Division Algorithm and Divisibility.

① If a divides b, then a is a divisor of b $\Rightarrow a|b \Rightarrow b = xa$. $0 < a < b$

② If $a|b$ then $a|bc$

③ If $a|b$ and $b|a \Rightarrow a = \pm b$

④ If $a|b$ and $b|c \Rightarrow a|c$

⑤ If $c \neq 0$, then $a|b$ if and only if $ac|bc$

*⑥ Any common divisor of a and b is also a divisor of linear comb^n of a and b. $\Rightarrow$ If $d|b$ and $d|a$, then $d|(ax+by)$

---

① # Division Algorithm

$\boxed{a = bq + r}$ $\quad 0 \leq r < b$. q: quotient r: remainder.

① square of any odd integer is of the form $8k+1$

$\Rightarrow$ Any integer is represented as $4q+r \quad 0 \leq r < 4$

In these only $r = 1, 3$ i.e $4q+1$ and $4q+3$ are odd.

$\therefore (4q+1)^2 = 8(2q^2+q)+1 = 8k+1$

$(4q+3)^2 = 8(2q^2+3q+1)+1 = 8k+1$

---

② Show that $a(a^2+2)/3$ is an integer for all $a \geq 1$.

$\Rightarrow$ a is of the form $3q+r \quad 0 \leq r \leq 3$

$r=0 \Rightarrow \frac{a(a^2+2)}{3} = \frac{3q((3q)^2+2)}{3} = q(9q^2+2) \Rightarrow$ Integer.

$r=1 \Rightarrow a = 3q+1 \Rightarrow \frac{a(a^2+2)}{3} = (3q+1)(3q^2+2q+1) \Rightarrow$ Integer

$r=2 \Rightarrow a = 3q+2 \Rightarrow \frac{a(a^2+2)}{3} = (3q+2)(3q^2+4q+2) \Rightarrow$ Integer

---

③ Show that 3 is not a divisor of n^2+1

$\Rightarrow$ Any integer is of the form $n = 3q+r \quad 0 \leq r < 3$

$r=0 \Rightarrow n = 3q \Rightarrow n^2+1 = (3q)^2+1 = 9q^2+1 \Rightarrow$ remainder $= 1$

$r=1 \Rightarrow n = 3q+1 \Rightarrow n^2+1 = (3q+1)^2+1 = 3(3q^2+2q)+2 \Rightarrow$ rem $= 2$

$r=2 \Rightarrow n = 3q+2 \Rightarrow n^2+1 = (3q+2)^2+1 = 3(3q^2+4q)+2 \Rightarrow$ rem $= 2$

$\therefore$ Not Div by 3.

④ Divisibility by 2 . ⇒ check for 758x

758x = 758 × 10 + x

= 758 × 5 × 2 + x → ∴ 758x is div by 2 if and only if 2 | x

(758 × 5 × 2 : Divisible by 2)

⑤ Divisibility by 3 ⇒ check for 8215

8215 = 8(1000) + 2(100) + 1(10) + 5

= 8(999+1) + 2(99+1) + (9+1) + 5 = 8(999) + 2(99) + 9 + 8+2+1+

= 3(8(333) + 2(33) + 3) + (8+2+1+5)

(3(8(333) + 2(33) + 3) : Div by 3)

If 3 | (8+2+1+5) then only 3 | 8215.

*⑥ If b|g and b|h then b|(g+h) if there is some integer (x₁+x₂)

Similarly If b|g and b|h then b|(mg+nh) if there — " — (mx₁+nx₂)

David M. Burton Problems 2.2

Greatest Common Divisor (GCD)

② of special significance is the case in which remainder of Division Algorithm = 0.

Def^n :- gcd of two numbers (not both 0) is the largest integer that divides them both

$$gcd(a,b) = d \quad (d \in z,\ d|a \ \&\ d|b)$$

* gcd(a, b) = 1 ⇒ means a, b are coprimes

---

* For integers a, b, c the following hold.

(i) a|0 , 1|a , a|a , 0|0. 0|a ✗ Not possible

(ii) a|1 if and only if a = ±1

(iii) a|b and c|d then ac|bd

(iv) If a|b and b≠0 then |a| ≤ |b|

* **Theorem 1:-** (GCD as a linear combinat^n)

Given integers a and b, (not both 0)
Then gcd(a, b) is the smallest +ve linear combination of a and b.

$$\boxed{\gcd(a,b) = ax + by}$$ { This is the smallest +ve linear comb^n }

---

* **Theorem 2:** If a and b are integers and $g = \gcd(a,b)$ then

$$\gcd(a/g, b/g) = 1$$

Proof:- Let- $\gcd(a/g, b/g) = h$

$\Rightarrow h \mid a/g$ and $h \mid b/g$ $\Rightarrow$ $\frac{a}{g} = hx_1 \Rightarrow a = hx_1 g = (hg)x_1$

$\frac{b}{g} = hx_2 \Rightarrow b = (hg)x_2$

$\therefore hg$ is a common divisor of both a and b.

$\therefore$ If $g = \gcd(a,b)$ then h must be = 1

If h is any other no. than 1 this contradicts that $g = \gcd(a,b)$

---

* **Corollary :-** If a and b are given integers (not both zero) then set $T = \{ax+by \mid x, y \in \text{Integers}\}$ is precisely a set of all multiples of $d = \gcd(a,b)$

Proof :- We know $\gcd(a,b) = d$

$\therefore d \mid a$ and $d \mid b$ $\Rightarrow$ Therefore $d \mid (ax+by)$

This $(ax+by)$ is a multiple of d

i.e every member of T is a multiple of d.

---

* **Theorem 3:-** a and b are relatively prime if and only if $1 = ax + by$.

proof:- If a, b are rel. prime then $\gcd(a,b) = 1$ — ①

From def^n of gcd $\Rightarrow$ ~~$ax+by =$~~ $\gcd(a,b) = ax+by$

$\therefore$ Put in ① $\Rightarrow$ $ax+by = 1$

Conversely :- Suppose $1 = ax + by$

For some x and y, if $d = gcd(a, b)$ $\Rightarrow d \mid a$ and $d \mid b$

$\therefore d \mid (ax + by)$ $\Rightarrow$ This gives us $d \mid 1$

This $d \mid 1$ is only possible if $d = 1$

and if this is the case $gcd(a, b) = 1$ $\therefore a, b$ are co-prime

---

Corollary :- If $gcd(a, b) = d$ then $gcd(a/d, b/d) = 1$

Proof :- $\because gcd(a, b) = d$

$\therefore ax + by = d$

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

$\therefore$ By above theorem the integers $\left(\frac{a}{d}\right)$ and $\left(\frac{b}{d}\right)$ are relatively prime $\Rightarrow \therefore gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Corollary 2 :- If $a \mid c$ and $b \mid c$ with $gcd(a, b) = 1$ then $ab \mid c$

proof :- If $a \mid c$ and $b \mid c$ then there exist x_1 and x_2 such that $c = ax_1 = bx_2$ — (1)

Given $gcd(a, b) = 1$ $\Rightarrow 1 = ax + by$

multiply by c $\Rightarrow c = acx + bcy$

from eqn (1) $\Rightarrow c = a(bx_2)x + b(ax_1)y$

$\therefore c = ab(xx_2 + yx_1)$

$\Rightarrow \therefore ab \mid c$

Theorem :- Euclids Lemma.

This theo. is of fundamental importance

If p is a prime and $p|ab$., then $p|a$ or $p|b$.

(or)

If $a|bc$ with $\gcd(a,b) = 1$ (means a, b are relatively prime) then $a|c$

Note :- Observe that this result is false if p is not prime

Eg :- $12 | 9.8$ but $12 \nmid 9$ and $12 \nmid 8$

$4 | 6.10$ but $4 \nmid 6$ and $4 \nmid 10$

---

* Corollary :- For $d = \gcd(a,b)$ if and only if

a) $d|a$ and $d|b$

b) Whenever $c|a$ and $c|b$ then $c|d$.

(or) If $d|a$ and $d|b$ then $d | \gcd(a,b)$

Proof :- Suppose $d = \gcd(a,b) \Rightarrow d|a$ and $d|b \Rightarrow$ we can write $d = ax+by$ for some x, y. — (1)

Thus, if $c|a$ and $c|b$ then $c|(ax+by)$

$\therefore$ from (1) $\Rightarrow c|d$.

David M. Burton Problems. 2.3

---

* Lemma 1 :- For any integers a & b.

$$\gcd(a,b) = \gcd(b,a) = \gcd(\pm a, \pm b) = \gcd(a, b-a) = \gcd(a, b+a)$$

Proof :- $\gcd(a,b) = x \Rightarrow x|a \Rightarrow a = xx_1$; $x|b \Rightarrow b = xy_1$ $\Big\}$ $b-a = x(y_1 - x_1)$

$\Rightarrow x|(b-a) \Rightarrow \gcd(a, b-a)$

* Lemma 2 :- $\gcd(a,b) = \gcd(a, b-an)$ $\quad a,b,n \in \mathbb{Z}$

Proof :- We know $\gcd(a,b) = \gcd(a, b-a)$

$\Rightarrow \gcd(a,b-a) = \gcd(a, b-2a)$

$= \gcd(a, b+na)$

---

* Lemma 3 :- Let $a,b,c \in \mathbb{Z}$ then $\gcd(a,b) = \gcd(a+cb, b)$

Proof :- $\gcd(a,b) = k \Rightarrow k \mid a$ and $k \mid b$

$\therefore$ By Theorem $\Rightarrow k \mid a+cb \Rightarrow \gcd(a+cb, b)$

---

(3) # The Euclidean Algorithm:

First apply Division algo to a and b $\Rightarrow$

$a = q_1 b + r_1 \qquad 0 \le r_1 < b$

If $r_1 \neq 0$, divide b by r_1

$\Rightarrow b = q_2 r_1 + r_2 \qquad 0 \le r_2 < r_1$

This process continues until zero remainder appears.

$r_{n-2} = q_n r_{n-1} + r_n$ ← we argue that r_n as the last non-zero remainder

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

$\therefore \gcd(a,b) = r_n$

---

* Lemma :- If $a = bq + r$ then ← $r = a \bmod b$

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

Proof :- $\gcd(a,b) = d \Rightarrow d \mid a$ and $d \mid b$ ← from Theorem

$\Rightarrow d \mid (a - qb)$

$\Rightarrow d \mid r$ ← Hence concludes that d divides both a & b also d divides both b and r

* Corollary :- For any integer $k \neq 0$,

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

$\Rightarrow \gcd(a,b)$ = least +ve integer value of $ax+by$ where x, y can vary over all integer.

* Theorem :- $\gcd(a,b)$ is the least +ve integer that is a linear comb^n of a & b.

Linear Diophantine equation :

$ax+by=c \Rightarrow$ $x = x_0 + t(b/d)$, $y = y_0 - t(a/d)$ where $d = \gcd(a,b)$

$\Rightarrow 172x + 20y = 1000$

Step ① $\Rightarrow$ Find gcd and values of x and y by Extended Euclidean algo

$172 = 20 \times 8 + 12$
$20 = 12 \times 1 + 8$
$12 = 8 \times 1 + 4$
$8 = 4 \times 2 + 0$

$\Rightarrow \therefore \gcd(172, 20) = 4$

Reverse subst^n $\Rightarrow$
$= 12 - 8 \times 1$
$= 12 - (20 - 12 \times 1)$
$= 12(2) - 20$
$= (172 - 20 \times 8)2 - 20$
$= 172(2) - 20(17)$

$\therefore \gcd(172, 20) = 4$ and $x = 2, y = -17$.

Step ② $\Rightarrow$ we know that $\gcd(172, 20)$ = linear comb^n of 172 & 20

$4 = 172x + 20y$

$\Rightarrow 172x + 20y = 4$

$172\left(\frac{x}{4}\right) + 20\left(\frac{y}{4}\right) = 1$

multiply by $c = 1000 \Rightarrow 172\left(\frac{x \times 1000}{4}\right) + 20\left(\frac{y \times 1000}{4}\right) = 1000$

compare with original eq^n $172x + 20y = 1000$

$\therefore$ we got $x_0 = \frac{x \times 1000}{4}$, $y_0 = \frac{y \times 1000}{4}$

$= \frac{2 \times 1000}{4}$, $= \frac{(-17) \times 1000}{4}$

$x_0 = 500$, $y_0 = -4250$

Step ① ⇒ calculate by formula

$X = x_0 + t(b/d)$

$Y = y_0 - t(a/d)$

⇒ $X = 500 + t\left(\frac{20}{4}\right)$ $\quad Y = -4250 + t(17/4)$

$X = 500 + 5t$ $\quad Y = -4250 - 43t$

If x and y are +ve Integers

$500 + 5t > 0$ and $-4250 - 43t > 0$

$t > -100$ and $t < -98.83$

$\therefore t = 99$

Step ④ :- Calculate X and Y

$X = x_0 + t(b/d)$ $\quad Y = y_0 - t(a/d)$

$X = 500 + 99(5)$ $\quad Y = -4250 + 99(43)$

$\boxed{X = 5}$ $\quad \boxed{Y = 7}$

④ Primes and Their Distribution

1) Fundamental Theorem of Arithmetic

An integer $p > 1$ is called a prime number, if its only positive divisors are 1 and p. An inter > 1 that is not prime is turned as composite

- 2 is the only even prime
- 1 is neither prime nor composite.

Theorem 3.1 : If p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof :- If $p \mid a$, then we need go no further.

Assume $p \nmid a$. Now, ∵ only the divisors of p are 1 and p itself then $\gcd(p, a) = 1$.

Hence According to Euclids lemma,

If $p \mid ab$ and $\gcd(p, a) > 1$ then $p \mid b$.

* **Corollary 1.** If p is a prime and $p \mid a_1 a_2 \cdots a_n$ then $p \mid a_k$ for k, where $1 \le k \le n$.

  ↳ This is the extension of theorem 3-1.

* **corollary 2 :** If $p, q_1, q_2 \cdots q_n$ are all primes and $p \mid q_1, q_2, \cdots q_n$, then $p = q_k$ for some k, $1 \le k \le n$.

Theorem 3.2 : Fundamental Theorem of Arithmetic.

Every +ve integer $n > 1$ is either a prime or product of primes ; this representation is unique, apart from the order in which factors occur.

* **Corollary :-** Any positive integer $n > 1$ can be written uniquely in a canonical form

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

for $i = 1, 2 \ldots r$, each k_i is the integer and each p_i is prime with $p_1 < p_2 < \cdots p_r$

* Theorem :- A composite number a will always have a prime factor p satisfying $p \leq \sqrt{a}$.

Proof :- • If $a > 1$ is composite, $\Rightarrow a = bc$ where $1 < b < a$ & $1 < c < a$

• Assume $b \leq c$ $\Rightarrow$ multiply by b both sides $= b^2 \leq bc = a$ so $b \leq \sqrt{a}$

• Because $b > 1$, Theorem 3.2 ensures b has atleast one prime factor p.

• Then $p \leq b \leq \sqrt{a}$.

• Furthermore if $p \mid b$ and $b \mid a$ then $p \mid a$.

$\therefore$ a composite no a will always have a prime divisor p satisfying $p \leq \sqrt{a}$.

* Sieve of Eratosthenes.

for finding all primes below a given number n.

*

1) Write down integers 2 to n.

2) Strike out all multiples ~~of~~ $2p, 3p, 4p, 5p, \ldots\ldots$ of primes $p \leq \sqrt{n}$.

3) The integers that are left out are primes.

* Theorem 3.4 :

Euclid. There is an infinite number of primes.

* Theorem 3.5 :

If p_n is the n^{th} prime number, then $p_n \leq 2^{2^{n-1}}$

* corollary :-

For $n \geq 1$, there exist atleast $n+1$ primes less than 2^{2^n}.

(5) CONGRUENCE (Also called as Arithmetic of Remainders)

* **Defination:-** Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by '$a \equiv b \pmod n$' if n divides the difference $a-b$; that is $a-b = kn$ for some $k \in \mathbb{Z}$.

Eg:- (i) $n = 7$;

$3 \equiv 24 \pmod 7 \Rightarrow 7 \mid 3-24 \Rightarrow 7 \mid -21$

(a ↓, b ↓)

$\therefore a \equiv b \pmod n$ if $n \mid (a-b)$ (or) $a-b = kn$.

* **Remarks**

(i) Any two integers are congruent modulo 1

$a \equiv b \pmod 1 \Rightarrow 1 \mid (a-b)$

(ii) Two integers are congruent modulo 2; if both are even or both are odd.

(iii) Let $n > 1$; By Div. Algo. $\exists q$ and r consider an integer a

$a = qn + r \quad , \quad 0 \le r < n$

$\Rightarrow a - r = qn$

$\therefore a \equiv r \pmod n$ — remainder.

* Possible values of r.

1) $n = 2$; $a \equiv r \pmod 2$ → r: 0 (even), 1 (odd). $\therefore r = \{0, 1\}$

2) $n = 3$; $a \equiv r \pmod 3$ → $r = \{0, 1, 2\}$

$\therefore a \equiv r \pmod n$ ⇒ Possible values of $r = \{0, 1, 2, \ldots, n-1\}$

$a \equiv 0$ or 1 or $2 \pmod 3$

* Complete System Residues.

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

$$a = qn + r \qquad 0 \le r < n$$

Then by def^n of congruence $\Rightarrow$ $a \equiv r \pmod n$ → least non-ve residue modulo n.

and the choices of $r = \{0, 1, 2, \dots n-1\}$

In general, A collection of n integers $\{a_1, a_2, \dots a_n\}$ is **Complete System of Residues modulo n**, if every integer in collec^n is congruent to one and only one of a_k

(or) $\{a_1, a_2 \dots a_k\} \equiv \{0, 1, \dots n-1\} \pmod n$

Eg:- $a = nq + r \quad ; 0 \le r < n$

$a - r = nq$

$a \equiv r \pmod n \longrightarrow r = \{0, 1, 2, \dots n-1\}$

Let $n = 2$ ∴ $a = \{1, 3, 5, 7 \dots\}$ $(\because n=2, r = \{0,1\})$

- Let a = odd

$\therefore 1 \equiv 1 \pmod 2$
$3 \equiv 1 \pmod 2$
$5 \equiv 1 \pmod 2$
} all elements of a congruent to 1 mod 2

- Let a = even ∴ $a = \{0, 2, 4, 6 \dots\}$ $(\because n=2, r = \{0,1\})$

$\therefore 4 \equiv 0 \pmod 2$
$6 \equiv 0 \pmod 2$
} all elements of a congruent to 0 mod 2

Two integers are congruent to mod 2 when they are both even or both odd.

∴ All integers that belong to a collection a: either belong to class 0 (or) class 1.

∴ Every Integer in the collection is congruent to one and only one of $r = \{0, 1, 2, \dots n-1\}$ } This collection is called Complete system of residue modulo n.

Example:- Let $n=4$
$S=\{12, 11, 8, 3\}$ does S forms a CSR modulo 4.

Soln: Since $n=4$, least non-ve residue $\{0,1,2,3\}$

Checking:- $12 \equiv 0 \pmod 4$; $8 \equiv 0 \pmod 4$
$11 \equiv 3 \pmod 4$; $3 \equiv 3 \pmod 4$

$\therefore$ 1 and 2 are missing $\therefore$ S is not CSR modulo 4.

* In Above Example

$12 \equiv 0 \pmod 4$
$8 \equiv 0 \pmod 4$
$\therefore 12 \equiv 8 \pmod 4$

Similarly,
$11 \equiv 3 \pmod 4$
$3 \equiv 3 \pmod 4$
$\therefore 11 \equiv 3 \pmod 4$

* Condition for CSR mod n.
If set S is a CSR, then (i.e non-ve residues)

(1) No of elements in S = No of possibilities of remainder
(2) set $S=\{a_1, a_2, a_3 \dots\}$ None of the elements must be $(a_i \equiv a_j \pmod n)$ ← This should not happen.
(None of the elements in set S must be congruent to each other)

Some Characterization of Congruences and Basic Properties -

* Theorem 1: For arbitrary integers a and b, $a \equiv b \pmod n$ iff a and b leaves the same non-ve remainder when divided by n.

Proof:- Assume $a \equiv b \pmod n \Rightarrow n \mid (a-b) \Rightarrow a = b+kn$

Assume on division, b leaves a remainder r when divided by n.

$\therefore b = qn + r \quad ; \quad 0 \le r < b$

$\therefore a = b+kn = (qn+r)+kn = (q+k)n + r$

$a = (q+k)n + r \Rightarrow \therefore a$ & b leaves same non-ve remainder

* Theorem 2: Let $n>1$ be fixed and $a,b,c,d \in \mathbb{Z}$. Then the following properties hold.

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

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

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

(iv) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

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

(v) If $a \equiv b \pmod{n}$, then $a+c \equiv b+c \pmod{n}$ and $ac \equiv bc \pmod{n}$

(vi) If $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$ for any +ve k.

* Theorem 3: Cancellation law in Congruence.

If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c,n)$

Case 1: If $\gcd(c,n) = 1$; then $ca \equiv cb \pmod{n}$

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

Proof: As $ca \equiv cb \pmod{n}$

$ca - cb = kn \Rightarrow c(a-b) = kn$.

Let $\gcd(c,n) = d \Rightarrow d|c$, $d|n$

$\Rightarrow c = dr$, $n = ds$; $r,s \in \mathbb{Z}$, $(r,s) = 1$

$\therefore c(a-b) = kn$

$r(a-b) = ks$

$\therefore$ By Euclid's lemma,

$s \mid r(a-b)$ or $r \mid ks$

$\downarrow$

$\because (r,s) = 1 \Rightarrow s \mid (a-b)$

$\Rightarrow a-b = sq$

$a \equiv b \pmod{s} \Rightarrow a \equiv b \pmod{n/d}$

Example: (i) $33 \equiv 15 \pmod 9$

$3 \cdot 11 \equiv 3 \cdot 5 \pmod 9$

$11 \equiv 5 \pmod{9/3}$ ← $\gcd(c, n)$ ⇒ $\gcd(3, 9) = 3$

(ii) $-35 \equiv 45 \pmod 8$

$5(-7) \equiv 5(9) \bmod 8$ ⇒ $\gcd(5, 8) = 1$

$-7 \equiv 9 \pmod 8$

* Remark:-

$a \cdot b = 0$ either $a = 0$ or $b = 0$

But $4 \cdot 3 \equiv 0 \pmod{12}$

$4 \not\equiv 0 \pmod{12}$ and $3 \not\equiv 0 \pmod{12}$

But if n is prime

i.e if $ab \equiv 0 \pmod p$ then

$a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$ ← holds

Eulers totient function ($\phi(m)$)

Eulers totient fⁿ $\phi(m)$ = Counts the no. of +ve integers less than m that are relatively prime to m

* Eulers formula ⇒ If $\gcd(a, m) = 1$

then $\boxed{a^{\phi(m)} \equiv 1 \pmod m}$

Que) Find the power of 7 that is congruent to 1 modulo 10.

Soln $7^x \equiv 1 \bmod 10$.

we know $\gcd(7, 10) = 1$

$\therefore 7^{\phi(10)} \equiv 1 \pmod{10}$

$\phi(10)$ = values less than 10 that are coprime with 10

$= \{1, 3, 7, 9\}$ ← count = 4

$\therefore 7^4 \equiv 1 \pmod{10}$

Fermat's little theorem

- Let p denote a prime. If $p \nmid a$ then $\gcd(p, a) = 1$

∴ By Eulers formula $\Rightarrow a^{\phi(p)} \equiv 1 \bmod p$

Hence $\boxed{a^{p-1} \equiv 1 \pmod p}$ $\left(\because \phi(p) = p-1 \text{ if } p \text{ is prime}\right)$

$\Rightarrow \boxed{a^p = a \bmod p}$

Theorem:- Linear diophantine eqn (Proof)

The linear diophantine eqn $ax+by=c$ has a soln iff and only if $d \mid c$ where $\gcd(a,b) = d$.

If x_0 and y_0 is any particular soln of this eqn, then all other soln are given by $x = x_0 + \left(\frac{b}{d}\right)t$; $y = y_0 - \left(\frac{a}{d}\right)t$ $t \in \mathbb{Z}$

Proof :- Given $\gcd(a,b) = d \Rightarrow d = ax + by$

also $d \mid a$ & $d \mid b$

$a = dr$ $b = ds$

$d = drx + dsy$

$= d(rx + sy)$

$ax + by = c$ admits a soln x_0, y_0 (say)

$\therefore ax_0 + by_0 = c$

Let $d = \gcd(a,b) \Rightarrow a = dr$, $b = ds$.

$\therefore d \mid a$ & $d \mid b$

$\therefore c = drx_0 + dsy_0$

$c = d(rx_0 + sy_0)$

$\therefore d \mid c$

If x_0, y_0 is any particular soln of $ax+by=c$ then

$$x = x_0 + \left(\frac{b}{d}\right)t \quad \text{and} \quad y = y_0 - \left(\frac{a}{d}\right)t \quad ; \; t \in \mathbb{Z}$$

where $x', y' \rightarrow$ any other soln

$\therefore ax_0 + by_0 = c = ax' + by'$

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

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

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

$\therefore \boxed{r(x'-x_0) = s(y_0-y')}$.

[Now By Euclids lemma $\Rightarrow a|bc$ where $(a,b)=1 \Rightarrow$ then $a|c$]

$\therefore r \mid s\cdot(y_0-y')$ or $s \mid r(x'-x_0)$

$\Rightarrow r \mid (y_0-y')$ or $s \mid (x'-x_0)$ $(\because \gcd(r,s)=1)$

or $x'-x_0 = st$

$\Rightarrow y_0 - y' = r\cdot t$ or $x' = x_0 + st$

$y' = y_0 - rt$ $\boxed{x' = x_0 + \left(\frac{b}{d}\right)t}$

$\boxed{y' = y_0 - \left(\frac{a}{d}\right)t}$

Linear Congruence and its soln.

Any eqn of the form $ax \equiv b \pmod n$ is called a linear congruence.

Theorem :- The linear congruence $ax \equiv b \pmod n$ has a soln iff and only if $d|b$ where $d = \gcd(a,n)$.
If $d|b$, then it has 'd' mutually incongruent soln modulo n.

Proof Linear Diophantine eqn $ax+by=c$ has a soln iff $d|c$ where $d = \gcd(a,b)$

If x_0 & y_0 are particular soln then other solns can be found by

$x = x_0 + (b/d)t$, $y = y_0 - (a/d)t$

Given $ax \equiv b \pmod{n}$

$ax - b = ny \quad ; \quad y \in \mathbb{Z}$

$ax - ny = b$ ← This linear Diophantine eqn has a soln iff $d \mid b$ where $d = \gcd(a, n)$

Let x_0, y_0 be a particular soln of $ax - ny = b$ and $\begin{cases} x = x_0 + \left(\frac{n}{d}\right)t \\ y = y_0 + \left(\frac{a}{d}\right)t \end{cases}$ are all other soln's.

Choose 't' takes values $0, 1, 2, \ldots d-1$

(1) # Elliptic Curve Cryptography (Finding points on Elliptic curve)

$y^2 = x^3 + ax + b \pmod p$; $E_{11}(1,6) = ?$

$a=1$, $b=6$, $p=11$

$\Rightarrow y^2 = x^3 + x + 6 \pmod{11}$

Since we are operating in mod 11, we can have remainders 0 to 10. (Given p : find 0 to p-1)

- Find values of x, y such that L.H.S. = R.H.S.
  Those points will lie on the elliptic curve

$$\boxed{y^2 = x^3 + x + 6 \pmod{11}}$$

x	R.H.S $x^3+x+6 \pmod{11}$
0	6
1	8
2	5
3	3
4	8
5	4
6	8
7	4
8	9
9	7
10	4

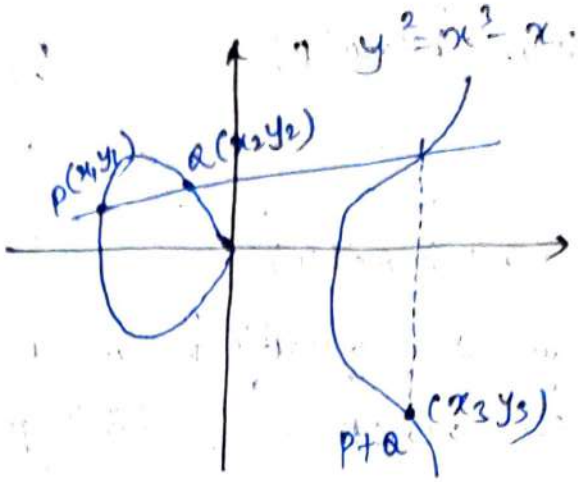
y	L.H.S $y^2 \pmod{11}$
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

Now, a point lies on elliptic curve if L.H.S. = R.H.S

$\therefore E_{11} = \{ (2,4)\ (2,7)\ (3,5)\ (3,6)\ (5,2)\ (5,9)\ (7,2)\ (7,9)\ (8,3)\ (8,8)\ (10,2)\ (10,9) \}$

* Finding Points $P+Q$, $2P$ in curve $y^2 = ax^3 + ax + b$.

(2)



For finding $P+Q$, we need x_3, y_3

It is given by

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$
$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p$$

where $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases}$

(Que) On Elliptic curve, $y^2 = x^3 - 36x$, Let $P = (-3, 9)$ and $Q = (-2, 8)$ find $P+Q$ and $2P$.

Sol^n $P(x_1, y_1) = (-3, 9)$

$Q(x_2, y_2) = (-2, 8)$

$P+Q(x_3, y_3) = ?$, $2P = P + P = (x_1, y_1) + (x_1, y_1) = ?$

$\therefore$ a. Find $P+Q$ where $P \neq Q$ $\lambda = (y_2 - y_1)/(x_2 - x_1)$

$\therefore x_3 = \lambda^2 - x_1 - x_2 \pmod{} = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$

$= \left(\frac{8-9}{-2+3}\right)^2 + 3 + 2 = 6$

$y_3 = \lambda(x_1 - x_3) - y_1 = \left(\frac{8-9}{-2+3}\right)(-3 - 6) - 9$

$= 0$

$\therefore \boxed{P+Q = (6, 0)}$

• finding $2P = P+P$, here $P=Q$ $\therefore \lambda = \frac{3x_1^2+a}{2y_1}$

$x_3 = \lambda^2 - x_1 - x_2$

$= \left(\frac{3(-3)^2+(-36)}{2(9)}\right)^2 - (-3) - (-2) = \left(\frac{27-36}{18}\right)^2 + 3 + 2$

$= 1/4 + 5 = 21/4$

$y_3 = \lambda(x_1 - x_3) - y_1 = \left(\frac{3(9)-36}{18}\right)\left(-3-\frac{21}{4}\right) - 9 = -35/8$

$\therefore 2P = (21/4, -35/8)$

Q) $E_{23}(1,1) = ?$

Soln $y^2 \equiv x^3 + ax + b \pmod p$ here $a=1$, $b=1$, $p=23$.

$\therefore y^2 = x^3 + x + 1 \pmod{23}$

∵ we are operating in mod 23, we will only get values $(0 \text{ --- } 22)$ ← The coordinates of points P+Q or 2P will be one of these values only. (we will not get fractions)

(i) If $P=(13,7)$, $-P = ?$

Formula :- If $P=(x_1,y_1)$, $-P = (x_1, -y_1)$

$\therefore -P = (13, -7)$ → but -7 is invalid in mod 23

$\therefore -P = (+13, 16)$ → (add. : $-7+23 = 16$)

(ii) $R = P+Q$? , $P = (3,10)$ $Q = (9,7)$

Soln $x_3 = \left(\frac{7-10}{9-3}\right)^2 - 3 - 9 = \frac{1}{4} - 12 \pmod{23}$

$= 4^{-1} = 12 \bmod 23$

$= \bullet 4^{-1} + 11 \bmod 23.$ ← $-12 \bmod 23 = 11$ (add : $-12+23$)

$= 4^{-1} \bmod 23 + 11$

$= 6 + 11 \quad = 17$

$\bullet\ y_3 = \left(\frac{7-10}{1-3}\right)(3-17) - 10 \pmod{23}$

$= 7 - 10 \pmod{23} = -3 \bmod 23$

$= 20$

$\therefore \boxed{P+Q = (x_3, y_3) = (17, 20)}$

(ii) $2P = ?$ $\quad P = (3, 10)$ $\quad y^2 = x^3 + x + 1 \pmod{23}$

$(x_1, y_1) = (x_2, y_2) = (3, 10)$

$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - x_1 - x_2 \bmod p.$

$y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1 \bmod p.$

$\Rightarrow x_3^2 \left(\frac{28}{20}\right)^2 - 6 = \left(\frac{7}{5}\right)^2 - 6 \pmod{23}$

$= \frac{49}{25} - 6 \bmod 23 \equiv \frac{3}{2} - 6 \bmod 23$

$\equiv 3 \times 12 - 6 \bmod 23$

$= 30 \bmod 23 = 7$

$y_3 = \left(\frac{28}{20}\right)(3-7) - 10 \mod 23$

$y_3 \equiv \left(\frac{5}{20}\right)(-4) - 10 \mod 23$

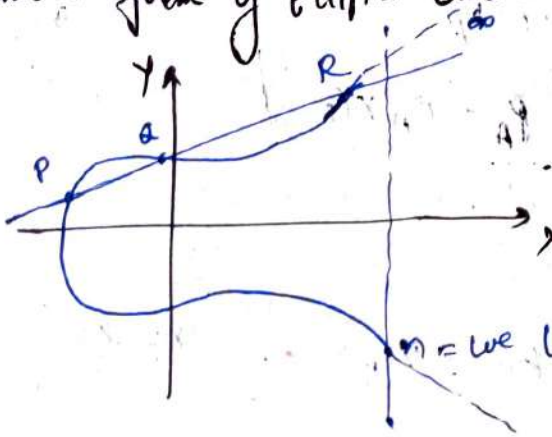
$\equiv \left(\frac{1}{4}\right)(-4) + 13 \mod 23$

$= -1 + 13 \mod 23 = 12.$

$\therefore (x_3, y_3) = 2P = (7, 12)$

(3) Encryption and Decryption

General form of Elliptic curve $\Rightarrow y^2 = x^3 + ax + b$.



$E_p(a,b)$ be elliptical curve, where P and Q are points on elliptic curve, $Q = kP$ $k < n$ (limit)

* Here both Encrypt^n and Decrypt^n is Assymmetric (Public key Cryptosystem)

* Ecc : key Exchange :- We need to find Global public Elements.

- $E_q(a,b)$:- Elliptic curve with parameters a, b
  q :- prime no, integer of form 2^m
- G : point on the EC whose order is a large value of n.

$$y^2 = x^3 + ax + b$$

a) User A key generation
- Select a private key : n_A , $n_A < n$
- Calculate public key P_A

$$P_A = n_A \times G$$

b) User B key generation
- Select a private key : n_B $\quad n_B < n$.
- Calculate public key P_B

$$P_B = n_B \times G$$

⇒ Calculation of Secret key:

- By user A: $\text{key} = n_A \times P_B$ ⟷ Same ⟷ - By user B: $\text{key} = n_B \times P_A$

This key is not shared, both users have obtained it individually. It will be used for Encrypt & Decrypt

* Encrypt^{n} :- M → Message

- Encode M into a point format on Elliptic curve
- Let this point be P_M ← This encoded message (i.e point) lies on the curve
- Now this point is encrypted.

→ For encrypt^{n}, choose a random +ve integer k.

The cipher point coordinates will be

$$C_M = \{kG, P_M + kP_B\}$$

For encrypt^{n}, public key of B is used.

- This point will be sent to receiver

* Decryption :-

For decrypt^{n} multiply 1st coordinate in cipher point with receivers ~~secret~~ private key $\Rightarrow kG * n_B$

→ Then, subtract it from 2nd coordinate

$$P_M + kP_B - (kG * n_B)$$

$$= P_M + k(n_B \times G) - kG \times n_B$$

$$= P_M$$ ← original encoded point.

ECC is used because we get same level of security as that of RSA/DSA but with less no of keys

ECC (n)	RSA / DSA
112	512
256	3072
512	15360

Calculating Inverse modulo m,

$x = a^{-1} \bmod m \Rightarrow ax \equiv 1 \bmod m$

(1) Mental trick for small modulus

$x = 5^{-1} \bmod 11 \Rightarrow 5x \equiv 1 \bmod 11$

→ By trial & error

$5 \times 9 = 45 \equiv 1$ ✓ → inverse = 9

(2) Fermat's Little Theorem (when m is prime)

→ if m is prime

$$a^{-1} \equiv a^{m-2} \pmod m$$

eg:- $3^{-1} \bmod 11$

$\equiv 3^{11-2} \bmod 11$

$= 3^9 \bmod 11$

$= 4$

(3) Extended ~~gcd~~ Euclid Algo.

→ This is when $\gcd(a, m) = 1$

1. Apply Euclid until rem = 1
2. Back Substitute
3. Reduce coefficient of a modulo m

in $(1) = ax + by$

↑ gcd.

#	Situation	Method
(1)	Small no's	→ Trial + Error
(2)	General case	→ Extended Euclid
(3)	Prime modulus	→ Fermat

Method 2 :: Negative shortcut

If a number is close to modulus

Then: $a \equiv m \Rightarrow a = m - k \equiv -k \pmod m$

Then: $a^{-1} \equiv (-k)^{-1}$

Eg:- $9^{-1} \bmod 11$

- $9 \equiv -2 \pmod{11}$
- $2^{-1} = 6 \Rightarrow -6 \equiv 5 \bmod 11$ ← So inverse of 9 is 5

---

a | Inverse

$y^3 = x^2 + x + 6 \pmod{11}$

Que) For the curve $E_{11}(1,6)$ with point $G=(2,7)$, random integer $k=2$, $n_B = 3$ and plaintext point $P_m = (5,9)$ Perform Encrypt^n & decrypt^n using ECC

Sol^n $Cm = \{kG ; P_m + kP_B\}$

① Computat^n of kG

$kG = 2G = G + G$ ← $G = (x_1, y_1) = (2,7) = (x_2, y_2)$

(x_3, y_3)

- $\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3(2)^2 + 1}{2(7)} \bmod 11 = \frac{13}{14} \bmod 11$

$= \frac{2}{14} \bmod 11 = 7^{-1} \bmod 11$

$= 8$

$x_3 = \lambda^2 - x_1 - x_2 \bmod 11$

- $x_3 = 8^2 - 2 - 2 \bmod 11 = 5$
- $y_3 = \lambda(x_1 - x_3) - y_1 \bmod 11$

$= 8(2-5) - 7 \bmod 11 = -31 \bmod 11 = 2$

$kG = (5,2)$

② Computation of P_B :- $P_B = n_B \times G$

$P_B = 3G$

$P_B = 3G = 2G + G$, $2G = (5, 2)$, $G = (2, 7)$

(x_3, y_3) (x_1, y_1) (x_2, y_2)

- $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{7-2}{2-5} = \frac{5}{-3} \bmod 11 = 5(-3)^{-1} \bmod 11$

$\equiv 5(8)^{-1} \bmod 11$

$\equiv 5 \times 7 \bmod 11$

$= 2$

- $x_3 = 2^2 - 5 - 2 \bmod 11 = 8$
- $y_3 = 2(5-8) - 2 \bmod 11 = -8 \bmod 11 = 3$

$\therefore P_B = (8, 3)$

③ Computation of kP_B :- $2P_B = P_B + P_B$ (x_3, y_3)

$P_B = (x_1, y_1) = (x_2, y_2) = (8, 3)$

- $\lambda = \frac{3(8)^2 + 1}{2(8)} \bmod 11 = \frac{193}{6} \bmod 11 = 1$
- $x_3 = (1^2 - 8 - 8) \bmod 11 = 7$
- $y_3 = (1(8-7) - 3) \bmod 11 = -2 \bmod 11 = 9$

$kP_B = (7, 9)$

* Computation of $P_m + kP_B \leftarrow (x_3, y_3)$

$P_m = (x_1, y_1) = (5, 9)$ $kP_B = (x_2, y_2) = (7, 9)$

- $\lambda = \left(\frac{9-9}{7-5}\right) \bmod 11 = 0$
- $x_3 = 0^2 - 5 - 7 \bmod 11 = 10$
- $y_3 = 0(5-10) - 9 \bmod 11 = 2$

∴ Cipher text points are

$$C_m = \{kG, P_m + kP_B\} = \{(5,2), (10,2)\}$$

Decrypt^n

$$P_m = P_m + kP_B - n_B(kG)$$

* $n_B \times kG$:

$n_B = 3, \quad kG = (5,2)$

$\therefore 3(5,2) = 2(5,2) + (5,2)$

① Computat^n of $2(5,2)$

→ Point is $(10,2)$

② computat^n of $3(5,2)$

→ Point is $3(5,2) = n_B \times kG = (7,9)$

③ Computat^n of $P_m + kP_B - n_B(kG)$

- $P_m + kP_B = (10,2)$
- $-n_B(kG) = -(7,9) = (7,-9)$

$\therefore (10,2) + (7,-9)$

- $\lambda = \frac{-2-2}{7-10} \bmod 11 = 0$
- $x_3 = (0^2 - 10 - 7) \bmod 11 = 5$
- $y_3 = (0(10-5) - 2) \bmod 11 = -2 \bmod 11$
  $= 9$

∴ Decrypted pt = $(5,9)$

Chinese Remainder Theorem.

If $m_1, m_2, \ldots, m_k$ are pairwise relatively prime positive integers, and if $a_1, a_2 \ldots a_k$ are any integers, then the simultaneous congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2} \ldots x \equiv a_k \pmod{m_k}$$

has a solution, and sol^n is unique modulo m, where $m = m_1 \cdot m_2 \cdots m_k$.

$k=4$

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$x \equiv a_3 \pmod{m_3}$
$x \equiv a_4 \pmod{m_4}$

we need to show there exist a sol^n that is unique and $m = m_1 \cdot m_2 \cdot m_3 \cdot m_4$

Aim is to :- Find integers w_1, w_2, w_3, w_4

	value mod m_1	value mod m_2	value mod m_3	value mod m_4
w_1	1	0	0	0
w_2	0	1	0	0
w_3	0	0	1	0
w_4	0	0	0	1

- Once we have this, it is easy to construct x!

$$x = a_1 w_1 + a_2 w_2 + a_3 w_3 + a_4 w_4$$

- As long as moduli (m_1, m_2, m_3, m_4) remain same, we can use the same w_1, w_2, w_3, w_4 with a_1, a_2, a_3, a_4

First we need to define $z_1 = \frac{m}{m_1} = m_2 \cdot m_3 \cdot m_4$

Similarly $z_2 = \frac{m}{m_2} = m_1 \cdot m_3 \cdot m_4$

$z_3 = \frac{m}{m_3} = m_1 \cdot m_2 \cdot m_4$

$z_4 = \frac{m}{m_4} = m_1 \cdot m_2 \cdot m_3$

Note that

i) $z_1 \equiv 0 \pmod{m_j}$ for $j = 2, 3, 4$

ii) $\gcd(z_1, m_1) = 1$

(If a prime p dividing m_1 also divides $z_1 = m_2 m_3 m_4$, then p divides m_2, m_3 or m_4)

and likewise z_2, z_3 & z_4

Next define

$y_1 \equiv z^{-1} \pmod{m_1}$

$y_2 \equiv z_2^{-1} \pmod{m_2}$

$y_3 \equiv z_3^{-1} \pmod{m_3}$

$y_4 \equiv z_4^{-1} \pmod{m_4}$

The inverse exist by (ii), and we can find them by Euclid's extended algo.

(iii) $y_1 z_1 \equiv 0 \pmod{j}$ for $j = 2, 3, 4$ $(z_1 \equiv 0 \pmod{m_j})$

(iv) $y_1 z_1 \equiv 1 \pmod{m_1}$ and likewise $y_2 z_2$, $y_3 z_3$ & $y_4 z_4$

* Lastly define

$w_1 \equiv y_1 z_1 \pmod{m}$

$w_2 \equiv y_2 z_2 \pmod{m}$

$w_3 \equiv y_3 z_3 \pmod{m}$

$w_4 \equiv y_4 z_4 \pmod{m}$

Exp :- Solve the simultaneous congruences.

$x \equiv 6 \pmod{11}$

$x \equiv 13 \pmod{16}$

$x \equiv 9 \pmod{21}$

$x \equiv 19 \pmod{25}$

first Check if 11, 16, 21, 25 are relative prime or not.

So, they are relative prime, so CRT is applicable here. So, there exist a unique soln

$m = m_1 \cdot m_2 \cdot m_3 \cdot m_4$

$= 11 \times 16 \times 21 \times 25 = 92400$

K=4

Now,

① apply CRT ⇒ $k = 4$, $m_1 = 11$, $m_2 = 16$, $m_3 = 21$, $m_4 = 25$

$a_1 = 6$, $a_2 = 13$, $a_3 = 9$, $a_4 = 19$

② Calculate

$z_1 = m_2 m_3 m_4 = 8400$

$z_2 = m_1 m_3 m_4 = 5775$

$z_3 = m_1 m_2 m_4 = 4400$

$z_4 = m_1 m_2 m_3 = 3696$

③ Calculate

$y_1 = z_1^{-1} \pmod{m_1} = 8400^{-1} \pmod{11} = 7^{-1} \pmod{11} = 8 \pmod{11}$

$y_2 = z_2^{-1} \pmod{m_2} = 5775^{-1} \pmod{16} = 15^{-1} \pmod{16} = 15 \pmod{16}$

$y_3 = z_3^{-1} \pmod{m_3} = 4400^{-1} \pmod{21} = 11^{-1} \pmod{21} = 2 \pmod{21}$

$y_4 = z_4^{-1} \pmod{m_4} = 3696^{-1} \pmod{25} = 21^{-1} \pmod{25} = 6 \pmod{25}$

(4) Calculate

$w_1 = 8 \cdot 840 \pmod{92400} = 67200 \pmod{92400}$

$w_2 = 86625 \pmod{92400}$

$w_3 = 8800 \pmod{92400}$

$w_4 = 22176 \pmod{92400}$

(5) The soln which is unique modulo 92400 is

$$x = a_1 w_1 + a_2 w_2 + a_3 w_3 + a_4 w_4 \pmod{M}$$

$= 6 \cdot 67200 + 13 \cdot 86625 + 9 \cdot 8800 + 19 \cdot 22176 \pmod{92400}$

$= 2029869 \pmod{92400}$

$x = 51669 \pmod{92400}$ ← This is unique soln modulo m

$m = 92400$

Theorem :- CRT

Let $n_1, n_2, \ldots n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2}$

$x \equiv a_3 \pmod{n_3}$

$\vdots \quad \vdots$

$x \equiv a_r \pmod{n_r}$

has a simultaneous soln, which is unique modulo the integers $n_1 n_2 \ldots n_r$.

Proof - we start by forming the product

$n = n_1 \cdot n_2 \cdot \cdots n_r$ for each $k = 1, 2, \cdots r$

Next, Let $N_k = \frac{n}{n_k} = n_1 \cdot n_2 \cdots n_{k-1} \cdot n_{k+1} \cdots n_r$

here N_k is product of all integers n_i with n_k omitted from it. where all n_i are relatively prime.

by hypothesis, the n_i are relatively prime in pairs, so that gcd $(N_k, n_k) = 1$.

According to the theory of a single linear congruence It is therefore possible to solve the congruence

$$N_k x \equiv 1 \pmod{n_k}$$

And our aim is to show that integer

$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots a_r N_r x_r$ is a simultaneous soln of the given system.

First, observe the $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$ because $n_k \mid N_i$ in this case, The result is

$$\bar{x} = a_1 N_1 x_1 + \cdots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}$$

But the integer x_k was chosen to satisfy the Congruence $N_k x \equiv 1 \pmod{n_k}$, which forces

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

This shows that a soln of the given system of Congruence exists.

As for the uniqueness assertion, suppose that x' is any other integer that satisfies these congruences to

$$\bar{x} \equiv a_k \equiv x' \pmod{n_k} \quad \text{for } k = 1, 2, \ldots r$$

And so,

$$n_k \mid (\bar{x} - x') \quad \text{for each value of } k$$

Because $\gcd(n_i, n_j) = 1$

$$n_1, n_2, \ldots n_r \mid (\bar{x} - x')$$

$$\bar{x} \equiv x' \pmod{n}$$

Que) Find all solutions of $x^2 \equiv 1 \pmod{144}$

→ This is given unique soln modulo M

So, we will break $M = 144$ into factors such that all factors are relatively prime

$$\begin{aligned} 144 &= 12 \times 12 \\ &= 4 \times 3 \times 3 \times 4 \\ &= 16 \times 9 \leftarrow \gcd(16, 9) = 1 \end{aligned}$$

∴ We can replace given congruence by two simultaneous congruences.

$$x^2 \equiv 1 \pmod{16}$$

and $$x^2 \equiv 1 \pmod{9}$$

Now, we need to identify how many sol^n each of these congruences have.

- $x^2 \equiv 1 \pmod{16}$ has 4 sol^{ns}

  $x \equiv \pm 1$ or $\pm 15 \pmod{16}$

  ~~1) ±1, ±15~~
  2) $\pm 1, \pm 7$
  3) ± 9

- $x^2 \equiv 1 \pmod{9}$ has 2 sol^{ns}

  $x^2 = \pmod{9}$

  $\pm 1, \pm 8$

These are

i) $x \equiv 1 \pmod{16}$ and $x \equiv 1 \pmod{9}$
ii) $x \equiv 1 \pmod{16}$ and $x \equiv -1 \pmod{9}$
iii) $x \equiv -1 \pmod{16}$ and $x \equiv 1 \pmod{9}$
iv) $x \equiv -1 \pmod{16}$ and $x \equiv -1 \pmod{9}$
v) $x \equiv 7 \pmod{16}$ and $x \equiv 1 \pmod{9}$
vi) $x \equiv 7 \pmod{16}$ and $x \equiv -1 \pmod{9}$
vii) $x \equiv -7 \pmod{16}$ and $x \equiv 1 \pmod{9}$
viii) $x \equiv -7 \pmod{16}$ and $x \equiv -1 \pmod{9}$

By CRT,

$k = 2$, $m_1 = 16$, $m_2 = 9$

Each case above has a unique sol^n for x modulo 144

$z_1 = m_2 = 9$

$y_1 \equiv 9^{-1} \equiv 9 \pmod{16}$

$w_1 \equiv 9 \cdot 9 \pmod{144}$

$\equiv 81 \pmod{144}$

$z_2 = m_1 = 16$

$y_2 = 16^{-1} \equiv 4 \pmod{9}$

$w_2 \equiv 16 \cdot 4 \equiv 64 \pmod{144}$

$\uparrow$ $M_2 m_1 \cdot m_2$

The Eight sol^ns are

i) $x \equiv 1 \cdot 81 + 1 \cdot 64 \equiv 145 \equiv 1 \pmod{144}$

ii) $x \equiv 1 \cdot 81 + (-1)(64) \equiv 17 \equiv 17 \pmod{144}$

iii) $x \equiv (-1) \cdot 81 + 1 \cdot 64 \equiv -17 \equiv -17 \pmod{144}$

iv) $x \equiv (-1)81 + (-1) \cdot 64 \equiv -145 \equiv -1 \pmod{144}$

v) $x \equiv 7 \cdot 81 + 1 \cdot 64 \equiv 631 \equiv 55 \pmod{144}$

vi) $x \equiv 7 \cdot 81 + (-1) \cdot 64 \equiv 503 \equiv 71 \pmod{144}$

vii) $x \equiv (-7)81 + 1(64) : -503 \equiv -71 \pmod{144}$

viii) $x \equiv (-7)(81) + (-1)(64) \equiv -631 \equiv -55 \pmod{144}$

Test (10-11)