Number Theory

Date. No.

Unit 1 : Divisibility Theory in the Integers

Division Algorithm

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

~~Divi~~ Division Algorithm Theorem

Let 'a' be any integer and 'b' be a positive Integer. Then there exist a unique quotient 'q' and a remainder 'r' such that $a = bq + r$ where $0 \leq r < b$.

Proof: The proof of this theorem consists of two parts. First we establish the existence of such integers 'q' and 'r' and then we show they are unique;

Proof of existence

Let us define a set $S = \{a - bn : n \in \mathbb{Z} \text{ and } a - bn \geq 0\}$

We first show that S is non empty as

Case 1: Suppose $a \geq 0$ then $a = a - b.0 \in S$

$\Rightarrow a \in S$

So, S contains an element.

Case II: If $a < 0$ then since $b \in \mathbb{Z}^+$. So

$$b \geq 1$$

Then $$-ba > -a$$

$$\Rightarrow a - ba > 0$$

$$\Rightarrow a - ba \in S$$

In both cases, S contains atleast one element. So 'S' is non-empty.

Then by well ordering principle, S contains a least element 'r' i.e. $r \in S$ then by defining the nature of S, there exist an integer 'q' such that $r = a - bq$ where $r \geq 0$

To show $r < b$

We prove this by method of contradiction

Let us assume that

$$r \geq b$$

$$\Rightarrow r - b \geq 0$$

Now; $r - b = a - bq - b$

$$= a - b(q+1)$$

$$r - b = a - (q+1)b$$

which is of the form $a - b \cdot n$ and ~~and~~ is greater than or equal to 0. because $r - b \geq 0$

So; $a - b(q+1) \in S \Rightarrow r - b \in S$

Since; $b > 0$; so $r - b < r$

i.e. $r - b$ is smaller than r and is in S.

This contradicts the assumption that 'r' is the least element in S.

So; $r < b$

Hence there exists 'q' and 'r' such that

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

Uniqueness proof

If possible assume that there are integers q, q', r and r' such that;

$$a = bq + r$$
$$a = bq' + r'$$

where;
$$0 \leq r < b$$
$$0 \leq r' < b$$

Assume $q \geq q'$;

Then; $r' - r = a - bq' - (a - bq)$
$$= bq - bq'$$
$$= b(q - q') \geq 0$$

i.e. $r' - r \geq 0$

As $r' < b$ and $r < b$ then $r - r' < b$

Now if we assume $q > q'$ then $q - q' > 1$
$$\Rightarrow b(q - q') > b$$
$$\Rightarrow r' - r > b$$

which contradicts $r' - r < b$

Therefore 'q' can not be greater than q'. Hence $q = q'$.

Consequently $r' - r = 0 \Rightarrow r = r'$
Thus integers q and r are unique.
This completes the proof of the theorem.

Q. ① Prove that if a and b are integers with $b > 0$, then there exists unique integers q and r satisfying $a = qb + r$ where $2b \leq r < 3b$.

$\Rightarrow$ we have; $a = qb + r$

To show uniqueness;

$$a = q'b + r' = qb + r$$

$$\Rightarrow (q' - q)b + (r' - r) = 0$$

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

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

As $2b \leq r < 3b$

$$\Rightarrow 2b \leq (r' - r) < 3b$$

$$2b \leq (q - q')b < 3b$$

$$2 \leq (q - q') < 3$$

This will be possible only if $q = q'$

if $q = q'$; $(q - q')\,b = (r' - r)$

$0 = r' - r$

$\Rightarrow \boxed{r' = r}$

This shows there exists unique integers.

Q 2. Prove that if a positive integer is of the form $6q + 5$, then it is also of the form $3q + 2$ for some integer q; but not Conversely.

$\Rightarrow$ Let $n = 6q + 5$; $q \rightarrow$ +ve integer

We know that any positive integer of form $3k$, $3k+1$, $3k+2$

$q = 3k$ or $3k+1$ or $3k+2$

If $q = 3k$;

$n = 6q + 5$

$n = 6 \cdot 3k + 5$

$n = 18k + 5$

$= 18k + 3 + 2$

$n = 3(6k+1) + 2$

$n = 3m + 2$ $\quad m = 6k + 1$ someinteger.

Now; $q = 3k + 1$

$n = 6q + 5$

$n = 6(3k+1) + 5$

Date No.

$n = 18k + 11$

$n = 3(6k+3) + 2$

$n = 3m + 2$ where; $m = 6k+3$ integer.

Now;

$q = 3k + 2$

$n = 6q + 5$

$n = 6(3k+2) + 5$

$n = 18k + 17$

$n = 18k + 12 + 5$

$n = 18k + 15 + 2$

$n = 3(6k+5) + 2$

$m = 6k+5$

$n = 3m + 2$

Hence if positive integer of the ferm $6q+5$, it is the ferm of $3q+2$ for some integer(q).

Conversly; Let $n = 3q + 2$

we know that +ve integer is of form

$6k+1$, $6k+2$, $6k+3$, $6k+4$ or $6k+5$

$n = 3q + 2$

$n = 3(6k+1) + 2$; $m = 3k$

$n = 18k + 5$

$n = 6.(3k) + 5 = 6m+5$

Now $q = 6k+2$

$n = 3q + 2$

$n = 3(6k+2) + 2$

$n = 18k + 8$

$n = 18k + 6 + 2$

$n = 6(3k+1) + 2$

$n = 6m + 2$ where $m = 3k+1$

Now this is not of the ferm $6m+5$
Hence if n is of the ferm $3q+2$, then it would not of the ferm $6q+5$ always.

Alternative

Q.1. By division algorithm $\exists$ unique q' and r' s.t

$a = q'b + r'$, $0 \leq r' < b$

$\therefore$ $a = q'b + r' + 2b - 2b$

$a = (q'-2)b + r' + 2b$

Let $q = q' - 2$ & $r = r' + 2b$

Since; $0 \leq r' < b$

$2b \leq r' + 2b \leq 3b$

$2b \leq r < 3b$.

Q.2. $a = 6k+5 = 6$ ~~$6(k+2)$~~ $3 \cdot 2k + 3 + 2 = 3(2k+1) + 2$

$= 3j + 2$

where $j = 2k+1$

Conversly $a = 3j + 2$

(5) Use the division algorithm to establish the following

(a) the square of any integer is either of the form $3k$ or $3k+1$

$\Rightarrow$ sol^n: If a be any integer then

$a^2 = 3k$ or $3k+1$

By division algorithm $\exists$ a 'q' such that $a = bq + r$ $r = 0, 1, 2$

$a = 3q$ or $3q+1$ or $3q+2$

if $a = 3q$; $\therefore a^2 = 9q^2 = 3(3q^2)$

$a^2 = 3k$ where $k = 3q^2$

if $a = 3q+1$; $a^2 = 9q^2 + 6q + 1$

$a^2 = 3(3q^2 + 2) + 1$

$a^2 = 3k + 1$ let $k = 3q^2 + 2$

If $a = 3q+2$; $a^2 = 9q^2 + 12q + 4$

$a^2 = 3(3q^2 + 2q + 1) + 1$

$a^2 = 3k + 1$ where $k = 3q^2 + 2q + 1$

(b) The cube of any integer has the forms $9k$, $9k+1$, or $9k+8$

$\Rightarrow$ Let $a = 3q+r$; $r = 0, 1, 2$

if $a = 3q$; $a^3 = (3q)^3 = 27q^3 = 9(3q^3)$

$= 9k$

(c) The fourth power of any integer is of the form $5k$ or $5k+1$

$\Rightarrow$ Let $a = 5q+r$; $0 \le r < 5$

$r = 0$;

$a^4 = (5q)^4 =$

$r = 1$;

$a^4 = (5q+4)^4$

(1) Prove that $3a^2-1$ is never a perfect square.

$\Rightarrow$ If possible let us suppose $3a^2-1$ is perfect square.

$$3a^2-1 = n^2$$

As the square of any integer is of the form $(3k+1)$ or $3k$

$$3a^2-1 = 3k+1$$

$$3(a^2-k) = 2$$

or $\quad 3a^2-1 = 3k$

$$3(a^2-k) = 1$$

$$\Rightarrow \quad 3(a^2-k) = 2 \quad \text{or} \quad 3(a^2-k) = 1$$

each impossible since by div algorithm.

$$2 = 3.0 + 2$$

$$1 = 3.0 + 1$$

This is contradiction so $(3a^2-1)$ is not perfect square.

(5) For $n \geq 1$ prove that $\dfrac{n(n+1)(2n+1)}{6}$ is an integer.

$\Rightarrow$ By divisibility theorem; n has following values $6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5$

for $n = 6k$;

$$\frac{n(n+1)(2n+1)}{6}$$

$$= \frac{6k \cdot (6k+1)(2 \cdot 6k+1)}{6}$$

$$= k \cdot (6k+1)(12k+1)$$

which is integer

for $n = 6k+1$. - - - -

(6) Show that the cube of any no. is of the form $7k$ or $7k \pm 1$

$\Rightarrow$ Let $A = 7q + r$; $0 \leq r < 7$

$r = 0$; $A^3 = (7q)^3 = 7(49q^3)$

$= 7k$; $k = 49q^3$

$r = 1$; $A^3 = (7q+1)^3 = 7(7^2q^3 + 3.7q^2 + 3q) + 1$

$= 7k + 1$

where;

$k = 7^2q^3 + 3.7q^2 + 3q$.

Upto $r = 6$

(7) obtain the following version of division algorithm:

For integers a & b with $b \neq 0$ there exist unique integers q & r that satisfy $a = bq + r$ where;

$$-\frac{1}{2}|b| \leq r \leq \frac{1}{2}|b|$$

$\Rightarrow$ Break up $0 < |b|$ into

$$0 < \frac{|b|}{2} \text{ and } \frac{|b|}{2} < |b|$$

$\exists$ unique q' & r' s.t. $a = bq' + r'$

s.t. $0 \leq r' < b$

If $0 \leq r' \leq \frac{|b|}{2}$ let $r = r'$

$q = q'$

if $\frac{1}{2}|b| < r' < |b|$

then $-\frac{1}{2}|b| < r' - |b| < 0$

subtracting $|b|$.

$\therefore a = bq' + r' - |b| + |b|$

If $b \geq 0$; then $a = b(q'+1) + r' - |b|$

let $r = r' - |b|$, ~~$q = |q$~~

$q = q' + 1$

If $b < 0$; $|b| = -b$

so $a = bq' + r' - |b| - b$.

$a = b(q'-1) + r' - |b|$ so

let $q = q' - 1$, ; $r = r' - |b|$

Common divisor

Let 'a' and 'b' are two integers, then a integer 'd' is called the common divisor of 'a' and 'b' if $d|a$ and $d|b$. Since $1|a$ for all $a \in \mathbb{Z}$, then 1 is Common divisor of any integers 'a' & 'b'.

Any integer b is said to be divisible by an integer $a \neq 0$, in symbols $a|b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to denote that b is not divisible by a.

Greatest Common divisor (gcd)

Let a and b be any two integers with atleast one of them different from zero. The greatest Common divisor of a and b is denoted by $\gcd(a,b)$, is the positive integer 'd' satisfying following.

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

(b) If $c|a$ and $c|b$, then $c \leq d$.

e.g. $\gcd(-12, 30) = 6$

$\gcd(-5, 5) = 1$

$\gcd(3, 11) = 1$

$\gcd(-12, -28) = 4$

Properties of gcd

Date. No.

If a and b are nonzero integers then';

(i) $\gcd(a,b) = \gcd(-b,a) = \gcd(-a,b)$
$= \gcd(-a,-b) = \gcd(|a|,|b|)$

(ii) $\gcd(a,b) = \gcd(b,a)$

(iii) if $\gcd(a,b) = d$, then $d \geq 1$

(IV) $\gcd(a,a) = a$

(v) $\gcd(a,b) = a$ iff $a|b$

(vi) $\gcd(a,0) = |a|$

Theorem

Given integers a and b, not both of which are zero has a unique greatest common divisor $d = \gcd(a,b)$ which can be expressed in the form $d = ax+by$ for some integers x & y.

Proof let us consider the set of all positive ~~integers~~ linear combination of 'a' and 'b':

$$S = \{ au + bv : au + bv > 0 ; u \text{ and } v \text{ are integers} \}$$

(i) We first show that S is non empty

if $a \neq 0$ then $|a| = au + b \cdot 0$ lies in S. where we can choose $u = 1$ or -1 according as 'a' is positive or negative. Then by well ordering principle, S must contain smallest element 'd'. But ~~the~~ by ~~the~~ defining the nature of S, there exists integers x and y for which $d = ax + by$.

(ii) We claim $d = \gcd(a, b)$

Since d is positive integers then by division algorithm there exists integers q and r such ~~that~~ satisfying

$$a = qd + r \quad \text{with } 0 \leq r < d$$

i.e. $r = a - qd$

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

$r = a(1 - qx) + b(-qy)$

Which is of the form $au+bv$ & $r \geq 0$.

Now if $r \neq 0$, then $r>0$

$$\Rightarrow r = a(1-qx)+b(-qy)>0$$

implies that $r \in S$ and also we have $0 \leq r < d$ which contradicts d is minimum value in S.

Hence $r=0 \Rightarrow a=qd \Rightarrow d \mid a$

Similarly we can show $d \mid b$

Hence $d \mid a$ & $d \mid b$.

If d' is any integer such that $d' \mid a$ & $d' \mid b$ then

$a=d'u$ & $b=d'v$ for some integers u & v.

Since, $d=ax+by$ for some integers x & y.

$$d = d'ux+d'vy$$
$$d = d'(ux+vy)$$
$$\cancel{d=d} \Rightarrow d' \mid d$$

Since $d > 0$ & $d' | d$ we must have $d' \leq d$

Hence $gcd(a,b) = d$

(iii) To show $gcd(a,b)$ is unique.

Let d_1 and d_2 be any two gcd's of a & b.

Then; $d_1 | a$ and $d_1 | b$ (Com divi)

Since; ~~Since~~ $d_2 = gcd(a,b)$

$\Rightarrow d_1 | d_2$

Also since $d_2 = gcd(a,b)$, $d_2 | a$ & $d_2 | b$

Since $d_1 = gcd(a,b)$, $\Rightarrow d_2 | d_1$

Since, $d_1 \geq 1$, $d_2 \geq 1$, $d_1 | d_2$

$d_2 | d_1$

Hence ~~d=~~ ~~d~~ . implies $d_1 = d_2$

$d = gcd(a,b)$ uniquely exist

Property

① If $a|b$ & $b \neq 0$ then $|a| \leq |b|$

⇒ If $a|b$ there exists an integer c such that $b = ac$ also $b \neq 0$ implies that $c \neq 0$

By taking absolute value $|b| = |ac|$

$$|b| = |a||c|$$

Because $c \neq 0$ this follows that

$$|c| \geq 1$$

Hence; $|b| = |a||c| \geq |a|$

$$\Rightarrow |b| \geq |a|$$

② If $a|b$ and $a|c$ then

$a|(bx + cy)$ for arbitrary integers x and y.

⇒ As $a|b$ and $a|c$ we can ensure that;

$$b = ar \quad \text{and} \quad c = as$$

for some suitable integers r & s.

Then; $bx + cy = arx + asy = a(rx + sy)$
which is divisible by a. ⇒ $a | bx + cy$.

Corollary If a and b are given integers, not both zero then the set

$$T = \{ax+by \mid x, y \text{ are integers}\}$$

is precisely the set of all multiples of

$$d = \gcd(a,b)$$

Proof. As $d|a$ and $d|b$ we know that $d|(ax+by)$ for all integers x & y.

Thus every member of T is a multiple of d.

Conversely, d may be written as.

$d = ax_0 + by_0$ for suitable integers x_0 & y_0., so that any multiple ~~of~~ nd of d is of the form

$$nd = n(ax_0+by_0) = a(nx_0) + b(ny_0)$$

Hence nd is a linear combination of ~~as~~ a and b and by definition lies in T.

Definition Two integers a and b not both of which are zero are said to be relatively prime whenever $\gcd(a,b)=1$

Theorem : Let a and b be integers not both zero. Then a and b are relatively prime if and only if ~~ax+by=1~~ there exists x and y such that

$$1 = ax+by.$$

Proof : If ~~a~~ a and b are relatively prime so that $\gcd(a,b)=1$ then we can ~~gaure~~ guarantees the existence of x and y satisfying $1 = ax+by$

As for converse suppose $1 = ax+by$ for some choice of x and y and that

$$d = \gcd(a,b)$$

Because $d \mid a$ and $d \mid b$ by Th.

$d \mid (ax+by)$ or $d \mid 1$

This 'd' is positive integer this forces d to be equal to 1.

Corollary 1 If $\gcd(a,b) = d$

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

$\Rightarrow$ As $\gcd(a,b) = d$

we can find integers x and y such that

$$d = ax + by$$

dividing both sides by d

$$1 = \left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y$$

(d - divisor)

As $\frac{a}{d}$ and $\frac{b}{d}$ are integers

This shows $\frac{a}{d}$ & $\frac{b}{d}$ are relatively prime.

Corollary 2 If $a|c$ and $b|c$

with $\gcd(a,b) = 1$ then $ab|c$

$\Rightarrow$ As $a|c$ and $b|c$

there exists integers r & s

such that $c = ar = bs$

for the relation $\gcd(a,b) = 1$

It allows us to write $1 = ax + by$
for some choice of integers x & y.

Multiplying this eqn by c.

$$c = c \cdot 1 = c \cdot (ax + by)$$

$$= acx + bcy$$

$$c = a \cdot (bs)x + b \cdot (as)y$$

$$c = ab(sx + by)$$

which is divisible by ab.

so; $ab \mid c$.

<u>Theorem</u> Euclid formula :

If $a \mid bc$ with $\gcd(a,b) = 1$ then $a \mid c$.

$\Rightarrow$ As $\gcd(a,b) = 1$

we can write $ax + by = 1$
where x & y are integers.

Multiplying above by c

$$acx + bcy = c$$

$c = 1 \cdot c = (ax+by) \cdot c = acx + bcy$

Because $a|ac$ and $a|bc$ it follows that

$a|(acx+bcy)$ which can be recast as $a|c$

Theorem Let a and b be integers not both zero. For a positive integer d, $d = \gcd(a,b)$ if and only if

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

$\Rightarrow$ Suppose $d = \gcd(a,b)$

Certainly $d|a$ & $d|b$.

d can be expressed as $d = ax+by$ for some integers a & b.

Thus if $c|a$ & $c|b$ then $c|(ax+by)$ or $c|d$.

Conversely, let d be positive integers satisfying the above condition. Given any common divisor c of a and b, we have $c|d$. The implication is $d \geq c$ & consequently d is ~~common~~ greatest common divisor of a & b.

Euclidean Algorithm

Date. No.

Let a and b be two integers whose gcd is desired.

As $\gcd(|a|, |b|) = \gcd(a,b)$

We can assume that $a \geq b > 0$

Let us apply division algorithm to a & b

$$a = q_1 b + r_1 \quad ; \quad 0 \leq r_1 < b$$

If $r_1 = 0$ then $b \mid a$ and $\gcd(a,b) = b$

when $r_1 \neq 0$ divide b by r_1 to produce integers q_2 & r_2 satisfying

$$b = q_2 r_1 + r_2 \quad ; \quad 0 \leq r_2 < r_1$$

If $r_2 = 0$ we stop otherwise proceed as before; to obtain

$$r_1 = q_3 r_2 + r_3 \quad ; \quad 0 \leq r_3 < r_2$$

This division process continues till zero remainder appears say at $(n+1)$ stage.

 here r_{n-1} is divided by r_n.

$$b > r_1 > r_2 \cdots \geq 0$$

The result is the following system of equation.

$$a = q_1 b + r_1 \;;\; 0 < r_1 < b$$

$$b = q_2 r_1 + r_2 \;;\; 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3 \;;\; 0 < r_3 < r_2$$

$$- \cdot - \cdot$$

$$r_{n-2} = q_n r_{n-1} + r_n \;;\; 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0$$

Lemma If $a = qb + r$ then $\gcd(a,b) = \gcd(b,r)$

Proof: If $d = \gcd(a,b)$ then

$d \mid a$ and $d \mid b$

together imply that ; $d \mid (a - qb)$ or $d \mid r$

Thus d is a common divisor of b and r.
On the otherhand, if c is an arbitrary common divisor of b and r then
$c \mid (qb + r)$ hence $c \mid a$.

This makes c a common divisor of a and b so that ~~c ≤ b~~

$c \leq d$

It follows from the definition that

$gcd(b, r)$ then $d = gcd(b, r)$

Using this lemman we can write;

$$gcd(a, b) = gcd(b, r_1) = \dots gcd(r_{n-1}, r_n)$$

$$= gcd(r_n, 0) = r_n$$

we know if $d = gcd(a, b)$ then we Can write

$$d = ax + by$$

By Euclidean algorithm

$$r_n = r_{n-2} - q_n r_{n-1}$$

$$r_n = r_{n-2} - q_n [r_{n-3} - q_{n-1} r_{n-2})$$

$$r_n = (1 + q_n q_{n-1}) r_{n-2} + (-q_n) r_{n-3}$$

Euclidean Algorithm

Date. No.

This represents r_n as a linear combination of r_{n-2} and r_{n-3}.

Continuing backboward through the system of equations we can successively eliminate the remainders $r_{n-1}, r_{n-2}, \dots r_n, r_1$ until a stage is reached where $r_n = gcd(a,b)$ is expressed as a linear combination of a & b.

Example let us find gcd(12378, 3054)

$$12378 = 4 \cdot 3054 + 162$$

$$3054 = 18 \cdot 162 + 138$$

$$162 = 1 \cdot 138 + 24$$

$$138 = 5 \cdot 24 + 18$$

$$24 = 1 \cdot 18 + 6$$

$$18 = 3 \cdot 6 + 0$$

Here 6 is gcd.

To represent 6 as a linear combination of the integers 12378 & 3054

$$6 = 24 - 18$$

$$= 24 - (138 - 5 \cdot 24)$$

$$= \cancel{6}\, 1 \cdot 24 - (138 - 5 \cdot 24)$$

$$= 6 \cdot 24 - 138$$

$$= 6(162 - 138) - 138$$

$$= 6 \cdot 162 - 7 \cdot 138$$

$$= 6 \cdot 162 - 7 \cdot (3054 - 18 \cdot 162)$$

$$= 132 \cdot 162 - 7 \cdot (3054)$$

$$= 132(12378 - 4 \cdot 3054)$$

$$- 7 \cdot (3054)$$

$$= 132 \cdot (12378) + (-535)\ 3054$$

Hence: $6 = \gcd(12378, 3054)$

$= 12378x + 3054y$

$x = 132, \quad y = -535.$

<u>Theorem</u> If $k > 0$ then $\gcd(ka, kb) = k \gcd(a, b)$

<u>Proof</u>: If each of the equations appearing in the Euclidean algorithm for a and b is multiplied by k. we obtain.

$$ak = q_1(bk) + r_1 k \qquad 0 < r_1 k < bk$$

$$bk = q_2(r_1 k) + r_2 k \qquad 0 < r_2 k < r_1 k$$

$$\cdots\cdots\cdots\cdots$$

$$r_{n-2}k = q_n(r_{n-1}k) + r_n k \qquad 0 < r_n k < r_{n-1}k$$

$$r_{n-1}k = q_{n+1}(r_n k) + 0$$

But this is clearly the Euclidean algorithm applied to the integers ak & bk so that their ~~gt~~ gcd is the last non zero remainder $r_n k$ that is;

$$\gcd(ka, kb) = r_n k = k \gcd(a, b)$$

Corollary For any integer $k \neq 0$,

$$\gcd(ka, kb) = |k| \gcd(a,b).$$

$$\Rightarrow \cancel{\gcd}(ak, bk) = \gcd(-ak, -bk)$$

$$= \gcd(a|k|, b|k|)$$

$$= |k| \gcd(a,b)$$

$\gcd(ka, kb) = \gcd(|k|a, |k|b)$

$d = (|k|a)x + (|k|b)y$

$d = |k|(ax + by)$

$d = |k| \gcd(a,b)$

$\gcd(ka, kb) = |k| \gcd(a,b)$

definition The least common multiple (lcm) of two non zero integers a & b is denoted by lcm (a,b) is the positive integer (m) satisfying the following

(a) $a|m$ and $b|m$

(b) If $a|c$ and $b|c$ with $c>0$ then $m \leq c$

eg Positive common multiples of

-12 and 30 are;

60, 120, 180 hence least one is

$\boxed{60}$

Given non zero integers a and b, lcm(a,b) always exists and lcm(a, b) $\leq |ab|$

Theorem for positive integer a and b.

$$\gcd(a,b)\ \mathrm{lcm}(a,b) = ab$$

$\Rightarrow$)

To begin with put $d = \gcd(a,b)$

and write $a = dr$, $b = ds$

for integers r & s.

If $m = ab/d$ then $m = as = rb$

The effect of which is to make

(m) a positive common multiple of a & b.

Now let c be any positive integer that is a common multiple of a & b say for definiteness

$$c = au = bv$$

As we know, there exist integers x & y satisfying $d = ax + by$

In consequence;

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab}$$

$$= \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y$$

$$= vx + uy.$$

This eqn tells $m \mid c$ allowing us to conclude $m \le c$. Thus in accordance with defn $m = \text{lcm}(a,b)$

$$\text{lcm}(a,b) = \frac{ab}{d} = \frac{ab}{\gcd(a,b)}$$

$$\text{lcm}(a,b)\,\gcd(a,b) = ab$$

Corollary for any choice of positive integers a and b,

$$\text{lcm}(a,b) = ab \text{ if and only if } \gcd(a,b) = 1$$

⇒ from Euclidean algorithm let us consider positive integers 3054 and 12378 for instance, we found

$$\gcd(3054, 12378) = 6$$

$$\text{lcm}(3054, 12378) = \frac{3054 \cdot (12378)}{6}$$

$$= 6,300,402$$

Let us ~~ab~~ ~~ob~~ observe that the notion of the greatest common divisor can be extended to more than two integers in an obvious way.

In case of three integers a, b, c not all zero.

Date. No.

gcd(a,b,c) is defined to be the positive integer d having the following properties.

(a) d is a divisor of each a, b, c

(b) If e divides the integers a, b, c then $e \le d$

#

$\gcd(39, 42, 54) = 3$

$\gcd(49, 210, 350) = 7$

If $\gcd(a,b,c) = 1$ ~~there~~ Three integers are said to be relatively prime.

#

Q. (1) find gcd(143, 227)

$227 = 1 \cdot 143 + 84$

$143 = 1 \cdot 84 + 59$

$84 = 1 \cdot 59 + 25$

$59 = 2 \cdot 25 + 9$

$25 = 2 \cdot 9 + 7$

$9 = 1 \cdot 7 + 2$

$7 = 3 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

1

Q. Use the Euclidean algorithm to obtain integers x & y.

$$\gcd(56, 72) = 56x + 72y.$$

First, find $\gcd(56, 72) =$

Then Reverse back!

Linear diophantine equation

A linear Diophantine equation (in two variables x & y) is an equation;

$$ax + by = c$$

with integers $a, b, c \in Z$ to which we seek integer solution.

It is not obvious that all such equations is solvable

For eg. the equation $2x + 2y = 1$ does not have integer solution

Some finite Diophantine equations have finite number of solution. eg. $2x = 4$

And some have infinite number of solutions

$$2x + 2y = 110$$

<u>Theorem</u>: The linear diophantine equation

$ax + by = c$ has a solution if and only if $d \mid c$ where $d = gcd(a, b)$

If (x_0, y_0) is any particular sol^n of this eq^n then all other sol^{n}s are given by

$$x = x_0 + \left(\frac{b}{d}\right)t \quad \& \quad y = y_0 - \left(\frac{a}{d}\right)t$$

Proof: Suppose that linear diophantine equation $ax + by = c$ has a solution then we need to show that $d \mid c$ where $d = \gcd(a,b)$

Let (x_0, y_0) be a set of solution of the given equation for some integers.

Then; $c = ax_0 + by_0$ ——— (i)

In which $d = \gcd(a,b)$

$\Rightarrow d \mid a$ and $d \mid b$

Then there exists r & s such that
$a = dr$ & $b = ds$

Putting this in eqⁿ (i)

$c = dr\,x_0 + ds\,y_0$

$c = d(rx_0 + sy_0)$

$\Rightarrow d \mid c$. because $rx_0 + sy_0$ is

Date No.

Conversely, suppose $d|c$ then we need to show $ax+by=c$ has a solution

If $d = \gcd(a,b)$ then there exists integers x_0 & y_0 such that:

$$d = ax_0 + by_0$$

Again $d|c \Rightarrow c = dt$ for some $t \in \mathbb{Z}$

$$\Rightarrow c = (ax_0 + by_0)t$$

$$c = atx_0 + bty_0$$

$$c = a(tx_0) + b \cdot (ty_0)$$

This shows (tx_0, ty_0) satisfies on the given eq^n $c = ax+by$

Therefore tx_0 & ty_0 is the sol^n of $ax+by=c$

Second Part

If (x_0, y_0) is any particular solution of this eq^n then $ax_0 + by_0 = c$

Again if (x', y') is any particular solution of the equation then $ax' + by' = c$

Then;
$$ax_0 + by_0 = c = ax' + by'$$

$$ax_0 + by_0 = ax' + by'$$

$$by_0 - by' = ax' - ax_0$$

$$b(y_0 - y') = a(x' - x_0) \quad \text{—— } (2)$$

Since; $d = \gcd(a,b)$ so $d|a$ and $d|b$.

Then there exists 'r' & 's' such that

$$a = dr \qquad b = ds$$
$$\gcd(r,s) = 1$$

so; $r = \frac{a}{d}$ and $s = \frac{b}{d}$

Then eqn (2) becomes:

$$ds(y_0 - y') = dr(x' - x_0)$$

$$s(y_0 - y') = r(x' - x_0) \quad \text{—— } (3)$$

Hence; $r \mid r(x' - x_0) \Rightarrow r \mid s(y_0 - y')$

Then, $r | s$ or $r | (y_0 - y')$

But since $\gcd(r, s) = 1$

so $r \nmid s$ hence $r | (y_0 - y')$

Then there exists $t \in \mathbb{Z}$ such that

$$y_0 - y' = r \cdot t$$

So eqn (3) becomes:

$$s(y_0 - y') = r(x' - x_0)$$

$$s \cdot rt = r(x' - x_0)$$

$$x' - x_0 = st$$

$$x' = x_0 + st$$

$$\boxed{x' = x_0 + \left(\frac{b}{d}\right) t}$$

Again from (3)

$$s(y_0 - y') = r(x' - x_0)$$

$$\cancel{s(y_0 - y') = r \cdot st}$$

Then $s | r(x' - x_0)$ then $s | r$ or $s | (x' - x_0)$

But since $\gcd(r,s)=1$ so $r \nmid s$

hence, $s \mid (x' - x_0)$

Then there exists $t \in \mathbb{Z}$ such that

$$x' - x_0 = st$$

Then,

$$s(y_0 - y') = r(x' - x_0) = r(st)$$

$$s(y_0 - y') = r(st)$$

$$y_0 - y' = rt$$

$$y' = y_0 - rt$$

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

Q. find all the integers x & y such that $147x + 258y = 369$

$\Rightarrow \gcd(147, 258)$

$$258 = 1 \cdot 147 + 111$$
$$147 = 1 \cdot 111 + 36$$
$$111 = 3 \cdot 36 + 3$$
$$36 = 12 \boxed{3} + 0$$

Here, $3 \mid 369$ so above eq^n is solvable.

$3 = 111 - 3 \cdot 36$

$3 = 111 - 3(147 - 1 \cdot 111)$

$3 = 4 \cdot 111 - 3 \cdot 147$

$3 = 4 \cdot 258 - 7 \cdot 147$.

Multiplying b-s by 123

$3 \cdot 123 = 492 \cdot 258 - 861 \cdot 147$

$x = 492 \quad y = -861$

\# Prove that $ax + by = a + c$ is solvable if $ax + by = c$ is solvable.

⇒

Let $ax + by = a + c$ is solvable
let $d = \gcd(a, b)$ then $d \mid a + c$

since; $d = \gcd(a, b)$ then d/a.

From (1) & (2) $d \mid a+c-a$

$\Rightarrow d \mid c$

So $ax+by=c$ is solvable.

Conversely let $ax+by=c$ is solvable then d/c.

where; $d = gcd(a,b)$

Since $d = gcd(a,b)$. then d/a.

From above; $d \mid a+c$.

So $ax+by=c$ is solvable.

Unit 3 Primes & their distribution

1. Concept of prime & composite numbers
2. Fundamental Th. of arithmetic
3. The sieve of Eratosthenes.

Prime: Any integer $p>1$ is called prime number if its only positive divisors are 1 and p.

Composite number: Any integer greater than 1 which is not prime is composite.

Among first 10 natural numbers 2, 3, 5, 7 are primes & 4, 6, 8, 9, 10 are composite. 2 is only even prime. '1' is neither prime nor composite

Theorem If p is a prime & $p|ab$ then $p|a$ or $p|b$.

$\Rightarrow$ Let p is a prime and $p|ab$.
If $p|a$ then we are done.

So let us assume $p\nmid a$

Since p is a prime then only positive divisors are p or 1 of prove p or 1 and this implies $\gcd(p,a)=1$

Then $1 = px + ay$ where x & y are integers.

$\Rightarrow$ $b = pbx + aby$ (multiply by b)

We have $p \mid ab$ then $ab = pk$ for some integers k.

$$b = p(bx) + (pk)y$$

$$b = p(bx + ky)$$

$\Rightarrow$ $p \mid b$ for some integer $bx + ky$.

<u>Theorem</u>: Every integer $n > 1$ has a prime factor.

<u>Proof</u>: We use induction on n. It is true for $n = 2$ because 2 is itself prime

Assume the result of the theorem is true for every positive integer $n \leq k-1$ where $k \geq 3$. Now we show for k. Then we have two cases.

Since p is a prime then only positive divisors are p or 1 of p are p or 1 and this implies $\gcd(p, a) = 1$

Then $1 = px + ay$ where x & y are integers.

$\Rightarrow$ $b = pbx + aby$ (multiply by b)

We have $p \mid ab$ then $ab = pk$ for some integers k.

$$b = p(bx) + (pk)y$$

$$b = p(bx + ky)$$

$\Rightarrow$ $p \mid b$ for some integer $bx + ky$.

<u>Theorem</u>: Every integer $n > 1$ has a prime factor.

<u>Proof</u>: We use induction on n. It is true for $n = 2$ because 2 is itself prime

Assume the result of the theorem is true for every positive integer $n \leq k-1$ where $k \geq 3$. Now we show for k. Then we have two cases.

(i) If k is prime then k is a prime factor of itself

(ii) If k is not prime then k must be composite. So it must have a factor k with $d < k$. Then by induction hypothesis 'd' must be prime factor say 'p' & consequently p is also the prime factor of k as well.

Hence every integer $n > 1$ has a prime factor.

Corollary : If p is a prime and $p \mid a_1 a_2 a_3 \cdots a_n$ then $p \mid a_k$ for some k with $1 \leq k < n$.

Proof: We use induction on 'n', i.e. on the number of factors. If $n = 1$ then stated condition holds obviously. If $n = 2$, then it has proved in the previous Th. as if p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$. So let us assume that the result is true for less than 'n' factors i.e. p divides a product of less than n factors

 $p \mid a_1 a_2 a_3 \ldots a_{n-1}$

Now we show for 'n' factors.

$p \mid a_1 a_2 a_3 \ldots a_n$

$p \mid (a_1 a_2 a_3 \ldots a_{n-1}) a_n$

$\Rightarrow p \mid (a_1 a_2 a_3 \ldots a_{n-1})$ or $p \mid a_n$

Then by induction hypothesis $p \mid a_k$ for some $k = 1, 2, 3 \ldots n-1$ or $p \mid a_n$

$\Rightarrow p \mid a_k$ for some integer $k = 1, 2, \ldots n$

Hence if p is a prime & $p \mid a_1 a_2 \ldots a_n$ then $p \mid a_k$ for some k with $1 \le k < n$.

Fundamental Theorem of Arithmetic

Every positive integer $n > 1$ is either a prime or a product of ~~primes~~ primes, this representation is unique.

Proof: Let $n>1$ is an integer.

Then it is either prime or composite.
If ~~n is a prime~~ it is a prime then there is nothing to prove.

If n is composite, then there exists an integer d satisfying $d|n$ and $1<d<n$.

Among all such integers 'd' let us select p_1 to be the smallest (according to well ordering principle). Then p_1 must be prime otherwise it would have a divisor q with $0<q<p_1$. But we have $q|p_1$ and $p_1|n$ implies $q|n$.

which contradict the choice that p_1 as the smallest positive diviser not equal to 1 of n.

Therefore we may write $n = p_1 n_1$ where p_1 is prime & $1<n_1<n$. If n_1 is prime then proof is complete.

If possible let n_1 is not a prime then by repeating the same process as above we can get a second prime p_2

 So that $n_1 = p_2 n_2$ where $1 < n_2 < n_1$

Then $n = p_1 p_2 n_2$

Similarly if n_2 is prime then there is nothing to prove.

otherwise in the same way

$$n_2 = p_3 n_3 \text{ with } p_3 \text{ is prime}$$

Therefore we obtain a decreasing sequence $n > n_1 > n_2 \cdots > 1$ which can not continue infinitely.

Thus leads to the factorization

$$n = p_1 p_2 p_3 \cdots p_k \text{ for some } k.$$

To establish the uniqueness of prime factorization let us assume that integer can be represented as product of primes in two ways as;

$$n = p_1 p_2 p_3 \cdots p_r = q_1 q_2 q_3 \cdots q_s$$

with $r \leq s$

where p_i and q_i all primes written in increasing order as :

$$p_1 \le p_2 \le \cdots \le p_r$$

with $q_1 \le q_2 \cdots \le q_s$

— (A)

Since $p_1 \mid p_1 p_2 p_3 \cdots p_r$

$$\Rightarrow p_1 \mid q_1 q_2 q_3 \cdots q_s$$

But since p_i and q_i all are primes so p_1 must be any one of $q_1, q_2, \cdots q_s$

With loss of generality assume

$p_1 = q_1$ then (A) can be written as :

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

Then repeat same process to get

$$p_2 = q_2$$

Then again

$$p_3 \cdots p_r = q_3 \cdots q_s$$

Continue this proces we get at last $r < s$.

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

is contradiction because all $q_i > 1$

Therfore $r = s$

Hence representation is unique.

The Sieve of Eratosthenes

Eratosthenes (276 - 194 BC) used clever idea called the Sieve of Eratosthenes. for finding all the primes below ~~belo~~ a given integers (n). To apply this technique, we first write all the integers from 2 to n in their natural order then systematically eliminate all composite numbers by cutting out the multiples ~~of~~ 2p, 3p, ... of the prime p. Those integers that are left on the list are the primes.

Date. No.

Theorem: There are infinite number of primes. (Euclid proof)

Proof: If possible let are finitely many primes $p_1 = 2$, $p_2 = 3$, $p_3 = 7$, $\cdots$ p_k

where p_k is the last prime. Now we consider

a positive integer $p = p_1 p_2 \cdots p_{k+1}$

Since $p > p_k$ then p is a composite number

because p_k is last prime. The p is divisible

by some prime (If $a > 1$ is a composite

then 'a' will always have prime divisor

$p \leq \sqrt{a}$)

Since there are finite number of primes in

the above mentioned list so p is also one

of the primes $p_1, p_2, \cdots p_k$ &

$$p \mid p_1 p_2 \cdots p_k \quad \text{——} \; (A)$$

And also we have $p \mid p \quad \text{——} \; (B)$

From (A) and (B) $P \mid p - p_1 p_2 \ldots p_k$

and consequently we get $p \mid 1$ which is a contradiction.

Hence there are infinite number of primes

<u>Theorem</u> If p_n is the n_{th} prime number then

$$p_n \le 2^{2^{n-1}}$$

<u>Proof:</u> We use induction on 'n'.

If $n = 1$; then $p_1 \le 2$

Let us assume the result of the theorem is true for $n = k$. Then we show for $n = k+1$

As we know; $p_{k+1} \le p_1 p_2, \ldots p_k + 1$

$$\le 2 \cdot 2^2 \cdot \ldots 2^{2^{k-1}} + 1$$

$$= 2^{(1+2+2^2+\ldots 2^{k-1})} + 1 \qquad \left(\because 1+2+2^2+\ldots 2^{k-1} = 2^k - 1\right)$$

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

$$\le 2^{2^k-1} + 2^{2^k-1} \qquad \because 1 \le 2^{2^k-1}$$

$$= 2 \cdot 2^{2^k-1}$$

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

which is true # proves

Chapter 4 The theory of Congruence

Definition :- Let 'n' be a positive integer. Two integers 'a' and 'b' are said to congruent modulo (n) (a is congruent to b modulo n) and is written as $a \equiv b \pmod{n}$ if $n \mid a-b$

Examples

$8 \equiv 23 \pmod{5}$ $5 \mid (8-23)$

$27 \equiv 6 \pmod{7}$ $7 \mid (27-6)$

$19 \not\equiv 5 \pmod{4}$ $4 \nmid (19-5)$

Note: (i) Since $1 \mid (a-b)$ for any two integers a and b. Therefore we have any two integers are cogruent modulo 1.

(ii) If any two integers are congruent to modulo 2 then either both are even or both are odd. i.e. if $a \equiv b \pmod{2}$ then either both a and b are even or both are odd.

(iii) Since $n \mid (xn-0)$, we have $xn \equiv 0 \pmod{n}$ for any integer x.

Theorem : Let n be a non zero positive integers then $a \equiv b \pmod{n}$ iff $a \equiv r \pmod{n}$, where r is remainder upon division of b by n.

Eg: $27 \equiv 7 \pmod 5$

and $27 \equiv 2 \pmod 5$

where 2 is the remainder upon division of 7 by 5.

Proof: Let 'n' be a non zero positive integer with $a \equiv b \pmod n$

then we show $a \equiv r \pmod n$ where 'r' is the remainder upon division of 'b' by 'n'.

we have, $a \equiv b \pmod n$

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

$(a-b) = q' \cdot n$ for some integer q'.

$$a = q' \cdot n + b \quad \text{—— (A)}$$

For any integers 'b' and 'n' we have by division algorithm there exists q & r such that $b = qn + r$

Hence from (A)

$$a = q'n + qn + r$$

$= (q' + q)\, n + r$

$a - r = (q' + q) \cdot n$

$n \mid (a - r)$

$a \equiv r \pmod{n}$

Conversely suppose that $a \equiv r \pmod{n}$ where r is remainder upon division of b by 'n'.

If 'r' is the remainder upon division of 'b' by 'n' then $b = qn + r$ with quotient 'q'.

$\Rightarrow r = b - qn$

We have $a \equiv r \pmod{n}$

$a \equiv (b - qn) \pmod{n}$

$a - b \equiv -qn \pmod{n}$

$\cancel{a \equiv b}\; a - b \equiv 0 \pmod{n}$

$\Rightarrow a \equiv b \pmod{n}$ because $qn \equiv 0 \pmod{n}$

Note Given a positive integer 'n'

Let 'q' and 'r' be quotient and remainder 'r' upon the division of a by 'n' so $a = qn + r$ with $0 \le r < n$

$$a - r = qn$$

$$n \mid (a - r)$$

$$a \equiv r \pmod{n}$$

i.e. 'a' is congruent to modulo n to exactly one of the integers $0, 1, 2, \ldots (n-1)$

So every integer is concurrent to modulo 'n' exactly one of the values $0, 1, 2, \ldots (n-1)$.

Complete Set of Residue modulo 'n'

A collection of integers $a_1, a_2, \ldots a_n$ is said to form complete set of residue modulo 'n' if each $a_1, a_2, \ldots, a_n$ is congruent to modulo 'n' to exactly one of $0, 1, 2, \ldots (n-1)$ and each $0, 1, \ldots n-1$ is congruent to modulo 'n' to exactly one of $a_1, a_2, \ldots a_n$

e.g. The set $\{-12, -4, 11, 13, 22, 82, 91\}$ form a complete set of residue modulo 7 because,

$$\Rightarrow \quad -12 \equiv 2 \pmod 7$$

$$-4 \equiv 3 \pmod 7$$

$$11 \equiv 4 \pmod 7$$

$$22 \equiv 1 \pmod 7$$

$$82 \equiv 5 \pmod 7$$

$$91 \equiv 0 \pmod 7$$

i.e. each of $-12, -4, 11, 13, 22, 82, 91$ is congruent to modulo 'n' exactly one of $0, 1, 2, 3, 4, 5, 6$

Theorem : for any integers 'a' and 'b', $a \equiv b \pmod n$ iff a and b leave the same non-negative remainder when divided by 'n'.

Eg: The set $\{-12, -4, 11, 13, 22, 82, 91\}$ form a complete set of residue modulo 7 because;

$\Rightarrow$ $-12 \equiv 2 \pmod 7$

$-4 \equiv 3 \pmod 7$

$11 \equiv 4 \pmod 7$

$22 \equiv 1 \pmod 7$

$82 \equiv 5 \pmod 7$

$91 \equiv 0 \pmod 7$

i.e. each of $-12, -4, 11, 13, 22, 82, 91$ is congruent to modulo 'n' exactly one of $0, 1, 2, 3, 4, 5, 6$

Theorem: for any integers 'a' and 'b', $a \equiv b \pmod n$ iff a and b leave the same non-negative remainder when divided by 'n'.

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

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

$\Rightarrow (a-b) = k \cdot n$

$\Rightarrow a = b + kn$ —— (A)

Let 'r' be the remainder that b leaves upon division by n.

Therefore; $b = qn + r$ where $0 \leq r < n$

from (A)

$$a = qn + r + kn$$

$$a = (q+k)n + r$$

This shows 'r' is the remainder when 'a' is divided by 'n'.

Conversely; suppose that 'a' and 'b' leave the same non-negative remainder 'r' upon division by 'n' then we have to show

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

Now, let $a = qn + r$

and $b = q'n + r$

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

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

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

Hence for any integers 'a' and 'b' $a \equiv b \pmod{n}$ iff a and b leave the same non-negative remainder when divided by 'n'.

Properties of Congruence

Let $n > 0$ be a fixed integer and a, b, c, d be arbitrary integers then the following properties holds

(1) $a \equiv a \pmod{n}$

Since $n \mid (a-a)$ for all $n > 0$

(2) If $a \equiv b \pmod{n}$ then

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

$\Rightarrow$

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

$\Rightarrow n \mid a-b$

$(a-b) = kn$ for some integer k.

$-(a-b) = -kn$

$b-a = -k.n$

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

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

(3) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$

then $a \equiv c \pmod{n}$

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

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

$(a-b) = k_1.n$ for some integer k_1.

Date. No.

And $b \equiv c \pmod{n}$

$\Rightarrow n \mid (b-c)$

$\Rightarrow (b-c) = k_2 \cdot n$ for some integer k_2.

Now; $(a-b) + (b-c) = k_1 n + k_2 n$

$$a - c = (k_1 + k_2) n$$

$$n \mid (a-c)$$

$$a \equiv c \pmod{n}$$

(4) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

then $a+c \equiv b+d \pmod{n}$ and

$$ac \equiv bd \pmod{n}$$

Proof:

$$(a+b) = k_1 \cdot n$$

$$(c-d) = k_2 \cdot n$$

Adding: $(a-b) + (c-d) = (k_1+k_2) n$

$$(a+c) - (b+d) = (k_1 + k_2) n$$

$n \mid (a+c) - (b+d)$

$\Rightarrow (a+c) \equiv (b+d) \pmod{n}$

As $(a-b) = k_1 \cdot n \Rightarrow a = k_1 \cdot n + b$

$(c-d) = k_2 \cdot n \Rightarrow c = k_2 \cdot n + d$

$ac = (k_1 \cdot n + b)(k_2 \cdot n + d)$

$ac = k_1 k_2 n + k_1 d n + k_2 b \cdot n + bd$

$ac = bd + (k_1 k_2 + k_1 d + k_2 d) \cdot n$

$ac - bd = (k_1 k_2 + k_1 d + k_2 d) n$

$\Rightarrow n \mid (ac - bd)$

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

(5) If $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$ for any positive ~~q~~ integer k.

$\Rightarrow$ We use induction on k.
if $k=1$, then obviously $a \equiv b \pmod{n}$

Let us suppose the result of the theorem is true for $k-1$

i.e. $a^{k-1} = b^{k-1} \pmod n$

Now we show for k.

Since, we have $a \equiv b \pmod n$

and $a^{k-1} \equiv b^{k-1} \pmod n$

By using property

$a \cdot a^{k-1} \equiv b \cdot b^{k-1} \pmod n$

$a^{k} \equiv b^{k} \pmod n$

~~Theorem : If $ac \equiv bc \pmod n$ and $\gcd(c,n)$ = then $a \equiv b \pmod n$~~

Theorem If $ac \equiv bc \pmod n$ then

$a \equiv b \left(\bmod \frac{n}{d}\right)$ where $d = \gcd(c,n)$

$\Rightarrow$ we have $ac \equiv bc \pmod n$

$\Rightarrow n \mid (ac - bc)$

$\Rightarrow ac - bc = k \cdot n$ for some integer k.

Let $d = \gcd(c, n)$ then

there exists integers r & s such that

$$c = dr \quad ; \quad n = ds$$

Then $ac - bc = kn$

$$(a-b)c = k \cdot ds$$

$$(a-b)\cancel{d}r = k\cancel{d}s$$

$$(a-b)r = k \cdot s$$

Therefore $s \mid (a-b)r$

But since $s \nmid r$ so $s \mid (a-b)$

$$a \equiv b \pmod{s}$$

$$a \equiv b \left(\bmod \frac{n}{d}\right)$$

Theorem : If $ac \equiv bc \pmod{n}$

and $\gcd(c, n) = 1$ then $a \equiv b \pmod{n}$

$\Rightarrow$ From previous Theorem:

$$ac \equiv bc \pmod{n}$$

Then, $a \equiv b \left(\bmod \frac{n}{d}\right)$

where $d = \gcd(c, n)$

Now, since $\gcd(c,n) = 1$

we get $a \equiv b \left(\bmod \frac{n}{1}\right)$

we get $a \equiv b \pmod{n}$

<u>Theorem</u> If $a \equiv b \pmod{n}$ and $m \mid n$

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

$\Rightarrow$ we have; $a \equiv b \pmod{n}$

$n \mid a-b$

$\Rightarrow (a-b) = nk$ for some integer k.

Again;

$m \mid n$

$\Rightarrow n = k_1 m$

$\Rightarrow nk = k_1 k m$ (multiplying by k)

$(a-b) = m \cdot (k k_1)$

$\Rightarrow m \mid a-b$

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

Date No.

Theorem If $a \equiv b \pmod{n}$ and $c > 0$ then
$$ca \equiv cb \pmod{cn}$$

Proof: We have $a \equiv b \pmod{n}$

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

$$\Rightarrow (a-b) = k \cdot n$$

$$\Rightarrow (a-b)c = k(nc)$$

$$\Rightarrow ab - bc = \cancel{kn)}\, k(nc)$$

$$\Rightarrow nc \mid (ab - bc)$$

$$\Rightarrow ab \equiv bc \pmod{nc}$$

Theorem If $a \equiv b \pmod{n}$ and the integers a, b and n are divisible by $d > 0$ then
$$\frac{a}{b} \equiv \frac{b}{d} \left(\bmod \frac{n}{d}\right)$$

Proof: Given that $a \equiv b \pmod{n}$

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

$$\Rightarrow (a-b) = k \cdot n \text{ for some integer}$$

Since $d|a$, $d|b$ and $d|n$

then there exists x, y, z such that

$$a = dx, \quad b = dy \quad n = dz$$

$$x = \frac{a}{d} \quad y = \frac{b}{d} \quad z = \frac{n}{d}$$

Now; $a - b = Kn$

$$dx - dy = Kdz$$

$$x - y = Kz$$

$$z \mid x - y$$

$$x \equiv y \pmod{z}$$

$$\frac{a}{d} \equiv \frac{b}{d} \left(\text{mod } \frac{n}{d}\right)$$

Theorem: If $ab \equiv cd \pmod{n}$;

$b \equiv d \pmod{n}$ with $\gcd(b, n) = 1$

then $a \equiv c \pmod{n}$

Proof: Given that

$$ab \equiv cd \pmod{n}$$

$ab - cd = k_1 n$ for some integer k_1.

Again $b \equiv d \pmod{n}$

$b - d = k_2 n$ for some Integer k_2

Now $ab - cd = k_1 n$

$ab - bc + bc - cd = k_1 n$

$b(a-c) + c(b-d) = k_1 n$

$b(a-c) + c \cdot k_2 n = k_1 n$

$b(a-c) = (k_1 - k_2 c)\, n$

$\Rightarrow \quad n \mid b(a-c)$

Since $\gcd(b, n) = 1$ so $n \nmid b$

$\Rightarrow \quad n \mid (a-c)$

$a \equiv c \pmod{n}$

<u>Theorem</u> : If $a \equiv b \pmod{n_1}$,

$a \equiv b \pmod{n_2} \ldots,\ a \equiv b \pmod{n_k}$

then $a \equiv b \pmod{\operatorname{lcm}(n_1, n_2, \ldots n_k)}$

Proof. We have. $a \equiv b \pmod{n_1}$

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

$$a \equiv b \pmod{n_2} \Rightarrow n_2 \mid (a-b)$$

$$a \equiv b \pmod{n_k} \Rightarrow n_k \mid (a-b)$$

Therefore $\text{lcm}(n_1, n_2, \ldots n_k) \mid (a-b)$

$$a \equiv b \left(\bmod \text{ lcm}(n_1, n_2, \ldots, n_k)\right)$$

Q. If it is 7 am then what will be the time in 100 hrs.

$\Rightarrow$ Since we are starting at 7 am and we are using modulo 12.

$$1000 \equiv 4 \pmod{12}$$

because $100 = 8 \cdot 12 + 4$; 4 is remainder.

Also we have

$$7 \equiv 7 \pmod{12}$$

we have from previous Th.

$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

then $a + c \equiv b + d \pmod{n}$

$7+100 \equiv 7+4 \pmod{12}$

$\equiv 11 \pmod{12}$

There fore it will be 11 am in 100 hrs.

Linear ~~eq~~ Congruence

Any equation of the form $ax \equiv b \pmod{n}$ is called linear congruence

Note: 1) The congruence $ax \equiv b \pmod{n}$ is equivalent to the eq^n $ax - ny = b$

2) If two solutions $x = x_0$ and $x = x_1$ Satisfying the linear congruence $ax \equiv b \pmod{n}$ then they are congruent 'n' i.e. $x_0 \equiv x_1 \pmod{n}$ then these solutions are Considered as one of the solutions.

Let us example following example;

$$2x \equiv 1 \pmod{5}$$

we can construct the table of integers for x as;

x	0	1	2	3	4	5	6	7	8
$2x \pmod 5$	0	2	4	1	3	0	2	4	1

Here $x=3$ and $x=8$ satisfying the relation $2x \equiv 1 \pmod 5$ and $8 \equiv 3 \pmod 5$ we they are considered as one of the solutions since we are dealing on calculation of modulo 5.

$$3 \equiv 8 \equiv 13 \equiv \cdots \pmod 5$$

Similarly we only need to consider the integers amongst the list $x = 0, 1, 2, 3 \ldots$ because all other solution will one of these in modulo 5.

Theorem: The linear congruence $ax \equiv b \pmod n$ has a solution iff $d \mid b$ where $d \mid \gcd(a, n)$. If $d \mid b$ then it has 'd' mutually incongruent solution modulo n.

Proof: Let ~~we have~~, $ax \equiv b \pmod n$ has a solution say x_0. So

$$ax_0 \equiv b \pmod n$$

$$\Rightarrow n \mid (ax_0 - b)$$

$$\Rightarrow ax_0 - b = ny_0$$

$$\Rightarrow ax_0 - ny_0 = b$$

Date. No.

This is of the form Diophantine eqn

~~ax - by = b~~. $ax - ny = b$.

$\Rightarrow$ $d \mid b$ where $d = \gcd(a, n)$

Hence the linear congruence $ax \equiv b \pmod{n}$ has a soln iff $d \mid b$ with $d = \gcd(a, n)$

Again let $d \mid b$ then we have $ax \equiv b \pmod{n}$ is solvable i.e. $ax - ny = b$ is solvable

Let x_0 and y_0 be the particular set of solution then we know other solutions are of the form.

$$x = x_0 + \frac{n}{d} t \; ; \; y = y_0 + \frac{a}{d} t$$

Then by taking $t = 0, 1, 2, \ldots, d-1$

then the solns are

$$x = x_0, \; x_0 + \frac{n}{d}, \; x_0 + \frac{2n}{d}, \; \ldots, \; x_0 + \frac{(d-1)n}{d}$$

(a) We first show that these integers are incongruent solution modulo n.

 this if possible let

Date. No.

$$x_0 + \frac{n}{d} t_i = x_0 + \frac{n}{d} t_j \pmod n$$

with $0 \le t_i \le t_j \le d-1$

$$\frac{n}{d} t_i \equiv \frac{n}{d} t_j \pmod n$$

$$t_i \equiv t_j \pmod d$$

$$t_i = t_j \pmod d$$

$d \mid t_i - t_j$ where contradicts that $t_j - t_i \le d$

Hence, the integers $x = x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d} t$

are incongruent solution modulo n.

(b) Now show that any other sol^n

$x_0 + \frac{n}{d} t$, o $t > d$ is congruent

to modulo (n) to one of the integers

$$x_0, x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d}, \ldots,$$

$$x_0 + \frac{(d-1)n}{d}$$

Since $t > d$ then by division algorithm there exists q, r s.t

$$t = qd + r \quad \text{with} \quad 0 \leq r < d$$

$$x_0 + \frac{n}{d} t = x_0 + \frac{n}{d}(qd + r)$$

$$= x_0 + nq + \frac{n}{d} r$$

$$\equiv x_0 + \frac{nr}{d} \pmod{n}$$

where $x_0 + \frac{n}{d} r$ is one of the integers $x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots$

$x_0 + \frac{(d-1)n}{d}$ because $r < d$

proved

Theorem

Date. No.

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

Proof. We already know that the linear congruence $ax \equiv b \pmod{n}$ is equivalent to Diophantine eq^n $ax - ny = b$

We also know from a theorem ;"
The diophantine eq^n $ax + by = c$ has a sol^n if and only if $d \mid c$ where $d = \gcd(a, b)$ and ~~the sol^{n}s are~~

~~a_0~~ x

if the x_0 and y_0 is any particular solution of this eq^n then all other sol^{n}s are given by;

$$x = x_0 + \left(\frac{b}{d}\right) t$$

$$y = y_0 + \left(\frac{a}{d}\right) t.$$

where 't' is arbitrary integer.

So ~~it~~ in this $ax - ny = b$ can be solved only if $d \mid b$ moreover if it is ~~solved~~ solvable and x_0, y_0 is one specific sol^n then any other sol^n has the form

Date. No.

$x = x_0 + \frac{n}{d} t \quad ; \quad y = y_0 + \frac{a}{d} t$

for some choice of t

Let us take $t = 0, 1, 2, \ldots\ldots, d-1$

$x_0, \; x_0 + \frac{n}{d}, \; x_0 + \frac{2n}{d}, \ldots,$

$x_0 + \frac{(d-1)n}{d}$

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

$$x_0 + \frac{n}{d} t_1 \equiv x_0 + \frac{n}{d} t_2 \pmod{n}$$

where

$$0 \le t_1 \le t_2 \le d-1$$

then we write

$$\frac{n}{d} t_1 \equiv \frac{n}{d} t_2 \pmod{n}$$

Since $\gcd\left(\frac{n}{d}, n\right) = n/d$

 Then we have

$$t_1 \equiv t_2 \pmod{n}$$

which is to say that $n \mid t_1 - t_2$

But this is impossible in the view of inequality $0 < t_2 - t_1 < d$

The division algorithm permits us to write 't' as

$$t = qd + r$$

where; $0 \leq r \leq d-1$

$$x_0 + \frac{n}{d} t = x_0 + \frac{n}{d}(qd + r)$$

$$= x_0 + nq + \frac{n}{d} r$$

$$\equiv x_0 + \frac{n}{d} r \pmod{n}$$

with $x_0 + \left(\frac{n}{d}\right) r$ be one of our 'd' selected solution.

proved

Note: If $\gcd(a, n) = 1$ then linear congruence $ax \equiv b \pmod{n}$ has unique sol^n modulo n.

Q. Decide whether the following linear congruence is solvable. Find the incongruent solution if it is solvable.

$$8x \equiv 10 \pmod 6$$

⇒ The linear congruence $8x \equiv 10 \pmod 6$ is solvable because $\gcd(8, 6) = 2 = d$ which divides 10 ($d \mid b$). So there are two incongruence solutions of $8x \equiv 10 \pmod 6$

They are of the form $x = x_0 + \frac{n}{d} t$

for some integer 't'.

$$x = x_0 + \frac{n}{d} t = x_0 + \frac{6}{2} t = x_0 + 3t$$

Where x_0 is the particular solution of $8x \equiv 10 \pmod 6$ and $0 \leq t \leq 2$

i.e $t = 0, 1$.

By the trial and error. $x_0 = 2$

So $x = 2 + 3t$

$x = 2 + 3 \cdot 0 = 2$

$x = 2 + 3 \cdot 1 = 5$

Hence two incongruence sol^{ns} are 2 and 5.

H(4) Problem $12x \equiv 18 \pmod 6$

Comparing; $ax \equiv b \pmod n$

$\gcd(a,n) = d =$

$\gcd(12,6) = 6 = d$

$d \mid b = 6 \mid 18$

So above congruence is solvable.

The solution is of the form

$$x = x_0 + \frac{n}{d} t$$

$$x = x_0 + \frac{6}{6} t = x_0 + t$$

$$0 \le t < d$$

$$0 \le t < 6$$

$$t = 0, 1, 2, 3, 4, 5.$$

By trial and error; $x_0 = 2$

$$x = 2 + t$$

$x = 2 \quad (t = 0, 1, 2, 3, 4, 5)$

$x = 3, 4, 5, 6, 7$

Theorem The linear congruence $ax \equiv b \pmod{n}$ has a solution iff $d \mid b$ where $d = \gcd(a,n)$. If $d \mid b$ then it has 'd' mutually incongruent solution modulo n.

Proof: We have $ax \equiv b \pmod{n}$ has a soln

Say x_0

$$ax_0 \equiv b \pmod{n}$$

$$n \mid ax_0 - b$$

$$ax_0 - b = ny_0$$

$$ax_0 - ny_0 = b$$

It is of the form ~~line~~ Diophantine eqn $ax - ny = b$ has a set of soln x_0 and y_0.

$$\Leftrightarrow d \mid b \text{ where } d = \gcd(a,n)$$

Hence linear congruence $ax \equiv b \pmod{n}$ has a soln iff $d \mid b$ with $d = \gcd(a,n)$

Again let $d|b$ then we have

$ax \equiv b \pmod{n}$ is solvable i.e.

$ax - ny = b$ is solvable. Let x_0 and y_0 be the particular set of solⁿ then

$$x = x_0 + \frac{n}{d} t \ \& \ y = y_0 + \frac{a}{d} t$$

Then by taking

$$t = 0, 1, 2, \ldots, d-1$$

then solⁿs are

$$x = x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d},\ \ldots,\ x_0 + \frac{(d-1)n}{d}$$

(a) we first show that these integers are incongruent solⁿ in modulo n.

For this if possible let

$$x_0 + \frac{n}{d} t_i \equiv x_0 + \frac{n}{d} t_j \pmod{n}$$

with $0 \le t_i < t_j \le d-1$

$$\Rightarrow \frac{n}{d} t_i \equiv \frac{n}{d} t_j \pmod{n}$$

$$\Rightarrow t_i \equiv t_j \pmod{n}$$

$$\Rightarrow d \mid t_i - t_j$$

which contradicts that $t_j - t_i \leq d$

Hence the integers $x_0, x_0 + \frac{n}{d} t,$ $\ldots, x_0 + \frac{(d-1)n}{d}$ is incongruent modulo n.

(b) Now we show any sol^n $x_0 + \frac{n}{d} t$, $t > d$ is congruent to modulo n to one of the integers $x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots$

$$x_0 + \frac{(d-1)}{d} n.$$

Since $t > d$ then by division algorithm $t = qd + r$ with

$$0 \leq r < d.$$

So, $x = x_0 + \frac{n}{d} t = x_0 + \frac{n}{d}(qd + r)$

$$x = x_0 + nq + \frac{n}{d} r$$

$$\cancel{x - nq = x_0} + \frac{n}{d} r$$

$$x - \left(nq + \frac{n}{d} r\right) = nq$$

$$\Rightarrow n \mid x - \left(nq + \frac{n}{d} r\right)$$

$$\Rightarrow x \equiv$$

$$x - \left(x_0 + \frac{n}{d} r\right) = \cancel{00}.nq$$

$$n \mid x - \left(x_0 + \frac{n}{d} r\right)$$

$$\Rightarrow x \equiv x_0 + \frac{n}{d} r \pmod{n}$$

where $x_0 + \frac{n}{d} r$ is one of the integers $x_0, x_0 + \frac{n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$;

So, $x = x_0 + \frac{n}{d} t = x_0 + \frac{n}{d}(qd + r)$

$$x = x_0 + nq + \frac{n}{d} r$$

$$x - nq = x_0 + \frac{n}{d} r$$

$$x - \left(nq + \frac{n}{d} r\right) = nq.$$

$$\Rightarrow n \mid x - \left(nq + \frac{n}{d} r\right)$$

$$\Rightarrow x \equiv$$

$$x - \left(x_0 + \frac{n}{d} r\right) = nq$$

$$n \mid x - \left(x_0 + \frac{n}{d} r\right)$$

$$\Rightarrow x \equiv x_0 + \frac{n}{d} r \pmod{n}$$

where $x_0 + \frac{n}{d} r$ is one of the integers $x_0, x_0 + \frac{n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$.

with $r < d$.

Chinese Remaider Theorem

No.

Let $m_1, m_2, \ldots, m_r$ be a collection of pairwise relatively prime integers. Then the system of simultaneous Congruence are;

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_3 \pmod{m_3}$$

$$\text{------}$$

$$x \equiv a_r \pmod{m_r}$$

has a unique solution modulo $M = m_1 \cdot m_2 \cdots m_r$ for any integers ~~$m_1, m_2, \ldots$~~ m_r, $a_1, a_2, \ldots a_r$

Or

Suppose that $m_1, m_2, \ldots, m_r$ are pairwise relatively prime positive integers, and let $a_1, a_2, \ldots a_r$ be integers. Then the system of Congruence

$x \equiv a_i \pmod{m_i}$ for $1 \leq i \leq r$ has a unique solution modulo

$M = m_1 \cdot m_2 \cdots m_r$ which is given by;

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r \pmod{M}$$

Where; $M_i = \dfrac{M}{m_i}$

and $y_i \equiv (M_i)^{-1} \pmod{m_i}$ for $1 \leq i \leq r$

<u>Proof</u>

Note that $\gcd(M_i, m_i) = 1$ for $1 \leq i \leq r$

Now notice that $M_i y_i \equiv 1 \pmod{m_i}$

Then we have $a_i M_i y_i \equiv a_i \pmod{m_i}$ for $1 \leq i \leq r$

On the otherhand $a_i M_i y_i \equiv 0 \pmod{m_j}$ if $j \neq i$ (Since $m_j \mid M_i$ in this case)

Date. No.

This we see that

$$x \equiv a_i \pmod{m_i} \text{ for } 1 \le i \le r$$

If x_0 and x_1 were sol^ns then we would have $x_0 - x_1 \equiv 0 \pmod{m_i}$ for all i.

$$\Rightarrow x_0 - x_1 \equiv 0 \pmod{M} \text{ i.e}$$

they are the same modulo M.

Example : Find the smallest multiple of 10 which has ~~a~~ remainder 2 when divided by 3 and remainder 3 when divided by 7.

$\Rightarrow$ we are looking for a number which satisfies the congruence

$x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{7}$

& $x \equiv 0 \pmod{2}$ multiple of 10

& $x \equiv 0 \pmod{5}$

Since 2, 3, 5, 7 all are relatively primes, the chinese remainder Th. tells us that there is a unique ~~number~~ modulo 210 $(2 \times 3 \times 5 \times 7)$

We know calculate M_i's & y_i's

$$M_2 = \frac{210}{2} = 105$$

$$M_2 y_2 \equiv 1 \pmod 2$$

$$105\, y_2 \equiv 1 \pmod 2$$

$$\Rightarrow 1\, y_2 \equiv 1 \pmod 2 \quad 2 / \underline{105} = 1$$

$$\Rightarrow y_2 \equiv 1$$

$$M_3 = \frac{210}{3} = 70$$

$$M_3 y_3 \equiv 1 \pmod 3$$

$$70\, y_3 \equiv 1 \pmod 3$$

$y_2 \equiv 1 \pmod 3$

$\boxed{y_2 \equiv 1}$

$M_5 = \frac{210}{5} = 42$

Now $M_5 y_5 \equiv 1 \pmod 5$

$42 y_5 \equiv 1 \pmod 5$

$2 \cdot y_5 \equiv 1 \pmod 5$

$2.3\, y_5 \equiv 3 \pmod 5$

$1\, y_5 \equiv 3 \pmod 5$

$\boxed{y_5 \equiv 3}$

$M_7 = \frac{210}{7} = 30$

$M_7 y_7 \equiv 1 \pmod 7$

$y_7 = 4$

Now:

multiple of 10

$$x \equiv 0\cdot(M_2 y_2) + 2\cdot(M_3 y_3) + 0(M_5 y_5) + 3(M_7 y_7)$$

multiple of 10

$$x \equiv 0 + 2\cdot 70\cdot 1 + 0 + 3\cdot 30\cdot 4$$

$$x \equiv 500 \pmod{210}$$

$$x \equiv 80 \pmod{210}$$

HW

Find all the integers x which leave remainder of 1, 2, 3, 4 when divided by 5, 7, 9, 11 respectively.

$$x \equiv 1 \pmod 5$$
$$x \equiv 2 \pmod 7$$
$$x \equiv 3 \pmod 9$$
$$x \equiv 4 \pmod{11}$$

Invertible (mod n)

If $\gcd(a, n) = 1$ then there exists an integer x such that $ax \equiv 1 \pmod{n}$ then a is said to be invertible and x is ~~said to be~~ called an inverse of 'a' modulo n and is denoted by a^{-1} i.e. $aa^{-1} \equiv 1 \pmod{n}$

If $a = a^{-1}$ then a is called self invertible.

For e.g. we have $\gcd(11, 8) = 1$ then there exists integer such that

$$11 \cdot 3 \equiv 1 \pmod{8}$$

and 3^{-1} is 11 in mod 8.

e.g. Q. $\gcd(7, 9) = 1$ find the inverse of 7 in modulo 9.

Q. We have $\gcd(10, 11) = 1$

Then there exists least integer 10 Such that $10 \cdot 10 \equiv 1 \pmod{11}$

So ~~10 is~~ The inverse of 10 is 10 itself in modulo 11 so 10 is self invertible

Theorem A positive integer 'a' is self invertible modulo p iff

$$a \equiv \pm 1 \pmod{p}$$

For eg by previous example 10 is self invertible in modulo 11.

then $10 \equiv -1 \pmod{11}$

Proof let the positive integer 'a' is self invertible in modulo p

$\Rightarrow a \cdot a^{-1} \equiv 1 \pmod{p}$

$\Rightarrow a \cdot a \equiv 1 \pmod p$

(Since a is inverse of itself)

$$a^2 \equiv 1 \pmod p$$

$$p \mid a^2 - 1$$

$$p \mid (a-1)(a+1)$$

either $p \mid a-1$ or $p \mid a+1$

$\Rightarrow a \equiv 1 \pmod p$ $\quad\downarrow$

$a \equiv -1 \pmod p$

$\Rightarrow a \equiv \pm 1 \pmod p$

Conversely suppose that

$$a \equiv \pm 1 \pmod p$$

Then either $a \equiv 1 \pmod p$

or $a \equiv -1 \pmod p$

Let $a \equiv 1 \pmod p$

$a \cdot a \equiv 1 \pmod p$

$a^2 \equiv 1 \pmod p$ (Since $a = 1$)

$a \cdot a \equiv 1 \pmod p$

$a = a^{-1}$

Again; $a \equiv -1 \pmod p$

$a \cdot a = -1 \cdot -1 \pmod p$

$a \cdot a = 1 \pmod p$ (Since $a = -1$)

$\therefore a \equiv a^{-1} \pmod p$

Hence a is self-invertible modulo p.

Date. No.

Note

There are exactly two self invertible residue modulo p they are 1 & p-1

$\Rightarrow$ we have a is self invertible modulo p so either

$$a \equiv 1 \pmod{p}$$

or $a \equiv -1 \pmod{p}$

These condition satisfies only if $a = 1$ or $a = p-1$

Example

→ for the modulo 5, 1 and $5-1=4$ are the self invertible modulo 5

$1 \cdot 1 \equiv 1 \pmod 5$

$4 \cdot 4 \equiv 1 \pmod 5$

For modulo 3, 1 and 2 are self invertible modulo 3

$1 \cdot 1 \equiv 1 \pmod 3$ $\quad 2 \cdot 2 \equiv 1 \pmod 3$

Creating foundation of Wilson Theorem.

Let us discuss following example

Let $p = 11$ $\quad (p-1)! = 1 \cdot 2 \cdot \text{-----} \cdot 9 \cdot 10$

$(10)! = 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9)(7 \cdot 8) \cdot 10$

$\quad = 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 10 \pmod{11}$

$(10)! \equiv 10 \pmod{11}$

$(10!) \equiv -1 \pmod{11}$

$\therefore (p-1)! \equiv -1 \pmod p$

In this example we arranged $\frac{p-3}{2} = 4$ pairs.

Wilson Theorem

If p is a prime then

$$(p-1)! \equiv -1 \pmod{p}$$

Proof: If $p = 2$, then $(p-1)! = 1$

Then. $1 \equiv -1 \pmod{2}$

So assume $p > 2$; as we know that 1 and $p-1$ are self invertible modulo p.

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1)$$

Now arranging remaining $(p-3)$ factors other than 1 and $p-1$ into $\frac{p-3}{2}$ pairs of inverse with each other

Thus;

$$2 \cdot 3 \cdot 4 \cdots p-2 = 1 \cdot 1 \cdots 1 \pmod{p}$$
$$\equiv 1 \pmod{p}$$

Now,

Date. No.

$$(p-1)! = 1\cdot\left(2\cdot3 \ldots (p-2)\right)\cdot(p-1)$$

$$\equiv 1.\,(p-1).\,1 \pmod p$$

$$(p-1)! \equiv (p-1) \pmod p$$

$$(p-1)! \equiv -1 \pmod p$$

Example: Verify Wilson Theorem for the prime $p=13$.

Application of Wilson Theorem

Determine x in the congruence

$$x \equiv 10! \pmod{13}$$

$\Rightarrow$ By Wilson Th.

$$(13-1)! \equiv -1 \pmod{13}$$

$$12! \equiv -1 \pmod{13}$$

$$\underline{12\cdot11}\cdot10! \equiv -1 \pmod{13}$$

$$\downarrow$$

$$2\cdot10! \equiv -1 \pmod{13}$$

$$2 \cdot 10! \equiv -1 \pmod{13}$$

$$7 \cdot 2 \cdot 10! \equiv -7 \pmod{13}$$

$$1 \cdot 10! \equiv -7 \pmod{13}$$

$$10! \equiv 6 \pmod{13}.$$

$$x_0 \equiv 6 \pmod{13}$$

<u>Example</u> Determine x in the Congruence $x \equiv 8! \pmod{11}$

Q. Find the remainder when $9!$ is divided by 11.

$$\Rightarrow \quad 9! \equiv x \pmod{11}$$

By Wilson Th.

$$10! \equiv -1 \pmod{11}$$

$$\Rightarrow 10 \cdot 9! \equiv -1 \pmod{11}$$

$$(-1) \cdot 9! \equiv -1 \pmod{11}$$

$$(-1) \cdot (-1) \cdot 9! \equiv (-1) \cdot (-1) \pmod{11}$$

$$9! \equiv 1 \pmod{11}$$

Comparing it with

$$9! \equiv x \pmod{11}$$

$\boxed{x = 1}$ remainder 1

Example find remainder when 13! is divided by 17.

$\Rightarrow \quad 13! \equiv x \pmod{17}$

Converse of Wilson Theorem

If n is positive integer such that $(n-1)! \equiv -1 \pmod{n}$, then n is a prime
$\Rightarrow \quad n \mid ((n-1)! + 1)$

Proof: If possible let us assume that n is not a prime so is a composite

Then.

$$n = a \cdot b \text{ with } 1 < a ; b < n$$

Since $a \mid n$ and $n \mid (n-1)! + 1$ given

so; $a \mid \{(n-1)! + 1\}$ —— (A)

Again since $1 < a < n$ so 'a' must be one of the integer from 2 to n-1 implies

$a \mid (n-1)!$ —— (B)

From (A) & (B) $a \mid \{(n-1)! + 1\}$ Date $(n-1)!$

$\therefore$ Implies $a \mid 1$ which is contradiction so n must be prime.

Problem let a be a solution of the congruence $x^2 \equiv 1 \pmod{m}$. Then show that $m-a$ is also the solution of $x^2 \equiv 1 \pmod{m}$

Proof:

Since we have given that 'a' be a solution of ~~cog~~ congruence $x^2 \equiv 1 \pmod{m}$

so $a^2 \equiv 1 \pmod{m}$

Now, $(m-a)^2 = m^2 - 2ma + a^2 \equiv a^2 \pmod{m}$

$\equiv 1 \pmod{m}$

Implies $(m-a)^2 \equiv 1 \pmod{m}$

Hence, $(m-a)$ is the solution of the congruence $x^2 \equiv 1 \pmod{m}$

Fermats Factorization Theorem

For a given number(n) fermats factorization ~~theorem~~ method looks for integers x and y such that $n = x^2 - y^2$

Then; $n = (x+y)(x-y)$

and n is factored.

Every positive odd integer can be represented in the form of $n = x^2 - y^2$ which gives us $n = ab$ with $a > b$

and $a = (x+y)$ $b = (x-y)$

adding $2x = a+b$

$2y = a-b$

solving $x = \frac{a+b}{2}$ $y = \frac{a-b}{2}$

Therefore; $x^2 - y^2 = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$

$$x^2 - y^2 = ab = n$$

i.e. $x^2 - n = y^2$

Let us determine smallest ($k \ge 0$) for which $k^2 \ge n$ i.e. $k \ge \sqrt{n}$

Then we look successively at the numbers $k^2 - n$, $(k+1)^2 - n^2$, $(k+2)^2 - n^a$

until the value $m \ge \sqrt{n}$ makes

$m^2 - n$ is a perfect square

i.e. $m^2 - n = b^2$ then such value of m is known as 'a' and 'a+b' and (a-b) are the factors of n.

for instance let $n = 51$.

let us take smallest k such that $k^2 \ge n$ i.e. $k \ge \sqrt{n}$ so $k = 8$

$k = 8$; $k^2 - n = 13$ which is not perfect square so try for $k+1$

$k+1 = 9$; $(k+1)^2 - n = 30$ which is not perfect square so try for $k+2$

$k+2 = 10$; $(k+2)^2 - n = 49$ which is perfect square.

The factors are $10+7$ and $10-7$
17 & 3

Because; $n = (k+2)^2 - 49$
$= (k+2)^2 - 7^2$
$= 10^2 - 7^2$
$= (10-7)(10+7)$
$\boxed{n = 3 \cdot 17}$

q. Factorize 63.

Factorize 45

Lemma Let p be a prime and 'a' be any integer such that $p \nmid a$. Then least residue of the integers $a, 2a, 3a \ldots (p-1)a$ modulo p are the permutation of the integers. $1, 2, 3 \ldots (p-1)$

Proof: Let $1, 2, 3 \ldots p-1$ are possible remainders in modulo p.

Now proof of the theorem consists of two parts

(i) $ia \not\equiv 0 \pmod p$ for $1 \le i \le p-1$

(ii) The least residue of ia & $ja \pmod p$ are distinct for $i \neq j$.

First if possible let $ia \equiv 0 \pmod{p}$

then $p \mid ia$

And since $p \nmid a$ so $p \mid i$

But since $1 \leq i \leq p-1$ so $p \mid i$

is impossible. Hence $ia \not\equiv 0 \pmod{p}$

(i.e. remainder can not be 0, means remainder is any one of $1, 2, 3, \ldots p-1$)

Secondly we need to show no two of $a, 2a, 3a \ldots (p-1)a$ in modulo p are congruent

If possible let $ia \equiv ja \pmod{p}$ then we need to show $i = j$

i.e. $i \equiv j \pmod{p}$

Since both i and j are $\leq p-1$
So $i = j$

Hence least residue ~~integers~~ of the integers $a, 2a, 3a, \ldots (p-1)a$ modulo p are the permutations of integers $1, 2, 3 \ldots (p-1)$

Fermat's Little Theorem

Date. No.

Let p be a prime and 'a' be any integer such that $p \nmid a$ Then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof: Let p be a prime and 'a' be any integer

We know that the least residue of $a, 2a, 3a, \ldots, (p-1)a$ in modulo p are the permutation of the integers $1, 2, 3, \ldots, p-1$

i.e. $a, 2a, 3a, \ldots (p-1)a = 1.2.3 \ldots (p-1) \pmod{p}$

$$(p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$$

proved

Note: Let p be a prime and a be any integer then $a^{p} \equiv a \pmod{p}$

$\Rightarrow$ Here the proof consists of two parts as $p \nmid a$ or $p \mid a$.

If $p \nmid a$ then by Fermat's little theorem

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a \cdot a^{p-1} \equiv a \pmod{p}$$

$$a^{p} \equiv a \pmod{p}$$

If $p \mid a$ then $a \equiv 0 \pmod{p}$

$$\Rightarrow a^p \equiv 0 \pmod{p}$$

And $a \equiv 0 \pmod{p} \Rightarrow 0 \equiv a \pmod{p}$

combining these two

$$a^p \equiv a \pmod{p}$$

<u>Note II</u> If p and q are distinct primes such that $a^p \equiv a \pmod{p}$ and $a^q \equiv a \pmod{p}$ then

$$a^{pq} \equiv a \pmod{pq}$$

$\Rightarrow$ we have

$$a^{pq} \equiv (a^p)^q \equiv a^p (\text{mod}$$

Show by fermats little Th

Date. No.

$$2^{341} \equiv 2 \pmod{341}$$

$\Rightarrow$ $341 = 11 \cdot 31$ here 11 and 31 are two distinct primes.

Since $2 \nmid 11$ then by fermats little Th.

$$2^{10} \equiv 1 \pmod{11}$$

Now, $2^{341} = 2^{11 \cdot 31}$

$$= 2^{(10+1)31}$$

$$= (2^{10})^{31} \cdot 2^{31}$$

$$= \cancel{2^{31} \cdot 2}$$

$$= (2^{10})^{31} \cdot 2^{10 \cdot 3 + 1}$$

$$= (2^{10})^{31} \cdot (2^{10})^{3} \cdot 2$$

$$\equiv 1^{31} \cdot 1^{3} \cdot 2 \pmod{11}$$

$$2^{341} \equiv 2 \pmod{11} \longleftarrow (i)$$

Date. No.

Again; $2 \nmid 31$ by fermats little

Th. $2^{30} \equiv 1 \pmod{31}$

$$2^{341} = 2^{31 \cdot 11}$$

$$= \left(2^{31}\right)^{11}$$

$$= \left(2^{30+1}\right)^{11}$$

$$= \left(2^{30}\right)^{11} \cdot 2^{10 \cdot 1 + 1}$$

$$= \left(2^{30}\right)^{11} \cdot \left(2^{5}\right)^{2} 2^{1}$$

$$= \left(2^{30}\right)^{11} \cdot \left(2^{5}\right)^{2} \cdot 2^{1} \pmod{31}$$

$$\equiv 1 \cdot 1^{2} \cdot 2$$

$$2^{341} \equiv 2 \pmod{31} \longrightarrow (2)$$

Combining (1) & (2)

$$2^{341} \equiv 2 \pmod{11 \cdot 31}.$$

Divisibility Theorem for 9.

<u>divisibility test of 9</u>

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

be a positive integer with $0 \le a_k \le 9$

and $S = a_0 + a_1 + \dots + a_m$ then

$9 \mid N$ iff $9 \mid S$

<u>Proof:</u> We have $p(x) = \sum_{k=0}^{m} a_k x^k$ be a polynomial function with integral coeff.. we have

$P(10) = N$ & $P(1) = S$

Now;

$10 \equiv 1 \pmod 9$

$\Rightarrow p(10) \equiv P(1) \pmod 9$

$N \equiv S \pmod 9$

$N \equiv 0 \pmod 9$ iff $S \equiv 0 \pmod 9$

$\Rightarrow 9 \mid N$ iff $9 \mid S$.

Q. Test whether 3458976547896 is divisible by 9 or not.

$\Rightarrow$ we have

$S = 3+4+5+8+9+7+6+5+4+7+8+9+6 = $

So $9 | S$ hence ——— is divisible by 9.

divisibility Test of 11

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

be a positive integer with $0 \le a_k \le 9$

~~and $S = a_0 + a_1 + \cdots + a_m$~~

and $T = a_0 - a_1 + a_2 - \cdots + (-1)^n a_m$

then $11 | N$ iff $11 | T$

$\Rightarrow$ we have $p(x) = \sum_{k=0}^{m} a_k x^k$ be a polynomial fx^n with the integral coeff. we have

$P(10) = N$ & $P(-1) = T$

Now, $10 \equiv -1 \pmod{11}$

$P(10) \equiv P(-1) \pmod{11}$

$N \equiv T \pmod{11}$

$N \equiv 0 \pmod{11}$ iff

$T \equiv 0 \pmod{11}$

$\Rightarrow$ $11 | N$ iff $11 | S$

e.g. Test whether No 15802367454575 is divisible by 11 or not.

$T = 1-5+8-0+2-3+6-7+4-5+4-5+7-5$

$= 0$

So $11 | T$

Hence $11 | N$.

divisibility test of 2

Let $N = a_m b^m + a_{m-1} b^{m-1} + \dots + a_2 b^2 + a_1 b^1 + a_0$ be a positive integer with $0 \le a_k \le 9$ is divisible by 2 iff it's unit digit is 0, 2, 4, 6, 8

divisibility Test of 3

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

be a positive integer with $0 \le a_k \le 9$ is divisible by 3 if sum of digitals is divisible by 3.

divisibility test of 5

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

be a positive integer with $0 \le a_k \le 9$ is divisible by 5 iff its unit

digit is 0 or 5

divisibility test of 4.

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

be a positive integer with $0 \le a_k \le 9$

(i) is divisible by 4 iff the number formed by it's ~~&~~ ten and unit digit is divisible by 4.

Divisibility test of 8

Date. No.

Let $N = a_m b^m + a_{m-1} b^{m-1} + \dots + a_2 b^2 + a_1 b^1 + a_0$ be a positive integer with $0 \le a_k \le 9$ is divisible by 8 iff the number formed by it's hundreds, tens & unit digit is divisible by 8

divisibility test of 10

Let $N = a_m b^m + a_{m-1} b^{m-1} + \dots + a_2 b^2 + a_1 b^1 + a_0$ be a positive integer with $0 \le a_k \le 9$ is divisible by 10 iff it's unit digit is 0

Unit 5 Numbers theoretic functions [11]

The functions τ and φ; Basic properties of τ and σ; The Mobius μ function; Eulers phi function; Basic properties of φ function; Multiplicative nature of τ, σ and φ function, generalized form of Fermats theorem (Eulers Theorem)

Number theoretic function (Arithmetic function)

Any function whose domain is the set of positive integers is said to be number-theoretic function or arithmetic function.

Tau and Sigma function

Let n be the positive integer then $\tau(n)$ is tau function which denotes the number of positive divisors of n. and $\sigma(n)$ is sigma function which denotes the sum of the divisors of n.

Ex. find the values of $\tau(12)$ and $\sigma(12)$

$\Rightarrow$ We have the divisers of $12 = 1, 2, 3, 4, 6, 12$

So No. of positive divisers of 12 are 6.

$$\tau(12) = 6$$

Again the sum of divisors =

$1+2+3+4+6+12=28$

$\sigma(12) = 28$

Multiplicative function

A number theoretic function 'f' is called multiplicative if $f(mn) = f(m) \cdot f(n)$ with $\gcd(m,n) = 1$.

Euler's Phi function

Let n be a positive integer then Euler Phi function $\phi(n)$ denotes the number of positive integers $\leq n$ and relatively prime to n

Eg. → If $n=1$, $\phi(n) = 1$

→ If $n = 2$ then $\phi(n) = 1$ Because

$\gcd(2,1) = 1$ and no any other digit ≤ 2 which is relatively prime to 2.

→ If $n=3$ then $\phi(3) = 2$ because $\gcd(3,1) = 1$ $\gcd(3,2) = 1$ so there are two positive integers ≤ 3 and relatively prime to 3.

If $n = 4$ then $\phi(4) = 2$ because

$\gcd(4,1) = 1$, $\gcd(4,3) = 1$

Theorem: A positive integer p is prime iff $\phi(p) = p-1$

$\Rightarrow$ Let p be a prime we have $\gcd(1,p) = 1$

$\gcd(2,p) = 1$, $\gcd(3,p) = 1$, ... $\gcd(p-1,p) = 1$

$\gcd(p,p) = p \neq 1$. Hence there are $(p-1)$ number of positive integers not greater than p which are relatively prime to p.

Hence $\phi(p) = p-1$

Conversely, suppose that $\phi(p) = p-1$

If possible let p is not a prime then there exists d such that $d \mid p$ with $1 < d < p$. As we know that there are exactly $(p-1)$ positive integers less than p and d is also one of them with $\gcd(p,d) \neq 1$

which implies $\phi(p) < (p-1)$ which is contradiction hence p is a prime.

$\boxed{\text{Lemma}}$ Let n be a positive integer and 'a' be any integer relatively prime to n. Let $r_1, r_2, \dots$ ~~$r_{phi(\phi}$~~ $r_{\phi(n)}$ be the integers less than or equal to n and relatively prime to n then the least residue of the integers $ar_1, ar_2, ar_3, \dots a.r_{\phi(n)}$ in the modulo n are a permutation of the integers $r_1, r_2, \dots r_{\phi(n)}$.

Eulers Theorem

Date. No.

Let n be a positive integer and 'a' be any integer with $\gcd(a,n)=1$ then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Proof: From the lemma the least residue of the integers $ar_1, ar_2, \ldots ar_{\phi(n)}$ in modulo (n) are a permutation of the integers $r_1, r_2, \ldots r_{\phi(n)}$.

So, ~~$ar_1,$~~

$$ar_1 \cdot ar_2 \cdot \ldots ar_{\phi(n)} \equiv r_1 \cdot r_2 \ldots r_{\phi(n)} \pmod{n}$$

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

proved

Theorem: If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is a prime factorization of $n > 1$ then the positive divisors of n are precisely those integers d of the ferm;

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

where; $0 \leq a_i \leq k_i \quad (i = 1, 2, \cdots r)$

Proof: The divisor $d = 1$ is obtained when $a_1 = a_2 = \cdots = a_r = 0$

and n itself occurs when
$a_1 = k_1, \; a_2 = k_2, \cdots \; a_r = k_r$

Suppose that d divides 'n' say
$$n = d \cdot d'$$
where; $d > 1 \quad d' > 1$

Express both d & d' as the products of primes:

$$d = q_1 q_2, \cdots q_s$$
$$d' = t_1 t_2 \cdots t_u$$

With q_i, t_j prime then.

Date. No.

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

$(\because n = dd')$

are two prime factorization of positive integer (n). By uniqueness of the prime factorization each prime q_i must be one of p_j. Collecting the equal primes into a single integral power

$$d = q_1 q_2, \cdots q_s = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where the possibility that $a_i = 0$ is allowed.

Conversly every ~~integer~~ number

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \quad (0 \le a_i \le k_i)$$

turns out to be divisor of n.

We can write;

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

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

$$n = d\,d'$$

with $d' = p_1^{k_1-a_1} \cdot p_2^{k_2-a_2} \cdots p_r^{k_r-a_r}$

& $k_i - a_i \geq 0$ for each i.

Then $d' > 0$ & $d \mid n$

#

<u>Theorem</u> If p is a prime and $k > 0$ then

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

<u>Proof:</u> We know that $\gcd(n, p^k) = 1$

iff $p \nmid n$. There are p^{k-1} integers between

1 and p^k divisible by p namely;

$p, 2p, 3p, \cdots, (p^{k-1})p$

Date. No.

Thus the set $\{1, 2, \cdots p^k\}$ Contains exactly $p^k - p^{k-1}$ integers that are relatively prime to p^k. So by definition of Euler phi function

$$\phi(p^k) = p^k - p^{k-1}$$

for e.g. $\phi(9) = \phi(3^2) = 3^2 - 3 = 6$

The six integers less than and relatively prime to 9 being 1, 2, 3, 4, 5, 6, 7, 8.

Theorem : For $n > 2$; $\phi(n)$ is an even integer.

Proof:

First assume that n is a power of 2 let $n = 2^k$ with $k \geq 2$

By Theorem $\phi(p^k) = p^k - p^{k-1}$

$$\phi(n) = \phi(2^k) = 2^k\left(1 - \frac{1}{2}\right) = 2^{k-1}$$

which is an even integer.

If n does not happen to be power of 2, then it is divisible by an odd prime p; we may write n as

$$n = p^k \cdot m$$

where $k \geq 1$ and $\gcd(p^k, m) = 1$

By multiplicative nature of phi-function

$$\phi(n) = \phi(p^k \cdot m)$$

$$= \phi(p^k) \cdot \phi(m)$$

$$\phi(n) = p^{k-1}(p-1)\,\phi(m)$$

which is again even because $2 \mid (p-1)$.

Eulers Theorem

From the Fermats theorem;

$$a^{p-1} \equiv 1 \pmod{p}$$

generalized fermats theorem is;

If $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$

For eg. $n = 30$ $a = 11$ Date. No.

$\phi(30) = 8$

$11^{\phi(30)} \equiv 11^{8} \equiv (11^2)^4 \equiv (121)^4 \equiv 1^4 = 1 \pmod{30}$

Lemma : Let $n > 1$ and $\gcd(a, n) = 1$

If $a_1, a_2, \dots, a_{\phi(n)}$ are the positive integers less than n and relatively prime to (n) then $aa_1, aa_2, \dots, aa_{\phi(n)}$ are congruent modulo n to

$a_1, a_2, \dots, a_{\phi(n)}$

Theorem : If $n \geq 1$ and ~~gc~~ $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$

$\Rightarrow$ Let $a_1, a_2, \dots, a_{\phi(n)}$ be the positive integers less than (n) that are relatively prime to (n)

Now,

Date. No.

$$aa_1 \equiv a_1' \pmod n$$

$$aa_2 \equiv a_2' \pmod n$$

$$aa_{\phi(n)} \equiv a'_{\phi(n)} \pmod n$$

Multiplying

$$(aa_1)(aa_2) \cdots (aa_{\phi(n)}) \equiv$$

$$a_1' a_2' \cdots a'_{\phi(n)} \pmod n$$

$$a^{\phi(n)} \, a_1 a_2 \cdots a_{\phi(n)} \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod n$$

Since $\gcd(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$

dividing both sides by $a_1 a_2 \cdots a_{\phi(n)}$

$$\boxed{a^{\phi(n)} \equiv 1 \pmod n}$$

Chapter 6 Quadratic Reciprocity Law

- Primitive roots of an integer
- Quadratic residues & non-residues
- Eulers criterion.
- The Legendre symbol & their properties
- Gauss lemma & related theorem
- Quadratic reciprocity law.

Definition: Let $n>1$ and $\gcd(a,n)=1$. The order of 'a' modulo n (the exponent to which 'a' belongs modulo n) is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$

Theorem: Let the integer 'a' have order k modulo n. Then $a^h \equiv 1 \pmod{n}$ if and only if $k \mid h$ in particular $k \mid \phi(n)$.

Date. No.

$\Rightarrow$ Suppose $k \mid h$

$$\Rightarrow h = jk$$

for some integer ~~j~~ j.

As $a^k \equiv 1 \pmod{n}$

$$(a^k)^j \equiv 1^j \pmod{n}$$

$$a^h \equiv 1 \pmod{n}$$

Conversely let h be any positive integer satisfying $a^h \equiv 1 \pmod{n}$

~~The implication of which is~~

~~$a^r \equiv 1 \pmod{n}$~~

By division algorithm

$$h = qk + r \quad \text{where } 0 \le r < k$$

Consequently,

$$a^h = a^{qk+r} = (a^k)^q a^r$$

By hypothesis; both

$$a^h \equiv 1 \pmod{n} \text{ and}$$

$$a^k \equiv 1 \pmod{n}$$

the implication of which is

$$a^r \equiv 1 \pmod{n}$$

Because $0 \leq r < k$

we end with $r = 0$ otherwise the choice of k as the smallest positive integer such that

$a^k \equiv 1 \pmod{n}$ is contradicted

Hence; $h = qk$ and $k \mid h$.

Theorem : If the integer 'a' has order k modulo n then

$$a^i \equiv a^j \pmod n$$ if and only if $i \equiv j \pmod k$

Proof: First suppose that

$$a^i \equiv a^j \pmod n.$$

where $i \geq j$

because 'a' is relatively prime to n we may cancel a power of a to obtain $a^{i-j} \equiv 1 \pmod n$

According to previous Th. the congruence holds if $k \mid i-j$ which is just another way of saying that $i \equiv j \pmod k$

Conversely let $i \equiv j \pmod{k}$

Then we have $i = j + qk$

for some integer q.

By definition of k.

so that $a^k \equiv 1 \pmod{n}$

$$a^i \equiv a^{j+qk} \equiv a^j (a^k)^q$$

$$\equiv a^j \pmod{n}$$

which is desired

Conclusion.

<u>Theorem</u> If the integer 'a' has order k modulo n and $h > 0$ then a^h has order $\dfrac{k}{\gcd(h,k)}$ modulo n.

$\Rightarrow$ Let $d = \gcd(h,k)$

Then we may write $h = h_1 d$

and $k = k_1 d$

with $\gcd(h_1, k_1) = 1$

$$(a^h)^{k_1} = (a^{h_1 d})^{k/d} = (a^k)^{h_1} \equiv 1 \pmod{n}$$

If a^h is assumed to have order r modulo n Then $r \mid k_1$

On the other hand because a has order k modulo n the congruence,

$$a^{hr} \equiv (a^h)^r \equiv 1 \pmod{n}$$

indicates that $k \mid hr$ in other words $k_1 d \mid h_1 d r$

or $k_1 \mid h_1 r$

But $\gcd(k_1, h_1) = 1$ and therefore

$k_1 \mid r$. Then shows

$$r = k_1 = \frac{k}{d} = \frac{k}{\gcd(h, k)}$$

Corollary Let a have order k modulo n. Then a^h also has order k if and only if $\gcd(h, k) = 1$

definition If $\gcd(a, n) = 1$ and a is of order $\phi(n)$ modulo n then a is a primitive root of the integer.

$\Rightarrow$ 'n' has a ~~a~~ a primitive root if $a^{\phi(n)} \equiv 1 \pmod{n}$ but $a^k \not\equiv 1 \pmod{n}$ for all positive integers $k < \phi(n)$.

Corollary Let a have order k modulo n. Then a^h also has order k if and only if $\gcd(h, k) = 1$

definition If $\gcd(a, n) = 1$ and a is of order $\phi(n)$ modulo n then a is a primitive root of the integer.

$\Rightarrow$ 'n' has ~~a~~ a primitive root if $a^{\phi(n)} \equiv 1 \pmod{n}$ but $a^k \not\equiv 1 \pmod{n}$ for all positive integers $k < \phi(n)$.

#

Date. No.

Quadratic Reciprocity law deals with the solvability of a quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad (1)$$

where p is odd prime and

$$a \not\equiv 0 \pmod{p}$$

that is $\gcd(a, p) = 1$

The supposition that p is an odd prime implies that

$$\gcd(4a, p) = 1$$

Thus above congruence (1) is equivalent to;

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}$$

$$4a.(ax^2 + bx + c) \equiv (2ax + b)^2 - (b^2 - 4ac) \pmod{p}$$

The last written quadratic congruence can be written as:

$$(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}$$

Now put $y = 2ax + b$

$$d = b^2 - 4ac$$

$$\Rightarrow \boxed{y^2 \equiv d \pmod{p}}$$

For e.g. $5x^2 - 6x + 2 \equiv 0 \pmod{13}$

$ax^2 + bx + c \equiv 0 \pmod{p}$

$\cancel{y^2 \equiv d}$ (mod

$$y = 2ax + b = 2.5.x + (-6)$$

$$= 10x - 6$$

$$= 2(5x - 3)$$

$$d = b^2 - 4ac = (-6)^2 - 4.5.2$$

$$= 36 - 40$$

$$= -4$$

$$y^2 \equiv -4 \pmod{13}$$

$$y^2 = 9 \pmod{13}$$

$y = 3$; $y = 10$

Again, $10x - 6 \equiv 3 \pmod{13}$

$$10x \equiv 9 \pmod{13}$$

Date. No.

$10x \equiv 9 \pmod{13}$

$\Rightarrow x \equiv 10, 12 \pmod{13}$

$x^2 \equiv a \pmod{p}$

$\gcd(a, p) = 1$

Definition : Let p be an odd prime and $\gcd(a, p) = 1$ If quadratic Congruence $x^2 \equiv a \pmod{p}$ has a Solution then 'a' is said to be a quadratic residue of p otherwise 'a' is called quadratic non residue of p.

Note: If $a \equiv b \pmod{p}$ then a is a quadratic residue of p if & only if b is quadratic residue of p.

For eg Let $p=13$ To find out how many of integers $1, 2, 3, \dots, 12$ are quadratic residue of 13. we must know which of the congruence ~~$x^2 \equiv b$~~

$$x^2 \equiv a \pmod{13}$$

are solvable when 'a' runs through a set $\{1, 2, \dots, 12\}$ modulo 13.

$1^2 \equiv 12^2 \equiv 1$

$2^2 \equiv 11^2 \equiv 4$

$3^2 \equiv 10^2 \equiv 9$

$4^2 \equiv 9^2 \equiv 3$

$5^2 \equiv 8^2 \equiv 12$

$6^2 \equiv 7^2 \equiv 10$.

Quadratic residue of 13 are

1, 3, 4, 9, 10, 12

& non residue

2, 5, 6, 7, 8, 11.

Eulers Criterion

Date. No.

Let p be an odd prime and $\gcd(a, p) = 1$. Then a is a quadratic residue of p if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

<u>Proof:</u> Suppose that a is an quadratic residue of p so that

$$x^2 \equiv a \pmod{p}$$

This admits a solution call it as x_1

Because $\gcd(a, p) = 1$

evidently $\gcd(x_1, p) = 1$

(#) Quadratic Residue

'a' is quadratic residue of p :

If $x^2 \equiv a \pmod{p}$ is solvable,

$\gcd(a, p) = 1$; p - odd prime.

then we say 'a' is quadratic residue of p.

Eulers Criterion: Let p be an odd prime and $\gcd(a, p) = 1$ Then a is a quadratic residue of p iff

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

Example: $p = 13$ $a = 2$

$$2^{(13-1)/2} = 2^6 = 64 \equiv 12 \equiv -1 \pmod{13}$$

does not satisfy.

So 2 is not quadratic residue ~~modulo~~ 13.

let $a = 3$

$$3^{(13-1)/2} = 3^6 \equiv (3^3)^2 \equiv 27^2 \equiv 1 \pmod{13}$$

So 3 is quadratic residue of 13

$\Rightarrow$ Given a is a quadratic residue of p. by defn.

$x^2 \equiv a \pmod p$, has a soln

Call solution as x_1.

(1) $x_1^2 \equiv a \pmod p$

To <u>prove:</u>

Noting $\gcd(a, p) = 1$

$\gcd(x_1, p) = 1$

If $\gcd(x_1, p) \neq 1$ $p \mid x_1 \Rightarrow x_1 \equiv 0 \pmod p$

$\Rightarrow x_1^2 \equiv 0 \pmod p$

So if $\Rightarrow a \equiv 0 \pmod p$

so $\gcd(a,p) \neq 1$ $\quad$ $\gcd(a,p) \neq 1$

contradiction.

Hence $\gcd(x_1, p) = 1$

By fermat's Theorem if $\gcd(x_1, p) = 1$

$$x_1^{p-1} \equiv 1 \pmod p$$

$$(x_1^2)^{\frac{p-1}{2}} \equiv 1 \pmod p$$

$$(a)^{\frac{p-1}{2}} \equiv 1 \pmod p$$

above congruence holds. $\quad a = x_1^2$

Conversely given $a^{p-1/2} \equiv 1 \pmod p$ holds.

Let r be primitive root of p &

$$\left(\equiv r^1, r^2, \ldots r^{\phi(p) = p-1} \right)$$

$1, 2, 3 \ldots p-1$

$(a,p) = 1$

Then $a \equiv r^k \pmod p$ for some integer Z

$$1 \leq k \leq p-1$$

$$r^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod p$$

$$r^{k(p-1)/2} \equiv 1 \pmod p$$

$$\left(r^{\phi(p)} \equiv 1 \pmod p \right)$$

$\cancel{r} \equiv$ order of r is $\phi(p)$

$$\phi(p) = p-1$$

$$\Rightarrow \phi(p) \mid \frac{k(p-1)}{2}$$

$$\frac{k(p-1)}{2} \equiv \phi(p) \cdot l$$

$$\frac{k(p-1)}{2} = (p-1) \cdot l$$

$\frac{k}{2} = l$

$\boxed{k = 2l}$

$r^{k} \equiv a \pmod{p}$

$r^{2l} \equiv a \pmod{p}$

$(r^{l})^{2} \equiv a \pmod{p}$

$x^{2} \equiv a \pmod{p}$

for $x \equiv r^{l}$ then above

congruence is solvable

$\Rightarrow$ a is quadratic

residue of p

We further

Date. No.

if $\gcd(a, n) = 1$ and a ~~has~~ is of order $\phi(n)$ modulo n, then a is a primitive root of the integer (n).

$\Rightarrow$ if $a^{\phi(n)} \equiv 1 \pmod{n}$

Corollary : Let p be an odd prime and $\gcd(a, p) = 1$. Then 'a' is a quadratic residue or non residue of p according as;

$a^{(p-1)/2} \equiv 1 \pmod{p}$ quadratic residue

$a^{(p-1)/2} \equiv -1 \pmod{p}$ quadratic Non residue.

The Legendre Symbol and its properties

definition: Let p - odd prime and let gcd(a, p) = 1. The legendre symbol denoted by $\left(\frac{a}{p}\right)$ is given by;

$$\frac{a}{p} \text{ or } a/p \text{ or } a|p = \begin{cases} 1 & \text{if } a \text{ is quadratic residue of } p \\ -1 & \text{if } a \text{ is quadratic non residue of } p. \end{cases}$$

Note: 'a' is quadratic residue of p

$x^2 \equiv a \pmod p$ is solvable

$x^2 \equiv a \pmod p$ not solvable.
quadratic non residue.

Eg $p = 13 \quad a = 1$

$\left(\frac{1}{13}\right) \Rightarrow x^2 \equiv 1 \pmod{13}$

if so this is solvable

$x_0 = 1$ is solⁿ of above

$\left(\frac{1}{13}\right) = +1$

$p = 13 ; \quad a = 2$

$x^2 \equiv 2 \pmod{13}$

not solvable by Eulers criteria

$a^{(p-1)/2} \equiv 1 \pmod{p}$

$2^6 \equiv 64 \pmod{13}$

$2^6 \equiv 12 \pmod{13}$

So not solvable.

Means non quadratic residue.

$\left(\frac{2}{13}\right) = -1$

Similarly

$\left(\frac{1}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{10}{13}\right) =$

$\left(\frac{12}{13}\right) = 1$

$\Rightarrow \left(\frac{2}{13}\right) = \left(5/13\right) = \left(6/13\right) = \left(7/13\right)$

$= \left(8/13\right) = \left(11/13\right) = -1$

Basic properties

Theorem : Let p be odd prime and let $\gcd(a, p) = 1$ $\gcd(b, p) = 1$ then legendre symbol has following properties

(a) If $a \equiv b \pmod p$

then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(b) $\left(\frac{a^2}{p}\right) = 1$

(c) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$

(d) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(e) $\left(\frac{1}{p}\right) = 1$ & $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

(f) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \frac{a}{p}$