^n - 1 = 0$, not prime (contradiction against $a^n - 1$ is prime)
If $a > 2$. Then $a^n - 1$ is divisible by $a - 1$. ($\because a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + 1)$
but the only positive divisors of

$a^n - 1$ are 1 & $a^n - 1$, Contradiction, ∴ It follows that $a = 2$.
This proves the first part of the theorem.
Now, Let n be composite, then

$$n = n_1 \cdot n_2 \; ; \; n_1 > 1 \; \& \; n_2 > 1.$$

Hence $a^n - 1 = a^{n_1 \cdot n_2} - 1$

$$= (a^{n_1})^{n_2} - 1$$

which is divisible by $a^{n_1} - 1$ where $a = a$
But this contradicts the assumption that $a^n - 1$ is prime. Therefore n is a prime number.

*Corollary: If $2^n - 1$ is a prime then n is prime.
OR If M_n is Mersenne prime then n is prime.

Proof: First, we will show if $a^n - 1 \; ; \; n > 1$ is prime then $a = 2$.
Suppose $a^n - 1$ is prime then it has 1 & $a^n - 1$ as its positive divisors. Also either $a - 1$ divides $a^n - 1$.
So either $a - 1 = 1$ or $a^n - 1 = a - 1$
But $a - 1 \neq a^n - 1$ as $n > 1$.

27

Hence $a-1=1$

$\Rightarrow a=2.$

Thus $M_n = 2^n - 1.$

On contrary, suppose that n is composite. then

$n = n_1 \cdot n_2 \; ; \; n_1 > 1 \; \& \; n_2 > 1.$

then

$$2^n - 1 = 2^{n_1 \cdot n_2} - 1$$
$$= (2^{n_1})^{n_2} - 1$$
$$= (2^{n_1} - 1)\left[2^{n_1(n_2-1)} + \cdots + 1\right]$$

$\Rightarrow 2^{n_1} - 1 \mid 2^n - 1$, contradiction.

Hence n is prime.

H.M KHALID MAHMOOD

28

Observation: (MARCH 1992)

$$6 = 2(2^2 - 1)$$
$$28 = 2^2(2^3 - 1)$$
$$496 = 2^4(2^5 - 1)$$
$$8128 = 2^6(2^7 - 1)$$
$$33550336 = 2^{12}(2^{13} - 1)$$

(32 perfect number have introduced by March in 1992).

2^2-1, 2^3-1, 2^5-1, 2^7-1, $2^{13}-1$ are primes.

THEOREM: If $2^n - 1$ is prime then $2^{n-1}(2^n - 1)$ is perfect.

Proof: Suppose $2^n - 1$ is prime and let $2^n - 1 = P$

then $2^n = P + 1$ —— (1)

Now $2^{n-1}(2^n - 1) = 2^{n-1} \cdot P$

then the positive divisors of $2^{n-1} \cdot P$ are $1, 2, 2^2, \cdots, 2^{n-1}, P, 2P, 2^2P, \cdots, 2^{n-1} \cdot P$

Sum of divisors

$$= 1 + 2 + 2^2 + \cdots + 2^{n-1} + P(1 + 2 + \cdots 2^{n-1})$$
$$= (1 + 2 + 2^2 + \cdots + 2^{n-1})(1 + P)$$

29

$$= \frac{1 \cdot (2^n - 1)}{2-1} (1+P)$$

$$= (2^n - 1)\, 2^n \quad \text{using (1)}$$

$$= 2^n (2^n - 1)$$

$$= 2\, 2^{n-1} (2^n - 1)$$

Hence by def of perfect number $2^{n-1}(2^n - 1)$ is perfect. which compt the proof.

Fermat number:

A number of the form $F_n = 2^{2^n} + 1$ where $n = 0, 1, 2 \cdots$ is called Fermat number.

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 25$

Observe that Fermat numbers are always odd.

THEOREM: Any two Fermat numbers a relatively prime.

PROOF: Let F_m and F_n be Ferma number. let $(F_m, F_n) = d$; then $m = n + r$ ... for som and d is odd.

30

Consider

$$\frac{F_m - 2}{F_n} = \frac{2^{2^m} + 1 - 2}{2^{2^n} + 1}$$

$$= \frac{2^{2^m} - 1}{2^{2^n} + 1}$$

$$= \frac{2^{2^{n+r}} - 1}{2^{2^n} + 1}$$

$$= \frac{(2^{2^n})^{2^r} - 1}{2^{2^n} + 1}$$

$$= \frac{a^{2^r} - 1}{a + 1} \quad \text{where } a = 2^{2^n}$$

Note

$$\frac{F_m - 2}{F_n} = a^{2^r - 1} - a^{2^r - 2} + \cdots - 1, \text{ which is an integer.}$$

Hence $F_n \mid F_m - 2$

(⇒ [illegible])

$\Rightarrow d \mid F_m - 2$ and $d \mid F_n$

$\Rightarrow d \mid 2$ But d is odd.

which is a contradiction.
Thus only possibility that $d = 1$
which complete the proof.

31

THEOREM: The product of the first n Fermat numbers is $2^{2^n} - 1$

PROOF: We know

$$F_0 = 2^{2^0} + 1 = 3$$

$$F_1 = 2^{2^1} + 1 = 5$$

$$F_0 \cdot F_1 = 3 \cdot 5$$

$$= 15$$

$$= 16 - 1$$

$$= 2^{2^2} - 1$$

Statement is true for $n = 2$.

Suppose that statement is true for $n = K$

i.e $F_0 \cdot F_1 \cdots F_{K-1} = 2^{2^K} - 1$

Hence $(F_0 \cdot F_1 \cdots F_{K-1}) \cdot F_K$

$$= (2^{2^K} - 1)(2^{2^K} + 1)$$

$$= \left(2^{2^K}\right)^2 - (1)^2$$

$$= 2^{2^{K+1}} - 1$$

Thus Statement is true for $n = K+1$.
Hence by induction theorem is true.

31

THEOREM:
The product of the first n Fermat numbers is $2^{2^n} - 1$

PROOF: We know

$$F_0 = 2^{2^0} + 1 = 3$$
$$F_1 = 2^{2^1} + 1 = 5$$
$$F_0 \cdot F_1 = 3 \cdot 5$$
$$= 15$$
$$= 16 - 1$$
$$= 2^{2^2} - 1$$

Statement is true for $n = 2$.

Suppose that statement is true for n
i.e $F_0 \cdot F_1 \cdots F_{K-1} = 2^{2^K} - 1$

Hence $(F_0 \cdot F_1 \cdots F_{K-1}) \cdot F_K$
$$= (2^{2^K} - 1)(2^{2^K} + 1)$$
$$= (2^{2^K})^2 - (1)^2$$
$$= 2^{2^{K+1}} - 1$$

This statement is true for $n = K+1$
Hence by induction theorem is true

THEOREM: (i) For each $m > 0$ 32

$$F_{m+1} = F_0 \cdot F_1 \cdot F_2 \cdots F_m + 2$$

(ii) $F_n \mid F_m - 2$ if $m > n$

(iii) $(F_m, F_n) = 1$ for each $m \neq n$

PROOF: Let $m = 1$, then

$$F_0 \cdot F_1 + 2$$

$$= (2^{2^0}+1)(2^{2^1}+1) + 2$$

$$= 3 \cdot 5 + 2$$

$$= 17$$

$$= 16 + 1 = 2^{2^2} + 1 = F_2$$

i.e $F_2 = F_0 \cdot F_1 + 2$

Statement is true for $m = 1$

Next suppose this statement is true for $m = K-1$

i.e $F_{K-1} + 1 = F_0 \cdot F_1 \cdots F_{K-1} + 2$

or $F_K = F_0 \cdot F_1 \cdots F_{K-1} + 2$ —— (1)

Consider $F_{K+1} = 2^{2^{K+1}} + 1$

$$= (2^{2^K})^2 + 1$$

$$= (F_K - 1)^2 + 1 \quad \because F_K = 2^{2^K} + 1$$
$$\therefore F_K - 1 = 2^{2^K}$$

$$= F_K^2 - 2F_K + 2.$$

DIVISION ALGORITHM:

Statement: 34

Let a and b be any two integers, $b>0$ then there exist unique integers q and r such that

$$a = bq + r \; ; \; 0 \le r < b.$$

Proof: Let S be the set of integers defined as

$$S = \{a - bt : t \in I\}$$

i.e $S = \{\ldots, a-b(-1), a, a-b, \ldots\}$

Obs: $a \in S$ is either negative or positive.

If $a < 0$, then $a - ba = a(1-b) \ge 0 \left(\because \begin{matrix} b>0 \\ \Rightarrow b \ge 1 \end{matrix}\right)$

Thus S has atleast one non-negative element. This implies that S has one least non-negative element. Let this be $a - bq$ for some integer q.

Then $0 \le a - bq$ — (1)

It means every element less then $a-bq$ is negative.

Then $a - b(q+1) < 0$

or $a < b(q+1)$

or $a - bq < b$ — (2)

(1) & (2) $\Rightarrow$ $0 \le a - bq < b$ — (3)

Let $r = a - bq$, then (3) imply $0 \le r < b$.

Also $a = bq + a - bq$

$a = bq + r \; ; \; 0 \le r < b.$

which complete first part. 35

Uniqueness: Suppose integers q & r are not unique.

then there exist integers q_1 & r_1 such that

$$a = bq_1 + r_1 \quad ; \quad 0 \le r_1 < b \quad \text{---} (1)^*$$

Also $a = bq + r \quad ; \quad 0 \le r < b. \quad \text{---} (2)^*$

both imply

$$r_1 - r = b(q_1 - q) \quad \text{---} (3)^*$$

$$\Rightarrow b \mid |r_1 - r|$$

But $r_1 < b$ & $r < b \Rightarrow |r_1 - r| < b$

this only possibility

$|r_1 - r| = 0 \iff r_1 = r$ put in $(3)^*$

$q_1 = q$

which complete the uniqueness.

Remark: bq is the largest multiple of b which does not exceed a.

Example let $a = 47$, $b = 7$

(i) $47 = 7(6) + 5 \; ; \; 0 < 5 < 7$

Also 42 is the largest multiple of 7 which does not exceed 47.

(ii) $a = -73$, $b = 19$

$-73 = 19(-4) + 3 \; ; 0 < 3 < 19.$

Observation: 36

$$5694 = 5\times10^3 + 6\times10^2 + 9\times10 + 4 \quad \text{---(1)}$$

b.c. $P(x) = 5x^3 + 6x^2 + 9x + 4$

then $P(10) = 5694$

Hence 5694 is the value of the polynomial $P(x) = 5x^3+6x^2+9x+4$ at $x=10$

(1) is known as decimal notation or the name of the form $5\times10^3+\cdots+4$ is 5694

In this notation if a number N such that

$$N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

then $N = a_k a_{k-1} a_{k-2} \cdots a_1 a_0$

where $0 \le a_0, a_1, \cdots, a_k \le 9$ & $a_k \neq 0$

Here $a_0, a_1, \cdots a_k$ are called the digits of the number and 10 is called the base (or radix) of the number.

Now if b is the base, then

$$N = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

where $a_k \neq 0$ & $0 \le a_0, a_1, \cdots, a_k \le b-1$

then $N = (a_k a_{k-1} \cdots a_1 a_0)_b$

37

Basic Representation (or Radix Representation) Theorem.

Statement: Let $b > 1$. Then every positive integer n has a unique representation in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

(b-adic expansion of n) $0 \le a_i \le b-1$; $0 \le i \le k$, $a_k \neq 0$

PROOF:

Case(i) If $n < b$ then n $0 \le n < b$ is the unique representation

Case(ii) If $n = b$

Then $n = 1 \cdot b + 0$ is the unique representation.

Case(iii) If $n > b$, then by division algorithm

$$n = q_1 b + a_0 \quad , \quad 0 \le a_0 < b \quad \text{---(1)}$$

If $q_1 < b$ then take

$q_1 = a_1$ imply

$n = a_1 b + a_0$ is the unique representation.

Suppose $q_1 \geq b$, then by division algorithm 38

$$q_1 = q_2 b + a_1 \quad 0 \leq a_1 < b \quad \text{---(2)}$$

This process is continued till we obtain $q_K < b$ and then process is stopped

Thus, we have

$$q_1 = q_2 b + a_2 \quad \text{---(3)}$$

$$q_3 = q_4 b + a_3 \quad \text{---(4)}$$

$$\vdots$$

$$q_{K-1} = q_K b + a_{K-1} \quad \text{---(K)}$$

where $0 \leq q_K < b$.

Now from equations (2) to K

$$\begin{aligned} n &= q_1 b + a_0 \\ &= (q_2 b + a_1) b + a_0 \\ &= q_2 b^2 + a_1 b + a_0 \\ &= (q_3 b + a_2) b^2 + a_1 b + a_0 \\ &= q_3 b^3 + a_2 b^2 + a_1 b + a_0 \\ &\vdots \\ &= q_K b^K + a_{K-1} b^{K-1} + \cdots + a_1 b + a_0 \end{aligned}$$

Put $a_K = q_K$ 39

Then

$$n = a_K b^K + a_{K-1} b^{K-1} + \cdots + a_1 b + a_0$$

which is required representation.

The above representation is true and unique by the successive application of division algorithm therefore the quotients and remainders in equations (1) to (K) are unique. It follows that the representation is unique.

Alternative Suppose on contrary

$$n = t_K b^K + t_K b^{K-1} + \cdots + t_1 b + t_0$$

$$0 \le t_i \le b-1 \; ; \; 0 \le i \le K$$

$$t_K \neq 0$$

Then

$$(a_K - t_K) b^K + (a_{K-1} - t_{K-1}) b^{K-1} + \cdots + (a_i - t_i) b^i = 0$$

$$b > 1 \; \& \; i \le K.$$

Then

$$(a_i - t_i) \frac{b^{i+1}}{b} = -\left[(a_K - t_K) b^K + \cdots + (a_{i+1} - t_{i+1}) b^{i+1} \right]$$

$$a_i - t_i = -b \left[(a_K - t_K) b^{K-i-1} + \cdots + (a_{i+1} - t_{i+1}) \right]$$

$\Rightarrow a_i - t_i \mid b$ but $a_i < b$ & $t_i < b$

So only possibility $a_i - b_i = 0 \quad \forall i$

$\Rightarrow a_i = b_i \quad \forall i$

which completes the uniqueness.

Example: Convert 4385 to the base 9.

$4385 = 487(9) + 2$

$487 = 54(9) + 1$

$54 = 6(9) + 0$

Last quotient is $6 < 9 \quad (q_k < b)$

Hence $4385 = (6012)_9$

Example Express 5163 in the notation of base 12.

Sol The remainders of 12 are

$0, 1, 2, \ldots, 9, t, \epsilon$ where $t = 10, \epsilon = 11$

Then $5163 = (430)12 + 3$

$430 = (35)12 + t$

$35 = 2(12) + \epsilon$

Hence $5163 = (2\epsilon t3)_{12}$

41

Example In base 12 name the integers $1, 2, \ldots, 9, \alpha = 10, \beta = 11$.

Evaluate $(9179) \times (\beta 370)$

Sol

$$\begin{array}{r} \beta\ 3\ 7\ 0 \\ 9\ 1\ 7\ 9 \\ \hline 8\ 5\ 8\ 3\ 0 \\ 1\ \alpha\ 7\ 2\ 0 \\ \beta\ 3\ 7\ 0 \\ 1\ \alpha\ 7\ 9\ 0 \\ \hline 1\ \beta\ 9\ 0\ 7\ \alpha\ 3\ 0 \end{array}$$

1 carry

Thus $(\beta 370) \times (9179) = (1\beta 907\alpha 30)_{12}$

Alternative

$$(9179)_{12} = 9 \times 12^3 + 1 \times 12^2 + 7 \times 12 + 9$$
$$= 3633$$

Also

$$(\beta 370)_{12} = \beta \times 12^3 + 9 \times 12^2 + 7 \times 12 + 0$$
$$= 19594$$

$(3633)(1954) = 7093069_{12}$ $42 =$

12	7093069_{12}	Remainders
	5910891	0
	499574	3
	41647	α
	3470	7
	295	0
	23	9
	1	β

Here $1 < 12$.

Thus

$(2139) \times (\beta 370)$

$= (1\beta 907\alpha 30)_{12}$.

Example: Find $(256, 1166)$. Also write gcd as a linear combination of 256 & 1166. 48

Sol

$$1166 = 4 \cdot 256 + 142$$
$$256 = 1 \cdot 142 + 114$$
$$142 = 1 \cdot 114 + 28$$
$$114 = 4 \cdot 28 + 2$$
$$28 = 14 \cdot 2$$

Hence $(256, 1166) = 2$.

For linear combination

$$\begin{aligned} 2 &= (256, 1166) \\ &= 114 - 4 \cdot 28 \\ &= 114 - 4(142 - 1 \cdot 114) \\ &= 114 - 4 \cdot 142 + 4 \cdot 114 \\ &= 5 \cdot 114 - 4 \cdot 142 \\ &= -4 \cdot 142 + 5 \cdot 114 \\ &= -4 \cdot 142 + 5(256 - 1 \cdot 142) \\ &= -4 \cdot 142 + 5 \cdot 256 - 5 \cdot 142 \\ &= -9 \cdot 142 + 5 \cdot 256 \\ &= 5 \cdot 256 - 9 \cdot 142 \\ &= 5 \cdot 256 - 9(1166 - 4 \cdot 256) \\ &= 5 \cdot 256 - 9 \cdot 1166 + 36 \cdot 256 \\ &= 41 \cdot 256 - 9 \cdot 1166 \end{aligned}$$

or $2 = 41(256) + (-9)(1166)$

Thus $2 = 256x + 1166y$

where $x = 41$ & $y = -9$.

i.e 2 is a linear combination of 256 & 1166.

Assignment:

Find gcd(1106, 497) and express it as a linear combination of 1106 & 49

Ans $x = -31$, $y = 69$.

Exercise: Find the gcd of 48, 72, 30 & 27.

Now $(48, 72) = 24$

$(24, 30) = 6$

$(6, 27) = 3$

Hence $(48, 72, 72, 30) = 3$.

Assignments:

Express the following gcd's as a linear combination of given integers.

(i) $(952, 580)$ Ans $x = -23$, $y = 10$

(ii) $(952, 576)$ Ans $x = 7$, $y = -3$

THEOREM: The gcd of positive integers a and b exists. Further it can be written in the form $ax + by$ for some integers x & y.

PROOF: Let S be the set of all positive integers of the form $ma + mb$. Let $d = ax + by$ be the least element of S. We will show that $d = (a, b)$.

Since d is the least element of S and $a \in S$, Hence $d \leq a$

then by division algorithm

$$a = qd + r \quad \text{---} (1)$$ for some integers q & r provided $0 \le r < d$. So

$a = q(ax+by) + r$

$\Rightarrow r = (1-qx)a + (-y)b$

$\Rightarrow r \in S$ but $r < d$

So only possibility $r = 0$ put in (1)

$a = qd$

$\Rightarrow d \mid a$.

Similarly $d \mid b$ (when $d \le b$)

If c is any divisor of both a and b then $c \mid d$ because $d = ax+by$

Hence $(a,b) = d$

$d = ax+by$ for some integers x and y.

Remark: For integers a & b at least one of which is non-zero. Then $\gcd(a,b)$ is the least positive integer of the set $\{ax+by : x,y \in Z\}$ and all other elements are multiple of (a,b).

e.g. $(4,6) = 2$

$\{4x+6y : x,y \in Z\} = \{\dots, 0, -10, -16, -22, \dots, 4, 10, 16, \dots\}$

51

THEOREM: Let K be any integer and a, b any integers atleast one of which is non-zero, then $(Ka, Kb) = |K|(a, b)$

Proof: Let $d = (a, b)$ & $t = (Ka, Kb)$

It is enough to take K as positive since $(a, b) = (|a|, |b|)$

Since $d = (a, b)$, there exist integers u & v such that

$$d = ua + bv$$

$$dK = u(Ka) + b(Kv)$$

$$dK = t \cdot r \quad \because u(Ka) + b(Ku) \text{ is a multiple of } (Ka, Kb)$$

$$\Rightarrow t \mid dK \quad \text{---(i)}$$

Also $d \mid a$ & $d \mid b$

$$\Rightarrow dK \mid Ka \text{ & } dK \mid Kb$$

~~$\Rightarrow dK \mid Ka + Kb$~~

which shows that dK is the common divisor of Ka & Kb.

Hence $dK \mid t$ ---(ii) as $t = (Ka, Kb)$

(i) & (ii) imply

$$t = dK$$

$$t = Kd$$

$$(Ka, Kb) = K(a, b)$$

If $d = (a,b)$, then

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

5

OR Given non-zero integers a and b $\frac{a}{\gcd(a,b)}$ and $\frac{b}{\gcd(a,b)}$ are Co-prime.

i-e $$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$$

PROOF:

Since $d = (a,b)$

So $\frac{a}{d}$ & $\frac{b}{d}$ are both integers

Also

$$\begin{aligned} d &= (a,b) \\ &= \left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) \\ &= |d| \left(\frac{a}{d}, \frac{b}{d}\right) \\ &= d\left(\frac{a}{d}, \frac{b}{d}\right) \end{aligned}$$

$$\Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

OR

$$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1.$$

Lemma: If $a = bq + c$, then
$\gcd(a,b) = \gcd(b,c)$; OR
Every divisor of a and b is a divisor of b and c and conversely.

Corollary: If $a|c$ and $b|c$ and $(a,b)=1$ then $ab|c$. Conclusion is false if $(a,b)\neq 1$

Proof: Let $a|c$ & $b|c$

Then $c = ar$ & $c = bs$ for some integers r & s.

Also $(a,b) = 1$, then there exist integers x & y such that

$$ax + by = 1$$
$$\Rightarrow acx + bcy = c$$
$$cax + cby = c$$
$$bsax + arby = c$$
$$ab(sx + ry) = c$$
$$\Rightarrow ab|c.$$

Example

$a = 2, b = 4, c = 12$
$(a,b) = 2 \neq 1$
$a|c$, $b|c$
but $ab \nmid c$.

Euclid's Lemma: If $a|bc$ and $(a,b)=1$ then $a|c$.

Proof: As $(a,b) = 1$, $\exists$ integers x & y such that $ax + by = 1$

$$\Rightarrow acx + bcy = c.$$

Given $a|bc$, Also $a|ac$

Hence $a|c$.

54

THEOREM: Let a and b be two integers greater then 1 such that

$$a = \prod_{i=1}^{r} p_i^{m_i}, \quad b = \prod_{i=1}^{r} p_i^{l_i}$$

If $n_i = \text{Min}(m_i, l_i)$ $\forall i$

& $M_i = \text{Max}(m_i, l_i)$ $\forall i$

Then $(a,b) = \prod_{i=1}^{r} p_i^{n_i}$

and $[a,b] = \prod_{i=1}^{r} p_i^{M_i}$

PROOF: We observe that

(i) $\prod_{i=1}^{r} p_i^{n_i} > 0$ because p_i $\forall i$ are primes and $n_i \geq 0$ $\forall i$.

(ii) Since $n_i = \text{Min}(m_i, l_i)$

so $n_i \leq m_i$ & $n_i \leq l_i$

Thus $p_i^{n_i} \mid p_i^{m_i}$ & $p_i^{n_i} \mid p_i^{l_i}$

$\Rightarrow \prod_{i=1}^{r} p_i^{n_i} \mid \prod_{i=1}^{r} p_i^{m_i}$ & $\prod_{i=1}^{r} p_i^{n_i} \mid \prod_{i=1}^{r} p_i^{l_i}$

or $\prod_{i=1}^{r} p_i^{n_i} \mid a$ & $\prod_{i=1}^{r} p_i^{n_i} \mid b$ $\forall i = 1,2,\ldots,r$ ——— (1)

(iii) Let $c = \prod_{i=1}^{r} p_i^{t_i}$; $t_i \geq 0$ $\forall i$ ($t_i \leq m_i, l_i$)

be a common divisor of a & b.

i-e $c \mid a$ and $c \mid b$

then $t_i \le \min(m_i, l_i) \quad \forall i$ 55

$t_i \le n_i \quad \forall i$

$\Rightarrow p_i^{t_i} \mid p_i^{n_i} \quad \forall i$

$\Rightarrow \prod_{i=1}^{r} p_i^{t_i} \mid \prod_{i=1}^{r} p_i^{n_i}$

$\Rightarrow c \mid \prod_{i=1}^{r} p_i^{n_i}$ —— (2)

(1) & (2) clearly show that

$$(a,b) = \prod_{i=1}^{r} p_i^{n_i} \quad \text{where } n_i = \min(m_i, l_i) \ \forall i$$

LEAST COMMON MULTIPLE:

Let $a, b \in \mathbb{Z}$ such that $ab \neq 0$, then an integer d is called least common multiple if it satisfy the following properties

(i) $d > 0$

(ii) $a \mid d$ and $b \mid d$

(iii) If c is any integer such that $a \mid c$ and $b \mid c$.

then $d \mid c$.

It is denoted by lcm or $[a,b]$.

56

THEOREM: The least common multiple is unique

PROOF:

Suppose that M and M' be the lcm's of a and b.

Then $a \mid M$ & $b \mid M$ Also M' is the l.c.m

Then $M' \mid M$ — (1)

Similarly $M \mid M'$ — (2)

(1) & (2) imply ~~Hence~~ $M = M'$.

PROOF (ii) THEOREM Page 54

(i) clearly $\prod_{i=1}^{r} p_i^{M_i} > 0$ because each p_i for each i is prime and $M_i \geq 0 \; \forall i$.

(ii) Since $M_i = \max(m_i, l_i)$

$\Rightarrow m_i \leq M_i$ & $l_i \leq M_i \; \forall i$.

$\Rightarrow p_i^{m_i} \mid p_i^{M_i}$ & $p_i^{l_i} \mid p_i^{M_i}$

$\Rightarrow \prod_{i=1}^{r} p_i^{m_i} \mid \prod_{i=1}^{r} p_i^{M_i}$ & $\prod_{i=1}^{r} p_i^{l_i} \mid \prod_{i=1}^{r} p_i^{M_i}$

or $a \mid \prod_{i=1}^{r} p_i^{M_i}$ & $b \mid \prod_{i=1}^{r} p_i^{M_i}$

Second condition is satisfied.

(iii) If m is an integer such that a/m & b/m, then by taking

$$m = \prod_{i=1}^{r} p_i^{\beta_i},$$

since a/m and b/m

then $\beta_i \geq \text{Max}(m_i, \ell_i) = M_i$

i.e $\beta_i \geq m_i$ & $\beta_i \geq \ell_i$ $\forall i$

$\Rightarrow p_i^{m_i} / p_i^{\beta_i}$ & $p_i^{\ell_i} / p_i^{\beta_i}$

$\Rightarrow \prod_{i=1}^{r} p_i^{m_i} /$

$\Rightarrow M_i \leq \beta_i \quad \forall\, i = 1, 2, \ldots, r$

$\Rightarrow p_i^{M_i} / p_i^{\beta_i} \quad \forall i$

$\Rightarrow \prod_{i=1}^{r} p_i^{M_i} / \prod_{i=1}^{r} p_i^{\beta_i} = m$

$\Rightarrow \prod_{i=1}^{r} p_i^{M_i} / m$

Hence by def

$$[a, b] = \prod_{i=1}^{r} p_i^{M_i} \quad \text{where } M_i = \text{Max}(m_i, \ell_i)$$

58

Example: $a = 24 = 2 \times 2 \times 2 \times 3$
$b = 18 = 2 \times 3 \times 3$
$a = 2^3 \times 3^1$
$b = 2^1 \times 3^2$

$(a,b) = 2^1 \cdot 3^1 = 6$

$[a,b] = 2^3 \times 3^2 = 72.$

Relation between g.c.d and l.c.m

THEOREM Let a and b be any two positive integers. Then $(a,b)[a,b] = ab$.

PROOF: Let $a = \prod_{i=1}^{n} p_i^{\alpha_i}$; $\alpha_i \geq 0$

& $b = \prod_{i=1}^{n} p_i^{\beta_i}$; $\beta_i \geq 0$

be the prime power factorization of a & b.

Let $M_i = \max(\alpha_i, \beta_i)$

$m_i = \min(\alpha_i, \beta_i)$ $\forall i$

Then $(a,b)[a,b] = \prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i)} \cdot \prod_{i=1}^{n} p_i^{\max(\alpha_i,\beta_i)}$

$= \prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i) + \max(\alpha_i,\beta_i)}$

$= \prod_{i=1}^{n} p_i^{\alpha_i+\beta_i} = \prod_{i=1}^{n} p_i^{\alpha_i} \cdot \prod_{i=1}^{n} p_i^{\beta_i}$

$= ab$

★ $\max(x,y) + \min(x,y) = x+y$

54

Corollary: If a and b are positive integers, then $[a,b] = ab \Leftrightarrow (a,b)=1$

Example: Find the l.c.m of 8, 10, 12, 15 and 26.

Sol
$$[8,10] = \frac{8\times 10}{(8,10)} = 40$$
$$[40,12] = \frac{40\times 12}{(40,12)} = 120$$
$$[120,15] = \frac{120\times 15}{(120,15)} = 120$$
$$[120,26] = \frac{120\times 26}{(120,26)} = 1560$$

Hence

$$[8,10,12,15,26] = 1560$$

Alternative:

$8 = 2^3 \cdot 3^0 \cdot 5^0 \cdot 13^0$
$10 = 2 \cdot 3^0 \cdot 5 \cdot 13^0$
$12 = 2^2 \cdot 3 \cdot 5^0 \cdot 13^0$
$15 = 2^0 \cdot 3 \cdot 5 \cdot 13^0$
$26 = 2 \cdot 3^0 \cdot 5^0 \cdot 13$

Now
$$\text{l.c.m} = 2^3 \cdot 3 \cdot 5 \cdot 13$$
$$= 1560$$

Linear Diophantine Equation (Diophantos c.275) 60

A linear equation $ax+by=c$ with $a\neq 0, b\neq 0$ and c are integers is called a linear Diopantine equation in two unknown x and y. A pair of integers x_0, y_0 is called a solution of $ax+by=c$ if $ax_0+by_0=c$

A given diophantine equation may have more than one solutions. For example

$x+7y=31$ is satisfied by

$x=24, y=1$; $x=3, y=4$ and $x=17, y=2$

On the contrary the diophantine equation $15x+151y=14$ has no solution.

THEOREM: Let $a(\neq 0)$, $b(\neq 0)$ and c be any three integers and $d=(a,b)$. The linear diophantine equation $ax+by=c$ has a solution iff $d \mid c$.

Further if x_0, y_0 is a particular solution of $ax+by=c$, then any other solution will be of the form $x'=x_0-\frac{b}{d}t$

and $y'=y_0+\frac{a}{d}t$; $t\in Z$.

PROOF: let $d=(a,b)$ and suppose

$ax+by=c$ — ① has a solution

61

that is there exist integers x_0 & y_0 such that $ax_0 + by_0 = c$. — (2)

But we know $ax_0 + by_0$ is a multiple of d. Hence $ax_0 + by_0 = rd$ for some $r \in$

put in (2)

$$rd = c$$

$$\Rightarrow d \mid c.$$

Conversely, suppose $d \mid c$

$$\Rightarrow c = dt \; ; \; t \in Z.$$

Also $d = (a, b)$

$$\Rightarrow d = au + bv \text{ for some } u, v \in Z.$$

$$\Rightarrow dt = aut + bvt$$

$$\Rightarrow c = a(ut) + b(vt) \text{ — } (1)^*$$

Let $ut = x_0$ & $vt = y_0$

Then $(1)^*$ gives

$$ax_0 + by_0 = c \quad ; \; x_0, y_0 \in Z.$$

Thus (x_0, y_0) is one solution of $ax + by = c$.

Let (x', y') be any other solution of $ax + by = c$, then

$$ax' + by' = c \text{ ——— } (i)$$

62

$\therefore$ Also $ax_0 + by_0 = c$ ——(ii)

(i) − (ii) imply $a(x' - x_0) + b(y' - y_0) = 0$

$\Rightarrow a(x' - x_0) = -b(y' - y_0)$ ——(iii)

Since $d = (a, b)$.

imply $d \mid a$ & $d \mid b$

$\Rightarrow a = rd$ & $b = sd$; $(r, s) = 1$

then (iii) become

$$rd(x' - x_0) = -sd(y' - y_0)$$

$\Rightarrow r(x' - x_0) = -s(y' - y_0)$ ——(iv)

$\Rightarrow r \mid -s(y' - y_0)$

$\Rightarrow r \mid y' - y_0$ $\because$ $(r, s) = 1$.

$\Rightarrow y' - y_0 = rt$ for some $t \in Z$ ——(v)

$y' = y_0 + rt$

$y' = y_0 + \frac{a}{d}t$

Also from equation (iv) & (v) imply

$r(x' - x_0) = -srt$

$\Rightarrow -st = x' - x_0$

$\Rightarrow$ ~~$-s t = x' - x_0$~~

$\Rightarrow \quad x' - x_0 = -bt$

or $\quad x' = x_0 - \frac{b}{d}t \quad ; t \in Z$

Thus any other solution (x', y') is of the form

$$x' = x_0 - \frac{b}{d}t$$
$$y' = y_0 + \frac{a}{d}t$$

Exp: Find the solution of $37x + 47y = 15$

Sol Since $(37, 47) = 1$ and $1 \mid 15$.

Hence solution exists.

By division algorithm

$$47 = 37 \times 1 + 10$$
$$37 = 3 \times 10 + 7$$
$$10 = 7 \times 1 + 3$$
$$7 = 3 \times 2 + 1$$

$$1 = 7 - 2 \times 3$$
$$= 7 - 2(10 - 7 \cdot 1)$$
$$= 3 \cdot 7 - 2 \cdot 10$$
$$= 3(37 - 3 \cdot 10) - 2 \cdot 10$$
$$= 3 \cdot 37 - 11 \cdot 10$$
$$= 3 \cdot 37 - 11(47 - 37 \cdot 1)$$
$$= 14 \cdot 37 - 11 \cdot 47$$
$$= 37(14) + 47(-11)$$

Hence $15 = 37(14 \cdot 15) + 47(-11 \cdot 15)$

$= 37(210) + 47(-165)$

CONGRUENCES: BY Gauss (1777-1855) Q. MATHEMATICS 68

Def: Let a and b be any two integers. If a positive integer m divides $a-b$ then we say that a is congruent to b mod m and (write as $a \equiv b \pmod{m}$ —— ①

Expression ① is called the congruence, m is called the modulus of the congruence, and b is called a residue of $a \pmod{m}$

Example: 11 divides $98-65$, so $98 \equiv 65 \pmod{11}$

65 is the residue of 98 modulo 11

THEOREM: The relation $\equiv$ for fixed m is an equivalence relation on the set of integers

PROOF:

(i) Since $m \mid 0$

$\Rightarrow m \mid a-a \quad ; a \in Z$

$\Rightarrow a \equiv a \pmod{m}$

That relation is reflexive.

(ii) Let $a \equiv b \pmod{m}$

then $m \mid a-b$

$\Rightarrow m \mid (-1)(a-b)$

That is $m \mid b-a$

$\Rightarrow b \equiv a \pmod{m}$

Relation is Symmetric.

Anti Symmetric ?

(iii) let $a \equiv b \pmod m$ & $b \equiv c \pmod m$; $a, b, c \in Z$ 6

Then $m \mid a-b$ & $m \mid b-c$

$\Rightarrow m \mid a-b+b-c$

$\Rightarrow m \mid a-c$

$\Rightarrow a \equiv c \pmod m$.

Relation is transitive.

Remark:

The equivalence classes of congruence modulo m partitions the integers into disjoint sets. If $m=3$,

$$[0] = \{a : a \equiv 0 \pmod 3\}$$
$$= \{a : a - 0 = 3k \text{ for some integer } k\}$$
$$= \{a : a = 3k ; k \in Z\}$$
$$= \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\} = A$$

$$[1] = \{a : a \equiv 1 \pmod 3\}$$
$$= \{a : a = 3k+1 ; k \in Z\}$$
$$= \{\cdots, -5, -2, 1, 4, 7, \cdots\} = B$$

$$[2] = \{a : a \equiv 2 \pmod 3\}$$
$$= \{a : a = 3k+2\}$$
$$= \{\cdots -7, -4, -1, 2, 5, 8, 11, \cdots\} = C$$

Here $A \cap B \cap C = \Phi$, $A \cap B = \Phi$, $A \cap C = \Phi$
$B \cap C = \Phi$ & $A \cup B \cup C = Z$.

Def: Let m be a positive integer. The set of all equivalence classes modulo m is denoted by $\mathbb{Z}_m$ and is called the set of integers modulo m.

For example, for $m = 3$, there are three equivalence classes for congruence modulo 3 so that the set $\mathbb{Z}_3 = \{[0], [1], [2]\}$ has three members.

THEOREM: Let a, b, c, d be integers and

$$a \equiv b \pmod{m} \quad \& \quad c \equiv d \pmod{m}$$

Then

(i) $a \pm c \equiv b \pm d \pmod{m}$

(ii) $ac \equiv bd \pmod{m}$

PROOF: Since $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m}$

$$\Rightarrow m \mid a-b \quad \& \quad m \mid c-d$$

$$\Rightarrow m \mid a-b+c-d$$

$$\Rightarrow m \mid (a+c)-(b+d)$$

$$\Rightarrow a+c \equiv b+d \pmod{m}$$

Similarly $a-c \equiv b+d \pmod{m}$

(ii) Since

$$m \mid a-b \quad \& \quad m \mid c-d$$

$$\Rightarrow m \mid (a-b)c \quad \& \quad m \mid (c-d)b$$

$$\Rightarrow m \mid (a-b)c + (c-d)b$$

$$\Rightarrow m \mid ac - bd$$

$$\Rightarrow ac \equiv bd \pmod{m}$$

THEOREM:

If $a \equiv b \bmod m$, then $a^n \equiv b^n \pmod m$ for all n, but if $a^n \equiv b^n \pmod m$ for $n \geq 2$, then $a \equiv b \bmod m$ may not be true.

PROOF:

Since $a \equiv b \bmod m$

$\Rightarrow m \mid a-b$

$\Rightarrow m \mid (a-b)(a^{n-1} + \dots + b^{n-1})$

$\Rightarrow m \mid a^n - b^n$

$\Rightarrow a^n \equiv b^n \pmod m$

COUNTER EXAMPLE:

Take $a=4, b=8, m=3$

then $a^2 \equiv b^2 \pmod m$

i.e $16 \equiv 64 \pmod 3$

i.e $3 \mid 16-64$ true.

But $a \not\equiv b \pmod 3$

as $3 \nmid 4-8$

which complete the proof.

79

THEOREM (Cancellation Law):

Let a, b, n be integers such that

$na \equiv nb \pmod{m}$ and $(m,n) = d$

Then $a \equiv b \pmod{\frac{m}{d}}$

PROOF: Since $(m,n) = d$, so there exist integers m_1 and n_1 such that

① — $\begin{cases} m = m_1 d \\ n = n_1 d \end{cases}$ & where $(m_1, n_1) = 1$.

Moreover $na \equiv nb \pmod{m}$

imply $m \mid na - nb$

i.e. $na - nb = mq$ for some $q \in \mathbb{Z}$.

or $n(a-b) = mq$

$\Rightarrow$ $n_1 d (a-b) = m_1 d\, q$

$\Rightarrow$ $n_1 (a-b) = m_1 q$

$\Rightarrow$ $m_1 \mid n_1 (a-b)$

But $(m_1, n_1) = 1$

$\Rightarrow$ $m_1 \mid a-b$

$\Rightarrow$ $a \equiv b \pmod{m_1}$

$\Rightarrow$ $a \equiv b \pmod{\left(\frac{m}{d}\right)}$ as ①

Hence $a \equiv b \pmod{\frac{m}{d}}$ as required.

Counter example:

$16 \equiv 4 \bmod 3$ or $2 \cdot 8 \equiv 2 \cdot 2 \pmod 3$

$\Rightarrow 8 \not\equiv 2 \bmod 3$ as $(2,3) = 1$

73

On the other hand

$6 \equiv 2 \pmod 4$

i.e $2 \cdot 3 \equiv 2 \cdot 1 \bmod 4$

$\Rightarrow 3 \not\equiv 1 \bmod 4$ as $(2,4) \neq 1$.

Corollary: If $na \equiv nb \pmod m$ and $(m,n) = 1$

Then $a \equiv b \pmod m$

Proof: Given

$na \equiv nb \pmod m$

$\Rightarrow m \mid na - nb$

$\Rightarrow m \mid n(a-b)$

But $(m,n) = 1$

Hence $m \mid a - b$

$\Rightarrow a \equiv b \pmod m$

THEOREM: If $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$

then $a \equiv b \pmod{\langle m_1, m_2 \rangle}$ where $\langle m_1, m_2 \rangle = [m_1, m_2]$.

PROOF: Since

$a \equiv b \pmod{m_1}$ & $a \equiv b \pmod{m_2}$

$\Rightarrow m_1 \mid a-b$ & $m_2 \mid a-b$

both imply $\langle m_1, m_2 \rangle \mid a-b$

$\Rightarrow a \equiv b \pmod{\langle m_1, m_2 \rangle}$.

$4 \mid 16$, $8 \mid 16$ & $\langle 4, 8 \rangle = 16$

Hence $\langle 4, 8 \rangle \mid 16$.

If $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$ and $(m_1, m_2) = 1$, then $a \equiv b \pmod{m_1 \cdot m_2}$

Proof: Given

$m_1 \mid a-b$ & $m_2 \mid a-b$

Moreover $(m_1, m_2) = 1$

Hence $m_1 \cdot m_2 \mid a-b$

$\Rightarrow a \equiv b \pmod{m_1 \cdot m_2}$

Generalized form:

If $a \equiv b \pmod{m_i}$ $i = 1, 2, \cdots n$

and $(m_i, m_j) = 1$ $\forall\ i \neq j$

then $a \equiv b \pmod{\prod_{i=1}^{n} m_i}$.

PROOF:

For $i = 2$, theorem is true

Suppose it is true for $i = n-1$.

i-e If $a \equiv b \pmod{m_i}$ $i = 1, 2, \cdots n-1$.

then $a \equiv b \pmod{\prod_{i=1}^{n-1} m_i}$

$\Rightarrow a \equiv b \pmod{\prod_{i=1}^{n-1} m_i \cdot m_n}$ using step 2.

$\Rightarrow a \equiv b \pmod{\prod_{i=1}^{n} m_i}$

Hence by induction, it is true.

75

THEOREM:

If $r \equiv r' \pmod{n}$ and $0 \le r, r' < n$, then $r = r'$.

PROOF: Assume that $0 \le r' \le r < n$ so that $r - r' \ge 0$ and suppose that $r \equiv r' \pmod{n}$

$\Rightarrow n \mid r - r'$

$\Rightarrow r - r' = mn$ for some $m \in \mathbb{Z}$.

But $r - r' > 0$ (If $r - r' = 0$, then nothing to prove)

& $n \mid r - r'$

$\Rightarrow n \le r - r'$ — (1)

Since $r < n$ & $r' < n$

$\Rightarrow r - r' < n$, which is a contradiction against (1)

Hence $r = r'$.

Aliter: Suppose $r \equiv r' \pmod{n}$

$\Rightarrow n \mid r - r'$.

If $r - r' = 0$ then $r = r'$

Let $r - r' > 0$, Then $n \mid r - r'$ imply

$n \le r - r'$ — (1)

But $r - r' < n$ as $r, r' < n$.

which contradicts our assumption $n \le r - r'$. Thus first supposition $r - r' > 0$ is wrong. Only possibility

$r - r' = 0 \Rightarrow r = r'$.

76

THEOREM: If $a = nq + r$ & $b = nq' + r'$ where $0 \le r, r' < n$. Then $r = r'$ iff $a \equiv b \pmod{n}$

PROOF: Suppose $r = r'$

Then $a - b = nq + r - nq' - r'$

$\Rightarrow a - b = nq - nq'$

or $a - b = n(q - q')$

$\Rightarrow n \mid a - b$

$\Rightarrow a \equiv b \pmod{n}$

Conversely: Suppose $a \equiv b \pmod{n}$

$\Rightarrow n \mid a - b$

$\Rightarrow a - b = nm$ for some $m \in \mathbb{Z}$.

Putting value of a & b

$nq + r - nq' - r' = nm$

$\Rightarrow r - r' = n(m - q + q')$

$\Rightarrow n \mid r - r'$

But $r - r' < n$ as $r, r' < n$

only possibility

$r - r' = 0$

$\Rightarrow r = r'$

Alternative Statement: Let $a, b \in \mathbb{Z}$, then $a \equiv b \pmod{n}$ iff a and b have the same remainder after division by n.

THEOREM: If $a \equiv b \pmod{m}$ and K divides a, b and m. Then $\frac{a}{K} \equiv \frac{b}{K} \pmod{\frac{m}{K}}$

Proof: Suppose $a \equiv b \pmod{m}$

Then $m \mid a-b$

$\Rightarrow \frac{m}{K} \mid \frac{a}{K} - \frac{b}{K}$

$\Rightarrow \frac{a}{K} - \frac{b}{K} \equiv 0 \pmod{\frac{m}{K}}$

or $\frac{a}{K} \equiv \frac{b}{K} \pmod{\frac{m}{K}}$.

THEOREM:

(a) If $a \equiv b + mq$ then

If $a \equiv b \pmod{m}$, then $a = b + mq$ for some integer q.

(b) If $a \equiv b \pmod{m}$, then $(a, m) = (b, m)$

PROOF:

(a) Since $a \equiv b \pmod{m}$

$\Rightarrow m \mid a-b$

$\Rightarrow a - b = mq$ for some $q \in Z$.

$\Rightarrow a = b + mq$ as required.

(b) Since $a \equiv b \pmod{m} \Rightarrow a = b + mq$ — ①

Suppose $(a, m) = d$ — ②

Then $d \mid a$ & $d \mid m$

$\Rightarrow d \mid b$ $\because b = a - mq$

Also if $c \mid m$ & $c \mid b$, then $c \mid a$ using ①

Alternately $c \mid a$ using (2) to

Thus $(b, m) = d$

That is $(a, m) = (b, m)$

THEOREM: Let k divide both a and b and let $(k, m) = d$. Then $a \equiv b \pmod{m}$ imply $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{d}}$

PROOF: Let $a \equiv b \pmod{m}$

Then $m \mid a - b$.

$$\Rightarrow m \mid \left(\frac{a}{k} - \frac{b}{k}\right) k$$

$$\Rightarrow \frac{m}{d} \mid \left(\frac{a}{k} - \frac{b}{k}\right) \frac{k}{d}$$

But $\left(\frac{m}{d}, \frac{k}{d}\right) = 1$ as $(k, m) = d$.

Thus $\frac{m}{d} \mid \frac{a}{k} - \frac{b}{k}$.

$$\Rightarrow \frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{d}}$$

Corollary: If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$

Then $a \equiv b \pmod{m}$

This is also known as Cancellation law.

THEOREM: If $f(x)$ is a polynomial with integral co-efficients and $a \equiv b \pmod m$ Then $f(a) \equiv f(b) \pmod m$ 79

PROOF: let $f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$

we know

$$c_0 \equiv c_0 \pmod m \quad \text{---} \ (1)$$
$$a \equiv b \pmod m \quad \text{---} \ (2)$$
$$\Rightarrow a^2 \equiv b^2 \pmod m \quad \text{---} \ (3)$$
$$\vdots \quad \vdots \quad \vdots$$
$$a^n \equiv b^n \pmod m \quad \text{---} \ (n)$$

Multiplying eq (2) by c_1, (3) by c_2 and so on (n) by c_n, then adding above all.

$$c_0 + c_1a + c_2a^2 + \cdots + c_na^n \equiv c_0 + c_1b + c_2b^2 + \cdots + c_nb^n \pmod m$$

$$\Rightarrow f(a) \equiv f(b) \pmod m \text{ as required.}$$

Exp: If $f(x) = x^4 - 3x^2 + 2x - 1$

Find remainder when $f(15)$ is divided by 7.

Sol we know

$$15 \equiv 1 \pmod 7$$
$$\Rightarrow f(15) \equiv f(1) \pmod 7$$
$$\Rightarrow f(15) \equiv -1 \bmod 7$$
$$\text{or} \quad f(15) \equiv 6 \bmod 7$$

Hence remainder $= 6$ as $f(15) = 7q + 6$

$\because 6 < 7$

80

THEOREM: Let $a \equiv b \pmod{p^k}$. Then $a^p \equiv b^p \pmod{p^{k+1}}$

PROOF: Since $a \equiv b \pmod{p^k}$

$\Rightarrow a = b + p^k \cdot q$ for some $q \in Z$.

Now $a^p = (b + p^k \cdot q)^p$

$= b^p + p \cdot b^{p-1} \cdot p^k \cdot q +$ terms divisible by p^{k+1}.

$\Rightarrow a^p - b^p =$ Terms divisible by p^{k+1}

$\Rightarrow p^{k+1} \mid a^p - b^p$

$\Rightarrow a^p \equiv b^p \pmod{p^{k+1}}$ as required.

TESTS OF DIVISIBILITY:

THEOREM: Let N be a positive integer (such that)

$$N = a_m \cdot a_{m-1} \cdots a_3 \cdot a_2 \cdot a_1 \cdot a_0$$
$$= a_m \times 10^m + a_{m-1} \times 10^{m-1} + \cdots + a_3 \times 10^3 + a_2 \times 10^2 + a_1 10 + a_0$$

where $a_m \neq 0$ & $0 \leq a_i < 10$; $0 \leq i \leq m-1$.

Then

(i) $2 \mid N$ iff $2 \mid a_0$

(ii) $3 \mid N$ iff $3 \mid \sum_{i=0}^{m} a_i$

(iii) $4 \mid N$ iff $4 \mid a_0 + 2a_1$

(iv) $5 \mid N$ iff $5 \mid a_0$

(v) $9 \mid N$ iff $9 \mid \sum_{i=0}^{m} a_i$

(vi) $11 \mid N$ iff $11 \mid \sum_{i=0} (-1)^i a_i$ 81

(vii) N is divisible by 7 or 13 iff

$(a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - (a_{11} a_{10} a_9)_{10} + \cdots$

is divisible by 7 or 13 respectively.

(viii) N is divisible by 37 iff

$(a_2 a_1 a_0)_{10} + (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} + (a_{11} a_{10} a_9)_{10} + \cdots$

is divisible by 37.

(ix) N is divisible by 101 iff

$a_1 a_0 - a_3 a_2 + a_5 a_4 - a_7 a_6 + \cdots$ is divisible by 101.

PROOF:

(i) we know that

$$a_0 \equiv a_0 \pmod 2 \quad \text{---} ①$$

Also $10 \equiv 0 \pmod 2$ ---- ②

$\Rightarrow 10^2 \equiv 0 \pmod 2$ ---- ③

$\vdots$

$10^m \equiv 0 \pmod 2$ ---- (m+1)

Multiplying ① by 1 ② by a_1 and so on (m+1) by a_m and then adding we get

$$a_0 + 10 a_1 + 10^2 a_2 + \cdots + 10^m a_m \equiv a_0 \pmod 2$$

$\Rightarrow N \equiv a_0 \pmod 2$

$\Rightarrow 2 \mid N$ iff $2 \mid a_0$

82

(ii) We know

$$a_0 \equiv a_0 \pmod 3 \quad \text{---} (1)$$

Also $10 \equiv 1 \pmod 3$ ---(2)

$\Rightarrow 10^2 \equiv 1 \pmod 3$ ---(3)

$\vdots$

$$10^m \equiv 1 \pmod 3 \quad \text{---} (m+1)$$

Multiplying (1) by 1, (2) by a_0, ... (m+1) by a_m and then adding, we get.

$$a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^m a_m \equiv a_0 + a_1 + a_2 + \cdots a_m \pmod 3$$

$$\Rightarrow N \equiv \sum_{i=0}^{m} a_i \pmod 3$$

$$\Rightarrow 3 \mid N \Leftrightarrow 3 \mid \sum_{i=0}^{m} a_i$$

(iii) We know

$$a_0 \equiv a_0 \pmod 4 \quad \text{---} (1)$$

Also $10 \equiv 2 \pmod 4$ ---(2)

$\Rightarrow 10^2 \equiv 0 \pmod 4$ ---(3)

$10^3 \equiv 0 \pmod 4$ ---(4)

$\vdots$

$$10^m \equiv 0 \pmod 4 \quad \text{---} (m+1)$$

Multiplying (1) by 1; (2) by a_1; ..., (m+1) by a_m and then adding

$$a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^m a_m \equiv a_0 + 2a_1 \pmod 4$$

$\Rightarrow N \equiv a_0 + 2a_1 \pmod 4$

$\Rightarrow 4 \mid N \Leftrightarrow 4 \mid a_0 + 2a_1$.

(iv) Same as (i) Self

(v) Same as (ii) Self

(vi) we know

$$a_0 \equiv a_0 \pmod{11} \quad \text{---} (1)$$

Also $$10 \equiv -1 \pmod{11} \quad \text{---} (2)$$

$$\Rightarrow (10)^2 \equiv (-1)^2 \pmod{11} \quad \text{---} (3)$$

$$\vdots$$

$$(+10)^m \equiv (-1)^m \pmod{11} \quad \text{---} (m+1)$$

Multiplying (1) by 1; (2) by a_1 ... (m+1) by a_m and then adding

$$a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^m a_m \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m \pmod{}$$

$$\Rightarrow N \equiv \sum (-1)^m a_m \pmod{11}$$

or $$N \equiv \sum_{i=0}^{m} (-1)^i a_i \pmod{11}$$

$$\Rightarrow 11 \mid N \text{ iff } 11 \mid \sum_{i=0}^{m} (-1)^i a_i$$

(vii) Since $N = a_m \cdot a_{m-1} \cdots a_3 \cdot a_2 a_1 a_0$

$(N = a_m a_{m-1} \cdots a_3 a_2 a_1 a_0)$

we can write as

$$N = a_2 a_1 a_0 + a_5 a_4 a_3 \times 10^3 + a_8 a_7 a_6 (10^3)^2 + \cdots \quad \text{---} (1)$$

Moreover 84

$$1000 \equiv -1 \pmod{7 \text{ or } 13}$$

i.e $10^3 \equiv -1 \pmod{7 \text{ or } 13}$

Thus eq (i) becomes

$$N \equiv a_2 a_1 a_0 + a_5 a_4 a_3 (-1) + a_8 a_7 a_6 (-1)^2 + \cdots \pmod{7 \text{ or } 13}$$

Thus N is divisible by 7 or 13

iff $a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$ is

divisible by 7 or 13.

(viii) Again we can write N as

$$N = a_2 a_1 a_0 + (a_5 a_4 a_3) \times 10^3 + (a_8 a_7 a_6) \times (10^3)^2 + \cdots \quad \text{——(ii)}$$

But $1000 \equiv 1 \pmod{37}$

Thus eq (ii) becomes

$$N \equiv a_2 a_1 a_0 + a_5 a_4 a_3 (1)^3 + \cdots \pmod{37}$$

or simply

$$N \equiv a_2 a_1 a_0 + a_5 a_4 a_3 + a_8 a_7 a_6 + \cdots \pmod{37}$$

Hence $37 | N$ iff $37 | a_2 a_1 a_0 + a_5 a_4 a_3 + a_8 a_7 a_6 + \cdots$

(ix) We can write N as 85

$$N = a_1a_0 + a_3a_2 \times 10^2 + a_5a_4 \times (10^2)^2 + \cdots$$

But $100 \equiv -1 \pmod{101}$ —— (1)

i.e $(10)^2 \equiv -1 \pmod{101}$

Eq (1) becomes

$$N \equiv a_1a_0 + a_3a_2(-1) + a_5a_4(-1)^2 + \cdots \pmod{101}$$

or $N \equiv a_1a_0 - a_3a_2 + a_5a_4 - a_7a_6 + \cdots \pmod{101}$

Thus $101 \mid N \iff 101 \mid a_1a_0 - a_2a_2 + a_5a_4 - \cdots$

TEST OF Divisibility by 7.

Let us consider the number 48597. We first ignore the unit digit and subtract twice of unit digit(7) from 4859 to get 4845. Again ignore the unit digit and subtrat twice of unit digit(5) from 484 to get, 474. Again repeat above proceed, we get 39.

Since $7 \nmid 39$.

Hence $7 \nmid 48597$.

Generalized form: 86

An integer n is divisible by 7 iff $7 \mid q$ where $q = \frac{n-a_0}{10} - 2a_0$

Consider $q = \frac{n-a_0}{10} - 2a_0$

$\Rightarrow 10q = n - a_0 - 20a_0$

$\Rightarrow 10q = n - 21a_0$

or $n = 10q + 21a_0$

$\Rightarrow n - 10q = 3 \cdot 7 a_0$

$\Rightarrow 7 \mid n - 10q$

$\Rightarrow n \equiv 10q \pmod 7$

Now $7 \mid n$ iff $7 \mid 10q$

But $7 \nmid 10$

Hence $7 \mid q$.

Thus $7 \mid n$ iff $7 \mid q$

which complete the proof.

Divisibility by 8:

87

An integer n is divisible by 8 iff its last three digits divisible by 8.

PROOF: We can write n as

$$n = a_m a_{m-1} \cdots a_2 a_3 a_1 a_0$$

or

$$n = a_2 a_1 a_0 + a_5 a_4 a_3 \times 1000 + a_8 a_7 a_6 \times (1000)^2 + \cdots \longrightarrow (1)$$

But we know

$$1000 \equiv 0 \pmod 8$$

$$\Rightarrow (1000)^m \equiv 0 \pmod 8 \quad \forall\ m \geq 1.$$

Thus eq (1) becomes

$$n \equiv a_2 a_1 a_0 \pmod 8$$

Thus $8 \mid n$ iff $8 \mid a_2 a_1 a_0$

which complete the proof.

88

Exp: Find remainder when $S=1!+2!+3!+\cdots+1000!$ is divided by 4.

Sol: Since $K!$ is divisible by 4 $\forall K \geq 4$.

Thus $S = 1!+2!+3!+\cdots+1000!$

$\equiv 1!+2!+3! \pmod 4$

$\equiv 9 \pmod 4$

$\equiv 1 \pmod 4$

Thus $R = 1$.

Prob: Find R when 2^{57} is divided by 13.

Sol: we know

$$2^6 \equiv -1 \pmod{13}$$

$$\Rightarrow (2^6)^9 \equiv (-1)^9 \pmod{13}$$

$$\Rightarrow 2^3 \cdot 2^{54} \equiv 2^3(-1) \pmod{13}$$

$$\Rightarrow 2^{57} \equiv -8 \bmod 13$$

$$\equiv 5 \pmod{13}$$

Hence $R = 5$.

PROB ① 5^{48} is divided by 12

$5^2 \equiv 1 \pmod{12} \Rightarrow R = 1$.

② 3^{100} is divided by 5.

$3^2 = -1 \pmod 5 \Rightarrow R = 1$

③ 5^{48} is divided by 8.

$5^2 \equiv 1 \pmod 8$; $R = 1$

④ 3^{1000} is divided by 16

$3^4 \equiv 1 \pmod{16}$; $R = 1$

⑤ 9^{14} is divided by 17.

$9^4 \equiv -1 \pmod{17}$; $R = 13$

⑥ 3^{21} is divided by 8.

$3^2 \equiv 1 \pmod 8$; $R = 3$

⑦ 5^{84} is divided by 8.

$5^2 \equiv 1 \pmod 8$; $R = 1$

⑧ 11^{35} is divided by 13

$11^6 \equiv -1 \pmod{13}$

Also $11^5 \equiv 7 \pmod{13}$ $R = 6$

use ~~Transitive~~

$a \equiv c \pmod m$

$b \equiv d \pmod m$

$\Rightarrow ab \equiv cd \pmod m$

⑨ 5^{11} is divided by 7. $R = 3$.

$5^2 \equiv 4 \pmod 7$

$5^4 \equiv 2 \pmod 7$

$5^8 \equiv 4 \pmod 7$

$$5^{111} \equiv 5^3 \cdot 5^2 \cdot 5 \pmod 7$$
$$\equiv 4 \cdot 4 \cdot 5 \pmod 7$$
$$\equiv 16 \cdot 5 \pmod 7$$
$$\equiv 2 \cdot 5 \pmod 7$$
$$\equiv 3 \pmod 7$$

* (10) Show that F_5 is divisible by 641.

We know $F_5 = 2^{25} + 1$

Also
$$2^4 \equiv 16 \pmod{641}$$
$$2^8 \equiv 256 \pmod{641}$$
$$2^{16} \equiv (256)^2 \pmod{641}$$
or $$2^{16} \equiv 154 \pmod{641}$$
$$2^{32} \equiv (154)^2 \pmod{641}$$
$$2^{32} \equiv 640 \pmod{641}$$
or $$2^{32} \equiv -1 \pmod{641}$$
$$\Rightarrow 2^{32} + 1 \equiv 0 \pmod{641}$$
$$\Rightarrow F_5 \equiv 0 \pmod{641}$$
$$\Rightarrow F_5 \text{ is divisible by } 641.$$

(11) Remainder when 2^{340} is divided by 341

NOTE $11 \cdot 31 = 341$

Further $(11, 31) = 1$

Hence $[11, 31] = 341$.

Now $2^5 \equiv -1 \pmod{11}$

$(2^5)^{68} \equiv (-1)^{68} \pmod{11}$

$\Rightarrow 2^{340} \equiv 1 \pmod{11}$ — (1)

Also $2^5 \equiv +1 \pmod{31}$

$\Rightarrow 2^{340} \equiv 1 \pmod{31}$ — (2)

(1) & (2) imply

$2^{340} \equiv 1 \pmod{[11, 31]}$

$\Rightarrow 2^{340} \equiv 1 \pmod{341}$

Hence $R = 1$.

(12) Find the least residue of $5^{121} \pmod{27}$

Observe that

$121 = 64 + 32 + 16 + 8 + 1$.

Therefore over

$$5^2 \equiv -2 \pmod{27}$$

$$5^4 \equiv 4 \pmod{27}$$

$$5^8 \equiv 16 \pmod{27} \equiv -11 \pmod{27}$$

$$5^{16} \equiv 121 \pmod{27}$$

$$\equiv 13 \pmod{27}$$

$$5^{32} \equiv 169 \equiv 7 \pmod{27}$$

$$5^{64} \equiv 49 \equiv -5 \pmod{27}.$$

Therefore

$$5^{121} = 5^{64} \cdot 5^{32} \cdot 5^{16} \cdot 5^8 \cdot 5^1 \cdot 5^0 \cdot 5$$

$$\equiv (-5)(7)(13)(-11)(5) \pmod{27}$$

$$\equiv (-35)(13)(-55) \pmod{27}$$

$$\equiv (-35)(13)(-1) \pmod{27}$$

$$\equiv (-8)(13)(-1) \pmod{27}$$

$$\equiv 23 \pmod{27}$$

$R = 23.$

Assignment:

What is the remainder when 3^{287} is divided by 23.?

$R = 3$; $287 = 256 + 16 + 8 + 4 + 2 + 1.$

93

Definition: For integers a, b and $m > 0$.
If $a-b$ is not divisible by m then we say that a is incongruent to $b \pmod m$ and we write this as
$a \not\equiv b \pmod m$.

Example: Find the missing digit of the number $95555-4853$ so that it is divisible by 11.

Sol. Suppose that missing digit is x

Now $3-5+3-4+x-5+5-5+5-9 = x-12$.

Now $11 \mid 95555 \times 4353$

$\therefore$ $11 \mid x-12$

$\therefore$ $11 \mid x-1$

$\therefore$ $11 \mid x-1$; $x < 11$.

Thus only one possibility

$x-1=0$

$\Rightarrow x=1$.

H.M KHALID MAHMOOD

RESIDUE SYSTEM

94

Given integers a and m, the division algorithm gives $a = qm + r$; $0 \le r < m$

Moreover if $a \equiv r \pmod m$ & $a \equiv r' \pmod m$

Then $r = r'$

Thus a given integer a is congruent to one and only one of the integers $0, 1, 2, \cdots, \overline{m-1} \pmod m$.

Definition: CRS

Let m be a fixed positive integer. A set $a_1, a_2, \cdots, a_k$ of integers is called a Complete Residue System modulo m written as CRS(mod m) if (i) $a_i \not\equiv a_j \pmod m$ $\forall$ $(i \neq j)$

(ii) For each integer n, there exist a unique a_i such that $n \equiv a_i \pmod m$; $1 \le i \le k$.

Remark: $\{0, 1, 2, 3, \cdots, \overline{m-1}\}$ always form a CRS (mod m).

Examples:

① $\{5, 13, 27, 31, 34\}$ is a CRS(mod 5)

② $\{-5, 11, 59, -13, -57, 26, 49\}$ is a CRS(mod 7).

③ $\{-12, -15, 82, -1, 31\}$ is a CRS (mod 5)

because the set consists of 5 integers whose least residues (mod 5) are $3, 0, 2, 4, 1$ which is a permutation of the numbers $0, 1, 2, 3, 4$. Moreover $\{0, 1, 2, 3, 4\}$ always form CRS (mod 5).

Alternative definition:

A set of m integers whose least residues $(\bmod m)$ are $0, 1, 2, \ldots, \overline{m-1}$ in some order is called CRS or simply Complete System of incongruent residues $(\bmod m)$ or briefly a Complete System $(\bmod m)$

THEOREM: If K integers $a_1, a_2, \ldots, a_K$ form a CRS $(\bmod m)$ then $m = K$.

PROOF: We know that $\{0, 1, 2, \ldots, \overline{m-1}\}$ form a CRS $(\bmod m)$. Then for each j, there exist a unique i such that

$$a_j \equiv i \pmod m \; ; \quad 0 \le i \le m-1 \; \& \; 1 \le j \le K.$$

Thus $K \le m$ — (1)

But then $\{a_1, a_2, \ldots, a_K\}$ is also a a CRS System $(\bmod m)$. Hence for all i there exist unique a_j

Such that $i \equiv a_j \pmod m$; $0 \le i \le m-1$, $1 \le j \le K$

Thus $m \le K$ — (2)

(1) & (2) gives

$$K = m$$

Alternative definition: 96

Let m be a positive integer. Let $A = \{a_1, a_2, \cdots, a_k\}$ be the set of integers. Then A is called a CRS mod m if

(1) A has m elements.

(2) $a_i \not\equiv a_j \pmod{m}$ $\forall\, i \neq j$

THEOREM: Let $\{x_0, x_1, x_2, \cdots, x_{m-1}\}$ be a CRS (mod m), then for any $a, b \in \mathbb{Z}$ such that $(a, m) = 1$, then $\{ax_0 + b, \cdots, ax_{m-1} + b\}$ also a CRS (mod m). $= A$

PROOF: Observe that A contain m elements. On contrary suppose that

$$ax_i + b \equiv ax_j + b \pmod{m} \quad \forall\, i \neq j$$

$$\Rightarrow ax_i \equiv ax_j \pmod{m}$$

$$\Rightarrow x_i \equiv x_j \pmod{m} \quad \text{as } (a, m) = 1$$

Hence $x_i \equiv x_j \pmod{m}$ $\forall\, i \neq j$.

which is a contradiction against the fact that $\{x_0, x_1, \cdots, x_{m-1}\}$ is a CRS (mod m). Hence

$$ax_i + b \not\equiv ax_j + b \pmod{m} \quad \forall\, i \neq j$$

Thus A form a CRS (mod m).

Assignment: 97

If $a_1, a_2, \cdots, a_m$ is a CRS (mod m) and $(b, m) = 1$, then $ba_1, ba_2, \cdots, ba_m$ is also a CRS (mod m).

THEOREM:

Any m integers in arithmetical progression with common difference relatively prime to m form a CRS (mod m).

PROOF: Let the integers in AP are

$$a, a+t, a+2t, \cdots, a+(m-1)t; \quad (t, m) = 1$$

Observe that these are m integers.

Suppose that

$$a + it \equiv a + jt \pmod m; \quad i \neq j$$

$$\Rightarrow it \equiv jt \pmod m$$

$$\Rightarrow i \equiv j \pmod m \quad \text{as } (t, m) = 1$$

$$\Rightarrow m \mid i - j$$

But $i < m$ & $j < m$

only possibility

$$i - j = 0 \iff i = j$$

which is a contradiction as $i \neq j$

Hence $a + it \not\equiv a + jt \pmod m \ \forall\ i \neq j$

which complete the proof.

Hence $r \in S$. If then b is the unique member of C of which r is the least residue $(\text{mod } m)$ then obviously

$$r \equiv b \pmod m \quad \text{—} (2)$$

(1) & (2) imply $a \equiv b \pmod m$.

Example: The set $\{49, 20, 10, 17, -18, -27\}$ is a CRS $(\text{mod } 6)$. Find the integer of the set which is congruent $(\text{mod } 6)$ to 49.

Sol The least residues of the members of given set are 1, 2, 4, 5, 0 and 3.

Also least residue of $491 (\text{mod } 6)$ is:

Thus $491 \equiv 5 \pmod 6$

$\equiv 17 \pmod 6$

Thus 17 is the req member.

THEOREM: Let

(i) $\{a_1, a_2, \ldots, a_{m_1}\}$ be a CRS $(\text{mod } m_1)$

(ii) $\{b_1, b_2, \ldots, b_{m_2}\}$ be a CRS $(\text{mod } m_2)$

(iii) $(m_1, m_2) = 1$, then the set C defined by

$$C = \{a_i \cdot m_2 + b_j \cdot m_1 \; ; \; 1 \le i \le m_1, \; 1 \le j \le m_2\}$$

is a CRS $(\text{mod } m_1 m_2)$.

100

PROOF: Since $1 \le i \le m_1$ & $1 \le j \le m_2$.
Thus C contain $m_1 m_2$ different elements.
Next Suppose that

$$a_i m_2 + b_j m_1 \equiv a_k m_2 + b_e m_1 \pmod{m_1 m_2}$$

for some i, j, k and e.

$$\Rightarrow (a_i - a_k) m_2 + (b_j - b_e) m_1 \equiv 0 \pmod{m_1 m_2}$$

Hence we can write as

$$(a_i - a_k) m_2 + (b_j - b_e) m_1 \equiv 0 \pmod{m_1} \text{ —— } (1)$$

& $$(a_i - a_k) m_2 + (b_j - b_e) m_1 \equiv 0 \pmod{m_2} \text{ —— } (2)$$

Since $(a_i - a_k) m_2 \equiv 0 \pmod{m_2}$
& $(b_j - b_e) m_1 \equiv 0 \pmod{m_1}$ then
(1) & (2) becomes

$$(a_i - a_k) m_2 \equiv 0 \pmod{m_1} \text{ —— } (3)$$

& $$(b_j - b_e) m_1 \equiv 0 \pmod{m_2} \text{ —— } (4)$$

(3) $\Rightarrow$ $a_i \equiv a_k \pmod{m_1}$ —— (1*)
(4) $\Rightarrow$ $b_j \equiv b_e \pmod{m_2}$ —— (2*) as $(m_1, m_2) = 1$

which is a contradiction as
a_i, a_k, b_j, b_e are incongruent mod m_1 and mod m_2 respectively.

Hence 101

$$a_i m_2 + b_j m_1 \not\equiv a_K m_2 + b_e m_1 \pmod{m_1 m_2}$$

which complete the proof.

Definition:

For each positive integer n we define a number $\varphi(n)$ as

$$\varphi(n) = \begin{cases} 1 & \text{if } n = 1 \\ \text{the number of positive integers less than } n \text{ that are co-prime to } n & ; n \neq 1. \end{cases}$$

It is known as Euler's φ-function.

e.g. $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(6) = 2$.

Remark If n is prime, then $\varphi(n) = n - 1$

Reduced residue System (RRS):

The set of integers $a_1, a_2, \ldots, a_K$ is called a reduced residue system modulo m (written as RRS (mod m)) if

(i) $(a_i, m) = 1 \quad \forall\ i = 1, 2, 3, \ldots, K.$

(ii) $a_i \not\equiv a_j \pmod{m} \quad \forall\ i \neq j$

(iii) If n is an integer such that $(n, m) = 1$ then $n \equiv a_i \pmod{m}$ for a unique $i; 1 \leq i \leq K$.

Example: The set of integers $\{1, 5, 7, 11\}$ $\equiv 10^{\circ}$
is a RRS (mod 12). For (i) & (ii) hold clearly.
Let m be any integer such that $(m, 12) = 1$
By division algorithm

$$m = 12q + r \quad ; \quad 0 \le r < 12$$

Observe that $(r, 12) = 1$.
Thus r can be either 1 or 5 or 7 or 11.

e.g. $(25, 12) = 1$
& $25 = 2 \cdot 12 + 1$
& $(1, 12) = 12$
$(29, 12) = 1$
$29 = 2 \cdot 12 + 5$
& $(5, 12) = 1$

Also $12 \mid m - r$
$\Rightarrow m \equiv r \pmod{12}$

Example: The set of integers $\{1, 2, \cdots, 12\}$ is a RRS (mod 13). In fact for each prime P, $\{0, 1, 2, \cdots, \overline{P-1}\}$ is a CRS (mod P) and $\{1, 2, \cdots, \overline{P-1}.\}$ is a RRS (mod P).
Since $P = 13$, Thus $\{1, 2, \cdots, 12\}$ is a RRS (mod 13).

Example: Show that the set
$\{22, -1, 43, 46, -19, 79, 113, 452\}$
is a RRS (mod 15).

Sol: The least residues (mod 15) of the integers of the set are
① —— 7, 14, 13, 1, 11, 4, 8, 2 respectively.
Also the integers less than 15 and prime to 15 are 1, 2, 4, 7, 8, 11, 13, 14 —— ②

It is easily seen that ① is a permutation of ②. Therefore the given set is a RRS(mod 15).

* Exp: If p is an odd prime then the set $\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 1, 2, \ldots, \frac{p-1}{2}\}$ is a RRS(mod p).

Sol For, the least residues (mod m) of the integers of the given set are

① — $1, 2, \ldots, \frac{p+1}{2}, \frac{p+3}{2}, \ldots, \overline{p-1}$

$\frac{p+1}{2}, \frac{p+3}{2}, \ldots, \overline{p-1}, 1, 2, \ldots \frac{p-1}{2}$ which is a a permutation of ①

Hence Given set is a RRS(mod p).

CONSTUCTION: If we delete from a CRS(mod m) the integers which have a common factor with m, we get a RRS(mod m).

Observation:

$\{1, 9, 3, 4, 5, 6, 7, 8\}$ is a CRS(mod 8).

Now $(1, 8) = 1$, $(5, 8) = 1$

$(9, 8) = 1$, $(7, 8) = 1$

Also $\varphi(8) = 4$

More over $\{1, 3, 5, 7\}$ is RRS(mod 8).

Thus RRS(mod m) contain exactly $\varphi(m)$ integers

THEOREM: 1

If $a_1, a_2, a_3, \cdots, a_K$ form a RRS (mod m) then $K = \varphi(m)$

PROOF: Let $A = \{t_1, t_2, \cdots, t_{\varphi(m)}\}$ be the set of integers that are less than m and co-prime to m. then

(i) $(t_i, m) = 1 \quad ; \quad 1 \le i \le \varphi(m)$

by the choice of t_i's.

(ii) $t_i \equiv t_j \pmod m, i \ne j; 1 \le t_i, t_j \le \varphi(m)$

$\Rightarrow m \mid t_i - t_j$ —— ①

But $1 \le t_i, t_j < m$

$\Rightarrow t_i - t_j < m$, hence ① cannot be possible unless $t_i - t_j = 0$

$\Rightarrow t_i = t_j$, $i \ne j$, a contradiction.

Hence $t_i \not\equiv t_j \pmod m$ for $i \ne j$.

(iii) Let n be any integer such that $(n, m) = 1$

Then by division algorithm

$$n = qm + r \quad ; \quad 0 \le r < m.$$

and the quotien $q = 0$ if $n < m$ and $q \ge 1$ if $n > m$. Also $(r, m) = 1$

Hence $r = t_i$ for some i, $1 \le i \le \varphi(m)$

(as $m \mid n - r \Rightarrow n \equiv r \pmod m$)

and $n \equiv r \equiv t_i \pmod m$ 10

$\Rightarrow n \equiv t_i \pmod m$

Thus A is a RRS $\pmod{\varphi(m)}$.

Since $\{a_1, a_2, \cdots, a_K\}$ is a RRS (mod m.

So for each ℓ ; $1 \le \ell \le \varphi(m)$, there exist a unique i ; $1 \le i \le K$ such that

$$t_\ell \equiv a_i \pmod m$$

$$\Rightarrow \varphi(m) \le K \quad \text{—} ①^*$$

Similarly $K \le \varphi(m)$ —②*

①* & ②* imply

$$K = \varphi(m)$$

which complete the proof.

Alternative definition:

Let m be a positive integer, then the set of integers $A = \{a_1, a_2, \cdots, a_K\}$ is called a RRS (mod m) if

(i) The set A contain $\varphi(m)$ elements.

(ii) $a_i \not\equiv a_j \pmod m$ for $i \neq j$.

(iii) $(a_i, m) = 1$; $1 \le i \le K$.

106

THEOREM: If $\{a_1, a_2, a_3, \ldots, a_{\varphi(m)}\}$ is a RRS (mod m) and $(a, m) = 1$, then $\{aa_1, aa_2, \ldots, aa_{\varphi(m)}\}$ also form a RRS (mod m).

PROOF: Let $A = \{aa_1, aa_2, \ldots, aa_{\varphi(m)}\}$

(i) It is obvious that A contain $\varphi(m)$ elements.

(ii) Since $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ is a RRS (mod m)

Then $(a_i, m) = 1 \quad ; 1 \le i \le \varphi(m)$

Also $(a, m) = 1$ (given)

Thus $(aa_i, m) = 1$.

(iii) Let $aa_i \equiv aa_j \pmod m \quad ; (i \neq j)$

But $(a, m) = 1$

Hence $a_i \equiv a_j \pmod m \quad ; (i \neq j)$

which is a contradiction as $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$

Hence $aa_i \not\equiv aa_j \pmod m \quad ; (i \neq j)$

Remark:

① Let $(a, b) = 1$, then for any c.

$$(ac, b) = (c, b)$$

Let $(ac, b) = d$ Let $(c, b) = d_1$

Then $d \mid ac$ & $d \mid b$ | $d \mid c$ (1) | Also $d_1 \mid c$ & $d_1 \mid b$

$\Rightarrow d \mid ac$ & $d \mid bc$ | $\Rightarrow d \mid c$ | $\Rightarrow d_1 \mid ac$ & $d_1 \mid b$

$\Rightarrow d \mid (ac, bc)$ | Also $d \mid b$ | $\Rightarrow d_1 \mid (ac, b)$

$d \mid c\,(a, b)$ | $\Rightarrow d \mid (c, b)$ | $\Rightarrow (c, b) \mid (ac, b)$ — (2)*

| $\Rightarrow (ac, b) \mid (c, b)$ — (2)*

(1)* & (2)* Complete.

Now $(a_i, m) = 1$ & $(a, m) = 1$

Then $(aa_i, m) = (a, m) = 1$

107

Then $(\prod a_i, m) = 1$

In particular

$(a^m, b) = 1$, $(a, b^m) = 1$

Also $(a^m, b^m) = 1$.

} if $(a,b)=1$

If $a = bq + r$, then $(a,b) = (b,r)$

THEOREM: $\{1, 2, 3, \cdots, \overline{p-1}\}$ is a RRS(mod p) iff p is prime.

PROOF: Suppose p is prime.

let $A = \{1, 2, 3, \cdots, \overline{p-1}\}$

clearly $(i, p) = 1$; $1 \le i \le \overline{p-1}$

as p is prime.

Suppose $i \equiv j \pmod p$ $i, j < p$ then $i \neq j$

Then $p \mid i-j$

$\Leftrightarrow i = j$, a contradiction.

Hence $i \neq j$

Conversely Suppose

p is not prime.

Then p is composite.

So $\varphi(p) \le p-2$.

But $\{1, 2, \cdots, \overline{p-1}\}$ is a RRS mod p.

Hence it contain exactly $\varphi(p)$ elements. Thus $\varphi(p) = p-1$

a contradiction.

Hence p cannot be composite.

108

THEOREM: Let $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ be a RRS $(\bmod m)$ and $\{b_1, b_2, \ldots, b_{\varphi(n)}\}$ RRS $(\bmod n)$ & $(m,n)=1$ then $\{a_i \cdot n + b_j \cdot m \; ; \; 1 \le i \le \varphi(m) \;\&\; 1 \le j \le \varphi(n)\}$ is a RRS $(\bmod mn)$

PROOF: Let

$$C = \{a_i n + b_j m \; ; \; 1 \le i \le \varphi(m) \;\&\; 1 \le j \le \varphi(n)\}$$

(i) We will show that elements of C are relatively prime to mn.

Consider

$$\begin{aligned}
&(na_i + mb_j, mn) \\
&= (na_i + mb_j, m)(na_i + mb_j, n) \\
&= (na_i, m) \cdot (mb_j, n) \\
&= (n, m) \cdot (m, n) \quad \because (a_i, m) = 1 \;\&\; (b_j, n) = 1 \\
&= 1 \cdot 1 \\
&= 1
\end{aligned}$$

Thus elements of C are relatively prime to mn.

(ii) Suppose $na_i + mb_j \equiv na_k + mb_e \pmod{mn}$ $\quad i \neq k$, $j \neq e$.

$$\Rightarrow n(a_i - a_k) + m(b_j - b_e) \equiv 0 \pmod{mn}$$

$$\Rightarrow n(a_i - a_k) + m(b_j - b_e) \equiv 0 \pmod{n}$$

OR

$$n(a_i - a_k) \equiv 0 \pmod{m} \;\&\; m(b_j - b_e) \equiv 0 \pmod{n}$$

$$\Rightarrow a_i \equiv a_k \pmod{m} \;\&\; b_j \equiv b_e \pmod{n} \quad \because (m,n)=1$$

a contradiction.

Hence $a_i n + b_j m \not\equiv n a_k + m b_e \pmod{mn}$

(iii) let a be any integer co-prime to mn.

i.e $(a, mn) = 1$

Since $(m, n) = 1$

So there exist integers x & y such that

$$mx + ny = 1$$

$$\Rightarrow amx + any = a \quad \text{---} (1)$$

Moreover $(x, n) = 1$ & $(y, m) = 1$

because if $(x, n) = d > 1$ & $(y, m) = d > 1$

then in either case

$(a, mn) = 1$, a contradiction

(e.g $(x, n) = d \Rightarrow d \mid (am)x$ & $d \mid (ay)n$

$\Rightarrow d \mid (am)x + (ay)n = a$

$\Rightarrow d \mid a$ Also $d \mid n \Rightarrow d \mid mn$

$\Rightarrow d \mid (a, mn)$, contradiction)

Since $b_1, b_2, \ldots, b_{\varphi(m)}$ is a RRS, so for any integer ax, there exist a unique j ; $1 \le j \le \varphi(n)$

such that $ax \equiv b_j \pmod{n}$

$\Rightarrow ax = b_j + nq_1 \quad \text{---} (2)$; $q_1 \in Z$

Similary $ay = a_i + mq_2 \quad \text{---} (3)$; $q_2 \in Z$

(110)

Putting ② & ③ in eq ①, we get

$$m(bj + mq_1) + n(q_i + mq_2) = a$$

$$\Rightarrow na_i + mbj - a = -mn(q_1 + q_2)$$

$$\Rightarrow mn \mid na_i + mbj - a$$

$$\Rightarrow na_i + mbj \equiv a \pmod{mn}$$

or $a \equiv na_i + mbj \pmod{mn}$

Thus C satisfying all condition is a RRS (mod mn).

THEOREM:

Let R be any RRS (mod m) and let a be given integer such that $(a, m) = 1$. Then there exist in R a unique integer, corresponding to a, say b such that

$$a \equiv b \pmod{m}$$

PROOF: let r be the least residue of a (mod m) so that we have

① $\cdots a \equiv r \pmod{m}$; $0 \le r < m$

and $(a, r) = (a, m) = 1$. of R

But the set of least residues i.e.

$S = \{r_1, r_2, \cdots, r_{\phi(m)}\}$ where $r_1, r_2, \cdots r_{\phi(m)}$ are all positive integers less than m and co-prime to m. Hence $r \in S$. If then b is the unique member of R of which r is the least residue (mod m), then obviously $r \equiv b \pmod{m}$ — ②

LINEAR CONGRUENCE: 111

An expression of the form

① — $ax \equiv b \pmod m$; $a \not\equiv 0 \pmod m$ is called a linear congruence modulo m. Any value of x which satisfy ① is called a Solution (or root) of the congruence. Suppose $x = h$ satisfies ①. Then $x = h$ is a Solution of ①. Obviously all integers congruent to $h \pmod m$ also satisfies ①. Hence they are, by def, all Solutions of the congruence, but these congruent Solutions are not considered as distinct or different Solutions. They are considered to consitute a Single Solution which is written as $x \equiv r \pmod m$ — ②
where r is the least residue of $h \pmod m$. Obviously ② covers all integers congurent to $h \pmod m$. Moreover, Solutions are considered as distinct or different iff they are incongruent to each other $\pmod m$.

It follows that all distinct solutions $\equiv$ of ① lie in the complete system of least residues (mod m) namely $\{0, 1, 2, \ldots, m-1\} = S$ because

① S contains least residues of every integer (mod m), and

② The integers of S are all incongruent to each other (mod m).

Exp Solve the congruence

$$6x \equiv 3 \pmod 9$$

Sol All distinct solutions of the given congruence lie in $S = \{0, 1, 2, \ldots, 8\}$. We shall then find out which of these numbers satisfy ①. Therefore

$$x = 2, \quad x = 5 \quad \& \quad x = 8$$

Satisfy ①. Hence we write Solutions

$$x \equiv 2, 5, 8 \pmod 9.$$

11.3

THEOREM:

Let m be a positive integer, a and b any integers. The linear congruence $ax \equiv b \pmod{m}$ has a solution iff $d \mid b$, $d = (a, m)$. In case $d \mid b$, the given congruence has d mutually incongruent solutions $\pmod{m}$. — (1)

PROOF: We observed that the congruence $ax \equiv b \pmod{m}$ has solution

iff $m \mid ax - b$

$\Rightarrow \quad ax - b = my \quad ; \quad y \in Z$

or $\quad ax + (-m)y = b \quad$ — (2)

Eq (2) is linear diophantine equation and has solution iff $d \mid b$ where $d = (a, m)$

If (x_0, y_0) is a particular solution, then general solution given by

$$x' = x_0 + \frac{m}{d}t$$
$$y' = y_0 + \frac{a}{d}t \quad ; \quad t \in Z$$

Thus $\quad x' = x_0 + \frac{m}{d}t \quad ; \quad t \in Z$

are all solutions of (1). But then

$$x_0 + \frac{m}{d} \cdot d \equiv x_0 \pmod{m}.$$

114

$\Rightarrow x_0 + \frac{m}{d}(d+K) \equiv x_0 + \frac{m}{d}\cdot K \pmod m$ $\quad 0 \le K < d$

Thus

$x_0, x_0 + \frac{m}{d}, \cdots x_0 + \frac{m}{d}(d-1)$ * putting $K = 0, 1, \cdots d-1$ on R.H.S *

are d solutions of (1)

Next, we show that these d solutions are mutually incongruent.

Suppose $x_0 + \frac{j}{d} m \equiv x_0 + \frac{K}{d} m \pmod m$; $j \ne K$ $\quad 0 \le j, K < d$

$\Rightarrow m \mid \frac{m}{d}(j-K)$

$\Rightarrow \frac{m}{d}(j-K) = rm$; $r \in Z$

$\Rightarrow \frac{j-K}{d} = r$

$\Rightarrow d \mid j-K$

But $j-K < d$

only possibility

$j - K = 0$

$\Rightarrow j = K$, a contradiction.

Hence $x_0 + \frac{j}{d} m \not\equiv x_0 + \frac{K}{d} m \pmod m$; $j \ne K$.

which shows that solutions are mutually incongruent.

Now we will shows that there 115
exist exactly d solutions where
$d = (a, m)$.

Let x' be any other solution different from $x_0, x_0 + \frac{m}{d}, \cdots, x_0 + \frac{d-1}{d} m$.

Then $ax' \equiv b \pmod m$

Also $ax_0 \equiv b \pmod m$

$\Rightarrow ax' \equiv ax_0 \pmod m$ — (1)*

Since $d = (a, m)$, so there exist integers r & s such that

$a = rd$, $m = sd$; $(r, s) = 1$.

putting in (1)*, to get

$rd\, x' \equiv rd\, x_0 \pmod m$

$\Rightarrow m \mid rd(x' - x_0)$

$\Rightarrow sd \mid rd(x' - x_0)$

$\Rightarrow s \mid r(x' - x_0)$

But $(r, s) = 1$

Hence $s \mid x' - x_0$

116

$\Rightarrow x' - x_0 = hs \quad ; h \in \mathbb{Z}$ ——— (2)*

By division algorithm

$h = qd + t \quad ; \quad 0 \le t < d.$

$\Rightarrow hs = (qd+t)s$

$\Rightarrow x' - x_0 = (qd+t)s$

$\Rightarrow x' = x_0 + qds + ts$

$\Rightarrow x' = x_0 + mq + ts.$

$\Rightarrow x' - (x_0 + ts) = mq$

$\Rightarrow m \mid x' - (x_0 + ts)$

$\Rightarrow x' \equiv x_0 + ts \pmod{m}$

or $x' \equiv x_0 + \frac{m}{d} \cdot t \pmod{m}$

as $\frac{m}{d} = s$

Thus $x' \equiv x_0 + \frac{t}{d} m \pmod{m} \; ; t < d$

Hence there exist exactly d solutions.

117

Methods of Solving linear congruences:

1. Method of Trials (Inspection method):

A solution of congruence $ax \equiv b \pmod{m}$ can be found by substitution $x = 0, 1, 2, \ldots m-1$

Example $4x \equiv 5 \pmod{7}$

Since $(4, 7) = 1$, so there exist exactly one solution which lies among the numbers $0, 1, 2, 3, \ldots, 6$.

As $4(3) \equiv 5 \pmod{7}$

Hence $x \equiv 3 \pmod{7}$ is the solution of given congruence.

2. Symbolic fraction method:

Let the given congruence be

$ax \equiv b \pmod{m}$; $(a, m) = 1$ —— (1)

Then we know that $ax \equiv b + mh \pmod{m}$ for every value of h. If now h is so choosen that $b + mh$ is divisible by a, then the solution of (1) is $x \equiv \frac{b+mh}{a} \pmod{m}$. The process of solution may be written down as

$x \equiv b \pmod{m} \equiv \frac{b+mh}{a} \pmod{m}$.

118

Here $\frac{b}{a} \pmod m$ is a symbolic fraction representing an integer which is the solution of $ax \equiv b \pmod m$.

Example: Solve $7x \equiv 3 \pmod{19}$

Solution: $x \equiv \frac{3}{7} \equiv \frac{3+19\times5}{7} = 14 \pmod{19}$

Hence $x \equiv 14 \pmod{19}$ is the solution.

Example:

Solve $12x \equiv 44 \pmod{59}$

$$x \equiv \frac{44}{12} \equiv \frac{11}{3} \equiv 3 + \frac{2}{3} \pmod{59}$$

$$\equiv 3 + \frac{2+2\times59}{3} \equiv 43 \pmod{59}$$

Hence $x \equiv 43 \pmod{59}$ is the solution.

Example: Solve $126x \equiv 67 \pmod{209}$

$$x \equiv \frac{67}{126} \equiv \frac{67+209h}{126} \pmod{209}$$

To find h, consider

$126 \mid 67+209h$

$\Rightarrow 67+209h \equiv 0 \pmod{126}$

or $67-43h \equiv 0 \pmod{126}$

or $h \equiv \frac{67}{43} \equiv 1 + \frac{24}{43} \pmod{126}$

$\equiv 1 + \frac{24+126k}{\quad} \pmod{126}$

To find K, consider

$$24 + 126K \equiv 0 \pmod{43}$$

$$\Rightarrow \boxed{K \equiv 8 \pmod{43}}$$

Hence $$h \equiv 1 + \frac{24 + 126(8)}{43}$$

$$\equiv 25 \pmod{126}$$

Thus $$x \equiv 67 + \frac{909 \times 25}{126} \pmod{909}$$

$x \equiv 42 \pmod{909}$ is the required solution.

3 Diophantine Equation method:

Example

Solve $6x \equiv 15 \pmod{21}$

Solution: Since $21 \mid 6x - 15$

$$\Rightarrow 6x - 15 = 21y \; ; \; y \in Z$$

or $$6x - 21y = 15$$

or $$2x - 7y = 5$$

Since $(2, 15) = 1$

$\therefore$ linear diophantine equation has a solution.

Now $2(-3) - 7(-1) = 1$

$$\Rightarrow 2(-15) - 7(-5) = 5$$

Hence $x \equiv -15 \pmod{21} \equiv 6 \pmod{21}$ is the req. solution.

120

4 let the congruence be

$$ax \equiv b \pmod{m} \; ; \; (a, m) = 1$$

Then $x = b\, a^{\varphi(m)-1}$ is the solution of given congruence.

Example: Solve

$$17x \equiv 12 \pmod{44}$$

Sol: $(17, 44) = 1$

$$\varphi(44) = \varphi(2^2 \cdot 11) \qquad \text{If } (m,n) = 1$$
$$= \varphi(2^2) \cdot \varphi(11) \qquad \varphi(mn) = \varphi(m) \cdot \varphi(n)$$
$$= 20$$

Therefore $x = 12 \times 17^{19} \pmod{44}$ is the Solution.

Now $17^2 \equiv 289 \mod 44$

$\equiv 25 \mod 44$

$17^4 \equiv 625 \mod 44$

$\equiv 9 \pmod{44}$

$17^8 \equiv 81 \equiv -7 \pmod{44}$

$17^{16} \equiv 49 \equiv 5 \pmod{44}$

Now $17^{19} \equiv 17^{16} \cdot 17^2 \cdot 17 \mod 44$

$\equiv 5 \cdot 25 \cdot 17 \mod 44$

$= 13 \mod 44$

Now $12 \times 17 \overset{9}{\equiv} 12 \times 13$ 121

$\equiv 24 \bmod 44$

Hence $x \equiv 24 \pmod{44}$

is the required solution of given congruence.

5 **continued fraction method:**

let the given congruence be

$$ax \equiv b \pmod{m}; \quad (a, m) = 1 \qquad \text{—— (1)}$$

and let $\frac{a}{m} = \langle a_1, a_2, \ldots, a_n \rangle$

where n is even. Then $x = b q_{n-1}$ satisfies (1)

Here q_{n-1} is the denominator of the penultimate (Second last) convergent to the continued fraction expension of $\frac{a}{m}$.

Definition:

let a_1 be an arbitrary integer and $a_2, a_3, \ldots, a_N$ be positive integers. Then the expression

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots + \cfrac{1}{a_N}}} \qquad \text{—— (1)}$$

is called a simple continued fraction.

For convenience ① is usually written 122

as $a_1 + \frac{1}{a_2} + \frac{1}{a_3} + \cdots + \frac{1}{a_N}$

or as $\langle a_1, a_2, a_3, \cdots, a_N \rangle$

The terms $a_1, a_2, \cdots, a_N$ of ① are called partial quotients or simply quotients

Example: find continued fraction expension of $\frac{103}{24}$.

$$\frac{103}{24} = 4 + \frac{7}{24} = 4 + \frac{1}{\frac{24}{7}} = 4 + \frac{1}{3 + \frac{3}{7}}$$

$$= 4 + \frac{1}{3 + \frac{1}{\frac{7}{3}}} = 4 + \frac{1}{3 + \frac{1}{2 + \frac{1}{3}}}$$

$$= 4 + \frac{1}{3} + \frac{1}{2} + \frac{1}{3}$$

OR $\frac{103}{24} = 4 + \frac{7}{24} = 4 + \frac{1}{\frac{24}{7}}$

Now $\frac{24}{7} = 3 + \frac{3}{7} = 3 + \frac{1}{\frac{7}{3}}$

$$\frac{7}{3} = 2 + \frac{1}{3}$$

Hence $\frac{103}{24} = 4 + \frac{1}{3} + \frac{1}{2} + \frac{1}{3}$

OR $= \langle 4, 3, 2, 3 \rangle$

193

Alternative:

$$\begin{array}{c|c|c} 24 & \begin{matrix}103\\96\end{matrix} & 4 \\ \hline 7 & \begin{matrix}24\\21\end{matrix} & 3 \\ \hline 3 & \begin{matrix}7\\6\end{matrix} & 2 \\ \hline 1 & \begin{matrix}3\\3\end{matrix} & 3 \\ & 0 & \end{array}$$

$$\frac{103}{96} = \langle 4, 3, 2, 3 \rangle$$

Example: Find the continued fraction expension of of $\frac{21}{73}$.

$$\begin{array}{c|c|c} 73 & 21 & 0 \\ & 0 & \\ \hline 21 & 73 & 3 \\ & 63 & \\ \hline 10 & 21 & 2 \\ & 20 & \\ \hline 1 & \begin{matrix}10\\10\end{matrix} & 10 \\ & 0 & \end{array}$$

$$\frac{21}{73} = \langle 0, 3, 2, 10 \rangle$$

Example: Convert $\frac{-61}{93}$ into a CF.

Self

$$\frac{-61}{93} = \langle -3, 2, 1, 7 \rangle$$

124

Def: Let $x = \langle a_1, a_2, \cdots, a_N \rangle$ —— (1)
and let $0 < n \leq N$. Then $\langle a_1, a_2, \cdots, a_n \rangle$ is called nth convergent to the continued fraction (1).

Thus $\langle a_1 \rangle$ is the first convergent

$\langle a_1, a_2 \rangle$ is the 2nd convergent.

$\vdots$

$\langle a_1, a_2, \cdots a_n \rangle$ is the nth convergent.

It is usually denoted by $\frac{P_n}{q_n}$
where P_n and q_n are integers.

Example: Let $\langle 6, 4, 3, 4, 7 \rangle$

Then $\frac{P_1}{q_1} = \langle 6 \rangle = 6$

$\frac{P_2}{q_2} = \langle 6, 4 \rangle = 6 + \frac{1}{4} = \frac{25}{4}$

$\frac{P_3}{q_3} = \langle 6, 4, 3 \rangle = 6 + \frac{1}{4 + \frac{1}{3}} = \frac{81}{13}$

and so on.

Exp: Notice that

$$\frac{163}{38} = \langle 4, 3, 2, 5 \rangle$$

Here the CF has even number of partial quotients namely four. However we can

also express $\frac{163}{38}$ as a continued fraction with odd number of partial quotients. Thus

$$\frac{163}{38} = 4 + \frac{1}{3} + \frac{1}{2} + \frac{1}{5}$$

$$= 4 + \frac{1}{3} + \frac{1}{2} + \frac{1}{4} + \frac{1}{1}$$

$$= \langle 4, 3, 2, 4, 1 \rangle$$

Remark A rational number x can always be represented as a continued fraction with an odd or even number of partial quotients according to our choice.

Exp Solve $47x \equiv 11 \pmod{249}$

Sol: $(47, 249) = 1$. Hence there is only one solution.

Now $\frac{47}{249} = \langle 0, 5, 3, 2, 1, 4 \rangle$

With even number of partial quotients.

Therefore $x = 11 q_5$ satisfies the given congruence. The denominators of the successive convergents to $\frac{47}{249}$ are $1, 5, 16, 37, 53$. So $q_5 = 53$.

Hence $x \equiv 11 \times 53 \pmod{249}$

$x \equiv 85 \pmod{249}$ is the solution.

126

Exp Find the general solution of $37x \equiv 7 \pmod{127}$

Sol $(37, 127) = 1$, therefore only one solution exist.

Now $\frac{37}{127} = \langle 0, 3, 2, 3, 5 \rangle$.

This has odd number of quotients.

So we write this CF as

$\frac{37}{127} = \langle 0, 3, 2, 3, 4, 1 \rangle$. The denominators

Successive convergents to this CF are $1, 3, 7, 24, 103$. $q_5 = 103$.

Hence $x \equiv 7 \times 103 \pmod{127}$

$\equiv 86 \pmod{127}$ is the solution.

HM KHALID MAHMOOD

155

Assignment:

Solve the following linear congruences.

(1) $85x \equiv 10 \pmod{29}$ (2) $5x \equiv 2 \pmod{26}$

(3) $140x \equiv 133 \pmod{301}$ (4) $9x \equiv 12 \pmod{15}$

(5) $30x \equiv 52 \pmod{49}$ (6) $99x \equiv 100 \pmod{101}$

(7) $3x \equiv 5 \pmod{9}$ (8) $6x \equiv 3 \pmod{18}$

(9) $12x \equiv 36 \pmod{56}$ (10) $5x \equiv 3 \pmod{27}$

(11) $49x \equiv 93 \pmod{125}$ (12) $9x \equiv 3 \pmod{9}$

(13) $6x \equiv 15 \pmod{21}$ (14) $18x \equiv 60 \pmod{66}$

(15) $35x \equiv 14 \pmod{84}$ (16) $99x \equiv 100 \pmod{10}$

(17) $6x \equiv 15 \pmod{24}$ (18) $7x \equiv 4 \pmod{12}$

(19) $17x \equiv 14 \pmod{2}$ (20) $3x \equiv 5 \pmod{7}$

Solve the system of congruences

(1) $24x \equiv 20 \pmod{28}$
$10x \equiv 6 \pmod{32}$

(2) $6x \equiv 4 \pmod{8}$
$28x \equiv 21 \pmod{35}$
$22x \equiv 11 \pmod{99}$

(3) $28x \equiv 36 \pmod{40}$
$39x \equiv 33 \pmod{45}$
$32x \equiv 76 \pmod{84}$

(4) $4x \equiv 13 \pmod{15}$
$5x \equiv 4 \pmod{21}$

(5) Find an integer which leave remainder 1, 6 when divided by 5, 7 respectively and is divisible by 2 and 3. 136

(6) Find the multiple of 11 that leave remainder 1 when divided by 2, 3, 5 and 7 respectively.

(7) $x \equiv 1 \pmod 4$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

(8) $3x \equiv 2 \pmod 5$
$6x \equiv 4 \pmod{14}$
$10x \equiv 3 \pmod{11}$

(9) $x \equiv 1 \pmod 5$
$x \equiv 2 \pmod 6$
$x \equiv 3 \pmod 7$

(10) $x \equiv 5 \pmod 6$
$x \equiv 3 \pmod{10}$
$x \equiv 8 \pmod{15}$

(11) What is the smallest number of eggs in a basket if one egg is left over when the eggs are removed 2, 3, 4, 5 or 6 at a time, but no eggs are left over when they are removed 7 at a time.

(12) Solve the linear congruence $17x \equiv 9 \pmod{276}$ by chinese R. theorem

Hint $276 = 3 \cdot 4 \cdot 23$

(13) Find the smallest integer $a > 5$ such that $5 \mid a$, $6 \mid a+1$, $7 \mid a+2$ and $8 \mid a+3$.

137

Sol ① $\left.\begin{matrix} 24x \equiv 20 \pmod{28} \\ 10x \equiv 6 \pmod{32} \end{matrix}\right\}$ —①

Since $(24, 28) = 4$ & $4 \mid 20$

$(10, 32) = 2$ & $2 \mid 6$

Thus ① becomes

$\left.\begin{matrix} 6x \equiv 5 \pmod 7 \\ 5x \equiv 3 \pmod{16} \end{matrix}\right\}$ —②

Again the solutions of ② are

$\left.\begin{matrix} x \equiv 2 \pmod 7 \\ x \equiv 7 \pmod{16} \end{matrix}\right\}$ —③

Now solve ③ by chinese R.

we get $x \equiv 23 \pmod{112}$

is the solution of system ①

Sol (9) (Alternative method)

$x \equiv 1 \pmod 5$ —①

$x \equiv 2 \pmod 6$ —②

$x \equiv 3 \pmod 7$ —③

① $\Rightarrow$ $x = 5t + 1$, $t \in Z$ —④

put in ②

$5t + 1 \equiv 2 \pmod 6$

$5t \equiv 1 \pmod 6$

$\rightarrow t \equiv 5 \pmod 6$

138

$\Rightarrow t = 6u+5$ put in (4), $u \in Z$.

$6u+5 \equiv 3 \pmod 7$

or $6u \equiv -2 \pmod 7$

or $6u \equiv 5 \pmod 7$

or

$x = 5(6u+5)+1$

(5) $\longrightarrow$ $x = 30u + 26$ put in (3)

$30u+26 \equiv 3 \pmod 7$

or $u \equiv 6 \pmod 7$

or $u = 7v+6$ for $v \in Z$

put in (5)

$x = 30(7v+6)+26$

or $x = 210v + 206$

or $x \equiv 206 \pmod{210}$

which is the required simultaneous solution of given system.

139

Polynomial Congruence:

Def A polynomial congruence is a congruence of the form $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots a_n \equiv 0 \pmod m$, where $n \geq 1$ and $a_0, a_1, \cdots, a_n \in Z$ if $a_0 \not\equiv 0 \pmod m$, n is called the degree of $f(x) \pmod m$.

e.g $3x^3 + 5x^2 + 6x + 4 \equiv 0 \pmod 5$ is a polynomial congruence of degree $3 \pmod 5$.

If x_0 is an integer such that $f(x_0) \equiv 0 \pmod m$ then $x \equiv x_0 \pmod m$ is a solution of the polynomial congruence $f(x) \equiv 0 \pmod m$.

Furthermore, the solution of a polynomial congruence $f(x) \equiv 0 \pmod m$ can be found by substituting the integers $\{0, 1, 2, \cdots, m-1\}$.

Moreover if $f(x) = a_n x^n + \cdots + a_0$ &
$g(x) = b_n x^n + \cdots + b_0$
be two polynomials such that
$a_i \equiv b_i \pmod m \quad \forall i$
then $f(x) \equiv g(x) \pmod m$.

e.g $9x^3 + 15x^2 + 7x + 6 \equiv 4x^3 + 2x + 1 \pmod 5$.

1140

Factor Theorem:

Let $f(x) \equiv 0 \pmod m$ be a congruence of degree n. Then $x \equiv a \pmod m$ is a solution of $f(x) \equiv 0 \pmod m$ iff, there exist a polynomial $q(x)$ such that

$$f(x) \equiv (x-a)\, q(x) \pmod m$$

PROOF: Suppose $x \equiv a \pmod m$ is a solution of $f(x) \equiv 0 \pmod m$

Dividing the polynomial $f(x)$ by $x-a$. Then we must have a polynomial $q(x)$ and r such that

$$f(x) = (x-a)\, q(x) + r \quad \text{---} (1)$$

$$2\overline{)\begin{matrix}3\\7\\2\\1\end{matrix}}$$

$7 = 2(3)+1$

$2(q(x))+r)$

$x-a$

Then $f(a) = r$, put in (1)

$$f(x) = (x-a)\, q(x) + f(a) \quad \text{---} (2)$$

Since $x \equiv a \pmod m$ is a solution of $f(x) \equiv 0 \pmod m$ then $f(a) \equiv 0 \pmod m$

Then (2) becomes

$$f(x) = (x-a)\, q(x) + f(a)$$
$$\equiv (x-a)\, q(x) + 0 \pmod m$$

Hence $f(x) \equiv (x-a)\, q(x) \pmod m$

1+1

Conversely, suppose that there exist a polynomial $q(x)$ s.t $f(x) \equiv (x-a)\,q(x) \pmod m$

then $f(a) \equiv 0 \pmod m$

Hence $x \equiv a \pmod m$ is a solution of $f(x) \equiv 0 \pmod m$.

* **Lagrange's Theorem:**

If p is a prime then the congruence $f(x) \equiv 0 \pmod p$ of degree n has almost n mutually incongruent solutions.

Proof: By induction on degree of f.

Take $n = 1$

then $f(x) = a_1 x + a_0$; $a_1 \neq 0$

and we know that $a_1 x + a_0 \equiv 0 \pmod p$ with $p \nmid a_1$ has a unique solution.

Suppose that result is true for all polynomials of degree $k-1 \pmod p$.

and $f(x)$ is a polynomial of degree $k \pmod p$. (say) $f(x) = a_k x^k + \cdots + a_0$; $a_k \neq 0$

Let (if possible) $f(x)$ have $k+1$ incongruent solutions modulo p, say $\omega_1, \omega_2, \ldots, \omega_{k+1}$.

Define $g(x) = f(x) - a_k (x-\omega_1)(x-\omega_2)\cdots(x-\omega_k)$

term

$k-1 \quad k-2$

142

If $1 \le i \le K$, then $g(\omega_i) \equiv 0 \pmod p$

as $g(\omega_i) = f(\omega_i) - a_K(\omega_i - \omega_1)\cdots(\omega_i - \omega_K)$

Also degree of $g(x)$ is atmost $K-1$.

Hence by induction hypothesis $g(x)$ has atmost $K-1$ incongruent solutions.

Hence $g(x) \equiv 0 \pmod p$ $\xleftrightarrow{\text{if integers } x.}$ $\xleftarrow{x \text{ is congruent to any one of } K-1 \text{ of induction.}}$

In particular $x = \omega_{K+1}$

$$g(\omega_{K+1}) \equiv 0 \pmod p$$

$$\Rightarrow f(\omega_{K+1}) - a_K(\omega_{K+1} - \omega_1)\cdots(\omega_{K+1} - \omega_K) \equiv 0 \pmod p$$

$$\Rightarrow a_K(\omega_{K+1} - \omega_1)\cdots(\omega_{K+1} - \omega_K) \equiv 0 \pmod p$$

Then there exist i ; $1 \le i \le K$

$-7 \equiv 0 \bmod 2$
$7 \equiv (-0) \bmod 2$
$7 \equiv 0 \bmod 2$

Such that $\omega_{K+1} - \omega_i \equiv 0 \pmod p$

$$\Rightarrow \omega_{K+1} \equiv \omega_i \pmod p \; ; \; i \ne K+1$$

This contradicts our supposition that $\omega_1, \omega_2, \ldots, \omega_{K+1}$ are incongruent (mod p). Hence $f(x)$ has atmost K mutually incongruent solutions.

H.M KHALID MAHMOOD (P.U)

THEOREM: 143

* Let $f(x) \equiv 0 \pmod m$ where $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ $p_1 < p_2 \cdots < p_n$; $\alpha_i > 0$.

Then $x \equiv a \pmod m$ is a Solution iff $f(a) \equiv 0 \pmod{p_i^{\alpha_i}}$; $1 \le i \le n$.

PROOF: Since $f(x) \equiv 0 \pmod m$ ——— (1)

$\Rightarrow m \mid f(x)$

$\Rightarrow \prod_{i=1}^{n} p_i^{\alpha_i} \mid f(x)$ $\quad m = p_1^{\alpha_1} \cdots p_n^{\alpha_n} = \prod_{i=1}^{n} p_i^{\alpha_i}$

i-e $p_1^{\alpha_1} \mid f(x), \cdots, p_n^{\alpha_n} \mid f(x)$

OR

$$\left.\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) &\equiv 0 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_n^{\alpha_n}} \end{aligned}\right\} \text{——— (2)}$$

If $x \equiv a \pmod m$ is a Solution of (1)

then (2) gives

$$f(a) \equiv 0 \pmod{p_1^{\alpha_1}}$$
$$\vdots$$
$$f(a) \equiv 0 \pmod{p_n^{\alpha_n}}$$

i-e $f(a) \equiv 0 \pmod{p_i^{\alpha_i}}$; $1 \le i \le n$.

Conversely: Suppose that

$f(a) \equiv 0 \pmod{p_i^{\alpha_i}}$ $\quad 1 \le i \le n$

then $f(a) \equiv 0 \pmod{\prod_{i=1}^{n} p_i^{\alpha_i}}$ $\because p_1^{\alpha_1}, \cdots p_n^{\alpha_n}$ are relatively prime.

$\Rightarrow f(a) \equiv 0 \pmod m$

that is $x \equiv a \pmod m$ is a Solution of $f(x) \equiv 0 \pmod m$.

Remark: Notice that the number of solutions 1441
in ① is equal to the product of the number of solutions of each congruence of system in ②. Moreover every solution of $f(x) \equiv 0 \pmod{p^\alpha}$ is also a solution of $f(x) \equiv 0 \pmod{p}$ because if $x \equiv a \pmod{p^\alpha}$ is a solution of $f(x) \equiv 0 \pmod{p^\alpha}$

then $f(a) \equiv 0 \pmod{p^\alpha}$

$\Rightarrow p^\alpha \mid f(a)$

$\Rightarrow p \mid f(a)$

$\Rightarrow f(a) \equiv 0 \pmod{p}$

That is $x \equiv a \pmod{p}$ is a solution of $f(x) \equiv 0 \pmod{p}$ but converse may not be true. That is a solution $f(x) \equiv 0 \pmod{p}$ may not be a solution of $f(x) \equiv 0 \pmod{p^\alpha}$

Working Rule:

In order to solve $f(x) \equiv 0 \pmod{p^\alpha}$ we will solve $f(x) \equiv 0 \pmod{p^{\alpha-1}}$.
To solve $f(x) \equiv 0 \pmod{p^{\alpha-1}}$, we will solve $f(x) \equiv 0 \pmod{p^{\alpha-2}}$ and continue the process, we have to solve $f(x) \equiv 0 \pmod{p}$

145

Example: Solve the congruence,

$$x^2+1 \equiv 0 \pmod{5^3}$$

Solution: consider $x^2+1 \equiv 0 \pmod 5$

Then $x \equiv 2 \pmod 5$ and $x \equiv 3 \pmod 5$ are its solutions.

Then $x = 2+5t$ and $x = 3+5t$; $t \in Z$ are the general solutions.

Now consider

$$x^2+1 \equiv 0 \pmod{5^2}$$

If $x = 3+5t$ ——① is its solution, then

$$(3+5t)^2+1 \equiv 0 \pmod{5^2}$$

$$\Rightarrow \quad 10+30t \equiv 0 \pmod{5^2}$$

$$\Rightarrow \quad 2+6t \equiv 0 \pmod 5$$

$$\Rightarrow \quad t \equiv 3 \pmod 5$$

or $t = 3+5s$ put in ① $s \in Z$.

$$x = 3+5(3+5s)$$

$$x = 18+25s \text{ ——②}$$

Again consider

$$x^2+1 \equiv 0 \pmod{5^3}$$

Then $(18+25s)^2+1 \equiv 0 \pmod{5^3}$

$$\Rightarrow \quad 325+900s \equiv 0 \pmod{5^3}$$

$$\Rightarrow \quad 13+36s \equiv 0 \pmod 5$$

$$\Rightarrow \quad 3+s \equiv 0 \pmod 5$$

$$\Rightarrow \quad s = 2 \pmod 5$$

146

i.e. $s = 2 + 5r \; ; \; r \in Z$

put in (2)

$x = 18 + 25(2 + 5r)$

or $x = 68 + 625r$

or $x \equiv 68 \pmod{5^3}$ is the required solution.

Case 2 If $x = 2 + 5t$, we get

$x \equiv 57 \pmod{5^3}$ is the required solution.

Assignment:

(1) Solve $x^5 + x + 1 \equiv 0 \pmod{7^2}$

Starting $x \equiv 2 \pmod 7$ and $x \equiv 4 \pmod 7$

Ans $x \equiv 30 \pmod{7^2}$ and $x \equiv 11 \pmod{7^2}$

(2) $x^4 + x^3 + 1 \equiv 0 \pmod{5^3}$

Ans $x \equiv 27 \pmod{5^3}$

(3) $x^5 + x^3 + 8 \equiv 0 \pmod{3^4}$

Ans $x \equiv 50 \pmod{3^4}$

(4) $x^3 - 4x^2 + 5x - 6 \equiv 0 \pmod{3^3}$

Ans $x \equiv 3 \pmod{27}$

(5) $x^2 + x + 7 \equiv 0 \pmod{3^3}$

Ans $x \equiv 4, 13, 22 \pmod{3^3}$

(6) $x^2 - 7x + 2 \equiv 0 \pmod{5^3}$

Ans $x \equiv 93 \pmod{5^3}$ and $x \equiv 29 \pmod{5^3}$

(7) Show that $x^2+7x+1 \equiv 0 \pmod{3^3}$ has no solution. 147

*(8) Solve $x^3+x+30 \equiv 0 \pmod{7^2}$

Ans: $x \equiv 4, 11, 18, 25, 32, 39, 46 \pmod{7^2}$

*(9) $x^3+x^2+4x+9 \equiv 0 \pmod{5^3}$

Ans: $x \equiv 66 \pmod{5^3}$

THEOREM: Let $x=a$ be a least solution of $f(x) \equiv 0 \pmod{p^h}$ then the least solution of $f(x) \equiv 0 \pmod{p^{h+1}}$ corresponding to $x=a$ are as under:

Conditions	Solutions $\pmod{p^{h+1}}$
(i) If $f'(a) \not\equiv 0 \pmod{p}$	There is only one solution $a+p^h q$, $0 \le q < p$ and $f'(a)\, q \equiv -\frac{f(a)}{p^h} \pmod{p}$
(ii) If $f'(a) \equiv 0 \pmod{p}$ and $f(a) \equiv 0 \pmod{p^{h+1}}$	there are p solutions $a+p^h q$, $q = 0, 1, 2, \ldots, \overline{p-1}$
(iii) If $f'(a) \equiv 0 \pmod{p}$ and $f(a) \not\equiv 0 \pmod{p^{h+1}}$	There is no solution.

148

PROOF: Since $x \equiv a_1 \pmod{p^h}$ is a solution of $f(x) \equiv 0 \pmod{p^h}$

then $p^h \mid x - a$

$\Rightarrow x = a + p^h q \quad ; q \in Z.$

If x is a solution of $f(x) \equiv 0 \pmod{p^{h+1}}$

then $f(a + p^h q) \equiv 0 \pmod{p^{h+1}}$

By Taylor's theorem

$$f(a+p^h q) = f(a) + p^h q f'(a) + \frac{(p^h q)^2}{2!} f''(a) + \cdots + \frac{(p^h q)^n}{n!} f^{n}(a)$$

$$= f(a) + p^h q f'(a) + \text{terms divisible by } p^{h+1}$$

$$\equiv f(a) + p^h q f'(a) \pmod{p^{h+1}}$$

It follows that $a + p^h q$ is a solution

iff $f(a) + p^h q f'(a) \equiv 0 \pmod{p^{h+1}}$

or $f'(a) \cdot q \equiv -\frac{f(a)}{p^h} \pmod{p} \quad \text{---(1)}$

Case (i) If $f'(a) \not\equiv 0 \pmod{p}$

$\Rightarrow p \nmid f'(a)$

$\Rightarrow (f'(a), p) = 1$

and by (1) $1 \mid -\frac{f(a)}{p^h}$

Hence (1) is solvable and has only one solution

144

Case(ii) If $f'(a) \equiv 0 \pmod{p}$

$\Rightarrow p \mid f'(a)$

$\Rightarrow (f'(a), p) = p$ ⟵ (1*)

Also $f(a) \equiv 0 \pmod{p^{h+1}}$

or $\frac{f(a)}{p^h} \equiv 0 \pmod{p}$

$\Rightarrow p \mid \frac{f(a)}{p^h}$

or $p \mid -\frac{f(a)}{p^h}$

Hence (1) has p solutions corresponding to $q = 0, 1, 2, \cdots p-1$.

Case(iii) If $f'(a) \equiv 0 \pmod{p}$

then $(f'(a), p) = p$

Also $f(a) \not\equiv 0 \pmod{p^{h+1}}$

imply $p \nmid -\frac{f(a)}{p^h}$

Hence (1) has no solution

which completes the proof.

150

Exp 8 Solve $x^3+x+30 \equiv 0 \pmod{7^2}$ —— (1)

Solution: the Solutions of $f(x) \equiv 0 \pmod 7$ —— (2)

are $x \equiv 4, 6 \pmod 7$

Case When $x \equiv 6 \pmod 7$

$f'(x) = 3x^2+1$; $f(x) = x^3+x+30$

$f'(6) = 109$

$\equiv 4 \pmod 7$

This falls under case (i)

Therefore there is only one Solution namely $6+7q$ where q is given by

$$f'(6)\, q \equiv -\frac{f(6)}{7} \pmod 7$$

or $$4q \equiv -\frac{252}{7} \equiv -1 \pmod 7$$

So $q \equiv 5 \pmod 7$ and

required Solution is

$x = 6+7\cdot 5$

or $x \equiv 41 \pmod{7^2}$

Case When $x \equiv 4 \pmod 7$

$f'(4) = 49 \equiv 0 \pmod 7$

and $f(4) = 98 \equiv 0 \pmod{7^2}$

This falls under case (ii) Hence the Solutions of (1) are $x = 4, 4+7, 4+2\cdot 7, \ldots, 4+6\cdot 7 \pmod{7^2}$

Therefore the complete solution of ① is 151

$$x = 4, 11, 18, 25, 32, 39, 41, 46 \pmod{7^2}$$

Example (9) Find the solutions of

$$x^3 + x^2 + 4x + 9 \equiv 0 \pmod{5^3}$$

Solution: The solutions of $f(x) \equiv 0 \pmod 5$ are $x \equiv 1, 4 \pmod 5$

Case when $x \equiv 1 \pmod 5$

$$f'(x) = 3x^2 + 2x + 4$$
$$f'(1) = 9 \equiv (4 \bmod 5)$$

Hence there is only one solution.

So $$9q \equiv -\frac{f(1)}{5} \pmod 5$$

$$9q \equiv -\frac{15}{5} \equiv 2 \pmod 5$$

Thus $q \equiv 3 \pmod 5$

Then $x = 1 + 5 \times 3 = 16 \pmod{5^2}$

is the solution of ①

Now for $f(x) \equiv 0 \pmod{5^3}$

when $x \equiv 16 \pmod{5^2}$

$$f'(16) \equiv f'(1) \equiv 4 \pmod 5$$

So $$4q \equiv -\frac{f(16)}{5^2} \pmod 5$$

$$4q \equiv -\frac{4425}{25} \equiv 3 \pmod 5$$

or $q \equiv 2 \pmod 5$

152

Therefore Solution is

$$x \equiv 16 + 5^2 \cdot 2 \equiv 66 \pmod{5^3}$$

Case When $x \equiv 4 \pmod 5$

$$f'(4) = 60 \equiv 0 \pmod 5$$

Also $f(4) = 105 \not\equiv 0 \pmod{5^2}$

This falls under case (iii)

Hence there exist no Solution

$$f(x) \equiv 0 \pmod{5^2}$$

and therefore $f(x) \equiv 0 \pmod{5^3}$.

Thus given congruence has only one Solution namely $x \equiv 66 \pmod{5^3}$.

153

Example: Solve the congruence

$$2x^2 - 3x + 1 \equiv 0 \pmod{105} \quad \text{---} (1)$$

Solution: $105 = 3 \cdot 5 \cdot 7$, then (1) is equivalent to the system

$$\left.\begin{aligned} 2x^2 - 3x + 1 &\equiv 0 \pmod 3 \\ 2x^2 - 3x + 1 &\equiv 0 \pmod 5 \\ 2x^2 - 3x + 1 &\equiv 0 \pmod 7 \end{aligned}\right\} \quad \text{---} (2)$$

The solutions of above congruences are

$$x \equiv 1, 2 \pmod 3$$
$$x \equiv 1, 3 \pmod 5$$
$$x \equiv 1, 4 \pmod 7$$

Therefore (2) is equivalent to $2 \times 2 \times 2 = 8$ systems which are given by

$$x \equiv a \pmod 3 \; ; \; a = 1, 2$$
$$x \equiv b \pmod 5 \; ; \; b = 1, 3$$
$$x \equiv c \pmod 5 \; ; \; c = 1, 4$$

Solving by chinese remainder theorem, we get

$$x \equiv 1, 8, 11, 43, 46, 53, 71, 88 \pmod{105}$$

Assignment: Find all solutions of (1)

(1) $2x^3 + 3x^2 + 5x + 4 \equiv 0 \pmod{140}$ Ans 12 Solutions.

(2) $2x^3 + x^2 - 3x + 10 \equiv 0 \pmod{60}$ Ans 4 Solutions

(3) $x^2 + 3x + 2 \equiv 0 \pmod{35}$ Ans 4 Solutions.

154

(4) $x^2+4x+3 \equiv 0 \pmod{77}$; 4 Solutions.

(5) Show that $x^2 \equiv 1 \pmod{15}$ has four incongruent integral Solutions.

Fermat's Little Theorem (FLT$_1$):

Statement: If p is a prime and a is an integer, then $a^p \equiv a \pmod{p}$

PROOF: Since p is prime, so either $p \mid a$ or $(a, p) = 1$

case(i) If $p \mid a$

then $a \equiv 0 \pmod{p}$

$\Rightarrow a^p \equiv 0 \pmod{p}$

$\Rightarrow a^p \equiv a \pmod{p}$ (by Transitive law)

case(ii) If $(a, p) = 1$, then the integers $a, 2a, 3a, \cdots, \overline{p-1}$ are mutually incongruent $\overline{p-1}$ integers and co-prime to p.

But then $1, 2, \cdots, \overline{p-1}$ is a RRS $\pmod{p}$.

Hence for each j, $1 \le j \le p-1$, there exist a unique i, $1 \le i \le \overline{p-1}$ such that

$$ja \equiv i \pmod{p}$$

Therefore

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

$$\Rightarrow a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p} \quad \text{as } (p, (p-1)!) = 1$$

$$\Rightarrow a^p \equiv a \pmod{p}$$

Thus in either case, we have the

155

THEOREM: $x^{p-1} \equiv 1 \pmod{p}$ has exactly $p-1$ solutions where p is a prime number.

PROOF: By Fermat's theorem $x^{p-1} \equiv 1 \pmod{p}$ is satisfied by all values of x such that $(x, p) = 1$

Then $x = 1, 2, \ldots p-1$ all are solutions.

Moreover by Lagranges theorem

$x^{p-1} - 1 \equiv 0 \pmod{p}$ has atmost $p-1$ mutually incongruent solutions.

Combing the results of Fermats and Lagranges we get the theorem.

THEOREM: If p is a prime number and d is any positive divisor of $p-1$. Then $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions.

PROOF: Since $d \mid p-1$, so there exist polynomial $q(x)$ such that

$$x^{p-1} = (x^d - 1)\, q(x)$$

i.e. $$x^{p-1} \equiv (x^d - 1)\, q(x) \pmod{p}$$

where $q(x)$ is a polynomial of degree $p-1-d$.

By Lagrange's theorem

$q(x) \equiv 0 \pmod{p}$ has atmost $p-1-d$ solutions.

156

Also $x^{p-1} \equiv 0 \pmod{p}$ has exactly $p-1$ solutions where $(x, p) = 1$

thus $x^d - 1 \equiv 0 \pmod{p}$ must have atleast d solutions $(d = (p-1) - (p-1-d))$.

But by Lagrange's theorem,

$x^d - 1 \equiv 0 \pmod{p}$ has atmost d solutions. Combing above two results, $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions.

Lemma: Let p and q be distinct primes such that

$a^p \equiv a \pmod{q}$ & $a^q \equiv a \pmod{p}$

Then $a^{pq} \equiv a \pmod{pq}$

PROOF: By FLT,

$(a^p)^q \equiv a^p \pmod{q}$

But $a^p \equiv a \pmod{q}$ (given)

thus $a^{pq} \equiv a \pmod{q}$ by transitive law

$\Rightarrow q \mid a^{pq} - a$ — ①

Similarly $p \mid a^{pq} - a$ — ②

① & ② imply

$pq \mid a^{pq} - a$ ∵ p & q are distinct primes.

Hence $a^{pq} \equiv a \pmod{pq}$.

157

THEOREM: If p and q are distinct primes, then prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

PROOF: Since p and q are distinct primes, so by FLT,

$$p^q \equiv p \pmod{q}$$

$$\Rightarrow p^{q-1} \equiv 1 \pmod{q} \quad \text{---(i)}$$

Also $q^{q-1} \equiv 0 \pmod{q}$ ---(ii)

(i) & (ii) imply

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$$

or $$q \mid p^{q-1} + q^{p-1} - 1 \quad \text{---(1)}$$

Also $q^p \equiv q \pmod{p}$

$$\Rightarrow q^{p-1} \equiv 1 \pmod{p}$$

& $p^{q-1} \equiv 0 \pmod{p}$

both imply $p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$

$$\Rightarrow p \mid p^{q-1} + q^{p-1} - 1 \quad \text{---(2)}$$

(1) & (2) imply $pq \mid p^{q-1} + q^{p-1} - 1$ ∵ p & q are distinct primes

Hence $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

158

EULER'S THEOREM:

Statement: Let a and $m>0$ be integers such that $(a,m)=1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$

Proof: If $m=1$, then $\varphi(1)=1$

Also $1 \mid a-1 \quad \forall a.$

$\Rightarrow a \equiv 1 \pmod{1}$

$\Rightarrow a^1 \equiv 1 \bmod(\varphi(1))$

$\Rightarrow a^{\varphi(m)} \equiv 1 \pmod{\varphi m}$

Thus theorem is true for $m=1$.

Suppose $m>1$.

Let $\{a_1, a_2, \cdots a_{\varphi(m)}\}$ be a RRS(mod m) and consider

$A = \{aa_1, aa_2, \cdots aa_{\varphi(m)}\}$.

Then A is a RRS(mod m) (Self).

Then for each i; $1 \le i \le \varphi(m)$ there exist a unique j $1 \le j \le \varphi(m)$ s.t

$$aa_i \equiv a_j \pmod{m} \quad 1 \le i, i \le \varphi(m)$$

$$\Rightarrow aa_1 \cdot aa_2 \cdots aa_{\varphi(m)} \equiv a_1 \cdot a_2 \cdots a_{\varphi(m)} \pmod{m}$$

$$\Rightarrow a^{\varphi(m)} a_1 \cdot a_2 \cdots a_{\varphi(m)} \equiv a_1 \cdot a_2 \cdots a_{\varphi(m)} \pmod{m}$$

$$\Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m} \quad \because (a, a_i) = 1 \; ; 1 \le i \le \varphi(m)$$

which completes the theorem

159

Corollary (Alternative proof of FLT$_1$):
If p is prime and a is any integer, then
$a^p \equiv a \pmod{p}$

Proof: If $p \mid a$, then $a \equiv 0 \pmod{p}$
$\Rightarrow a^p \equiv 0 \pmod{p}$
$\Rightarrow a^p \equiv a \pmod{p}$

If $p \nmid a$, then $(a, p) = 1$
By Euler's theorem

$$a^{\phi(p)} \equiv 1 \pmod{p}$$
$$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$$
$$\Rightarrow a^p \equiv a \pmod{p}$$

REMARK:
(1) Converse of FLT$_1$ is false that is for $(a, m) = 1$ and $a^m \equiv a \pmod{m}$ then m is not necessarily prime.
e.g. $3^{91} \equiv 3 \pmod{91}$
where $(3, 91) = 1$
But $91 = 7 \cdot 13$, which is not prime.
(2) If $a^p \equiv a \pmod{q}$ & $a^q \equiv a \pmod{p}$
$\Rightarrow a^{pq} \equiv a \pmod{pq}$, then it is not necessary that p and q are primes.

160

Example: Let $(a, 77) = 1$, then $a^{30} \equiv 1 \pmod{77}$

Solution: Since $(a, 77) = 1$

$\Rightarrow (a, 7) = 1$ & $(a, 11) = 1$

By Euler's theorem

$a^{\phi(7)} \equiv 1 \pmod 7$ & $a^{\phi(11)} \equiv 1 \pmod{11}$

$\Rightarrow a^6 \equiv 1 \pmod 7$ & $a^{10} \equiv 1 \pmod{11}$

$\Rightarrow (a^6)^5 \equiv 1 \pmod 7$ & $(a^{10})^3 \equiv 1 \pmod{11}$

$\Rightarrow a^{30} \equiv 1 \pmod 7$ & $a^{30} \equiv 1 \pmod{11}$

$\Rightarrow 7 \mid a^{30} - 1$ & $11 \mid a^{30} - 1$

$\Rightarrow 77 \mid a^{30} - 1$.

$\Rightarrow a^{30} \equiv 1 \pmod{77}$.

Example: Find last two digits of 3^{100} in its decimal representation.

Solution: Since any number n has a decimal representation

$n = a_m a_{m-1} \cdots a_1 a_0$

$= a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$

$0 \le a_i \le 9$ $a_m \neq 0$

161

Therefore to find last two digits, we must find remainder when n is divided by 100. Now $(3, 100) = 1$

then $3^{\varphi(100)} \equiv 1 \pmod{100}$

$3^{40} \equiv 1 \pmod{100}$

$\varphi(100)$
$= \varphi(2^2 \cdot 5^2)$
$= \varphi(2^2)\ \varphi(5^2)$
$= 2 \cdot 2\ \ 2 \cdot 5$
$= 4 \cdot 10$
$= 40$

then $100 = 3^{40 \cdot 2 + 20}$

$= (3^{40})^2 \cdot 3^{20}$

$\equiv 3^{20} \pmod{100}$

$\equiv (3^5)^4 \pmod{100}$

$\equiv (43)^4 \pmod{100}$

$\equiv (1849)^2 \pmod{100}$

$\equiv (49)^2 \pmod{100}$

$\equiv 01 \pmod{100}$

Hence last two digits are 01

162

Assignment:

(1) Find Remainder

(i) when 5^{40} is divided by 13

$5^{13} \equiv 5 \pmod{13}$

(ii) when 2^{35} is divided by 13

(iii) when 41^{75} is divided by 3

(iv) when $(473)^{38}$ is divided by 5.

(v) when $(41)^{75}$ is divided by 13

(vi) when 5^{38} is divided by 11

(vii) 3^{57} is divided by 7

Ans 1, 7, 2, 4, 8, 4.

(2) Find last two digits in decimal representation of

(i) 7^{100} (ii) 11^{100}

Ans 01,

(3) Show that $5^{38} \equiv 4 \pmod{11}$

(4) Show by FLT, that 6 is the solution of $x^7 + x + 2 \equiv 0 \pmod{7}$

(5) Find Remainder when 72^{1001} is divided by 31, Ans = 19

$72 \equiv 10 \pmod{31}$

$(72)^{1001} \equiv (10)^{1001} \pmod{31}$

$(10, 31) = 1$, $10^{30} \equiv 1 \pmod{31}$

(6) Find least residue of $7^{973} \pmod{72}$, Ans = 7

163

THEOREM: Let the congruence be

(1) —— $ax \equiv b \pmod{m}$; $(a, m) = 1$

then $x = b\, a^{\varphi(m)-1}$ Satisfies (1)

PROOF: Since $(a, m) = 1$, then by Euler's theorem

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

$$\Rightarrow b\, a^{\varphi(m)} \equiv b \pmod{m}$$

$$\Rightarrow a\left(b a^{\varphi(m)-1}\right) \equiv b \pmod{m}$$

Thus $b\, a^{\varphi(m)-1}$ Satisfies (1).

Problem: prove that the following congruences hold for each positive integer n.

(i) $2^{2n} \equiv 1 \pmod{3}$

(ii) $2^{3n} \equiv 1 \pmod{7}$

(iii) $2^{4n} \equiv 1 \pmod{15}$

Hint: $2^2 \equiv 1 \pmod{3}$

Problem: Let p be an odd prime, then

(i) $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$

(ii) $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$

Solution: By Fermat Little theorem

$$1^p \equiv 1 \pmod{p}$$

$$2^p \equiv 2 \pmod{p}$$

$$\vdots$$

$$(p-1)^p \equiv p-1 \pmod{p}$$

$$\Rightarrow 1^p + 2^p + \cdots + (p-1)^p \equiv \frac{p(p-1)}{2} \pmod{p}$$

$\equiv 0 \pmod{p}$ if $p-1$ is even

Def: An integer n for which $2^n \equiv 2 \pmod{n}$ is called a pseudo prime.

e.g. 341, 561, 645, 1105

164

(ii) By Euler's theorem

$1^{\phi(p)} \equiv 1 \pmod p \Rightarrow 1^{p-1} \equiv 1 \pmod p$

$2^{\phi(p)} \equiv 1 \pmod p \Rightarrow 2^{p-1} \equiv 1 \pmod p$

$\vdots$

$(p-1)^{p-1} \equiv 1 \pmod p$

Adding $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv (p-1) \pmod p$

$\equiv -1 \pmod p$

Problem: Let $(a,p) = (b,p) = 1$ and $a^p \equiv b^p \pmod p$, then

(i) $a \equiv b \pmod p$

(ii) $a^p \equiv b^p \pmod{p^2}$

Solution: Since $a^p \equiv b^p \pmod p$

$\Rightarrow p \mid (a-b)(a^{p-1} + a^{p-1}q + \cdots + b^{p-1})$ —— (1)

But $(p,a) = 1$

$\Rightarrow p \nmid a$

$\Rightarrow p \nmid a^{p-1}$

Similarly $p \nmid b^{p-1}$

Then by (1)

$p \nmid (a^{p-1} + a^{p-1}q + \cdots + b^{p-1})$

Hence $p \mid a-b$

$\Rightarrow a \equiv b \pmod p$

(ii) $\Rightarrow a = b + pt \quad ; t \in Z$

Consider $a^p - b^p = (b+pt)^p - b^p$

$= b^p + p\,b^{p-1}pt + \cdots + (pt)^p - b^p$

$= p^2 b^{p-1} + \cdots + p^2 p^{p-2} t^p$

$\Rightarrow p^2 \mid a^p - b^p$

$\Rightarrow a^p \equiv b^p \pmod{p^2}$

165

THEOREM: If $(m,n)=1$, then $\varphi(mn)=\varphi(m)\cdot\varphi(n)$

Multiplication property of Euler-φ function.

PROOF: Let $a_1, a_2, \cdots, a_{\varphi(m)}$ be a RRS (mod m) and $b_1, b_2, \cdots, b_{\varphi(n)}$ be a RRS (mod n), then

$$C=\{na_i+mb_j \;;\; 1\le i\le \varphi(m),\ 1\le j\le \varphi(n)\}$$

is a RRS (mod mn) Self.

Hence C contain $\varphi(mn)$ elements.

Also by def of C, contain $\varphi(m)\cdot\varphi(n)$ elements. Thus $\varphi(mn)=\varphi(m)\cdot\varphi(n)$.

Generalized form:

If $(m_i, m_j)=1$ for $i\neq j$ $1\le i,j\le n$.

Then $\varphi(m_1\cdot m_2\cdots m_n)=\varphi(m_1)\,\varphi(m_2)\cdots\varphi(m_n)$

PROOF: Statement is true for $n=2$.

Suppose it is true for $n=K$.

that $\varphi(m_1\cdot m_2\cdots m_K)=\varphi(m_1)\,\varphi(m_2)\cdots\varphi(m_K)$

$(m_i, m_j)=1$, $1\le i,j\le K$.

Consider

$$\varphi\big((m_1\cdot m_2\cdots m_K)\cdot m_{K+1}\big)$$

$$=\varphi(m_1\cdot m_2\cdots m_K)\,\varphi(m_{K+1}) \quad \because (m_1\cdot m_2\cdots m_K, m_{K+1})=1$$

$$=\varphi(m_1)\cdot\varphi(m_2)\cdots\varphi(m_{K+1}) \quad \text{(Supposition)}$$

Thus by induction, we have theorem

H.M. KHALID MAHMOOD.

166

Order of integers (mod m):

The smallest positive value of x which satisfies $a^x \equiv 1 \pmod{m}$ is called the order of $a \pmod{m}$. This number is usually denoted by d. Since $1 \equiv 1 \pmod{m}$ $\forall m$. Hence order of 1 modulo any integer is 1.

Moreover we know that the congruence $a^x \equiv 1 \pmod{m}$ is solvable iff $(a, m) = 1$.

If $a > 1$ then the statement that the order of $a \pmod{m}$ is d implies

(i) $(a, m) = 1$.

(ii) $a^d \equiv 1 \pmod{m}$

(iii) $a^h \not\equiv 1 \pmod{m}$, $0 < h < d$.

Conversely (i), (ii) and (iii) imply that the order of $a \pmod{m}$ is d.

Example: Find order of $3 \pmod{16}$

$3^2 = 9$, $3^3 = 27$, $3^4 = 81$

$\equiv 1 \pmod{16}$

Thus $d = 4$, positive

Assignment: Find the orders of integers modulo 9 that are less than 9 and prime to 9.

Ans 1, 6, 3, 6, 3, 2

(mod m) are $\phi(m)$

16.7

Def: Let n be a fixed positive integer. Then arithmatic inverse of a given integer a coprime to n is an integer a^* such that $a a^* \equiv 1 \pmod{n}$. Then integer a^* is also called inverse of a.

e.g If $n=8$, then arithmatic inverse of 3 is 3 as $3 \cdot 3 \equiv 1 \pmod{8}$

Remark If n is positive integer greater than 2 and a is any other integer such that $(a,n)=1$, then by Euler's theorem

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$$\Rightarrow a \cdot a^{\varphi(n)-1} \equiv 1 \pmod{n}$$

Hence arithmatic inverse of a is $a^{\varphi(n)-1}$.

Wilson's theorem

Statement: An integer p is prime iff

$$(p-1)! \equiv -1 \pmod{p}$$

PROOF: Let p be a prime number and a be an integer such that ~~$(a,p)=1$~~

If $1 \le a \le p-1$, then $(a,p)=1$

Hence the congruence

$$ax \equiv 1 \pmod{p}$$ has a unique solution, (say) y.

168

Then $ay \equiv 1 \pmod{p}$ —— ①

Thus multiplicative inverse of a; $1 \le a \le p-1$ exist. If $a \equiv y \pmod{p}$, then ① becomes

$a^2 \equiv 1 \pmod{p}$ —— ② then ② is satisfied by

imply $a \equiv 1 \pmod{p}$ and $a \equiv -1 \pmod{p}$

i.e $a \equiv 1 \pmod{p}$ and $a \equiv (p-1) \pmod{p}$

Thus from ②,

either $(1)^2 \equiv 1 \pmod{p}$ and $(p-1)^2 \equiv 1 \pmod{p}$

Thus 1 and $(p-1)$ are the only elements which are the inverses of itself. and remaining from $\{1, 2, \cdots p-1\}$ occurs in pairing.

Hence

$$2 \cdot 3 \cdots p-2 \equiv 1 \pmod{p}$$

$$\Rightarrow 2 \cdot 3 \cdots \overline{p-2} \cdot \overline{p-1} \equiv p-1 \pmod{p}$$

$$\Rightarrow (p-1)! \equiv -1 \pmod{p}$$

Conversely, Suppose p is composite.

Then $p = m_1 m_2 \quad 1 < m_1, m_2 < p$.

Suppose $(p-1)! \equiv -1 \pmod{p}$

Then $p \mid (p-1)! + 1$

But $m_1 \mid p$ as $m_1 \cdot m_2 = p$

imply $m_1 \mid (p-1)! + 1$

But $m_1 \mid (p-1)!$ as $m_1 < p$ (m_1 is a factor of $(p-1)!$)

Th 6 S.B. Malik 169

THEOREM: Let p be an odd prime. The congruence $x^2 \equiv -1 \pmod{p}$ has a solution iff $p \equiv 1 \pmod{4}$

PROOF: Suppose $x^2 \equiv -1 \pmod{p}$ has a solution, say a

therefore $a^2 \equiv -1 \pmod{p}$ and $(a,p) = 1$ ——— (1)

$\because p$ is prime & $a \in \{1, 2, \ldots, p-1\}$

Also by FLT

$$a^{p-1} \equiv 1 \pmod{p}$$

$$\text{or } 1 \equiv a^{p-1} \pmod{p}$$

$$\text{or } 1 \equiv (a^2)^{\frac{p-1}{2}} \pmod{p}$$

$$\Rightarrow 1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \quad \text{by using (1)} \quad \text{——— (2)}$$

But (2) hold when $\frac{p-1}{2}$ is even

Let $\frac{p-1}{2} = 2K$

$$\Rightarrow p = 4K + 1$$

$$\Rightarrow 4 \mid p-1$$

$$\Rightarrow p \equiv 1 \pmod{4}$$

Conversely, suppose

$$p \equiv 1 \pmod{4}$$

$$\Rightarrow p = 1 + 4K \text{ for some integer } K.$$

By Wilson theorem

$$(p-1)! \equiv -1 \pmod{p}$$

$$\Rightarrow 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \frac{p+3}{2} \cdots \frac{p-1}{p-1} \equiv -1 \pmod{p} \quad \text{——— (3)}$$

17c

But $\frac{p+1}{2} \equiv -\frac{p-1}{2} \pmod p$

$\frac{p+3}{2} \equiv -\frac{p-3}{2} \pmod p$

$\vdots$

$p-1 \equiv -1 \pmod p$

Using above in (3), we get

$(-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \equiv -1 \pmod p$

or $(-1)^{2k} \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$

$\Rightarrow \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p$

Thus $\left(\frac{p-1}{2}\right)!$ is a solution of

$x^2 \equiv -1 \pmod p$.

THEOREM: let p be an odd prime with $p \equiv 3 \pmod 4$.
Then $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1 \pmod p$

PROOF From Last theorem

$-1 \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p$

$-1 \equiv (-1)^{2k+1} \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p$ $\because p = 3+4k;\ k \geq 0$
$\Rightarrow \frac{p-1}{2} = 2k+1$

$-1 \equiv (-1) \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p$

or $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1 \pmod p$.

171

THEOREM: (i) For any integer $n > 1$,
$\varphi(n) = n-1 \Leftrightarrow n$ is prime.

(ii) If p is prime and k is any positive integer, then $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$

(iii) let $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ distinct abd primes and integers $k_i \geq 1 \ \forall i$, $1 \leq i \leq r$
then $\varphi(n) = \varphi(p_1^{k_1})\ \varphi(p_2^{k_2}) \cdots \varphi(p_r^{k_r})$
$= (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$
$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$

PROOF: (i) Let n be prime, then $1, 2, 3, \cdots n-1$ are all integers less than n and co-prime to n.
Therefore $\varphi(n) = n-1$
Conversely, suppose n is composite, then
$\varphi(n) \leq n-2 < n-1$, a contradiction.
Hence 'n' is prime.

(ii) Let $k = 1$, then the integers less than p and prime to it are $1, 2, \cdots, p-1$. Hence
$\varphi(p^1) = p-1 = p - p^{1-1}$

Let $k > 1$, then among the integers ~~those~~ $1, 2, \cdots, p^k$ those which are not prime to p^k are $p, 2p, 3p, \cdots, p^k = p^{k-1} \cdot p$.
Thus these are p^{k-1} in number. Hence by def.
$\varphi(p^k) = p^k - p^{k-1}$
$= p^k\left(1 - \frac{1}{p}\right)$

172

(iii) Since $p_1, p_2, \ldots, p_r$ are distinct primes.

Hence $\varphi(n) = \varphi(p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r})$

$= \varphi(p_1^{k_1})\, \varphi(p_2^{k_2}) \cdots \varphi(p_r^{k_r})$

$= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$

$= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) p_2^{k_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{k_r}\left(1 - \frac{1}{p_r}\right)$

$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$

$= n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

Corollary: $\varphi(p^{k+1}) = p\, \varphi(p^k)$

$\varphi(p^{k+1}) = p^{k+1} - p^k$

$= p(p^k - p^{k-1})$

$= p\, \varphi(p^k)$

Corollary $\varphi(p^k) = p^k - p^{k-1}$

$\varphi(p^k) = p\, \varphi(p^{k-1})$

$= p^2\, \varphi(p^{k-2})$

$= p^3\, \varphi(p^{k-3})$

$\vdots$

$= p^{k-1}\, \varphi(p^{k-k+1})$

$= p^{k-1}\, \varphi(p) = p^{k-1}(p-1)$

$= p^{k-1} p\left(1 - \frac{1}{p}\right) = p^k\left(1 - \frac{1}{p}\right) = p^k - p^{k-1}$

175

Exercise: If $n = \prod_{i=1}^{r} p_i^{k_i}$, p_i distinct prime integers and $k_i \geq 1$, then

(a) $$\sum_{d|n} \frac{\varphi(d)}{d} = \prod_{i=1}^{r} \left(1 + k_i \cdot \frac{(p_i - 1)}{p_i}\right)$$

(b) $$\sum_{d|n} \frac{d}{\varphi(d)} = \prod_{i=1}^{r} \left(1 + \frac{k_i \cdot p_i}{p_i - 1}\right)$$

Solution: the divisors of $p_1^{k_1}$ are $1, p_1, p_1^2 \cdots p_1^{k_1}$; of $p_2^{k_2}$ are $1, p_2, p_2^2, \cdots p_2^{k_2}$; $\cdots$; of $p_r^{k_r}$ are $1, p_r, p_r^2, \cdots p_r^{k_r}$.

Hence by def.

$$\sum_{d|n} \frac{\varphi(d)}{d} = \left[\frac{\varphi(1)}{1} + \frac{\varphi(p_1)}{p_1} + \frac{\varphi(p_1^2)}{p_1^2} + \cdots \frac{\varphi(p_1^{k_1})}{p_1^{k_1}}\right] \cdot \left[\frac{\varphi(1)}{1} + \frac{\varphi(p_2)}{p_2} + \cdots \frac{\varphi(p_2^{k_2})}{p_2^{k_2}}\right]$$

$$\cdots \left[\frac{\varphi(1)}{1} + \frac{\varphi(p_r)}{p_r} + \frac{\varphi(p_r^2)}{p_r^2} + \cdots \frac{\varphi(p_r^{k_r})}{p_r^{k_r}}\right]$$

$1, 3, 3^2, 3^3$
$1, 2, 2^2$
$2, 2^1, 2^3$
$3^2, 3^3$
$3^1, 3^3$
$2^1, 2^2, 2^3$
$2^3 n$

$$= \left[1 + \frac{p_1 - 1}{p_1} + \frac{p_1^2 - p_1}{p_1^2} + \cdots \frac{p_1^{k_1} - p_1^{k_1 - 1}}{p_1^{k_1}}\right] \cdots$$

$$\times \left[1 + \frac{p_r - 1}{p_r} + \frac{p_r^2 - p_r}{p_r^2} + \cdots + \frac{p_r^{k_r} - p_r^{k_r - 1}}{p_r^{k_r}}\right]$$

$$= \left[1 + \left(1 - \frac{1}{p_1}\right) + \left(1 - \frac{1}{p_1}\right) + \cdots + \left(1 - \frac{1}{p_1}\right)\right] \cdots \left[1 + \left(1 - \frac{1}{p_r}\right) + \left(1 - \frac{1}{p_r}\right) + \cdots + \left(1 - \frac{1}{p_r}\right)\right]$$

$$= \left[1 + k_1\left(1 - \frac{1}{p_1}\right)\right] \cdots \left[1 + k_r\left(1 - \frac{1}{p_r}\right)\right]$$

$$= \prod_{i=1}^{r} \left[1 + k_i\left(1 - \frac{1}{p_i}\right)\right] = \prod_{i=1}^{r} \left[1 + k_i \frac{(p_i - 1)}{p_i}\right]$$

(b) Self.

174

THEOREM: (i) For $n \geq 1$, $n = \sum_{d|n} \varphi(d)$

(ii) For $n > 1$; $\sum_{\substack{(n,k)=1 \\ k \leq n}} k = \frac{1}{2} n \cdot \varphi(n)$

PROOF: By induction on number of distinct prime factors of n. Suppose first that $n = p^k$

Then $1, p, p^2, \cdots, p^k$ are all divisors of n. Thus

$$\sum_{d|n} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^k)$$

$$= 1 + p - 1 + p^2 - p + \cdots + p^k - p^{k-1}$$

$$= p^k$$

$$= n$$

Which shows that result is true for all integers that contain one prime factor.

We suppose that result is true for all integer $n > 1$ that contain $r-1$ distinct prime factors.

That is if $n' = \prod_{i=1}^{r-1} p_i^{k_i}$ where p_i's are distinct primes, $k_i \geq 1$

Then $n' = \sum_{d|n'} \varphi(d)$ —— (1)

Consider $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_{r-1}^{k_{r-1}} \cdot p_r^{k_r}$

$n = n' p_r^{k_r}$ where $(n', p_r^{k_r}) = 1$

Then any divisor d of n is of the form 175

$d' p_r^t$ where $d' | n'$ and $0 \le t \le k_r$

If $d_1, d_2, \dots, d_s$ are all divisors of n', then

$d_1, d_2, \dots, d_s, d_1 p_r, d_2 p_r, \dots, d_s p_r, d_1 p_r^2, d_2 p_r^2, \dots, d_s p_r^2$

$\dots, d_1 p_r^{k_r}, d_2 p_r^{k_r}, \dots, d_s p_r^{k_r}$ are all divisors of n.

Hence

$$\sum_{d|n} \varphi(d) = \sum_{i=1}^{s} \varphi(d_i) + \sum_{i=1}^{s} \varphi(d_i p_r) + \dots + \sum_{i=1}^{s} \varphi(d_i p_r^{k_r})$$

$$= \sum_{i=1}^{s} \varphi(d_i) + \sum_{i=1}^{s} \varphi(d_i)\varphi(p_r) + \dots + \sum_{i=1}^{s} \varphi(d_i)\varphi(p_r^{k_r})$$

$$= \sum_{i=1}^{s} \varphi(d_i) \left[1 + \varphi(p_r) + \dots + \varphi(p_r^{k_r}) \right]$$

$$= \sum_{i=1}^{s} \varphi(d_i) \cdot p_r^{k_r} \quad \text{using case } n = p^{k_1}$$

$$= \sum_{d|n'} \varphi(d) \cdot p_r^{k_r}$$

$$= n' \cdot p_r^{k} \quad \text{using (1)}$$

$$= n$$

Hence by induction, we have the theorem

Corollary: If p is a prime such that $p \nmid n$ and $k \geq 1$, then $\varphi(np^k) = \varphi(n)\varphi(p^k)$

176

(iii) We know that the $\varphi(n)$ integers $r_1, r_2, \ldots, r_{\varphi(n)}$ such that $(r_i, n) = 1$ form a RRS (mod n).

Let $(n - r_i, n) = d$

Then $d \mid n - r_i$ & $d \mid n$

$\Rightarrow d \mid n - r_i - n \Rightarrow d \mid r_i$

Also $d \mid n$

Hence $d \mid (n, r_i) = 1$

$\Rightarrow d \mid 1$

Hence $d = 1$

Thus $(n - r_i, n) = 1$

Which shows that

$n - r_1, n - r_2, \ldots, n - r_{\varphi(n)}$ also form a RRS (mod n)

So for each i, there exist a unique j such that

$$r_i \equiv n - r_j \pmod{n}$$

$$\Rightarrow r_i = n - r_j \quad \because r_i \text{ \& } n - r_i \text{ both are less than } n.$$

$$\Rightarrow \sum_{i=1}^{\varphi(n)} r_i = \sum_{j=1}^{\varphi(n)} (n - r_j)$$

$$\Rightarrow 2\sum_{i=1}^{\varphi(n)} r_i = \sum_{j=1}^{\varphi(n)} (n) = n \cdot \varphi(n)$$

$$\sum_{i=1}^{\varphi(n)} r_i = \frac{n \cdot \varphi(n)}{2}$$

$$\sum_{\substack{k=1 \\ (k,n)=1}}^{k} = \frac{1}{2} n \cdot \varphi(n).$$

THEOREM: Let m and n be integers both greater than 1 and every prime divisor of n is a prime divisor of m, then

(i) $\varphi(mn) = n\,\varphi(m)$

(ii) $\varphi(n^2) = n\,\varphi(n) \quad \forall n \geq 1$

PROOF: Since every prime divisor of n is also a prime divisor of m, then n and m can be written as

$$m = p_1^{r_1} \cdot p_2^{r_2} \cdots p_K^{r_K} \; ; \; n = p_1^{s_1} \cdot p_2^{s_2} \cdots p_K^{s_K} \cdot p_{K+1}^{s_{K+1}} \cdots p_t^{s_t}$$

p_i being primes, r_i, s_i integers each ≥ 1 and $t \geq K$

then

$$\varphi(mn) = \varphi\left(p_1^{r_1+s_1} \cdot p_2^{r_2+s_2} \cdots p_K^{r_K+s_K} \cdot p_{K+1}^{s_{K+1}} \cdots p_t^{s_t}\right)$$

$$= \varphi(p_1^{r_1+s_1})\,\varphi(p_2^{r_2+s_2}) \cdots \varphi(p_K^{r_K+s_K}) \cdot \varphi(p_{K+1}^{s_{K+1}}) \cdots \varphi(p_t^{s_t})$$

$$= (p_1^{r_1+s_1} - p_1^{r_1+s_1-1})(p_2^{r_2+s_2} - p_2^{r_2+s_2-1}) \cdots (p_K^{r_K+s_K} - p_K^{r_K+s_K-1}) \cdot \varphi(p_{K+1}^{s_{K+1}}) \cdots \varphi(p_t^{s_t})$$

$$= p_1^{r_1} \cdot p_2^{r_2} \cdots p_K^{r_K} (p_1^{s_1} - p_1^{s_1-1})(p_2^{s_2} - p_2^{s_2-1}) \cdots (p_K^{s_K} - p_K^{s_K-1}) \cdot \varphi(p_{K+1}^{s_{K+1}}) \cdots \varphi(p_t^{s_t})$$

$$= n\,\varphi(p_1^{s_1})\,\varphi(p_2^{s_2}) \cdots \varphi(p_K^{s_K}) \cdot \varphi(p_{K+1}^{s_{K+1}}) \cdots \varphi(p_t^{s_t})$$

$$= n\,\varphi(p_1^{s_1} \cdot p_2^{s_2} \cdots p_K^{s_K} \cdot p_{K+1}^{s_{K+1}} \cdots p_t^{s_t})$$

$$= n\,\varphi(m)$$

For (ii) put $m = n$ in (i)

208

Th: Let a be an integer having exponent $h \pmod m$. Then the following hold.

(i) $(a, m) = 1$

(ii) If $a^K \equiv 1 \pmod m$ for some integer K, then $h \mid K$.

(iii) If $a \equiv b \pmod m$, then b has exponent $h \pmod m$.

(iv) $a^i \equiv a^j \pmod m$ iff $i \equiv j \pmod h$.

PROOF:

(i) Let $d > 0$ be a common divisor of a and m. Then $d \mid a$ and $d \mid m$

Since $a^h \equiv 1 \pmod m$

So $a^h = 1 + \lambda m$ for some integer λ.

Now $d \mid a \Rightarrow d \mid a^h$ — (i)

Also $d \mid m \Rightarrow d \mid \lambda m$ — (ii)

(i) & (ii) imply

$$d \mid a^h - \lambda m = 1$$

Hence $d = 1$

(ii) If $a^K \equiv 1 \pmod m$, then by def of exponent $K \geq h$ and by division algorithm

$$K = hq + r \quad ; \quad 0 \leq r < h \quad \text{— (1)}$$

$$a^K = a^{hq+r}$$
$$= (a^h)^q \cdot a^r$$
$$\equiv 1^q \cdot a^r \pmod m$$

209

or $a^r \equiv 1 \pmod m$

But $r < h$ and h is exponent.

thus only possibility by $r = 0$ put in (1)

$K = hq$ or $h \mid K$.

(iii) Let $a \equiv b \pmod m$

then $a^h \equiv b^h \pmod m$

or $b^h \equiv a^h \pmod m$

$\equiv 1 \pmod m$ $\because a^h \equiv 1 \pmod m$

Hence b has exponent $h \pmod m$.

(iv) Let $a^i \equiv a^j \pmod m$

then $a^{i-j} \equiv 1 \pmod m$

But $a^h \equiv 1 \pmod m$ & h is exponent.

Hence $h \mid (i-j)$

thus $i \equiv j \pmod m$.

Remark: If $a^h \equiv 1 \pmod m$. then $1, a, \cdots, a^{h-1}$ are mutually incongruent $\pmod m$.

THEOREM: If a has exponent $h \pmod m$, then a^K has exponent $\frac{h}{d}$ where $d = (h, K)$.

PROOF: We will show $(a^K)^{\frac{h}{d}} \equiv 1 \pmod m$

Let a^K has exponent $t \pmod m$

then $a^{Kt} \equiv 1 \pmod m$ —(1)

Also a has exponent $h \pmod m$

210

then $h \mid Kt$ — (2)

Since $(h, K) = d$, so there exist integers h_1 and K_1 such that

$$h = h_1 d \quad \text{and} \quad K = K_1 d \quad ; (h_1, K_1) = 1$$

(2) becomes

$$h_1 d \mid K_1 d\, t$$

or $h_1 \mid K_1 t$

But $(h_1, K_1) = 1$

then $h_1 \mid t$

or $\frac{h}{d} \mid t$ — (3) $\quad \because h_1 = \frac{h}{d}$

Consider

$$(a^K)^{\frac{h}{d}} = (a^h)^{\frac{K}{d}} = (a^h)^{K_1}$$

$$\equiv (1)^{K_1} \pmod m$$

i.e $(a^K)^{\frac{h}{d}} \equiv 1 \pmod m$

But we have supposed $(a^K)^t \equiv 1 \pmod h$ for t as least.

Then $t \mid \frac{h}{d}$ — (4)

(3) & (4) imply

$$t = \frac{h}{d}$$

that is $(a^K)^{\frac{h}{d}} \equiv 1 \pmod h$ as required

Corollary 11 If a has exponent $h \pmod m$. Then a^K has exponent $h \pmod m$ iff $(h,K)=1$

Proof: Given $a^h \equiv 1 \pmod m$.

Suppose a^K has exponent $h \pmod m$.

Then $(a^K)^h \equiv 1 \pmod m$. — (1)

Suppose $(h,K)=d$.

Since a has exponent $h \pmod m$ and $(h,K)=d$. Then a^K has exponent $\frac{h}{d} \pmod m$.

That is $(a^K)^{\frac{h}{d}} \equiv 1 \pmod m$ — (2)

(1) and (2) gives

$Kh = \frac{Kh}{d}$ only possible if $d=1$

Hence $(h,K)=1$

Conversely, Suppose $(h,K)=1$.

Since a has exponent $h \pmod m$

Then a^K has exponent $\frac{h}{d} \pmod m$; $d=(h,K)$

Then a^K has exponent $(\frac{h}{1}) \pmod m$

That is

$(a^K)^h \equiv 1 \pmod m$.

212

Def If an integer a has exponent $\varphi(m)$ $(\text{mod } m)$, m a positive integer, then we say that a is primitive root $(\text{mod } m)$ or a is primitive root belonging to m. That is when $a^{\varphi(m)} \equiv 1 \ (\text{mod } m)$, then a is called primitive root $(\text{mod } m)$.

Remark (i) If primitive root exist, then number of primitive roots is $\varphi(\varphi(m))$.

(ii) Since $1^n = 1 \ \forall n \in \mathbb{N}$. So one can never be a primitive root of any integer greater than 2.

Examples:

213

THEOREM: If a is a primitive root $(\bmod m)$ then $1, a, a^2, \cdots, a^{\varphi(m)-1}$ is a RRS $(\bmod m)$.

PROOF:

(i) Since a is primitive root $(\bmod m)$

So $(a, m) = 1$

then $(a^k, m) = 1 \quad ; \quad 1 \le k \le \varphi(m) - 1$

Thus $1, a, a^2, \cdots, a^{\varphi(m)-1}$ are co-prime to m.

(ii) Suppose on contrary

$$a^i \equiv a^j \pmod m \qquad 0 \le i, j < \varphi(m) - 1$$

then $i \equiv j \pmod{\varphi(m)}$ $\because$ a is primitive root, so $a^{\varphi(m)} \equiv 1 \pmod m$

That is $\varphi(m) \mid i - j$

But $i - j < \varphi(m)$

thus $i - j = 0$

i-e $i = j$.

or simply $a^i \not\equiv a^j \pmod m \quad ; \quad (i \neq j)$.

(iii) Let $\{a_1, a_2, \cdots, a_{\varphi(m)}\}$ be a RRS $(\bmod m)$.

Let r be an integer s.t $(r, m) = 1$.

Then $r \equiv a_j \pmod m$ — (1) $1 \le j \le \varphi(m)$ and j is unique.

Moreover $1, a, a^2, \cdots, a^{\varphi(m)-1}$ are co-prime to m. For $a^h \quad ; \quad 0 \le h \le \varphi(m) - 1$

There exist a unique $j \quad ; \quad 1 \le j \le \varphi(m)$

s.t $a^h \equiv a_j \pmod m$ — (2)

214

(i) & (ii) imply

$$r \equiv a^h \pmod m$$

conditions (i), (ii) & (iii) shows that $1, a, a^2, \ldots, a^{\varphi(m)-1}$ is a RRS (mod m).

THEOREM: (i) If a is primitive root (mod m), then a^K is a primitive root (mod m) iff $(K, \varphi(m)) = 1$

(ii) If an integer m has a primitive root belonging to it then there are $\varphi(\varphi(m))$ primitive roots belonging to it.

PROOF: Suppose a^K is a primitive root (mod m)

then $(a^K)^{\varphi(m)} \equiv 1 \pmod m$ —— (i)

Suppose $(K, \varphi(m)) = d$.

Since a is a primitive root (mod m)

Then a^K has exponent $\frac{\varphi(m)}{d}$.

that is $(a^K)^{\frac{\varphi(m)}{d}} \equiv 1 \pmod m$ —— (2)

(1) & (2) imply $K\varphi(m) = \frac{K}{d}\varphi(m)$ imply

$$d = 1$$

Conversely Suppose $(K, \varphi(m)) = 1$

Since a is primitive root (mod m). Then a^K has exponent $\frac{\varphi(m)}{d}$ where $d = (K, \varphi(m))$

But $d = 1$. Then $(aK)^{\varphi(m)} \equiv 1 \pmod m$

this a^K is a primitive root (mod m).

915

(ii) Let a be a primitive root belonging to m.
Then $1, a, a^2, \ldots, a^{\varphi(m)-1}$ is a RRS (mod m).
If b is any other primitive root (mod m).
Then $(b, m) = 1$. Since $1, a, a^2, \ldots, a^{\varphi(m)-1}$ is RRS (mod m). Then there exist a unique t such that $b \equiv a^t \pmod m$; $1 \le t \le \varphi(m)-1$.
Again b is primitive root iff $(t, \varphi(m)) = 1$.
and number of such t is $\varphi(\varphi(m))$.
Thus m can have $\varphi(\varphi(m))$ primitive roots belonging to it.

eg Let $\varphi(m) = 4$, Then integers which are less than $\varphi(m)$ and co-prime to $\varphi(m)$ are $\varphi(4) = \varphi(\varphi(m))$

Lemma: Let a be any odd integer.
then $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ $\forall$ $n \ge 3$.

Proof: By induction on n.
For $n=3$, we must prove that
$a^2 \equiv 1 \pmod 8$.
Since a is odd, So a is congruent to either $1, 3, 5$ or 7. therefore a^2 is congruent to $1 \pmod 8$.
Suppose Statement holds for $n = k \ge 3$.
that is a is an odd integer, then
$a^{2^{k-2}} \equiv 1 \pmod{2^k}$ $\forall$ $k \ge 3$

216

Consider

$$a^{2^{(K+1)-2}} = a^{2^{K-1}}$$

$$= (a^{2^{K-2}})^2 \quad \text{---- (1)}$$

Since $a^{2^{K-2}} \equiv 1 \pmod{2^K}$

So $a^{2^{K-2}} = 1 + d\,2^K$ for $d \in Z$.

$$(a^{2^{K-2}})^2 = 1 + d\,2^{K+1} + d^2 2^{2K}.$$

$$a^{2^{K-1}} - 1 = d\,2^{K+1} + d^2 2^{K+1} \cdot 2^{K-1}.$$

As $K \geq 3 \Rightarrow K > 2$ or $K - 1 > 1$.

Thus $2^{K+1} \mid a^{2^{K-1}} - 1$

That is $a^{2^{K-1}} \equiv 1 \pmod{2^{K+1}}$

OR $a^{2^{(K+1)-2}} \equiv 1 \pmod{2^{K+1}}$

Hence by induction, we have the result.

217

THEOREM: There are no primitive roots belonging to 2^n $\forall$ $n \geq 3$.

PROOF: Suppose a is primitive root $(\text{mod } 2^n)$ then

(i) a has exponent $\varphi(2^n)$ $(\text{mod } 2^n)$

(ii) a must be odd.

If a is odd, then

$$a^{2^{n-2}} \equiv 1 \ (\text{mod } 2^n) \quad \forall \ n \geq 3$$

Also by (i) $a^{\varphi(2^n)} = a^{2^n - 2^{n-1}}$

$$= a^{2^{n-1}} \equiv 1 \ (\text{mod } 2^n)$$

a, contradiction. Thus there exist no integer a which serves as a primitive root $(\text{mod } 2^n)$.

Remark: Above theorem says that there are primitive roots belonging to 2^n only if $n < 3$.

If $n = 2$. Then 3 is a primitive root $(\text{mod } 2^2)$. $\because \varphi(2^1) = 2^{1-1} = 2$. and $3^2 \equiv 1 \ (\text{mod } 4)$.

If $n = 1$, then 1 is a primitive root $(\text{mod } 2^1)$. $\because \varphi(2^1) = 1$ & $1^1 \equiv 1 \ (\text{mod } 2)$.

218

Lemma: Let m, n each > 2 be any integers and $(m,n)=1$. Then there exist no primitive roots (mod (mn))

Proof: If possible, Let a be a primitive root belonging to mn. then

(i) a has exponent $\varphi(mn)$ (mod mn). and

(ii) $(a, mn) = 1$

By (ii) $(a,m) = 1$ &
$(a,n) = 1$

then by Euler's theorem

$$\left.\begin{aligned} a^{\varphi(m)} &\equiv 1 \pmod m \\ a^{\varphi(n)} &\equiv 1 \pmod n \end{aligned}\right\} \quad \text{——— (1)}$$

Let $h = \dfrac{\varphi(m)\cdot\varphi(n)}{(\varphi(m), \varphi(n))} = \dfrac{\varphi(m)\cdot\varphi(n)}{\langle \varphi(m), \varphi(n)\rangle}$ ——— (2)

Since m and n are both greater than 2.

So $(\varphi(m), \varphi(n)) \geq 2$ $\because$ $\varphi(m)$ = even for $n > 2$.

then $\dfrac{1}{(\varphi(m), \varphi(n))} \leq 2$ put in (2)

$$h \leq \frac{\varphi(m)\cdot\varphi(n)}{2} = \frac{\varphi(mn)}{2} \quad \because (m,n)=1$$

$$\Rightarrow h < \varphi(mn) \text{ ——— (3)}$$

811

Consider

$$a^h = \left(a^{\phi(m)}\right)^{\frac{\phi(n)}{(\phi(m),\phi(n))}}$$

$$\equiv 1 \pmod{m}$$

Similarly

$$a^h \equiv 1 \pmod{n}$$

But $(m,n) = 1$.

Hence

$$a^h \equiv 1 \pmod{mn} \; ; \; h < \phi(mn)$$

which contradicts the assumption that exponent of a is $\phi(mn)$.

Thus there exist no primitive roots (mod mn).

Example: There exist no primitive roots of 15.

$15 = 3 \cdot 5$; $3 > 2$, $5 > 2$. Also $(3,5) = 1$

Corollary: If n is an integer of the form $p^k \cdot q^\ell$ where p, q distinct odd primes and $k, \ell \geq 1$. then there exist no primitive roots belonging to n.

Proof Since p, q are distinct odd primes thus $(p,q) = 1$. Then $(p^k, q^\ell) = 1$ $\forall k, \ell \geq 1$

Moreover $p^k, q^\ell > 2$ $\because p, q$ odd primes

Thus there exist not primitive roots belonging to n.

Ex: there exist no primitive roots belonging to 45.

THEOREM: Let $(a, m) = 1$, then a is primitive root $(\bmod m)$ iff $a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod m$ for every prime divisor p of $\varphi(m)$.

PROOF: Let $a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod m$ for every prime divisor p of $\varphi(m)$.

Suppose that a is not primitive root of m.

Then $a^K \equiv 1 \pmod m$; $K < \varphi(m)$ — (1)

that is order of $a \pmod m$ is K.

Since $(a, m) = 1$

By Euler's theorem

$$a^{\varphi(m)} \equiv 1 \pmod m$$

then K divides $\varphi(m)$.

Thus $\frac{\varphi(m)}{K}$ is an integer and therefore divisible by some prime divisor p of $\varphi(m)$ $\quad \because \varphi(m) = K \cdot p^e$, $e \geq 1$

Hence $a^{\frac{\varphi(m)}{p}} = (a^K)^{\frac{\varphi(m)}{Kp}}$

$\equiv 1 \pmod m$ — using (1)

This contradicts our assumption.

Hence a is a primitive root of m.

Conversely, Suppose that a be a primitive root of m.

221

Then by def

$$a^{\varphi(m)} \equiv 1 \pmod m \text{ and } a^b \not\equiv 1 \pmod m \quad ; 0 < b < \varphi(m)$$

Since $\frac{\varphi(m)}{p} < \varphi(m)$ for every prime divisor p of $\varphi(m)$.

Hence $a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod m$.

Example: Find the primitive roots of 19.

$$\varphi(19) = 18 = 2 \cdot 3^2$$

thus 2 and 3 are the only prime divisors of 18. Also $\frac{18}{3} = 6$ and $\frac{18}{2} = 9$.

Thus a is a primitive root belonging to 19 iff $a^6 \not\equiv 1 \pmod{19}$ and $a^9 \not\equiv 1 \pmod{19}$.

Let $a = 2, 3, \cdots, 18 \because (a, 19) = 1 \ \forall a$.

$2^6 \equiv 7$ and $2^9 \equiv -1$ } primitive roots
$3^6 \equiv 7$ $3^9 \equiv -1$ } $a = 2, 3$

$4^6 \equiv 11$ $4^9 \equiv 1$
$5^6 \equiv 7$ $5^9 \equiv 1$
$6^6 \equiv 11$ $6^9 \equiv 1$
$7^6 \equiv 1$ $7^9 \equiv 1$
$8^6 \equiv 1$ $8^9 \equiv -1$
$9^6 \equiv 11$ $9^9 \equiv 1$
$10^6 \equiv 11$ $10^9 \equiv -1$ primitive root.
$11^6 \equiv 1$ $11^9 \equiv 1$
$12^6 \equiv 1$ $12^9 \equiv -1$
$13^6 \equiv 11$ $13^9 \equiv -1$ primitive root
$14^6 \equiv 17$ $14^9 \equiv -1$ primitive root
$15^6 \equiv 11$ $15^9 \equiv 1$ primitive root

222

$16^6 \equiv 7$ $\quad 16^9 \equiv 1$

$17^6 \equiv 7$ $\quad 17^9 \equiv 1$

$18^6 \equiv 1$ $\quad 18^9 \equiv -1$

It follows that primitive roots of 19 are 2, 3, 10, 13, 14, 15

Example: Find all the primitive roots of 15

Remarks: Let a be a primitive root belonging to m. Then m has exactly $\varphi(\varphi(m))$ primitive roots namely $a^{r_1}, a^{r_2}, \ldots, a^{r_{\varphi(\varphi(m))}}$ where $r_1, r_2, \ldots, r_{\varphi(\varphi(m))}$ are the positive integers less than $\varphi(m)$ and prime to $\varphi(m)$.

Example: Find all the primitive roots of 17.

Solution: $\varphi(17) = 16 = 2^4$.

Thus $\varphi(17)$ has only one prime factor.

But $\frac{16}{2} = 8$. Therefore a is a primitive root of 17 iff $a^8 \not\equiv 1 \pmod{17}$.

Letting $a = 2, 3, \ldots, 16$: $(a, 17) = 1 \; \forall a$.

$a = 2$, $2^8 \equiv 1 \pmod{17}$

$a = 3$, $3^8 \not\equiv 1 \pmod{17}$.

Hence 3 is the smallest primitive root of 17. The integers less than $\phi(17)$ and co-prime to $\phi(17)$ are 1, 3, 5, 7, 9, 11, 13 and 15.

Hence the primitive roots of 17 are

$3, 3^3, 3^5, 3^7, 3^9, 3^{11}, 3^{13}, 3^{15}$.

But (mod 17), we have

3, 5, 6, 7, 10, 11, 12 and 14 are the primitive roots belonging to 17.

THEOREM: Let the order of $a \pmod{p^k}$ be d. Then the order of $a \pmod{p^{k+1}}$ is either d or pd.

PROOF: Let the order of $a \pmod{p^{k+1}} = h$

then $a^h \equiv 1 \pmod{p^{k+1}}$

$\Rightarrow a^h \equiv 1 \pmod{p^k}$

$\Rightarrow d \mid h$ $\because$ the order of $a \pmod{p^k}$ is d.

$\Rightarrow h = dc$ —— (1) for some integer c.

Again $a^d \equiv 1 \pmod{p^k}$

or $a^d = 1 + p^k \cdot q$ for some integer q.

$\Rightarrow a^{pd} = (1 + p^k \cdot q)^p$

224

then $a^{pd} = 1 +$ terms divisible p^{k+1}

So $a^{pd} \equiv 1 \pmod{p^{k+1}}$

then $h \mid pd$ ——— (2)

From (1) & (2)

$c \mid pd$ But $cd = h$

thus $c \mid p$

Therefore $c = 1$ or $c = p$

and consequently by (1)

$h = d$ or $h = pd$

which complete the proof.

Example: Find the order of $5 \pmod{7^2}$.

Sol Order of $5 \pmod 7 = 6$.

then order of $5 \pmod{7^2}$ is

either 6 or $6 \cdot 7 = 42$.

But $5^6 \equiv 43 \pmod{7^2}$

Hence order of $5 \pmod{7^2} = 42$.

i.e $5^{42} \equiv 1 \pmod{7^2}$.

THEOREM 1: Let a be a primitive root of p. 225

(i) If $a^{p-1} \not\equiv 1 \pmod{p^2}$. Then a is a primitive root of p^2.

(ii) If $a^{p-1} \equiv 1 \pmod{p^2}$, then $a+p$ is a primitive root of p^2.

PROOF:

(i) Let $a^{p-1} \not\equiv 1 \pmod{p^2}$

Given a is a primitive mod p.

Then $a^{\varphi(p)} \equiv 1 \pmod{p}$

i.e $a^{p-1} \equiv 1 \pmod{p}$

Thatis order of $a \pmod{p} = p-1$

Then order of $a \pmod{p^2}$ is either

$p-1$ or $p(p-1) = \varphi(p^2)$

But $a^{p-1} \not\equiv 1 \pmod{p^2}$

Hence $a^{p(p-1)} \equiv 1 \pmod{p^2}$

or $a^{\varphi(p^2)} \equiv 1 \pmod{p^2}$

Which shows that a is a primitive root $\pmod{p^2}$.

226

(ii) Suppose $a^{p-1} \equiv 1 \pmod{p^2}$ ——— (1)*

Since a is a primitive root $\pmod p$

and $a+p \equiv a \pmod p$

Therefore $a+p$ is a primitive root $\pmod p$.

That is order of $(a+p) \pmod p = p-1$

Then order of $(a+p) \pmod{p^2}$ is either

$p-1$ or $p(p-1) = \varphi(p^2)$

But $(a+p)^{p-1} = a^{p-1} + p(p-1)a^{p-2} + \text{terms divisible by } p^2$

$= a^{p-1} - pa^{p-2} + \text{terms divisible by } p^2$

$\equiv 1 - pa^{p-2} \pmod{p^2}$ using (1)*

$\not\equiv 1 \pmod{p^2}$

Therefor order of $(a+p) \pmod{p^2} = p(p-1)$
$= \varphi(p^2)$

$\varphi(p^2)$

That $(a+p) \equiv 1 \pmod{p^2}$

Hence $a+p$ is a primitive root $\pmod{p^2}$.

Example: Find primitive roots (mod 5^2)? 227

Solution: the smallest primitive 5 is 2.

and $2^{5-1} \not\equiv 1 \pmod{5^2}$

That is 2 is a primitive root of 5^2.

Also $\varphi(5^2) = 5^2 - 5^1 = 20$

Therefore positive integers less than 20 and prime to it are 1, 3, 7, 9, 11, 13, 17 and 19.

Hence the primitive roots of 5^2 are

$2, 2^3, 2^7, 2^9, 2^{11}, 2^{13}, 2^{17}$ and 2^{19}.

These are

2, 8, 3, 12, 23, 17, 22 and 13

respectively (mod 5^2).

THEOREM: Let a be a primitive root (mod p).

(i) If $a^{p-1} \not\equiv 1 \pmod{p^2}$ then a is a primitive root (mod p^2)

(ii) If $a^{p-1} \equiv 1 \pmod{p^2}$, then $a+cp$ is a primitive root (mod p^2) for every c relatively prime to p.

228

THEOREM: Let a be a primitive root of p and p^2. Then a is a primitive root of p^k where k is any positive integer.

PROOF: Suppose that a is a primitive root of p^s and p^{s+1} for some integer s. Then statement is also true for $s=1$ We will show that a is also a primitive root of p^{s+1} and p^{s+2}.

Since a is a primitive root of p^s.

Then $a^{\varphi(p^s)} \equiv 1 \pmod{p^s}$

$$\Rightarrow a^{\varphi(p^s)} = 1 + cp^s \quad \text{---------- (1)}$$

for some integer c.

Here $(c, p) = 1$ otherwise $p \mid c$.

(1) gives $a^{\varphi(p^s)} \equiv 1 \pmod{p^{s+1}}$

which is a contradiction against the fact that a is a primitive root of p^{s+1}. Thus $(c, p) = 1$ ---------- (2)

229

From (1)

$$a = (1+cp^s)^{p^{\varphi(p^s)}}$$

$$= 1 + cp^{s+1} + \text{terms divisible by } p^{s+2}.$$

Then $a \equiv 1 + cp^{s+1} \pmod{p^{s+2}}$ $\because (c,p)=1$ & $\varphi(p^{s+1}) = p(p^s - p^{s-1}) = p\varphi(p^s)$

$$\not\equiv 1 \pmod{p^{s+2}} \quad \text{---} (2)^*$$

Since the order of $a \pmod{p^{s+1}} = \varphi(p^{s+1})$

therefore order of $a \pmod{p^{s+2}}$ is either

$\varphi(p^{s+1})$ or $p\varphi(p^{s+1})$.

But we know that

order of $a \pmod{p^{s+2}} \neq \varphi(p^{s+1})$ by $(2)^*$

Hence

order of $a \pmod{p^{s+2}} = p \cdot \varphi(p^{s+1})$

$= \varphi(p^{s+2})$

That is $a^{\varphi(p^{s+2})} \equiv 1 \pmod{p^{s+2}}$

Thus a is a primitive root $\pmod{p^{s+2}}$

Hence by induction a is a primitive root $\not\equiv 0 \pmod{p^K}$ for any $K > 0$.

THEOREM:

Let a be a primitive root of p^K, then

(i) If a is odd, it is also a primitive root of $2p^K$.

(ii) If a is even, then $a + p^K$ is a primitive root of $2p^K$. where p is an odd prime.

PROOF: Let a be odd, then

$$a \equiv 1 \pmod 2.$$

That order of $a \pmod 2 = 1$ ——— (1)

Also a is a primitive root mod p^K.

Then order of $a \pmod{p^K} = \varphi(p^K)$ ——— (2)

(1) & (2) gives

$$\text{order of } a \pmod{\langle 2, p^K \rangle} = \langle 1, \varphi(p^K) \rangle = \varphi(p^K)$$

That is order of $a \pmod{2p^K} = \varphi(p^K) = \varphi(2p^K)$

or $a^{\varphi(2p^K)} \equiv 1 \pmod{2p^K}$

Hence a is a primitive root of $2p^K$.

231

(ii) Let a be even then obviously $a+p^k$ is an odd primitive root of p^k. Hence by (i) $a+p^k$ is a primitive root of $2p^k$.

DEF: Let m be a positive integer and b be the smallest positive integer such that $a^b \equiv 1 \pmod m$ for every a relatively prime to m. Then b is called least universal exponent for m.)

THEOREM: There exist atleast one primitive root modulo each prime.

PROOF: Suppose p is prime and b be the least universal exponent for p. Let a be an integer of order $b \pmod p$.

Then $a^b \equiv 1 \pmod p$; $(a,p)=1$ ——①

Thus the congruence $x^b \equiv 1 \pmod p$ has $p-1$ solutions. As $(1,2,\cdots p-1, p)=1$.

But by Lagrange's theorem the congruence has atmost b solutions. Thus $b = p-1$ put in ①

232

$$a^{p-1} \equiv 1 \pmod{p}$$

or $$a^{\phi(p)} \equiv 1 \pmod{p}$$

which shows that a is a primitive root mod p. Thus there exist at least one primitive root modulo each prime.

THEOREM: There exist primitive roots belonging to p^k and $2p^k$, p being an odd prime and $k \geq 1$

PROOF: We first shows that there exists a primitive root $(\bmod p^k)$, p odd prime and $k \geq 1$

If $k = 1$, then there exist atleast one primitive root modulo each prime p.

let a be a primitive root $(\bmod p)$.

Let $a' = a + p$

Since $a' = a + p \equiv a \pmod{p}$ and

a is a primitive root $(\bmod p)$.

Hence a' is also a primitive root $(\bmod p)$.

Further

$$(a')^{p-1} = (a+p)^{p-1}$$

$$= a^{p-1} + p(p-1)a^{p-2} + \text{terms divisible by } p^2 \quad \text{——(1)}$$

We shall show that a is a primitive root $(\bmod p^K)$. If $a^{p-1} \equiv 1 \pmod{p^2}$

then (1) becomes

$(a')^{p-1} \not\equiv 1 \pmod{p^2}$ with $a'^{p-2} \not\equiv 1 \pmod{p^2}$

& $(p, p-1) = 1$

Thus we take a primitive root $a \pmod p$ the one for which

$a^{p-1} \not\equiv 1 \pmod{p^2}$. that is a'.

Next we will shows that a so selected obey $a^{p^{K-2}\cdot(p-1)} \not\equiv 1 \pmod{p^K}$ $\forall K \geq 2$. ——— (1)

For $K = 2$

$a^{p-1} \not\equiv 1 \pmod{p^2}$ By choice of $a = a'$.

Suppose $a^{p^{K-2}\cdot(p-1)} \not\equiv 1 \pmod{p^K}$ $\forall K > 2$. ——— (2)

we will shows

$a^{p^{(K+1)-2}\cdot(p-1)} \not\equiv 1 \pmod{p^{K+1}}$

that $a^{p^{K-1}\cdot(p-1)} \not\equiv 1 \pmod{p^{K+1}}$.

234

Since $(a, p) = 1$

So $(a, p^{K-1}) = 1$

Therefore by Euler's theorem

$$a^{\varphi(p^{K-1})} \equiv 1 \pmod{p^{K-1}}$$

$$a^{p^{K-2}\cdot(p-1)} \equiv 1 \pmod{p^{K-1}} \quad \because \varphi(p^{K-1}) = (p-1)\cdot p^{K-2}$$

or $$a^{p^{K-2}\cdot(p-1)} = 1 + t\,p^{K-1} \quad \text{---(3)}$$ for some integer t.

and by (2) $(t, p) = 1$ otherwise

$p \mid t$ and (3) gives

$$a^{p^{K-2}\cdot(p-1)} \equiv 1 \pmod{p^K}$$

contradiction against (2).

Now

$$a^{p^{(K+1)-2}\cdot(p-1)} = a^{p^{K-1}\cdot(p-1)}$$

$$= \left(a^{p^{K-2}\cdot(p-1)}\right)^p$$

$$= \left(1 + t\,p^{K-1}\right)^p$$

$$= 1 + t\cdot p\,p^{K-1} + \text{terms divisible by } p^{K+1}$$

235

that is

$$a^{p^{(K+1)-2}\cdot(p-1)} \equiv 1 + t\cdot p^K \pmod{p^{K+1}} \quad (t,p)=1$$

$$\not\equiv 1 \pmod{p^{K+1}} \quad \forall\ K \geq 2.$$

We have shown a with this choice works as a primitive root $\pmod{p^K}$.

Let n be the exponent of $a \pmod{p^K}$

then $a^n \equiv 1 \pmod{p^K}$ —— (4)

Also $a^{\varphi(p^K)} \equiv 1 \pmod{p^K}$ Euler's theorem

thus $n \mid \varphi(p^K) = p^{K-1}\cdot(p-1)$ —— (5)

As $p^K \mid a^n - 1$

$\Rightarrow p \mid a^n - 1 \Rightarrow a^n \equiv 1 \pmod{p}$ —— (4)*

But a has exponent $\varphi(p) \pmod{p}$.

$\Rightarrow \varphi(p) \mid n$ By (4)*

or $p-1 \mid n$

Hence $n = p^m(p-1)$ by (5)

$0 \leq m \leq K-1$

If $m < K$, then $m \leq K-2$

226

But by (1)

$m > K-2$; Thus

$m = K-1$

Hence $n = p^{K-1}\cdot(p-1)$

$= \phi(p^K)$.

$m \geq K-2 \geq 0$

$0 \leq K-2 < K-1 = m$

In (1)

If $n = p^{K-2}\cdot(p-1)$

then $a^n \not\equiv 1 \pmod{p^K}$

Thus $m > K-2$

Comparing with

$n = p^m\cdot(p-1)$

Hence exponent of a is $\phi(p^K) \pmod{p^K}$.

i.e a is a primitive root $\pmod{p^K}$.

We now show that $\forall p^K ; K \geq 1$ has primitive roots belonging to it.

Let a be a primitive root $\pmod{p^K}$. If a is even replace a by $a' = a+p$ so that we can assume that a is an odd primitive root $\pmod{p^K}$.

Suppose exponent of $a \pmod{2p^K}$ is n.

Then $n \mid \phi(2p^K) = \phi(p^K)$ — (1) $\because (2p^K, a) = 1$ &

$a^{\phi(2p^K)} \equiv 1 \pmod{2p^K}$

Also a is a primitive root $\pmod{p^K}$. Then $\phi(p^K)$ is an exponent of $a \pmod{p^K}$. $a^n \equiv 1 \pmod{2p^K}$ (by Supposition)

$\Rightarrow a^n \equiv 1 \pmod{p^K}$

But $\phi(p^K)$ is least

237

(i) & (ii) gives

$n = \varphi(p^K) = \varphi(2p^K)$

Thus $\varphi(2p^K)$ is an exponent of $a \pmod{2 \cdot p^K}$

that is a is a primitive root $(\text{mod } 2p^K)$.

Remark:

① By last theorem, Any odd primitive root $(\text{mod } p^K)$ serves as a primitive root $(\text{mod } 2 \cdot p^K)$.

② The only integers that has primitive root belonging to them are $2, 4, p^K$ or $2p^K$, p odd prime and $K \geq 1$

FORTEST (TELNGI)

THEOREM: Let $m > 2$ have a primitive root and let $(a, m) = 1$ then either

$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$ or

$a^{\frac{\varphi(m)}{2}} \equiv -1 \pmod{m}$

PROOF: Left

238

INDICES:

Let a be a primitive root belonging to an integer m. For any integer b co-prime to m if $b \equiv a^K \pmod m$, then K is called index of b modulo m relative to the primitive root a.

We write symbolically as

$\text{Ind}_a b = K$ if $b \equiv a^K \pmod m$ or simply

$\text{Ind}_b = K$.

Example: Make a table of indices for a prime 5 with primitive root 3.

Sol. We are given $a = 3$, $m = 5$.

Consider $b \equiv 3^K \pmod 5$

$K = 1$; $b \equiv 3 \pmod 5 \Rightarrow b = 3$

$K = 2$; $b \equiv 9 \pmod 5 \Rightarrow b = 4$

$K = 3$; $b \equiv 27 \pmod 5 \Rightarrow b = 2$

$K = 4$; $b \equiv 81 \pmod 5 \Rightarrow b = 1$

Table of indices is

b	1	2	3	4
Index	4	3	1	2

239

THEOREM:

Let a be a primitive root modulo m and b, c, K any integers, then the following hold

(i) $b \equiv c \pmod m \Rightarrow Ind\, b \equiv Ind\, c \pmod{\varphi(m)}$

(ii) $Ind(bc) \equiv Ind\, b + Ind\, c \pmod{\varphi(m)}$

(iii) $Ind\, b^K \equiv K\, Ind\, b \pmod{\varphi(m)}$

(iv) $Ind\, 1 \equiv 0 \pmod{\varphi(m)}$

PROOF:

(i) let $Ind\, b = r$ & $Ind\, c = s$

then by def

$b \equiv a^r \pmod m$ and

$c \equiv a^s \pmod m$

let $b \equiv c \pmod m$ ——— (1)

Also $m \mid b - a^r$ & $m \mid c - a^s$

then $b - a^r = m t_1$ & $c - a^s = m t_2$

for integers t_1 & t_2.

putting values in (1)

$a^r + m t_1 \equiv a^s + m t_2 \pmod m$

or $a^r \equiv a^s \pmod m$

240

But $(a, m) = 1$

$\Rightarrow (a^s, m) = 1$

Hence $a^{r-s} \equiv 1 \pmod m$

But a is primitive root $(\text{mod } m)$

Therefore $\varphi(m) \mid r - s$

or $r \equiv s \pmod{\varphi(m)}$

that is $\text{Ind } b \equiv \text{Ind } c \pmod{\varphi(m)}$

(ii) Consider

$bc = (a^r + mt_1)(a^s + mt_2)$

$= a^{r+s} +$ terms divisible by m.

or $bc \equiv a^{r+s} \pmod m$ —— (2)

let $\text{Ind } bc = t$ relative to primitive roots

Then $bc = a^t \pmod m$ —— (3)

(2) & (3) imply

$a^t \equiv a^{r+s} \pmod m$

$\Rightarrow a^{t-r-s} \equiv 1 \pmod m \quad \because (a^{r+s}, m) = 1$

But a is primitive root belonging to m.

Hence $\varphi(m) \mid t - r - s$

or $t \equiv r + s \pmod{\varphi(m)}$

That is

$$\text{Ind } bc \equiv \text{Ind } b + \text{Ind } c \pmod{\varphi(m)}.$$

General form $\text{Ind } a_1 a_2 \cdots a_k \equiv \text{Ind } a_1 + \cdots + \text{Ind } a_k \pmod{\varphi(m)}$

(iii) By def

$$b \equiv a^k \pmod{m}$$

Then put $b = c$ in (2), we get

$$\text{Ind } b^2 \equiv 2 \text{ Ind } b \pmod{\varphi(m)}$$

Suppose result is true for $k-1$.

that is

$$\text{Ind } b^{k-1} \equiv \overline{k-1} \text{ Ind } b \pmod{\varphi(m)} \quad \text{---------- (1)}$$

Consider

$$\begin{aligned} \text{Ind } b^k &\equiv \text{Ind } b^{k-1} \cdot b \\ &\equiv \text{Ind } b^{k-1} + \text{Ind } b \pmod{\varphi(m)} \\ &\equiv \overline{k-1} \text{ Ind } b + \text{Ind } b \pmod{\varphi(m)} \\ &\equiv k \text{ Ind } b \pmod{\varphi(m)} \end{aligned}$$

which completes the proof.

178

THEOREM: If $n > 2$, then $\varphi(n)$ is even.

Proof: Every integer $n > 2$ is either equal to 2^k for some $k > 1$ or is equal to $p^c q$ where p is an odd prime and q is some integer prime to p.

let $n = 2^k$. Then

$$\begin{aligned}\varphi(n) &= \varphi(2^k) \\ &= 2^k - 2^{k-1} \\ &= 2^{k-1}(2-1) \\ &= 2^{k-1}, \text{ which is always even.}\end{aligned}$$

let $n = p^c q$

Then $\varphi(n) = \varphi(p^c q)$

$$\begin{aligned}&= \varphi(p^c)\,\varphi(q) \\ &= (p^c - p^{c-1})\,\varphi(q)\end{aligned}$$

But $p^c - p^{c-1}$ is even as p is odd.

Hence $(p^c - p^{c-1})\varphi(q)$ is even. That is $\varphi(n)$ is even.

Exercise: If $d \mid n$, then $\varphi(d) \mid \varphi(n)$

Solution: Suppose that $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ where p_i are distinct primes.

Since $d \mid n$, so $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p^{\beta_s}$ $s \le r$ & $\beta_i \le k_i$.

Then $\varphi(n) = \varphi(p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r})$

$= (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) = n \prod_{i=1}^{r} (1 - p_i^{-1})$

179

Also $\varphi(d) = \varphi(p_1^{\beta_1} \cdots p_s^{\beta_s})$

$= d \prod_{i=1}^{s} (1 - p_i^{-1})$

Now $\dfrac{\varphi(n)}{\varphi(d)} = \dfrac{n}{d} \dfrac{\prod_{i=1}^{r} (1 - p_i^{-1})}{\prod_{i=1}^{s} (1 - p_i^{-1})}$

$= \dfrac{n}{d} \prod_{i=s+1}^{r} (1 - p_i^{-1})$ $\because s \le r$.

Since $d \mid n$, so R.H.S is an integer

Thus $\varphi(d) \mid \varphi(n)$.

ASSIGNMENT:

(i) If n is odd then $\varphi(2n) = \varphi(n)$

(ii) If n is even then $\varphi(2n) = 2\varphi(n)$

$n = 2m$, $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

$\varphi(n) = \varphi(2m) = \varphi(4m)\, \varphi(4 \cdot p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r})$

$= \varphi(2^2)\, \varphi(p_1^{\alpha_1} \cdots p_r^{\alpha_r})$

$= 2\varphi(2)\, \varphi(p_1^{\alpha_1} \cdots p_r^{\alpha_r})$

$= 2\varphi(2 p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = 2\varphi(2m)$

$= 2\varphi(n)$.

(iii) If p and $2p+1$ are both odd primes and $n = 4p$, then $\varphi(n+2) = \varphi(n) + 2$.

(iv) If p is prime such that p and $p+2$ are both primes, then prove that $\varphi(p+2) = \varphi(p) + 2$

(v) If p is prime & $p \mid n$, then $\varphi(pn) = p\varphi(n)$

$\because p \mid n$, so every divisor of p also divide n, hence $\varphi(pn) = p\varphi(n)$ by TH proved earlier.

If $p \nmid n$, then $\varphi(pn) = (p-1)\varphi(n)$ (v)(i) Evaluate

180

Arithmatic functions:

Def: An arithmatic function is a function with domain the set of positive integers. It may take real or complex values. For example $f(n) = n^K$, K is any positive integer, the Euler ϕ-function and the function f such that $f(n)$ is the nth prime.

Definition: Let n be a given positive integer. Then

(i) $\tau(n)$ (Tau) is the number of positive divisors of n.

(ii) $\sigma(n)$ is the sum of positive divisors of n.

(iii) $\sigma_K(n)$ is the sum of Kth power of positive divisors of n.

we can define (i), (ii) & (iii) as

(i) $\tau : N \to N$ such that $\tau(n) = \sum_{\substack{d|n \\ d\geq 1}} 1$

(ii) $\sigma : N \to N$ such that $\sigma(n) = \sum_{\substack{d|n \\ d\geq 1}} d$

(iii) $\sigma_K : N \to N$ such that $\sigma_K(n) = \sum_{\substack{d|n \\ d\geq 1}} d^K$

Exp let $n = 12$, the positive divisors of 12 are $1, 2, 3, 4, 6, 12$

Then $\tau(n) = \sum_{\substack{d|n \\ d\geq 1}} 1 = 1+1+1+1+1+1 = 6$

$\sigma(n) = \sum_{\substack{d|n \\ d\geq 1}} d = 1+2+3+4+6+12 = 28$

$\sigma_2(n) = \sum_{d|n} d^2 = 1^2+2^2+3^2+4^2+6^2+12^2 = 210$

181

Exercise: Let $n = p^k$, then find the followings

(i) $\tau(n)$ (ii) $\sigma(n)$ (iii) $\sigma_s(n)$.

Solution The positive divisors of p^k are $1, p, p^2, \ldots, p^k$

Then by def

(i) $\tau(n) = \sum_{\substack{d|n \\ d\geq 1}} 1 = k+1$

(ii) $\sigma(n) = \sum_{\substack{d|n \\ d\geq 1}} d = 1 + p + \cdots + p^k = \frac{p^{k+1}-1}{p-1}$

(iii) $\sigma_s(n) = \sum_{\substack{d|n \\ d\geq 1}} d^s = 1 + p^s + p^{2s} + \cdots + p^{ks} = \frac{(p^s)^{k+1}-1}{p^s-1}$

THEOREM: If $n = p_1^{s_1} \cdot p_2^{s_2} \cdots p_r^{s_r}$, p_i distinct primes and integers $s_i \geq 1$, then for each $r \geq 1$, the following hold

(i) $\tau(n) = (s_1+1)(s_2+1)\cdots(s_r+1)$

(ii) $\sigma(n) = \frac{p_1^{s_1+1}-1}{p_1-1} \cdot \frac{p_2^{s_2+1}-1}{p_2-1} \cdots \frac{p_r^{s_r+1}-1}{p_r-1}$

(iii) $\sigma_k(n) = \frac{p_1^{(s_1+1)k}-1}{p_1^k-1} \cdot \frac{p_2^{(s_2+1)k}-1}{p_2^k-1} \cdots \frac{p_r^{(s_r+1)k}-1}{p_r^k-1}$

PROOF: By induction on r.

Let $r=1$, then $n = p_1^{s_1}$

So $\tau(n) = s_1+1$, ——(1) $\sigma(n) = \frac{p_1^{s_1+1}-1}{p_1-1}$ ——(2)

$\sigma_k(n) = \frac{p_1^{(s_1+1)k}-1}{p_1^k-1}$ ——(3)

182

(1), (2) & (3) Shows that result is true for $r=1$

Suppose that result is true for $r-1$ where $r-1 \geq 2$.

Let $n' = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_{r-1}^{\beta_{r-1}}$

then $\tau(n') = (\beta_1+1)(\beta_2+1)\cdots(\beta_{r-1}+1)$

$$\sigma(n') = \frac{p_1^{\beta_1+1}-1}{p_1-1} \cdot \frac{p_2^{\beta_2+1}-1}{p_2-1} \cdots \frac{p_{r-1}^{\beta_{r-1}+1}-1}{p_{r-1}-1}$$

$$\sigma_K(n') = \frac{p_1^{(\beta_1+1)K}-1}{p_1^K-1} \cdot \frac{p_2^{(\beta_2+1)K}-1}{p_2^K-1} \cdots \frac{p_{r-1}^{(\beta_{r-1}+1)K}-1}{p_{r-1}^K-1}$$

Moreover $n = n' p_r^{\beta_r}$ where $(n', p_r^{\beta_r}) = 1$

Then divisors of n are of the form $d' p_r^t$; $d' | n'$ & $0 \leq t \leq \beta_r$.

Thus $d', d'p_r, d'p_r^2, \cdots d'p_r^{\beta_r}$ are divisors of n.

By def

(i) $$\tau(n) = \sum_{\substack{d|n \\ d\geq 1}} 1 = \sum_{d'|n} 1 + \sum_{d'p_r|n} 1 + \sum_{d'p_r^2|n} 1 + \cdots + \sum_{d'p_r^{\beta_r}|n} 1$$

$$= \tau(n') + \tau(n') + \cdots + \tau(n') \quad (\beta_r+1) \text{ times}$$

$$= (\beta_r+1)\,\tau(n')$$

$$= (\beta_r+1)(\beta_1+1)\cdots(\beta_{r-1}+1) \quad \text{by Supposition}$$

$$= (\beta_1+1)(\beta_2+1)\cdots(\beta_{r-1}+1)(\beta_r+1)$$

(ii) $$\sigma(n) = \sum_{\substack{d|n \\ d\geq 1}} d = \sum_{\substack{d'|n' \\ d'\geq 1}} d' + \sum_{\substack{d'|n' \\ d'\geq 1}} d'p_r + \cdots + \sum_{\substack{d'|n' \\ d'\geq 1}} d'p_r^{\beta_r}$$

$$= \sum d' + \left(\sum d'\right) p_r + \cdots + \left(\sum_{d'|n'} d'\right) p_r^{\beta_r}$$

183

$$= \sum_{\substack{d'/n' \\ d'\geq 1}} d' \left(1 + p_r + \cdots + p_r^{\beta_r}\right)$$

$$= \sum_{\substack{d'/n' \\ d'\geq 1}} d' \left(\frac{p_r^{\beta_r+1} - 1}{p_r - 1}\right)$$

$$= \sigma(n') \left(\frac{p_r^{\beta_r+1} - 1}{p_r - 1}\right)$$

$$= \frac{p_1^{\beta_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\beta_2+1} - 1}{p_2 - 1} \cdots \frac{p_{r-1}^{\beta_{r-1}+1} - 1}{p_{r-1} - 1} \cdot \frac{p_r^{\beta_r+1} - 1}{p_r - 1}$$

(iii) $$\sigma_k(n) = \sum_{\substack{d/n \\ d\geq 1}} d^k = \sum_{\substack{d'/n \\ d'\geq 1}} d'^k + \sum_{\substack{d'/n' \\ d'\geq 1}} (d' p_r)^k + \cdots + \sum_{\substack{d'/n' \\ d'\geq 1}} (d' p_r^{\beta_r})^k$$

$$= \sum_{\substack{d'/n' \\ d'\geq 1}} d'^k \left(1 + p_r^k + p_r^{2k} + \cdots + p_r^{k\beta_r}\right)$$

$$= \sum_{\substack{d'/n' \\ d'\geq 1}} d'^k \cdot \frac{\left(p_r^k\right)^{\beta_r+1} - 1}{p_r^k - 1}$$

$$= \sigma_k(n') \frac{p_r^{k(\beta_r+1)} - 1}{p_r^k - 1}$$

$$= \frac{p_1^{k(\beta_1+1)} - 1}{p_1^k - 1} \cdot \frac{p_2^{k(\beta_2+1)} - 1}{p_2^k - 1} \cdots \frac{p_r^{k(\beta_r+1)} - 1}{p_r^k - 1}$$

which complete the proof.

184

Exp Let $n = 1056 = 2^5 \cdot 3^2 \cdot 7^2$

Then $\tau(n) = (4+1)(2+1)(2+1) = 45$

$$\sigma(n) = \frac{2^5-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{7^3-1}{7-1} = 2997$$

$$\sigma_2(n) = \frac{2^{2(5)}-1}{2^2-1} \cdot \frac{3^6-1}{3^2-1} \cdot \frac{7^6-1}{7^2-1} = 2756981$$

THEOREM: Let $(m,n) = 1$, then

(i) $\tau(mn) = \tau(m) \cdot \tau(n)$

(ii) $\sigma(mn) = \sigma(m)\,\sigma(n)$

PROOF: Let $m = q_1^{b_1} \cdot q_2^{b_2} \cdots q_\ell^{b_\ell}$

$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$

Since $(m,n) = 1$. It follows $p_i \neq q_j$ $\forall i, j$ $1 \le i \le k$, $1 \le j \le \ell$.

Now $\tau(mn) = \tau(q_1^{b_1} \cdot q_2^{b_2} \cdots q_\ell^{b_\ell} \cdot p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k})$

$= (b_1+1)(b_2+1)\cdots(b_\ell+1)(a_1+1)\cdots(a_k+1)$

$= \tau(m) \cdot \tau(n)$

Similarly $\sigma(mn) = \sigma(m)\,\sigma(n)$

Corollary If $n = p_1^{s_1} \cdot p_2^{s_2} \cdots p_r^{s_r}$, $s_i \ge 1$ and p_i distinct primes

then (i) $\tau(n) = \tau(p_1^{s_1})\,\tau(p_2^{s_2}) \cdots \tau(p_r^{s_r})$

(ii) $\sigma(n) = \sigma(p_1^{s_1})\,\sigma(p_2^{s_2}) \cdots \sigma(p_r^{s_r})$

185

THEOREM: Let n be an integer > 1. Then the following hold

(i) $\tau(n)$ is odd iff n is a perfect square.

(ii) $\sigma(n)$ is odd iff n is a perfect square or twice a perfect square.

(iii) $\prod_{d/n} d = n^{\frac{\tau(n)}{2}}$

PROOF: Since $n > 1$, let

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}; \quad p_i \text{ distinct primes } \& k_i > 1$$

then $\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$, we know?

$\tau(n)$ is odd iff $(k_1+1)(k_2+1)\cdots(k_r+1)$ is odd

iff k_i+1 is odd $(i = 1, 2, \ldots, r.$ (Product of odd is odd).

iff k_i is even.

Suppose $k_i = 2m_i \quad i = 1, 2, \ldots, r.$

Then

$$\begin{aligned} n &= p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r} \\ &= p_1^{2m_1} \cdot p_2^{2m_2} \cdots p_r^{2m_r} \\ &= \left(p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}\right)^2 \end{aligned}$$

Hence $\tau(n)$ is odd iff n is a perfect square.

186

(ii) We know

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

$$= (1+p_1+\cdots+p_1^{k_1})(1+p_2+\cdots+p_2^{k_2})\cdots(1+p_r+\cdots+p_r^{k_r})$$

$\sigma(n)$ is odd iff $1+p_i+\cdots+p_i^{k_i}$ $\forall i=1,2,\cdots r$ is odd

iff k_i is even $\forall i$ if all p_i are odd

and if one of p_i, (say) $p_1=2$ then

k_i is even $\forall i=2,3,\cdots r$

iff $k_i = 2m_i$ $\forall i=1,2,\cdots r$.

Or case $k_i = 2m_i$.

When all p_i's are odd, then

$\sigma(n)$ is odd iff $k_i = 2m_i$ $1 \le i \le r$.

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r} = \left(p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}\right)^2$$

Thus $\sigma(n)$ is odd iff n is a perfect square.

case Take $p_1=2$ & $k_i = 2m_i$ $2 \le i \le r$.

Then $n = 2^{k_1}\left(p_2^{m_2} \cdot p_3^{m_3} \cdots p_r^{m_r}\right)^2$ ——— (1)

If k_1 is even, then n is a perfect square.

If k_1 is odd, then $k_1 = 2m_1+1$, (1) becomes

$n = 2 \cdot \left(2^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}\right)^2$; Twice of perfect square

Conversely $\sigma(n)$ is odd iff n is a perfect square

184

(iii) Since $d|n$, so there exist an integer d' such that $n = dd'$

$\Rightarrow d'|n$ and $d' = \frac{n}{d}$

Thus divisors of n are in pairs $(d, \frac{n}{d})$.

Product of all divisors of n

$$= \left(\prod_{d|n} d\right)^2$$

$$= n^{\tau(n)}$$

e.g. $2, -2, 3, -3$

$\pi = (2)^2(-3)^2 = (6)^2$

Then $\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$ where $\tau(n)$ is the number of +ve divisors of n ——— (1)

If $\tau(n)$ is even, then $\frac{\tau(n)}{2}$ is an integer, so that $n^{\frac{\tau(n)}{2}}$ is an integer and (1) is balanced.

If $\tau(n)$ is odd then n is a perfect square. let $n = m^2$, $m \in Z^+$.

Then $n^{\frac{\tau(n)}{2}} = (m^2)^{\frac{\tau(n)}{2}} = m^{\tau(n)}$ But $\tau(n)$ is always integer. Hence $m^{\tau(n)}$ is also integer. Again (1) is balanced.

Hence $\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$.

188

Assignment:

(1) Evaluate $\Lambda(n)$ & $T(n)$ where

$n = 487 ; 3655 ; 5939$

(2) $\sum_{d/n} \frac{1}{d} = \frac{\sigma(n)}{n}$; $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$; $k_i \geq 1$

p_i distinct primes & $1 \leq i \leq r$.

(3) Let n be a square free integer having 'r' prime factors, then $T(n) = 2^r$

(4) Let $n > 1$ and $n = \prod_{i=1}^{r} p_i^{k_i}$ be prime factorization, then

$$\Lambda(n)\, \varphi(n) = n^2 \prod_{i=1}^{r} \left(1 - \frac{1}{p_i^{k_i+1}}\right)$$

(5) Let k be an integer ≥ 2, then

(i) $\Lambda(2^{k-1}) = 2^k - 1$

(ii) If $2^k - 1$ is a prime and $n = 2^{k-1}(2^k - 1)$, then $\Lambda(n) = 2n$

(iii) If $2^k - 3$ is a prime and $n = 2^{k-1}(2^k - 3)$, then

$$\Lambda(n) = 2n + 2.$$

H.M KHALID MAHMOOD

HINTS (3) Since n is square free integer, it means n is not a multiple of an perfect square. Hence 187

$$n = p_1 \cdot p_2 \cdots p_r$$

$$\tau(n) = (1+1)(1+1)\cdots(1+1) \text{ } r \text{ factors}$$

$$= 2 \cdot 2 \cdots 2$$

$$= 2^r.$$

Möbius Function:

It is denoted by μ and is defined as

$$\mu : N \longrightarrow \{-1, 0, 1\} \text{ such that}$$

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \text{ has a square factor} \\ (-1)^r & \text{if } n = p_1 \cdot p_2 \cdots p_r \text{ ; } p_i \text{ distinct primes} \end{cases}$$

Thus if p is prime, then

$$\mu(p^k) = \begin{cases} -1 & \text{for } k = 1 \\ 0 & \text{for } k \geq 2. \end{cases}$$

$$\mu(6) = \mu(2 \cdot 3) = (-1)^2 = +1$$

$$\mu(20) = \mu(2^2 \cdot 5) = 0$$

$$\mu(125) = \mu(5^2 \cdot 5) = 0$$

$$\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3$$

$$= -1.$$

19c

THEOREM (F. Merten's Lemma):

For each integer $n \geq 1$ $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$

PROOF:

If $n=1$, $\sum_{d|n} \mu(d) = \mu(1) = 1$ by def.

Suppose $n>1$, then by FTA

$n = p_1^{K_1} \cdot p_2^{K_2} \cdots p_r^{K_r}$; p_i distinct primes and $K_i \geq 1$

Let $n' = p_1^{K_1} \cdot p_2^{K_2} \cdots p_{r-1}^{K_{r-1}}$

Then $n = n' p_r^{K_r}$; $(n', p_r^{K_r}) = 1$

Then divisors of n are of the form $d' p_r^t$ $0 \leq t \leq r$ where $d' | n'$

Then by def

$$\sum_{d|n} \mu(d) = \sum \mu(d') + \sum \mu(d' p_r) + \sum \mu(d' p_r^2) + \cdots + \sum \mu(d' p_r^{K_r})$$

$$= \sum \mu(d') + \sum \mu(d' p_r) + 0 + 0 + 0 + \cdots + 0$$

$$= \sum \mu(d') + \sum \mu(d') \mu(p_r)$$

$$= \sum \mu(d') + \sum \mu(d')(-1)$$

$$= 0$$

Hence

$$\sum_{d|n} \mu(d) = 0 \quad \text{for } n>1$$

191

THEOREM: For each positive integer $n \geq 1$

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

PROOF: If $n = 1$, $\varphi(1) = 1$ and $\sum_{d|n} \mu(d) \cdot \frac{n}{d} = \mu(1) = 1$

Suppose $n > 1$, then by F.T.A

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r} \; ; \; p_i \text{ distinct primes and } k_i \geq 1$$

By induction on r,

If $r = 1$, then $1, p_1, p_1^2, \cdots p_1^{k_1}$ are divisors of n.

Then $\sum_{d|n} \mu(d) \cdot \frac{n}{d} = \mu(1) \cdot \frac{p_1^{k_1}}{1} + \mu(p_1) \frac{p_1^{k_1}}{p_1} + \frac{\mu(p_1^2) p_1^{k_1}}{p_1^2} + \cdots + \mu(p_1^k) \cdot \frac{p_1^{k_1}}{p_1^{k_1}}$

$$= 1 \cdot p_1^{k_1} + (-1) \frac{p_1^{k_1}}{p_1} + 0 + 0 + \cdots + 0$$

$$= p_1^{k_1} - p_1^{k_1} \cdot \frac{1}{p_1}$$

$$= p_1^{k_1} \left(1 - \frac{1}{p_1}\right)$$

$$= n \prod \left(1 - \frac{1}{p_1}\right)$$

Suppose that result is true for $r-1$ distinct prime factors.

that is $\sum_{d'|n'} \mu(d') \frac{n'}{d'} = \varphi(n')$

$= n' \prod_{p|n'} \left(1 - \frac{1}{p}\right)$ is Satisfied

where $n' = p_1^{k_1} \cdot p_2^{k_2} \cdots p_{r-1}^{k_{r-1}}$

192

Then $n = n' p_r^{k_r}$; $(n', p_r^{k_r}) = 1$

Let $d \mid n$, then by def of Möbius function.

$$\sum_{d \mid n} \mu(d) \cdot \frac{n}{d} = \sum \mu(d') \frac{n}{d'} + \sum \mu(d' p_r) \cdot \frac{n}{d' p_r} + \text{terms}$$

$$= \sum_{d' \mid n} \mu(d') \frac{n' p_r^{k_r}}{d'} + \sum_{d' \mid n} \mu(d') \mu(p_r) \frac{n' p_r^{k_r}}{d' p_r}$$

$$= \sum_{d' \mid n'} \mu(d') \frac{n'}{d'} \left(p_r^{k_r} - \frac{p_r^{k_r}}{p_r} \right)$$

$$= \sum_{d' \mid n'} \mu(d') \frac{n'}{d'} \varphi(p_r)$$

$$= \varphi(n') \varphi(p_r^{k_r}) \quad \text{by Supposition}$$

$$= \varphi(n' p_r^{k_r})$$

$$= \varphi(n)$$

Moreover

$$\varphi(p_r^{k_r}) \varphi(n')$$

$$= (p_r^{k_r} - p_r^{k_r - 1}) n' \prod_{p \mid n'} (1 - \frac{1}{p})$$

$$= n' p_r^{k_r} \prod_{p \mid n'} (1 - \frac{1}{p})(1 - \frac{1}{p_r})$$

$$= n \prod_{p \mid n} (1 - \frac{1}{p}) \quad \text{Whit Complete the proof.}$$

Multiplicative Arithmatic functions:

Def: An arithmatic function f is called a multiplicative arithmatic function if for each pair of co-prime integers m and n $f(mn) = f(m) \cdot f(n)$

Moreover if there is no restriction on integers m & n and $f(mn) = f(m) \cdot f(n)$, then f is called complete arithmatic function.

THEOREM: The functions φ, σ, τ and μ are are multiplicative arithmatic functions.

PROOF: Let $m > 1$ and $n > 1$ be two co-prime integers and

$m = \prod_{i=1}^{r} p_i^{\alpha_i}$, $n = \prod_{j=1}^{s} q_j^{\beta_j}$ be their unique factorizations into primes

then $mn = \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} q_j^{\beta_j}$

Also

$$\mu(mn) = \begin{cases} 1 & \text{if } \alpha_i = \beta_j = 0 \ \forall i,j \\ 0 & \text{if at least one } \alpha_i\text{'s or } \beta_j\text{'s} > 1 \\ (-1)^{r+s} & \text{if } \alpha_i = \beta_j = 1 \ \forall i,j \end{cases}$$

case 1: If $\alpha_i = \beta_j = 0 \ \forall i,j$

then $\mu(mn) = \mu(p_1^0 p_2^0 \cdots p_r^0 q_1^0 \cdots q_s^0)$

$= \mu(1)$

$= 1$

Also $\mu(m) = 1$

174

Then $\mu(mn) = 1$

$= 1 \cdot 1$

$= \mu(m) \cdot \mu(n)$

case(ii) Suppose $\beta_i > 1$ for some i Then mn has a square factor.

Also $\mu(n) = 0$

Then $\mu(mn) = 0$

$= 0 \cdot \mu(m)$

$= \mu(n) \cdot \mu(m)$

$= \mu(m)\,\mu(n)$

Similarly if $\alpha_i > 1$ for some i

Then $\mu(m) = 0$

& mn has square factor.

Thus

$\mu(mn) = 0$

$= 0 \cdot \mu(n)$

$= \mu(m) \cdot \mu(n)$

If $\alpha_i > 1$ & $\beta_j > 1$ for some i & j

Then $\mu(m) = 0$ & $\mu(n) = 0$

Also mn has square factor.

$\mu(mn) = 0 = 0 \cdot 0 = \mu(m)\,\mu(n)$

case(iii) If $\alpha_i = \beta_j = 1$ $\forall i, j$

$\mu(mn) = \mu(p_1 \cdot p_2 \cdots p_r\, q_1 \cdot q_2 \cdots q_s) = (-1)^{r+s}$

Also $\mu(m) = \mu(p_1 \cdot p_2 \cdots p_r) = (-1)^r$

$\mu(n) = \mu(q_1 \cdot q_2 \cdots q_s) = (-1)^s$

Thus $\mu(mn) = \mu(m) \cdot \mu(n)$ which complete the proof

195

THEOREM 1:

If f is a multiplicative arithmatic function then $g_1(n) = \sum_{d|n} f(d)$ and $g_2(n) = \sum_{d|n} \mu(d) f(d)$ are both multiplicative arithmatic functions.

Proof: Let m, n be any two co-prime integers. Then every divisor d of m and every divisor d' of n are also co-prime.

Thus $g_1(mn) = \sum_{d|mn} f(d)$

$$= \sum_{\substack{d_1|m, d_2|n \\ (d_1,d_2)=1}} f(d_1 d_2) = \sum_{\substack{d_1|m, d_2|n \\ (d_1,d_2)=1}} f(d_1) f(d_2)$$

$$= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \quad \because \sum \text{ is over all divisors of } m, n$$

$$= g_1(m)\, g_1(n)$$

Also $g_2(mn) = \sum_{d|mn} \mu(d) f(d) = \sum_{\substack{d_1|m \\ d_2|n \\ (d_1,d_2)=1}} \mu(d_1 d_2) f(d_1 d_2)$

$$= \sum_{\substack{d_1|m, d_2|n \\ (d_1,d_2)=1}} \mu(d_1)\mu(d_2) f(d_1) f(d_2)$$

$$= \sum \mu(d_1) f(d_1) \sum_{d_2|n} \mu(d_2) f(d_2) \quad \because \sum \text{ is over all divisors of } m, n.$$

196

(iii) $J_3(n) = \sum_{d/n} \mu(d) f\left(\frac{n}{d}\right)$

$J_3(mn) = \sum_{\substack{d_1/m \\ d_2/n \\ (d_1,d_2)=1}} \mu(d_1 d_2) f\left(\frac{mn}{d_1 d_2}\right)$

$= \sum_{\substack{d_1/m \\ d_2/n \\ (d_1,d_1)=1}} \mu(d_1)\mu(d_2) f\left(\frac{m}{d_1}\right) f\left(\frac{n}{d_2}\right)$ $\because \frac{m}{d_1}$ & $\frac{n}{d_2}$ are integers.

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

$\because \sum$ is over all divisors of m, n

$= J_3(m) \cdot J_3(n)$

Integral part function:
Bracket function:

Let x be a real number, then we denote by $[x]$, the largest integer that does not exceed x.

e.g $[7] = 7$, $[4.35] = 4$, $[e] = 2$

$\left[-\frac{3}{2}\right] = -2$, $[\pi] = 3$, $\left[\frac{53}{59}\right] = 0$

For each real number x we can write

$x = [x] + \theta$; $0 \le \theta < 1$. It then follows that

$x - 1 < [x] \le x$

'θ' is called fractional part of x and $[x]$ is called integral part of x.

THEOREM:

Let x be a real number, then the following hold.

(i) $[x] \leq x < [x]+1$

(ii) $[x+m] = [x]+m$; m any integer.

(iii) $[x]+[y] \leq [x+y] \leq [x]+[y]+1$

(iv) $[x]+[-x] = \begin{cases} 0 & \text{if } x \text{ is an integer.} \\ -1 & \text{otherwise.} \end{cases}$

(v) $\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$; m is positive integer.

(vi) If $x, y \in R$ such that

(a) $[x]+[y] = [x+y]$

(b) $[-x]+[-y] = [-x-y]$

then atleast one of x and y is an integer and conversely.

(vii) If $m, n \in N$ such that $n = mq + r$; $0 \leq r < m$ then $\left[\frac{n}{m}\right] = q$.

PROOF: Since x is a real number, so by def

(i) $x = [x] + \theta$

$\Rightarrow [x] \leq x$ — (i)

Also $[x] + \theta < [x] + 1$ $\because \theta < 1$

$\Rightarrow x < [x] + 1$ — (ii)

(i) & (ii) imply $[x] \leq x < [x]+1$

(ii) Since $x = [x] + \theta$

then $x + m = [x] + m + \theta$

$\Rightarrow [x+m] = [[x] + m + \theta]$

$= [x] + m$ $\because [x]$ & m are integers

198

(iii) Since $x, y \in R$, so by def

$$x = [x] + \theta_1 \qquad 0 \le \theta_1 < 1$$
$$y = [y] + \theta_2 \qquad 0 \le \theta_2 < 1$$

$$x+y = [x]+[y] + (\theta_1+\theta_2)$$
$$[x+y] = \left[[x]+[y] + (\theta_1+\theta_2)\right]$$
$$= \begin{cases} [x]+[y] & \text{if } \theta_1+\theta_2 < 1 \\ [x]+[y]+1 & \text{if } \theta_1+\theta_2 \ge 1 \end{cases}$$

That is
$$[x+y] \le [x] + [y] + 1 \quad \text{---} (1)$$

Moreover $[x] \le x$, $[y] \le y$

$$[x]+[y] \le x+y$$

then $\left[[x]+[y]\right] \le [x+y]$

or $[x]+[y] \le [x+y]$ --- (2) $\because [x]$ & $[y]$ are integers.

(1) & (2) imply

$$[x]+[y] \le [x+y] \le [x]+[y]+1$$

(iv) If x is an integer, then

$$[x] = x \quad \& \quad [-x] = -x$$

So $[x]+[-x] = 0$

If x is not an integer, then

$$x = [x] + \theta \quad ; \ 0 \le \theta + 1$$
$$\Rightarrow -x = -[x] - \theta$$
$$\Rightarrow [-x] = [-[x] - \theta]$$
$$[-x] = -[x] - 1 \quad \text{---} (i)$$

199

Now $[x] + [-x] = [x] - [x] - 1$

$= -1$

Consequently

$$[x] + [-x] = \begin{cases} 0 & \text{if } x \text{ is an integer} \\ -1 & \text{otherwise.} \end{cases}$$

(V) By division algorithm

$[x] = mq + r \quad ; \quad 0 \le r < m$

Then $\left[\frac{[x]}{m}\right] = \left[\frac{mq+r}{m}\right]$

$= \left[q + \frac{r}{m}\right]$

$= q \quad \text{—(i)} \quad \because \frac{r}{m} < 1$

Also $\left[\frac{x}{m}\right] = \left[\frac{[x]+\theta}{m}\right]$

$= \left[\frac{mq + r + \theta}{m}\right]$

$= \left[q + \frac{r+\theta}{m}\right]$

$= q. \quad \text{—(ii)}$

$0 \le r < m$

$0 \le r \le m-1$

$0 \le r+1 \le m$

or $0 \le r+\theta < m$

$0 \le \frac{r+\theta}{m} < 1$

(i) & (ii) imply

$$\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$$

(vii) $\left[\frac{n}{m}\right] = \left[\frac{mq+r}{m}\right] = \left[q + \frac{r}{m}\right]$

$= q$ as required

Suppose x is an integer and $y \in R$, then

$$[x] = x, \quad y = [y] + \theta \qquad 0 \le \theta < 1$$

So $x + y = [x] + [y] + \theta$

$$[x+y] = [[x] + [y] + \theta]$$
$$= [x] + [y] \quad \text{---(i)}$$

Moreover $[-x] = -x$

$$[-y] = -[y] - \theta$$

$$-x - y = [-x] - [y] - \theta$$

$$[-x-y] = [[-x] - [y] - \theta]$$
$$= [-x] - [y] - 1$$

Also $[-x] + [-y] = -x + [-[y] - \theta]$

$$= -x - [y] - 1$$
$$= [-x-y]$$

Hence $[-x] + [-y] = [-x-y]$ —(ii)

Thus (a) & (b) are satisfied.

Conversely, Suppose that (a) & (b) hold and we will show that at least one of x or y is an integer.

Suppose both x and y are not integers.

Then $x = [x] + \theta_1 \qquad 0 \le \theta_1 < 1$

$y = [y] + \theta_2 \qquad 0 \le \theta_1 < 1$

$$[x+y] = [[x] + \theta_1 + [y] + \theta_2]$$
$$= [[x] + [y] + (\theta_1 + \theta_2)]$$

then $[x+y] = [x] + [y]$ —— (3)* if $\theta_1 + \theta_2 < 1$

Also $[-x-y] = [-[x]-\alpha_1-[y]-\alpha_2]$ — 201

$= [-[x]-[y]-(\alpha_1+\alpha_2)]$

$= -[x]-[y]-1$ if $\alpha_1+\alpha_2 < 1$

Also

$[-x]+[-y] = [-[x]-\alpha_1]+[-[y]-\alpha_1]$

$= -[x]-1+-[y]-1$

$= -[x]-[y]-2$

Hence $[-x-y] \neq [-x]+[-y]$

Thus (b) have a contradiction.

If $\alpha_1+\alpha_2 > 1$, Again we can generate, a contradiction.

Thus atleast one of a or b is an integer.

Exponent:

Let p be a prime and n be any positive integer, then the highest power of p which divide n! is called an exponent.

If e is exponent, then p^e divides n!

Practical way to find exponent:

✓ THEOREM: If p be a prime and n a positive integer. Then the exponent e is almost $\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$.

Proof: Let $n = a_s p^s + a_{s-1} p^{s-1} + \cdots + a_1 p + a_0 \; ; 0 \leq a_i < p$

be the p-adic representation of n. Then

$\left[\frac{n}{p}\right] = \left[a_s p^{s-1} + a_{s-1} p^{s-2} + \cdots + a_1 + \frac{a_0}{p}\right]$

202

$$\left[\frac{n}{p}\right] = a_s p^{s-1} + a_{s-1} p^{s-2} + \cdots + a_1$$

Similarly

$$\left[\frac{n}{p^2}\right] = a_s p^{s-2} + a_{s-1} p^{s-3} + \cdots + a_2$$

$$\vdots$$

$$\left[\frac{n}{p^s}\right] = a_s$$

Now

$$e = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^s}\right] + \cdots$$

$$= a_s p^{s-1} + a_{s-1} p^{s-2} + \cdots + a_1 + a_s p^{s-2} + \cdots + a_2 + \cdots + a_s$$

$$= a_s\left[p^{s-1} + p^{s-2} + \cdots + 1\right] + a_{s-1}\left[p^{s-2} + p^{s-3} + \cdots + 1\right]$$

$$+ \cdots + a_2(p+1) + a_1$$

$$= a_s \frac{p^s - 1}{p-1} + a_{s-1} \frac{p^{s-1} - 1}{p-1} + \cdots + a_2 \frac{p^2-1}{p-1} + a_1 \frac{p-1}{p-1}$$

$$= \frac{1}{p-1}\left[(a_s p^s + a_{s-1} p^{s-1} + \cdots + a_1 p) - (a_s + a_{s-1} + \cdots + a_1)\right]$$

$$= \frac{1}{p-1}\left[(a_s p^s + a_{s-1} p^{s-1} + \cdots + a_1 p + a_0) - (a_s + a_{s-1} + \cdots + a_1 + a_0)\right]$$

$$= \frac{1}{p-1}\left[n - \sum_{i=0}^{s} a_i\right]$$

Exp: Evaluate the exponent of 7 in 1000!

Method I $\quad e = \left[\frac{1000}{7}\right] + \left[\frac{1000}{7^2}\right] + \left[\frac{1000}{7^3}\right] + \left[\frac{1000}{7^4}\right] + \cdots$

$= 142 + 20 + 2 = 164$ NOTE $7^{164} \mid 1000!$

Method II $\quad n = 1000,\ p = 7,\ 1000 = 2\cdot 7^3 + 6\cdot 7^2 + 2\cdot 7 + 6.$

$$e = \frac{1}{7-1}\left[1000 - (2+6+2+6)\right] = 164.$$

203

Exp: Find exponent of 3 in 10! Ans 18

Exp: Find exponent of 2 and 5 in 553!

Ex Find the highest power of 136

(i) 3 contained in 31! Ans 14.

(ii) 7 contained in 2000! Ans 330

(iii) 13 contained in 15000! Ans 1247

PROOF (OF Last THEOREM):

If $p > n$, then $e = 0$

Suppose $p \leq n$. If $p^i > n$, then $\left[\frac{n}{p^i}\right] = 0$.

Hence the sum $\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$ is finite and not really an infinite series.

Consider the set $S = \{1, 2, 3, \cdots, n\}$

Then integers in S that are divisible by p are $p, 2p, \cdots, \left[\frac{n}{p}\right]p$. —— (1)

Also an integer which is divisible by p^2 is also divisible by p. Hence the integers in S that are divisible by p^2 are amongst the $\left[\frac{n}{p}\right]$ in (1) and are $p^2, 2p^2, \cdots, \left[\frac{n}{p^2}\right]p^2$. —— (2)

Again the integers that are divisible by p^3 are $p^3, 2p^3, \cdots \left[\frac{n}{p^3}\right]p^3$ amongst $\left[\frac{n}{p^2}\right]$ in (2) and so on.

Hence $e = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots$

$$= \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

Example: prove that $\frac{n!}{a_1!\,a_2!\,a_3!\cdots a_n!}$ is an integer

Where $a_i \geq 0$ and $n = a_1+a_2+a_3+\cdots+a_n$

Sol: We will show that the power of any prime in the numerator will exceed (or equal) the power of that prime in the denominator. Thus it is sufficient to show that

$$E_p(n!) \geq E_p(a_1!)+E_p(a_2!)+\cdots+E_p(a_n!)$$

Now

$$E_p(a_1!) = \left[\frac{a_1}{p}\right]+\left[\frac{a_1}{p^2}\right]+\cdots$$

$$E_p(a_2!) = \left[\frac{a_2}{p}\right]+\left[\frac{a_2}{p^2}\right]+\cdots$$

$$\vdots$$

$$E_p(a_n!) = \left[\frac{a_n}{p}\right]+\left[\frac{a_n}{p^2}\right]+\cdots$$

Adding above

$$E_p(a_1!)+E_p(a_2!)+\cdots+E_p(a_n!)$$

$$= \left[\frac{a_1}{p}\right]+\left[\frac{a_2}{p}\right]+\cdots+\left[\frac{a_n}{p}\right]+\left[\frac{a_1}{p^2}\right]+\left[\frac{a_2}{p^2}\right]+\cdots\left[\frac{a_n}{p^2}\right]+\cdots$$

$$\leq \left[\frac{a_1+a_2+\cdots+a_n}{p}\right]+\cdots+\left[\frac{a_1+a_2+\cdots+a_n}{p^n}\right] \quad \because [x]+[y] \leq [x+y]$$

or $E_p(a_1!)+\cdots+E_p(a_n!) \leq \left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^n}\right] = E_p(n!)$

or $E_p(n!) \geq E_p(a_1!)+E_p(a_2!)+\cdots+E_p(a_n!)$

205

Corollary: Prove that $\frac{n!}{r!\,(n-r)!}$ is an integer.

Take $a_1 = r$, $a_2 = n-r$

then $a_1 + a_2 = n$.

Ex Show that product of any n consecutive is divisible by $n!$

Sol. Let $m+1, m+2, \ldots, m+n$ be any given n consecutive integers.

Then

$$\frac{(m+1)(m+2)\cdots(m+n)}{n!} = \frac{1\cdot 2\cdot 3\cdots m\,(m+1)\cdots(m+n)}{m!\,n!} = \frac{(m+n)!}{m!\,n!}$$

which is an integer.

Hence $n! \mid \prod_{i=1}^{n}(m+i)$

which complete the sol.

Remark: Denote $J(n,p)$ as highest power of p in $n!$

Let n be a given integer and $p_1, p_2, \ldots, p_k$ be all primes $\le n$. Then obviously $n!$ is the product of these primes only, each raised to its highest power.

206

Hence $n! = p_1^{j(n,p_1)} \cdot p_2^{j(n,p_2)} \cdots p_k^{j(n,p_k)}$

$$= \prod_{p \le n} p^{j(n,p)}$$

Exp Express 17! as the product of primes in the canonical form.

Sol:

$$17! = \prod_{p \le 17} p^{j(n,p)}$$

the primes $p \le 17$ are 2, 3, 5, 7, 11, 13 and 17.

$j(17,2) = 8+4+2+1 = 15$

$j(17,3) = 5+1 = 6$

$j(17,5) = 3$

$j(17,7) = 2.$

$j(17,11) = 1$

$j(17,13) = 1$

$j(17,17) = 1$

Hence

$$17! = 2^{15} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17.$$

H.M. KHALID MAHMOOD

PRIMITIVE ROOTS

207

Def: Let $m > 1$ be an integer and a another integer. A positive integer h is called the exponent of a modulo m if h is the smallest positive integer such that $a^h \equiv 1 \pmod{m}$.

Exp (1) the exponent of $3 \pmod 5$ is 4. For

$$3^1 \equiv 3 \pmod 5$$
$$3^2 \equiv 4 \pmod 5$$
$$3^3 \equiv 2 \pmod 5$$
$$3^4 \equiv 1 \pmod 5$$

(2) the exponent of $2 \pmod 8$ is not defined

For
$$2 \equiv 2 \pmod 8$$
$$2^2 \equiv 4 \pmod 8$$
$$2^3 \equiv 0 \pmod 8$$
$$\vdots$$
$$2^n \equiv 0 \pmod 8 \quad \forall\ n \geq 3.$$

(3) the exponent of $3 \pmod 8$ is 2.

For
$$3 \equiv 3 \pmod 8$$
$$3^2 \equiv 1 \pmod 8.$$

Notice that if an integer a has exponent $h \pmod m$, we say a belongs to exponent $h \pmod m$.

942

Alter: let $\text{Ind}\, b = r$

then $b \equiv a^r \pmod m$

$\Rightarrow b^K \equiv a^{rK} \pmod m$

or $a^{rK} \equiv b^K \pmod m$ ——— (1)

Now if $\text{Ind}\, b^K = s$, then

$b^K \equiv a^s \pmod m$ ——— (2)

(1) & (2) gives

$a^{rK} \equiv a^s \pmod m$

$\Rightarrow a^{rK-s} \equiv 1 \pmod m \quad \because (a^s, m) = 1$

But a is primitive root $(\text{mod}\, m)$

therefore $\varphi(m) \mid rK - s$

or $rK \equiv s \pmod{\varphi(m)}$

or $s \equiv rK \pmod{\varphi(m)}$

that is $\text{Ind}\, b^K \equiv K\, \text{Ind}\, b \pmod{\varphi(m)}$

(iv) let $\text{Ind}\, 1 = r \Rightarrow 1 \equiv a^r \pmod m$

$\Rightarrow a^r \equiv 1 \pmod m$

But a is primitive root

Hence $\varphi(m) \mid r - 0$

$\Rightarrow r \equiv 0 \pmod{\varphi(m)}$

$\therefore \text{Ind}\, 1 \equiv 0 \pmod{\varphi(m)}$

343.

QUADRATIC CONGRUENCES AND RECIPROCITY LAW:

The general form of a quadratic congruence in one variable is

$$ax^2+bx+c \equiv 0 \pmod m \quad \text{---} (1)$$

where a is not divisible by m. To solve this congruence we discuss the following rules.

(1) The congruence $ay^2+by+c \equiv 0 \pmod m$ ---(1) provided $(2a, m)=1$ can be reduced to the form $x^2 \equiv d \pmod m$.

Multiplying (1) by $4a$, we get

$$4a^2y^2+4ay+4ac \equiv 0 \pmod m$$

$$\Rightarrow (2ay+b)^2 \equiv b^2-4ac \pmod m \quad \text{---} (2)$$

Set $x \equiv 2ay+b \pmod m$

& $d \equiv b^2-4ac \pmod m$

Then (2) can be reduced to

$$x^2 \equiv d \pmod m \quad \text{---} (3)$$

Suppose $x = x_0$ satisfies (3), then we have $2ay+b \equiv x_0 \pmod m$; $(2a, m)=1$

264

Since $(2a, m) = 1$.

Therefore above linear congruence is solvable for y. Consequently ① is solvable.

Example: Solve the congruence

$$3y^2+5y+9 \equiv 0 \pmod{11}$$

Sol Here $(2\cdot 3, 11) = 1$.

Multiply by $4\cdot 3 = 12$, we get

$$36y^2+60y+108 \equiv 0 \pmod{11}$$

$$\Rightarrow (6y+5)^2 \equiv 5 \pmod{11}$$

put $x \equiv 6y+5 \pmod{11}$ —— ①

we have $x^2 \equiv 5 \pmod{11}$ —— ②

Then $x \equiv \pm 4 \pmod{11}$ are the solutions of ②

putting in ①

$$6y+5 \equiv \pm 4 \pmod{11}$$

or $y \equiv 4, 9 \pmod{11}$

are the solutions of given congruence

Exercise: Solve following congruence

① $7y^2+3y-4 \equiv 0 \pmod{15}$; $y = 2, 4, 7, 14$

② $y^2+3y+11 \equiv 0 \pmod{13}$; $y = 4, 6$

③ $2y^2+4y+9 \equiv 0 \pmod{5}$; $y = 1$

345.

(ii) $49y^2 - 3y + 19 \equiv 0 \pmod{59}$.

Notice that the condition $(a, m) = 1$ is always satisfied if m is an odd prime unless p divides a.

Therefore rule (i) can also be stated as

Rule

" The congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ where $(a, p) = 1$ and p is an odd prime can always be reduced to the form

$$x^2 \equiv d \pmod{p}$$

Now there are only two possibilities

(i) $d \equiv 0 \pmod{p}$

or

(ii) $(d, p) = 1$

If $d \equiv 0 \pmod{p}$; we will deal as before

If $(d, p) = 1$. then add multiple of p in d so that square of an integer occur.

Let $x^2 \equiv x_0^2 \pmod{p}$

Then x_0 is the first solution.

Then 2nd solution will be $p - x_0$.

246

Example Solve

$$x^2 \equiv 5 \pmod{29} \quad \text{——} (1)$$

$$x^2 \equiv 5+29$$
$$\equiv 34 \equiv 63 \equiv 92 \equiv 121 \equiv (11)^2 \pmod{29}$$

Therefor $x \equiv 11 \pmod{29}$ is one Solution

Also $x \equiv 29-11 \pmod{29}$ is 2nd Solution.

Hence $x \equiv 18 \pmod{29}$. is the Solution of (1)

Example (1) Solve $x^2 \equiv 27 \pmod{59}$

Ans $x \equiv 26, 33 \pmod{59}$

(2) Solve $x^2 \equiv 52 \pmod{101}$

Ans $x \equiv 31, 70 \pmod{101}$.

Definition:

Let p be a prime and 'a' be an integer to prime to p. Then a is called a quadratic residue $(\bmod p)$ iff $x^2 \equiv a \pmod{p}$ has a Solution otherwise 'a' is called quadratic non-residue $(\bmod p)$.

Note that $x^2 \equiv 1 \pmod{p}$ is Solvable for all primes p. Thus 1 is a quadratic residue $(\bmod p)$ for all primes.

Examples:

(1) Since $x^2 \equiv 4 \pmod{5}$ has 2 and 3 as Solutions $(\bmod 5)$. Hence 4 is a quadratic

(2) 5 is a quadratic residue of 29 because 29 is prime.

$(5, 29) = 1$ and $(\pm 11)^2 \equiv 5 \pmod{29}$.

(2) $x^2 \equiv 3 \pmod 7$ has no solution.

Hence 3 is a quadratic non-residue of 7.

THEOREM:

Let $a \equiv b \pmod p$. If a is a quadratic residue $\pmod p$, then b is also a quadratic residue $\pmod p$.

PROOF: Let a be a quadratic residue $\pmod p$. Therefore $x^2 \equiv a \pmod p$ is solvable.

But $a \equiv b \pmod p$. Hence $x^2 \equiv b \pmod p$ is also solvable. This implies b is a quadratic residue $\pmod p$.

Remark: We call a and b as the same quadratic residue $\pmod p$ if $a \equiv b \pmod p$.

There two quadratic residue of p are distinct iff they are incongruent $\pmod p$. It follows that all the distinct quadratic residues of p lie in any reduced residue system $R = \{1, 2, \cdots, p-1\}$.

248

THEOREM:
(i) If a is a quadratic residue modulo p, then $x^2 \equiv a \pmod{p}$ has two solutions.
(ii) If a is a quadratic residue $\pmod{p}$ then $a \equiv t^2 \pmod{p}$ for some t, $1 \leq t \leq p-1$
(iii) Any RRS $\pmod{p}$ consists of $\frac{p-1}{2}$ quadratic residues that are in the set $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ and $\frac{p-1}{2}$ quadratic non residues.

PROOF:
(i) Since a is a quadratic residue $\pmod{p}$, $x^2 \equiv a \pmod{p}$ has a solution (say) x_0.
then $x_0^2 \equiv a \pmod{p}$ —— (1)
Consider
$$(p - x_0)^2 \equiv x_0^2 \pmod{p}$$
$$\equiv a \pmod{p}$$
which shows that $p - x_0$ is also a solution of $x^2 \equiv a \pmod{p}$.
Hence $x^2 \equiv a \pmod{p}$ has two solutions.
(ii) If a is a quadratic residue $\pmod{p}$ and x_0 is the solution of the congruence
$$x^2 \equiv a \pmod{p}$$
$$\pmod{p}$$ —— (1)

$\Rightarrow (x_0, p) = 1 \quad \because x_0 < p$

$\Rightarrow x_0 \equiv t \pmod p$ for some t ; $1 \le t \le p-1$.

$\Rightarrow x_0^2 \equiv t^2 \pmod p$

$\Rightarrow a \equiv t^2 \pmod p$ using (i) ; $1 \le t \le p-1$.

(iii) Since p is an odd prime, so $\frac{p-1}{2}, \frac{p+1}{2}$ are both integers.

Moreover
$$\left.\begin{aligned} \frac{p-1}{2} &= p - \frac{p-1}{2} \\ \frac{p+3}{2} &= p - \frac{p-3}{2} \\ &\vdots \text{ and so on.} \end{aligned}\right\} \quad \text{---- (1)}^*$$

Hence any integer a co-prime to p is congruent to $\pm 1, \pm 2, \cdots \pm \frac{p-1}{2} \pmod p$

thus if a is a quadratic residue mod p, then

$a \equiv t^2 \pmod p$ for some t $\quad -\frac{p-1}{2} \le t \le \frac{p-1}{2}$ (using (ii) & (1)*)

implying that the possible quadratic residues $\pmod p$ are amongst $1^2, 2^2, \cdots \left(\frac{p-1}{2}\right)^2$.

Let $r_1, r_2, \cdots, r_{p-1}$ be any RRS $\pmod p$.

If r_i is a quadratic residue $\pmod p$

Then $r_i \equiv j^2 \pmod p$; $1 \le j \le \frac{p-1}{2}$ explained above

250

Hence exactly $\frac{p-1}{2}$ r_i can be quadratic residues and remaining

$p-1 - \frac{p-1}{2} = \frac{p-1}{2}$ are quadratic non-residues.

THEOREM: (Euler's Criterion)

Statement: An integer a is a quadratic residue (mod p) iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

PROOF:

Suppose that a is a quadratic residue (mod p). Then $x^2 \equiv a \pmod{p}$ has a solution (say) x_0

then $x_0^2 \equiv a \pmod{p}$ —— (1)

$\Rightarrow (x_0, p) = 1$ $\because x_0 \in \{1, 2, \ldots, p-1\}$ and p is prime.

Therefore by FLT

$$x_0^{p-1} \equiv 1 \pmod{p} \quad \text{—— (2)}$$

Hence $a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \equiv x_0^{p-1} \pmod{p}$

or $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ using (1)

Conversely, let $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

If r is a primitive root (mod p), then 251.
$1, r, r^2, \cdots, r^{p-2}$ form a reduced residue system (mod p) and $a \equiv r^k \pmod p$ for some integer k; $1 \le k \le p-2$. —(3)

Now $1 \equiv a^{p-2} \equiv (r^k)^{\frac{p-1}{2}}$

$\equiv r^{\frac{k(p-1)}{2}} \pmod p$

But r is a primitive root (mod p)

Hence $\varphi(p) \mid \frac{k(p-1)}{2}$

$\Rightarrow 2 \mid k$ $\because \varphi(p) = p-1$

$\Rightarrow k = 2t$ for some integer t.

(3) becomes

$r^{2t} \equiv a \pmod p$

or $(r^t)^2 \equiv a \pmod p$

$\Rightarrow r^t$ is a solution of $x^2 \equiv a \pmod p$

Hence a is a quadratic residue (mod p).

952

Corollary: Let r be a primitive root $(\bmod p)$, Then r^k is a quadratic residue $(\bmod p)$ iff k is even.

Corollary: An integer a co-prime to p is a quadratic residue or a quadratic non-residue $(\bmod p)$ according as $a^{\frac{p-1}{2}} \equiv 1 (\bmod p)$ or $a^{\frac{p-1}{2}} \equiv -1 (\bmod p)$

Proof: Since $(a, p) = 1$, By FLT

$$a^{p-1} \equiv 1 (\bmod p)$$

$$\Rightarrow a^{p-1} - 1 \equiv 0 (\bmod p)$$

$$\Rightarrow \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 (\bmod p)$$

If a is a quadratic residue $(\bmod p)$ then by Euler's criterion

$$a^{\frac{p-1}{2}} \equiv 1 (\bmod p)$$

and is a quadratic non-residue $(\bmod p)$ if $a^{\frac{p-1}{2}} \equiv -1 (\bmod p)$.

Remark: To find quadratic residue (mod p), we should find the integers $1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2 \pmod p$.

Example: Find quadratic residue (mod 17).

Sol: All quadratic residue (mod p) are integers $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2 \pmod{17}$ that is $1, 4, 9, 16, 8, 2, 15, 13 \pmod{17}$.

Legendre Symbol:

Def: Let p be an odd prime and a any integer. The Legendre Symbol $\left(\frac{a}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue (mod } p) \\ 0 & \text{if } p \text{ divides } a \\ -1 & \text{if } a \text{ is quadratic non-residue (mod } p) \end{cases}$$

Examples ① Since $x^2 \equiv 2 \pmod{17}$ has a Solution so 2 is a quadratic residue (mod p=17). Hence $\left(\frac{2}{17}\right) = 1$

② Since $x^2 \equiv 3 \pmod{13}$ has a Solution. Hence $\left(\frac{3}{13}\right) = 1$

③ $x^2 \equiv 2 \pmod{13}$ has no Solution, Hence $\left(\frac{2}{13}\right) = -1$

95

Remark: ① $\left(\frac{a}{p}\right)$ is not a fraction within parenthesis. It says number of solutions of $x^2 \equiv a \pmod p$ is $1+\left(\frac{a}{p}\right)$.

If a is a quadratic residue mod p, then $1+\left(\frac{a}{p}\right) = 1+1 = 2$, solutions.

If a is a quadratic non-residue $\pmod p$, then $1+\left(\frac{a}{p}\right) = 1+(-1) = 0$, solution.

② Euler's theorem can be stated as "If p is an odd prime and a an integer co-prime to p, then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$"

THEOREM:
Let p be an odd prime and a, b any integers co-prime to p, then the following hold.

(i) If $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(iii) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

Proof: Since $a \equiv b \pmod p$, then $x^2 \equiv a \pmod p$ and $x^2 \equiv b \pmod p$ simultaneously have

955.

If $x^2 \equiv a \pmod{p}$ has a solution
then $x^2 \equiv b \pmod{p}$ has a solution
then a and b both are quadratic
residues $\pmod{p}$.
therefore $\left(\frac{a}{p}\right) = 1 = \left(\frac{b}{p}\right)$

$$\Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

If $x^2 \equiv a \pmod{p}$ has no solution,
then $x^2 \equiv b \pmod{p}$ has no so

$$\left(\frac{a}{p}\right) = -1 = \left(\frac{b}{p}\right)$$

$$\Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

(ii) Since $(a, p) = 1$ & $(b, p) = 1$
then by Euler's criterion

$$\left.\begin{aligned} a^{\frac{p-1}{2}} &\equiv \left(\frac{a}{p}\right) \pmod{p} \\ \text{&} \quad b^{\frac{p-1}{2}} &\equiv \left(\frac{b}{p}\right) \pmod{p} \end{aligned}\right\} \text{---- (1)}$$

256

Consider

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod{p}$$

$$\equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod{p}$$

$$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p} \quad \text{using (1)}$$

Since $\left(\frac{ab}{p}\right)$ & $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ both are less than p.

Hence $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(iii) Consider

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)^2$$

But $\left(\frac{b}{p}\right) = +1$ or -1

Thus $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

Generalized form of (ii)

Let $(a_i, p) = 1 \quad \forall\, i = 1, 2, \ldots n.$

Then $\left(\frac{a_1 a_2 \cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$

Proof follows.

256(1)

Corollary: If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Proof: By Euler's criterion

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$$

put $a = -1$

then $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$

$$\Rightarrow \left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \quad \text{---(1)}$$

: both sides give -1 or 1.

If $p \equiv 1 \pmod 4 \Rightarrow \frac{p-1}{2} = 2t$, (1) becomes $t \in \mathbb{Z}$.

$$\left(\frac{-1}{p}\right) \equiv (-1)^{2t} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \end{cases}$$

If $p \equiv 3 \pmod 4 \Rightarrow \frac{p-1}{2} = 1 + 2t_1 \; ; t_1 \in \mathbb{Z}$

then (1) becomes

$$\left(\frac{-1}{p}\right) \equiv (-1)^{2t_1+1} = -1 \quad \text{if } p \equiv 3 \pmod 4$$

Hence

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

THEOREM: There are infinitely many primes of the form $4K+1$. §56(2)

Example: $x^2 \equiv -a^2 \pmod{P}$ has a solution iff $P \equiv 1 \pmod 4$.

Sol Consider

$$\left(\frac{-a^2}{P}\right) = \left(\frac{-1}{P}\right)\left(\frac{a}{P}\right)^2$$

$$= \left(\frac{-1}{P}\right)$$

$$= (-1)^{\frac{P-1}{2}}$$

Thus $\left(\frac{-a^2}{P}\right) = (-1)^{\frac{P-1}{2}} = 1$ iff $P = 4K+1$

Result follows by Euler's criterion.

Example

$$\left(\frac{-168}{11}\right) = \left(\frac{-2^3 \cdot 3 \cdot 7}{11}\right)$$

$$= \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right)^3\left(\frac{3}{11}\right)\left(\frac{7}{11}\right)$$

$$= (-1)(-1)^3(1)(-1)$$

$$= -1.$$

THEOREM: ① The product of two quadratic residue mod p is a quadratic residue mod p.

PROOF: let a_1 and a_2 be two quadratic residues mod p. Then by Euler's criterion

$$a_1^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

& $$a_2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Consider

$$(a_1 a_2)^{\frac{p-1}{2}} \equiv a_1^{\frac{p-1}{2}} \cdot a_2^{\frac{p-1}{2}}$$

$$\equiv 1 \pmod{p}$$

iff $a_1 a_2$ is a quadratic residue mod p.

② The product of two quadratic non-residue mod p is a quadratic residue mod p.

③ The product of a quadratic residue and quadratic non-residue mod p is a quadratic non-residue (mod p).

Least Residue of an Integer:

Def: let m and n be any two integers. Then least residue of n modulo m denoted by $\angle R_m(n)$ is an integer x such that

$$-\frac{m}{2} < x \leq \frac{m}{2} \quad \text{and} \quad n \equiv x \pmod{m}$$

Gauss Lemma:

Statement: Let p be an odd prime and a an integer co-prime to p. If m denote the number of integers that leave negative least residue in the set $\{a, 2a, 3a, \cdots \frac{p-1}{2}a\}$, then $\left(\frac{a}{p}\right) = (-1)^m$ —— (1)

PROOF: Since $(a,p)=1$, therefore each integer in (1) is co-prime to p and no two are congruent to each other (mod p). Also for each

j: $\quad 1 \le j \le \frac{p-1}{2}$

$$ja \equiv LR_p(ja) \pmod p$$
$$\equiv \operatorname{Sgn}(LR_p(ja)) \cdot |LR_p(ja)| \pmod p \quad \because x = \operatorname{sgn}(x)\cdot|x|$$

Also $|LR_p(ja)| \equiv k \pmod p$ for some $1 \le k \le \frac{p-1}{2}$ —— (2)

Hence, we have

$$a \cdot 2a \cdots \tfrac{p-1}{2}a \equiv \operatorname{Sgn}(LR_p(a)) \cdot |LR_p(a)| \cdot \operatorname{Sgn}(LR_p(2a))|LR_p(2a)|$$
$$\cdots \operatorname{Sgn}\left(LR_p\left(\tfrac{p-1}{2}a\right)\right)\left|LR_p\left(\tfrac{p-1}{2}a\right)\right| \pmod p$$

$$a^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}\right)! \equiv (-1)^m \left(\tfrac{p-1}{2}\right)! \pmod p$$

where m is the number of negative least residues in (1)

But $\left(p, \left(\frac{p-1}{2}\right)!\right) = 1$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv (-1)^m \pmod p \quad —— (3)$$

958

Example: ① Let $m = 17$, $n = 31$

Then $-\frac{17}{2} < x \leq \frac{17}{2}$ imply

$-8.5 < x \leq 8.5$

Also $31 \equiv -3 \pmod{17}$

Hence $LR_{17}(13) = -3$

② $LR_6(15) = 3$

Definition: (Signum)

Let x be a real number. Then Signum of x is denoted by $Sgn(x)$ and is defined as

$$Sgn(x) = \begin{cases} 1 & x > 0 \\ 0 & x = 0 \\ -1 & x < 0 \end{cases}$$

Remark $x = Sgn(x) \cdot |x|$

e.g. $-2 = Sgn(-2) \cdot |-2|$

$= (-1)\, 2 \quad \because -2 < 0$

$= -2.$

H.M. KHALID MAHMOOD

By Euler's criterion 260

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$, (3) becomes

$$\left(\frac{a}{p}\right) \equiv (-1)^{m} \pmod{p}$$

Since both sides take values -1 or 1

Hence $\left(\frac{a}{p}\right) = (-1)^{m}$.

Example: $\{a, 2a, \cdots \frac{p-1}{2}a\} = \{3, 6, 9, \cdots 33\}$

Let $a = 3$, $P = 23$

$$-\frac{23}{2} < x < \frac{23}{2} = \{-11, -10, \cdots, 11\}$$

Here we will find $LR_{23}(3)$

$LR_{23}(3) = 3$

$LR_{23}(6) = 6$

$LR_{23}(9) = 9$

$LR_{23}(12) = -11$

$\because 12 \equiv -11 \pmod{23}$

$LR_{23}(15) = -8$

$LR_{23}(18) = -5$

$LR_{23}(21) = -2$

$LR_{23}(24) = 1$

$LR_{23}(27) = 4$

$LR_{23}(30) = 7$

$LR_{23}(33) = 10$

Hence $\left(\frac{3}{23}\right) = (-1)^{4}$

$= 1$

261

THEOREM: Let p be an odd prime, then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Consequently

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

PROOF:

By Gauss lemma

$$\left(\frac{2}{p}\right) = (-1)^m$$

where m is the number of integers having negative least residue (mod p) in the set

$$\left\{1\cdot 2, 2\cdot 2, \cdots, \frac{p-1}{2}\cdot 2\right\}$$

$-\frac{p}{2} < x \le \frac{p}{2}$

$x \equiv j \pmod p$

Now $2j < \frac{p}{2}$ imply $j < \frac{p}{4}$: $1 \le j \le \frac{p-1}{2}$

Thus $m = \frac{p-1}{2} - \left[\frac{p}{4}\right]$

Since p is prime, so it is of the form

$$8K+1,\ 8K+3,\ 8K+5,\ 8K+7.$$

If $p = 8K+1$, then $m = \left[\frac{8K+1-1}{2} - \frac{2K+1}{4}\right] = 2K$

Similarly $p = 8K+3$, $m = 2K+1$

$p = 8K+5$, $m = 2K+1$, $p = 8K+7 \Rightarrow m = 2K+2$.

Which clearly shows that

$$\left(\frac{2}{p}\right) = (-1)^m \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases} \quad \text{---------- (1)}$$

Consider 262

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} (-1)^{\frac{(8k+1)^2-1}{8}} & \text{if } p = 8k+1 \\ (-1)^{\frac{(8k+3)^2-1}{8}} & \text{if } p = 8k+3 \\ (-1)^{\frac{(8k+5)^2-1}{8}} & \text{if } p = 8k+5 \\ (-1)^{\frac{(8k+7)^2-1}{8}} & \text{if } p = 8k+7 \end{cases}$$

$$= \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

$= \left(\frac{2}{p}\right)$ wins eq (1)

Hence $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Give ALITER:

(Gauss's Lemma)

Let $(a, p) = 1$ and m be the number of integers in $a, 2a, \ldots, \frac{p-1}{2}a$ whose least residue (mod p) are greater than $p/2$

Then $$\left(\frac{a}{p}\right) = (-1)^m$$

Consider

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} (-1)^{\frac{(8k+1)^2-1}{8}} & \text{if } p = 8k+1 \\ (-1)^{\frac{(8k+3)^2-1}{8}} & \text{if } p = 8k+3 \\ (-1)^{\frac{(8k+5)^2-1}{8}} & \text{if } p = 8k+5 \\ (-1)^{\frac{(8k+7)^2-1}{8}} & \text{if } p = 8k+7 \end{cases}$$

$$= \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

$$= \left(\frac{2}{p}\right) \quad \text{by eq (1)}$$

Hence

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Give ALITER:

(Gauss's Lemma)

Let $(a, p) = 1$ and m be the number of integers in $a, 2a, \ldots, \frac{p-1}{2}a$ whose least residue (mod p) are greater than $p/2$

Then $\left(\frac{a}{p}\right) = (-1)^m$

26

THEOREM 1:

$$\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}$$

Proof: By Gauss's Lemma

$$\left(\frac{2}{p}\right) = (-1)^m \quad \text{---------- (1)}$$

where m is the number of integers in

$1\cdot 2, 2\cdot 2, \cdots, \frac{p-1}{2}\cdot 2$ ---------- (2) which are $> \frac{p}{2}$.

There are thus exactly $\frac{p-1}{2} - m$ integers in (2)

which are $< p/2$

Then $\left(\frac{p-1}{2} - u\right)\cdot 2 < \frac{p}{2} < \left(\frac{p-1}{2} - u + 1\right)\cdot 2$

$$\Rightarrow \quad \frac{p-1}{2} < 2m < \frac{p+2}{2}$$

$$\Rightarrow \quad \frac{p+2}{4} - 1 < m < \frac{p+2}{4}$$

It follows that $m = \left[\frac{p+2}{4}\right]$

But p is odd prime

Hence $\left[\frac{p+2}{4}\right] = \left[\frac{p+1}{4}\right]$.

Hence (1) becomes

$$\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}.$$

$\left(\frac{2}{23}\right) = (-1)^{\left[\frac{23+1}{4}\right]} = (-1)^{\left[\frac{24}{4}\right]} = (-1)^6 = 1$

$\left(\frac{2}{47}\right) = (-1)^{\left[\frac{47+1}{4}\right]} = (-1)^{12} = 1$

THEOREM: 264

Let p be an odd prime, then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Proof:

We know

$$\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}$$

If $p \equiv \pm 1 \pmod 8 \Rightarrow p = 8K \pm 1$ put in (i)

$$\left(\frac{2}{p}\right) = (-1)^{\left[\frac{8K\pm1+1}{4}\right]}$$

$$= (-1)^{2K}$$

$$= 1$$

If $p \equiv \pm 3 \pmod 8 \Rightarrow p = 8K \pm 3$

Then $\left(\frac{2}{p}\right) = (-1)^{\left[\frac{8K\pm3+1}{4}\right]}$

$$= (-1)^{2K\pm1}$$ using def of [ ] function

$$= -1$$

Which complete the theorem

965

THEOREM:

Let p and q be any odd primes.

(i) If one of p and q is of the form $4K+1$, Then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

(ii) If both p & q are of the form $4K+3$ Then $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$

Proof: Consider

(i) $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)\cdot\left(\frac{p}{q}\right)$

$= \left(\frac{q}{p}\right)\left(\frac{p^2}{q}\right)$

$= \left(\frac{q}{p}\right)$

$\Rightarrow \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ As $p = 4K+1$ & q is odd both $\frac{p-1}{2}$ & $\frac{q-1}{2}$ are even.

(ii) Since $p = 4K+3$ & $q = 4K+3$ types

So $\frac{p-1}{2}\cdot\frac{q-1}{2}$ is odd.

Then $(-1)^{\frac{p-1}{2}\cdot\left(\frac{q-1}{2}\right)}\left(\frac{p}{q}\right) = +\left(\frac{q}{p}\right)$

$\Rightarrow \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$

246.

Exp Evaluate

$$\left(\frac{59}{131}\right)$$

Since $59 \equiv 3 \pmod 4$ &
$131 \equiv 3 \pmod 4$

Therefore $\left(\frac{59}{131}\right) = -\left(\frac{131}{59}\right)$

$= -\left(\frac{13}{59}\right)$

$= -\left(\frac{59}{13}\right)$ $\because 13 \equiv 1 \pmod 4$

$= -\left(\frac{7}{13}\right)$

$= -\left(\frac{13}{7}\right)$

$= -\left(\frac{-1}{7}\right)$

$= -(-1)$

$= \underline{1}$

THEOREM

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p = 8K+1 \text{ or } p = 8K+3 \\ -1 & \text{if } p = 8K+5 \text{ or } p = 8K+7 \end{cases}$$

267

Proof: We know

$$\left(\frac{-2}{p}\right) = \left(\frac{-1 \cdot 2}{p}\right)$$

$$= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$$

Then $\left(\frac{-2}{p}\right) = (1)(1) = 1$ if $p = 8K+1$

$= (-1)(-1) = 1$ if $p = 8K+3$

$= (1)(-1) = -1$ if $p = 8K+5$

$= (-1)(1) = -1$ if $p = 8K+7$

$$= \begin{cases} 1 & \text{if } p = 8K+1 \text{ or } 8K+3 \\ -1 & \text{if } p = 8K+5 \text{ or } 8K+7. \end{cases}$$

Lemma: Let p and q be distinct odd primes, then $\left(\frac{p}{q}\right) = (-1)^{\sum_{K=1}^{\frac{q-1}{2}} \left[\frac{Kp}{q}\right]}$

(where $\left[\frac{Kp}{q}\right]$ denotes the greatest integer. In other words, the number of integers leaving negative least residue in the set $\left\{p, 2p, \ldots, \frac{q-1}{2}p\right\}$ is congruent to $\sum_{K=1}^{\frac{q-1}{2}} \left[\frac{Kp}{q}\right]$ modulo 2

PROOF: By division algorithm 268.

$$p = q\left[\frac{p}{q}\right] + r_1 \quad ; \quad 0 \le r_1 < q$$

$$2p = q \cdot \left[\frac{2p}{q}\right] + r_2 \quad ; \quad 0 \le r_2 < q$$

$$\vdots$$

$$\frac{q-1}{2} p = q \cdot \left[\frac{\frac{q-1}{2} p}{q}\right] + r_{\frac{q-1}{2}} \quad ; \quad 0 \le r_{\frac{q-1}{2}} < q$$

Adding above all equations

$$\sum_{K=1}^{\frac{q-1}{2}} Kp = q \cdot \sum_{K=1}^{\frac{q-1}{2}} \left[\frac{Kp}{q}\right] + \sum_{K=1}^{\frac{q-1}{2}} r_K$$

$$\Rightarrow p \cdot \frac{q^2-1}{8} = q \cdot \sum_{K=1}^{\frac{q-1}{2}} \left[\frac{Kp}{q}\right] + \sum_{K=1}^{\frac{q-1}{2}} r_K \qquad \text{——— (1)}$$

Let's assume that the integers $r_1, r_2, r_3, \ldots, r_t$ amongst $r_1, r_2, \ldots, r_{\frac{q-1}{2}}$ leave negative least residues (mod q).

then $q - r_1, q - r_2, \ldots, q - r_t, r_{t+1}, \ldots, r_{\frac{q-1}{2}}$

are a rearrangement of integers $1, 2, \ldots, \frac{q-1}{2}$

therefore

$$q - r_1 + q - r_2 + \cdots + q - r_t + r_{t+1} + \cdots + r_{\frac{q-1}{2}} = 1 + 2 + \cdots + \frac{q-1}{2}$$

$$\Rightarrow \left(q + \sum_{i=1}^{\frac{q-1}{2}} r_i - 2\sum_{i=1}^{t} r_i = \frac{q^2-1}{8}\right) \quad 269$$

$$\Rightarrow \sum_{i=1}^{\frac{q-1}{2}} r_i = 2\sum_{i=1}^{t} r_i + \frac{q^2-1}{8} - qt \quad \text{---(2)}$$

From (1) & (2)

$$P\cdot\frac{q^2-1}{8} = q\sum_{K=1}^{\frac{q-1}{2}}\left[\frac{Kp}{q}\right] + 2\sum_{i=1}^{t} r_i + \frac{q^2-1}{8} - qt$$

$$\Rightarrow (P-1)\left(\frac{q^2-1}{8}\right) = q\sum_{K=1}^{\frac{q-1}{2}}\left[\frac{Kp}{q}\right] + 2\sum_{i=1}^{t} r_i - qt$$

Since p & q are both distinct odd integers therefore $(p-1)\left(\frac{q^2-1}{8}\right)$ is an even integer.

Therefore

$$q\sum_{K=1}^{\frac{q-1}{2}}\left[\frac{Kp}{q}\right] - qt \equiv 0 \pmod 2$$

$$\Rightarrow \sum_{K=1}^{\frac{q-1}{2}}\left[\frac{Kp}{q}\right] \equiv t \pmod 2 \quad \because (q,2)=1. \quad \text{---(3)}$$

By Gauss Lemma $\sum_{K=1}^{\frac{q-1}{2}}\left[\frac{Kp}{q}\right] - 2s$ is $\in Z$

$$\left(\frac{p}{q}\right) = (-1)^{t} = (-1)^{\sum_{K=1}^{\frac{q-1}{2}}\left[\frac{Kp}{q}\right]}$$

using (3)

$$\Rightarrow \left(\frac{p}{q}\right) = (-1)^{a}$$

$a = t \pmod 2$
$a = t + 2s$
$t = a - 2s.$

PROOF: (Quadratic Reciprocity Law) 270.

Let t_1, t_2 denote the number of integers that leave negative least residues (mod q) and (mod p) respectively in the sets $\{p, 2p, \dots, \frac{q-1}{2}\cdot p\}$ and $\{q, 2q, \dots, \frac{p-1}{2}\cdot q\}$.

By Gauss lemma

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{t_1}\cdot(-1)^{t_2}$$

$$= (-1)^{t_1+t_2} \quad \text{——} (1)$$

But $t_1 = \sum_{K=1}^{\frac{q-1}{2}} \left[K\frac{p}{q}\right]$ & $t_2 = \sum_{K=1}^{\frac{p-1}{2}} \left[K\frac{q}{p}\right]$ ∵ p & q distinct odd primes.

(1) becomes $\sum_{K=1}^{\frac{q-1}{2}} \left[K\frac{p}{q}\right] + \sum_{K=1}^{\frac{p-1}{2}} \left[K\frac{q}{p}\right]$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1) \quad \text{——} (2)$$

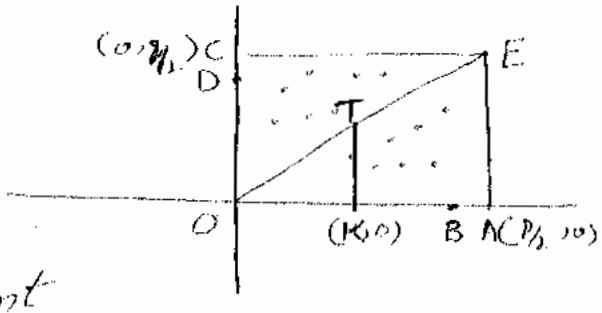
To complete theorem we must show

$$\sum_{K=1}^{\frac{q-1}{2}} \left[K\frac{p}{q}\right] + \sum_{K=1}^{\frac{p-1}{2}} \left[K\frac{q}{p}\right] = \frac{p-1}{2}\cdot\frac{q-1}{2}.$$

Taking rectangular coordinate axis and a convenient unit, mark off units from O along the x-axis to represent the

integers $1, 2, \cdots, \frac{p-1}{2}$ and in like manner 371

along the y-axis to represent $1, 2, \cdots \frac{q-1}{2}$.



then $OB = \frac{p-1}{2}$

$OD = \frac{q-1}{2}$

Let $OA = \frac{p}{2}$ & $OC = \frac{q}{2}$

We count lattice point with in rectangle OAEC and not on Boundry (clearly these are $\frac{p-1}{2} \cdot \frac{q-1}{2}$ —— (1)*

because a lattice point (m, n) within rectangle must satisfy $1 \le m \le \frac{p-1}{2}$ & $1 \le n \le \frac{q-1}{2}$.

Notice that no lattice point lie on diagonal OE. because;

Equation of diagonal $y = \frac{q}{p} x$; $m = \frac{q/2}{p/2}$

$m = q/p$

If (m, n) lie on diagonal, then

$$n = \frac{q}{p} m$$

$$\Rightarrow pn = qm$$

$$\Rightarrow p \mid qm$$

$$\Rightarrow p \mid m \quad \because (p, q) = 1$$

But $m < \frac{p-1}{2}$, so $p \mid m$ is not possible.

272

To count the lattice point in another way within the rectangle not on the boundary. Count these in OAE and in OEC.

The equation of diagonal $y = \frac{q}{p}x$ intersect $x = K$ say at T.

Then $T = (K, K\frac{q}{p})$

Therefore if K is positive integer, then $[K\frac{q}{p}]$ is the number of lattice point on $x = K$, above the x-axis and below of.

Hence number of lattice point in OAE and not on the boundary is $\sum_{K=1}^{\frac{p-1}{2}} [K\frac{q}{p}]$

Similarly for OCE, number of lattice points are $\sum_{K=1}^{\frac{q-1}{2}} [K\frac{p}{q}]$

Total lattice points $= \sum_{K=1}^{\frac{p-1}{2}} [K\frac{q}{p}] + \sum_{K=1}^{\frac{q-1}{2}} [K\frac{p}{q}]$ —— (2)*

(1)* × (2)* Since

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{K=1}^{\frac{p-1}{2}} [K\frac{q}{p}] + \sum_{K=1}^{\frac{q-1}{2}} [K\frac{p}{q}]$$

Which complete the proof.

273

THEOREM:

If p is an odd prime and $(a, p) = 1$ then $x^2 \equiv a \pmod{p^k}$, $k \geq 1$ has a solution iff $\left(\frac{a}{p}\right) = 1$

PROOF: Suppose $x^2 \equiv a \pmod{p^k}$ has a solution x_0.

Then $x_0^2 \equiv a \pmod{p^k}$

$\Rightarrow p^k \mid x_0^2 - a$

$\Rightarrow p \mid x_0^2 - a$

$\Rightarrow x_0^2 \equiv a \pmod{p}$

Thus x_0 is a solution of $x^2 \equiv a \pmod{p}$

by Euler's criterion $\left(\frac{a}{p}\right) = 1$

Conversely, Suppose $\left(\frac{a}{p}\right) = 1$, then $x^2 \equiv a \pmod{p}$ has a solution.

We will shows that $x^2 \equiv a \pmod{p^k}$ has a solution.

clearly for $k = 1$, Statement is true.

Assume $x^2 \equiv a \pmod{p^k}$, $k \geq 1$ has a solution. Say x_0.

274.

clearly $(x_0, p) = 1$, thus the linear congruence

$x_0 y \equiv 1 \pmod{p}$ has a unique solution (say) y_0. Therefore

$x_0 y_0 = 1 + sp$ — (1) for some integer s.

Define

$$x_1 = x_0 - t \cdot y_0 \cdot p^k \cdot \left(\frac{p+1}{2}\right)$$

then

$$x_1^2 = x_0^2 - t \cdot y_0 \cdot x_0 \cdot p^k (p+1) + t^2 y_0^2 p^{2k} \left(\frac{p+1}{2}\right)^2$$

$$x_1^2 = a + t p^k - t p^k (p+1)(1+sp) + t^2 y_0^2 p^{2k} \left(\frac{p+1}{2}\right)^2$$

using (1)

$$= a + t p^k - t p^k + p^{k+1} \cdot \text{some integer}$$

$$\equiv a \pmod{p^{k+1}}$$

Hence x_1 is a solution of

$$x^2 \equiv a \pmod{p^{k+1}}$$

thus by induction, we have the theorem.

Example: Solve the congruence $x^2 \equiv 91 \pmod{3^2}$

Sol $\left(\frac{91}{3}\right) = \left(\frac{1}{3}\right) = 1$. Then $x^2 \equiv 91 \pmod{3^2}$ does have a solution.

275

Since any Solution of $x^2 \equiv 91 \pmod{3^2}$ is also a Solution of $x^2 \equiv 91 \pmod 3$.
So we first Solve $x^2 \equiv 91 \pmod 3$

$\Rightarrow x^2 \equiv 1 \pmod 3$

clearly $x_0 = 1$ (also 2) is its Solution.

Then $x_0 y \equiv 1 \pmod 3$ —— (1)

$\Rightarrow y \equiv 1 \pmod 3$ is a Solution of (1)

$\Rightarrow y_0 = 1$, then $x_0^2 = a + tp^k = 91 + 3(-30) = 1$

Then $x_1 = x_0 - t \cdot y_0 \cdot p^k \left(\frac{p+1}{2}\right)$ $\boxed{t = -30}$

$x_1 = 1 - (-30)(1)\cdot(3)\left(\frac{3+1}{2}\right)$

$\boxed{x_1 = 181}$ is a Solution of $x^2 \equiv 91 \pmod{3^2}$

To find Solution of $x^2 \equiv 91 \pmod{3^3}$

Repeat above process.

First Solve $x_1 y \equiv 1 \pmod 3$

$181\, y \equiv 1 \pmod 3$ —— (2)

$\Rightarrow y \equiv 1 \pmod 3$ is a Solution of (2)

let $\boxed{y_1 = 1}$

Now $x_1^2 = (181)^2 = a + t \cdot p^k = 91 + 3^2(3630)$

Here $\boxed{t = 3630}$

Then $x_2 = 181 - (3630)(1)(3^2)\left(\frac{3+1}{2}\right) = -65759$

which is required Solution.