Divisibility: An integer b is divisible by an integer a $(a \neq 0)$ if there is an integer k such that $b = ka$, and we write $a \mid b$.

If b is not divisibly by a, we write $a \nmid b$.

Thm 1: i) $a \mid b$ implies $a \mid bc$ for any integer c.

ii) $a \mid b$ and $b \mid c$ imply $a \mid c$.

iii) $a \mid b$ and $a \mid c$ imply $a \mid (bx + cy)$ for any integers x and y.

iv) $a \mid b$ and $b \mid a$ imply $a = \pm b$

v) $a \mid b$, $a > 0$, $b > 0$, imply $a \leq b$.

Thm 2: [Division algorithm]:

Given any integers a and b, $(a > 0)$ there exist unique integers q and r such that

$b = qa + r$, $0 \leq r < a$.

(dividend, quotient, divisor, remainder)

$2 \overline{)15}$ (7

14

1 $\quad 15 = 7(2) + 1$

If $a \nmid b$, then $0 < r < a$. (and if $a \mid b$, $r = 0$)

Ex: $a = 11$, $b = 101$

$101 = 11 \cdot 9 + 2$

$$\begin{array}{r} 9 \\ 11 \overline{)\,101} \\ \underline{99} \\ 2 \end{array}$$

Ex: $a = 3$, $b = -11$

$-11 = -4 \cdot 3 + 1$

$$\begin{array}{r} -4 \\ 3 \overline{)\,-11} \\ \underline{-12} \\ 1 \end{array}$$

Greatest common divisor (gcd)

Defn: Let b and c be integers. Then d is a common divisor of b and c if

$$d \mid b \text{ and } d \mid c.$$

g is called gcd of b and c $(b \neq 0, c \neq 0)$ if

i) $g \mid b$ and $g \mid c$

ii) If d is any common divisor, then $d \mid g$.

Notation: gcd of b and c is denoted by (b, c).

Ex. i) Let $a = 5$, $b = 15$

$(a, b) = 5$

ii) $(12, 20) = 4$

iii) $(13, 155) = 1$

ex. $16, 20$

$d = 2$

$g = 4$

$2 \mid 4$

Defn: Integers a and b are said to be relatively prime (coprime) if $(a, b) = 1$.

Thm 3: If $(b, c) = g$, then there exist integers x_0 and y_0 such that $g = bx_0 + cy_0$. (This is called Bézout's Thm)

ex:- $3 = 12(-1) + 15(1)$

Moreover

least positive integer of $\{bx + cy,\ x, y \in \mathbb{Z}\}$ is gcd of b and c.

Note: If $d = bx + cy$ for some integers x and y, then $g \mid d$.

Thm 4: If $d|a$ and $d|b$ and $d>0$, then

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

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

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

$3|24$, $3|18$

$\left(\frac{24}{3}, \frac{18}{3}\right) = \frac{1}{3}(24,18)$

$(8,6) = 2.$

Ex: $(12, 15) = 3$,

$\left(\frac{12}{3}, \frac{15}{3}\right) = (4,5) = 1$

Thm 5: For any integer x, $(a,b) = (b,a) = (a,-b) = (a, b+ax)$

Pf: Denote (a,b) by d and $(a, b+ax)$ by g.

We need to S.T $d=g$.

Since $(a,b) = d$, there exist integers x_0 and y_0 such that

$$d = a x_0 + b y_0.$$

$$\Rightarrow d = a x_0 + b y_0 + a x y_0 - a x y_0$$

$$\Rightarrow d = a(x_0 - x y_0) + (b + ax) y_0$$

$$\Rightarrow d = a\, x_0' + (b+ax)\, y_0 \quad (x_0' = x_0 - x y_0)$$

Thus, $g|d$. (From thm 3)

Now we p.T $d|g$.

Since $d|a$ and $d|b$, ($(a,b) = d$)

we see that $d \mid (ax+b)$ (From thm 1 (iii))

$\Rightarrow$ d is common divisor of a and $ax+b$.

Thus $d|g$ ($\because$ g is gcd of a and $ax+b$)

$\Rightarrow \quad d = g.$

Thm 6: If $c \mid ab$ and $(b, c) = 1$, then $c \mid a$

Ex: Find gcd of $(963, 657)$

Soln: By division algorithm

$$963 = 1 \cdot 657 + 306$$

$$\Rightarrow (963, 657) = (963 - 1 \cdot 657, 657) = (306, 657)$$

(because $(a, b) = (a, b + ax)$, put $a = 657$, $b = 963$, $x = -1$)

$$657 = 2 \cdot 306 + 45$$

$$\Rightarrow (306, 657) = (657 - 2 \cdot 306, 306) = (45, 306)$$

$$306 = 6 \cdot 45 + 36$$

$$\Rightarrow (45, 306) = (306 - 6 \cdot 45, 45) = (36, 45)$$

$$45 = 1 \cdot 36 + 9$$

$$\Rightarrow (36, 45) = (45 - 1 \cdot 36, 36) = (9, 36)$$

$$36 = 4 \cdot 9 + 0$$

$$\Rightarrow (9, 36) = (36 - 4 \cdot 9, 9) = (0, 9) = 9$$

Thus, $(963, 657) = 9$

Theorem 7 [Euclidean algorithm]:

Given two integers b and $c > 0$, we make a repeated application of division algorithm, we obtain

$$b = cq_1 + r_1, \quad 0 < r_1 < c,$$
$$c = r_1 q_2 + r_2, \quad 0 < r_2 < r_1,$$

5)7(1
5
2)5(2
4
1)2(2
2
0

$r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2$

$\vdots$

$r_{j-2} = r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}$

$r_{j-1} = r_j q_{j+1}$

12)15(1
12
3)12(4
12
0

The gcd (b, c) of b and c is r_j, the last nonzero remainder.

Values of x_0 and y_0 in $(b,c) = bx_0 + cy_0$ can be obtained by writing each r_i as linear combinations of b and c.

Ex: Find gcd g of 42823 and 6409 and find integers x and y to satisfy

$$42823x + 6409y = g$$

Soln:

$42823 = \underset{q_1}{6} \cdot 6409 + \underset{r_1}{4369} \quad -①$

$6409 = \underset{q_2}{1} \cdot 4369 + \underset{r_2}{2040} \quad -②$

$4369 = \underset{q_3}{2} \cdot 2040 + \underset{r_3}{289} \quad -③$

$2040 = \underset{q_4}{7} \cdot 289 + \underset{r_4}{17} \quad -④$

$289 = \underset{q_5}{17} \cdot 17 \quad -⑤$

$(42823, 6409)$
$= (6409, 4369)$
$= (4369, 2040)$
$= (2040, 289)$
$= (289, 17)$
$= 17$

Thus, $(42823, 6409) = 17$

To find x and y to satisfy

$$42823x + 6409y = 17$$

④ $\Rightarrow$ $17 = 2040 - 7 \cdot 289 \quad -⑥$

③ $\Rightarrow$ $289 = 4369 - 2 \cdot 2040 \quad -⑦$

Sub (7) in (6)

$$17 = 2040 - 7 \cdot (4369 - 2 \cdot 2040)$$

$$= 15 \cdot 2040 - 7 \cdot 4369 \quad \text{— (8)}$$

(2) $\Rightarrow$ $2040 = 6409 - 1 \cdot 4369$ — (9)

Sub (9) in (8),

$$17 = 15 \cdot (6409 - 1 \cdot 4369) - 7 \cdot 4369$$

$$= 15 \cdot 6409 - 22 \cdot 4369 \quad \text{— (10)}$$

(1) $\Rightarrow$ $4369 = 42823 - 6 \cdot 6409$ — (11)

Sub (11) in (10)

$$17 = 15 \cdot 6409 - 22 (42823 - 6 \cdot 6409)$$

$$\Rightarrow 17 = (-22) \cdot 42823 + (147) \cdot 6409$$

OR

Consider

$$42823 \cdot 1 + 6409 \cdot 0 = 42823 \quad \text{— (1)}$$

$$42823 \cdot 0 + 6409 \cdot 1 = 6409 \quad \text{— (2)}$$

Multiple (2) by $q_1 = 6$, and subtract the result from (1)

$$42823 \cdot 1 + 6409 \cdot (-6) = 4369 \quad \text{— (3)}$$

Multiple (3) by $q_2 = 1$, and subtract the result from (2)

$$42823 \cdot (-1) + 6409 \cdot 7 = 2040 \quad \text{— (4)}$$

Multiple (4) by $q_3 = 2$, and subtract the result from (3)

$$42823 \cdot 3 + 6409 \cdot (-20) = 289 \quad \text{— (5)}$$

Multiple (5) by $q_4 = 7$, and sub. the result from (4)

$$42823 \cdot (-22) + 6409 \cdot 147 = 17$$

The reqd $x = -22$, $y = 147$.

Defn: (least common multiple): The integers $a_1, a_2, \dots a_n$ all different from zero, have a common multiple b if $a_i \mid b$ for $i = 1, 2, \dots n$.

lcm

The least of the +ve common multiples is called lcm, and it is denoted by $[a_1, a_2, \dots, a_n]$.

Note: If $h = [a_1, a_2, \dots, a_n]$, then common multiples of a_i's are $0, \pm h, \pm 2h, \pm 3h, \dots$

Thm 8: Let a and b be integers. Then

$$[a,b] \cdot (a,b) = |ab|$$

Primes

Defn: An integer $p > 1$ is called a prime no., or a prime, in case there is no divisor d of p satisfying $1 < d < p$.
If an integer $a > 1$ is not a prime, it is called composite no.

Thm 9: [The fundmental Theorem of arithmetic]

Every integer $n > 1$ can be expressed as product of primes (with perhaps only one factor)

Ex: $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$
$641 = 641$
$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
$1024 = 2^{10}$.

$2^6 \equiv 17 \pmod{47}$
$(2^6)^3 \equiv 17^3 \pmod{47}$
$2^{18} \equiv 4913 \pmod{47}$
$2^{19} \equiv 25 \pmod{47}$
$2^{19} \cdot 2^5 \equiv 800 \pmod{47}$

Modular Arithmetic

Defn: If a and b are integers and m is a +ve integer, then a is congruent to b modulo m, we write $a \equiv b \pmod{m}$, if $m \mid (a-b)$ (m divides $(a-b)$)

if $a \not\equiv b \pmod{m}$, then $m \nmid (a-b)$

Notation: $a \bmod m$ is a remainder when a is divided by m.

Thm 10: Let a and b be integers, and m be a +ve int. Then $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$.

Thm 11: i) $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $(a-b) \equiv 0 \pmod{m}$ are equivalent st. mts

ii) If $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

iii) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

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

iv) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$

v) If $a \equiv b \pmod{m}$ and $d \mid m$, $d > 0$, then

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

vi) If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{mc}$ for $c > 0$.

pf iii) Let $a \equiv b \pmod m$ and $c \equiv d \pmod m$,

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

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

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

$\Rightarrow a+c \equiv b+d \pmod m$.

pf iv) Let $a \equiv b \pmod m$ and $c \equiv d \pmod m$,

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

$\Rightarrow m \mid [(a-b)x + (c-d)y]$ for any $x, y \in \mathbb{Z}$

put $x = c$, $y = b$

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

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

$\Rightarrow ac \equiv bd \pmod m$.

pf v) Given $a \equiv b \pmod m$ and $d \mid m$

$\Rightarrow m \mid (a-b)$ and $d \mid m$

$\Rightarrow d \mid m$ and $m \mid (a-b)$

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

$\Rightarrow a \equiv b \pmod d$

Thm 12: i) $ax \equiv ay \pmod m$ iff $x \equiv y \left(\mod \frac{m}{(a,m)}\right)$

ii) if $(a, m) = 1$ and $ax \equiv ay \pmod m$, then

$x \equiv y \pmod m$.

iii) $x \equiv y \pmod{m_i}$ for $i = 1, 2, 3, \ldots, r$ if f

$x \equiv y \pmod{[m_1, m_2, m_3, \ldots, m_r]}$

pf i) If $ax \equiv ay \pmod{m}$, Then $m \mid (ax - ay)$

$\Rightarrow ax - ay = km$ for some $k \in \mathbb{Z}$.

$\Rightarrow \frac{a}{(a,m)}(x-y) = \frac{k}{(a,m)} m$

$\Rightarrow \frac{m}{(a,m)} \mid \frac{a}{(a,m)}(x-y)$

∵ If $(a,b) = g$, $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$

∵ If $(a,b) = 1$ and $a \mid bc$, then $a \mid c$

But $\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1$. Therefore $\frac{m}{(a,m)} \mid (x-y)$

That is $x \equiv y \pmod{\frac{m}{(a,m)}}$.

Conversely, If $x \equiv y \pmod{\frac{m}{(a,m)}}$, then

$ax \equiv ay \pmod{\frac{km}{\frac{am}{(a,m)}}}$ $\quad k = \frac{a}{(a,m)}$

$\Rightarrow ax \equiv ay \pmod{m}$ (from thm 11(v))

pf ii) It is a special case of i)

pf iii) If $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$, then

$m_i \mid (x-y)$ for $i = 1, 2, \ldots r$.

That $(x-y)$ is multiple of $m_1, m_2, \ldots m_r$ and

$\therefore [m_1, m_2, \ldots, m_r] \mid (x-y)$

$\Rightarrow x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$

Conversely, if $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$, then

$x \equiv y \pmod{m_i}$ $\quad (\because m_i \mid [m_1, m_2, \ldots m_r])$

(from thm 11 (v))

Defn: If $x \equiv y \pmod m$ then y is called residue of x modulo m.

A set $x_1, x_2, \ldots, x_m$ is called complete residue system modulo m if for every integer y there is one and only x_j such that

$$y \equiv x_j \pmod m$$

Ex: $0, 1, 2, 3, 4$ is complete residue system modulo 5

Also, $5, 6, 7, 8, 9$ is "

$\Rightarrow$ There are infinitely many complete residue system.

Linear congruences

A congruence of the form

$$ax \equiv b \pmod m$$

where m is a +ve int, a and b are integers, and x is a variable, is called a linear congruence.

Thm 13: If $(a, m) = 1$ then there is an x such that $ax \equiv 1 \pmod m$.

Any two such x are congruent $\pmod m$.

If $(a, m) > 1$ then there is no such x.

pf: If $(a, m) = 1$, then there exist x and y such that

$ax + my = 1$.

$\Rightarrow \quad ax = 1 - my$

$\Rightarrow \quad ax - 1 = m(-y)$

$\Rightarrow \quad m \mid (ax-1)$

$\Rightarrow \quad ax \equiv 1 \pmod m.$

Conversely, if $ax \equiv 1 \pmod m$

$\Rightarrow m \mid ax-1$

$\Rightarrow \quad ax - 1 = m(k)$ for some $k \in \mathbb{Z}$

$\Rightarrow \quad ax + my = 1, \quad (y = -k)$

$\Rightarrow \quad (a, m) = 1$

If $ax_1 \equiv 1 \pmod m$ and $ax_2 \equiv 1 \pmod m$ $(x_1 \neq x_2)$

$\Rightarrow ax_1 \equiv 1 \pmod m$ and $1 \equiv ax_2 \pmod m$

$\Rightarrow ax_1 \equiv ax_2 \pmod m$

$\Rightarrow x_1 \equiv x_2 \pmod m$

If $a \equiv b \pmod m$, $c \equiv d \pmod m$, then $ac \equiv bd \pmod m$

Thus, there is only one soln in complete residue system mod m.

Note: If $ab \equiv 1 \pmod m$, then b is called inverse of a modulo m, denoted by $\bar{a}$.

Ex: Find an inverse of 3 mod 7.

Soln: To find x such that

$3x \equiv 1 \pmod 7$.

Inverse exist because $(3,7) = 1$

$\therefore$ Inverse of 3 mod 7 is 5. (we found it by inspection)

$x = 1, \quad 3 \not\equiv 1 \pmod 7$

$x = 2, \quad 6 \not\equiv 1 \pmod 7$

$x = 3, \quad 9 \not\equiv 1 \pmod 7$

$x = 4, \quad 12 \equiv 1 \pmod 7$

$x = 5, \quad 15 \equiv 1 \pmod 7$

Let us find inverse by Euclidean algorithm.

WKT $(3,7)=1$, $\exists$ x and y such that

$$3x+7y=1. \quad \text{——} (*)$$

$3(-2) \equiv 1 \pmod 7$

Consider

$$7 = 2.3 + 1$$
$$3 = 3.1$$

$1 = 1.7 + 3(-2)$

$3 = 3.(7-2.3)$

$3 = 3.7 - 6.3$

put $x=1$ and $y=0$ in $(*)$

$$3.1 + 7.0 = 3 \quad \text{——} (1)$$

put $x=0$ and $y=1$ in $(*)$

$$3.0 + 7.1 = 7 \quad \text{——} (2)$$

$\times$ by (1) by 2, then subtract from (2)

$$3(-2) + 7.1 = 1$$

Thus, inverse $x = -2$

In general, inverse $x \equiv -2 \pmod 7$.

Ex 2: Find an inverse of 101 modulo 4620. $5.29 \equiv 1 \pmod{72}$

Soln: We have to x such that

$$101x \equiv 1 \pmod{4620}$$

Consider

$$4620 = 101.\underset{q_1}{45} + \underset{r_1}{75}$$

$$101 = 75.\underset{q_2}{1} + \underset{r_2}{26}$$

$$75 = 26.\underset{q_3}{2} + \underset{r_3}{23}$$

$$26 = 23.\underset{q_4}{1} + \underset{r_4}{3}$$

$5x \equiv 1 \pmod{72}$

$72 = 5 \times 14 + 2$

$5 = 2.2 + 1$

$\Rightarrow 2 = 72 - 5.14$

$1 = 5 - 2.2$

$1 = 5 - 2(72 - 5.14)$

$1 = 29.5 - 2(72)$

$145 - 144$

$$23 = 3 \cdot \underset{\tilde{q}_5}{7} + \underset{\tilde{r}_5}{2}$$

$$3 = 2 \cdot \underset{\tilde{q}_6}{1} + \underset{\tilde{r}_6}{1}$$

$$2 = 1 \cdot \underset{\tilde{q}_7}{2} + 0$$

Thus $(101, 4620) = 1$. Hence inverse x exist.

Find x and y such that

$$101x + 4620y = 1 \quad \text{---} \quad (*)$$

put $y = 1$, $x = 0$ in $(*)$

$$101 \cdot 0 + 4620 \cdot 1 = 4620 \quad \text{---} \quad (1)$$

put $x = 1$, $y = 0$ in $(*)$

$$101 \cdot 1 + 4620 \cdot 0 = 101 \quad \text{---} \quad (2)$$

Multiply (2) by $q_1 = 45$, then subtract from (1).

$$101 \cdot (-45) + 4620 \cdot 1 = \underset{r_1}{75} \quad \text{---} \quad (3)$$

Multiply (3) by $q_2 = 1$, then subtract from (2),

$$101 \cdot (46) + 4620 \cdot (-1) = \underset{r_2}{26} \quad \text{---} \quad (4)$$

Multiply (4) by $q_3 = 2$, then subtract from (3),

$$101 (-137) + 4620 (3) = \underset{r_3}{23} \quad \text{---} \quad (5)$$

Multiply (5) by $q_4 = 1$, then sub. from (4),

$$101 (183) + 4620 \cdot (-4) = \underset{r_4}{3} \quad \text{---} \quad (6)$$

Multiply (6) by $q_5 = 7$, then sub. from (5)

$$101 \cdot (-1418) + 4620 \cdot (31) = \underset{r_5}{2} \quad \text{---} \quad (7)$$

Multiply (7) by $q_6 = 1$, then sub from (6)

$$101 \cdot (1601) + 4620(-35) = 1$$

$$\Rightarrow \quad 101 \cdot (1601) = 1 + 4620 \cdot (35)$$

$$\Rightarrow \quad 101 \cdot (1601) \equiv 1 \pmod{4620}$$

Thus, inverse of $101 \pmod{4620}$ is 1601.

Thm 14: Let a, b and $m > 0$ be given integers, and put $g = (a, m)$.

The congruence $ax \equiv b \pmod{m}$ has a soln iff $g \mid b$.

If this condition is met, then the solns form an arithmetic progression with common difference $\frac{m}{g}$, giving g solns $(\bmod m)$.

Pf: Let $ax \equiv b \pmod{m}$ has a soln.

$$\Rightarrow \quad m \mid (ax - b) \quad \text{for some } x \in \mathbb{Z}$$

$$\Rightarrow \quad ax - b = mk, \quad \exists\, k \in \mathbb{Z}$$

$$\Rightarrow \quad ax + m(-k) = b \quad \text{— (1)}$$

$g = (a, m) \Rightarrow g \mid a$ and $g \mid m$

$$\Rightarrow g \mid (ax + m(-k))$$

$$\Rightarrow g \mid b. \quad \text{(from (1))}$$

Conversely, let $g \mid b$ and $g = (a, m)$.

$$\Rightarrow \quad g \mid b, \; g \mid a \text{ and } g \mid m$$

$$\Rightarrow \quad b = u_1 g, \; a = u_2 g, \; m = u_3 g \quad \text{for some } u_1, u_2, u_3 \in \mathbb{Z}$$

Consider

$$ax \equiv b \pmod m$$

$$\Rightarrow u_2 g\, x \equiv u_1 g \pmod{u_3 g}$$

$$\Rightarrow u_2 x \equiv u_1 \pmod{u_3} \quad \text{— (2)}$$

(Note $(u_2, u_3) = 1$ $\because (a, m) = g \Rightarrow \left(\frac{a}{g}, \frac{m}{g}\right) = 1$)

$\because (u_2, u_3) = 1$, inverse of u_2 (i.e $\overline{u_2}$) exist.

$\therefore u_2 \overline{u_2} \equiv 1 \pmod{u_3}$

x by $\overline{u_2}$ to (2),

$$u_2 \overline{u_2}\, x \equiv u_1 \overline{u_2} \pmod{u_3}$$

($\because ax \equiv ay \pmod m \Rightarrow x \equiv y \pmod{\frac{m}{(a,m)}}$)

$$\Rightarrow x \equiv \underbrace{u_1 \overline{u_2}}_{x_0} \pmod{\underbrace{u_3}_{m/g}}$$

$\therefore$ Solns are

$$x_0,\ x_0 + \frac{m}{g},\ x_0 + 2\frac{m}{g},\ \cdots\ x_0 + (g-1)\frac{m}{g} \pmod m.$$

Ex: Find all solns of the congruence

a) $15x \equiv 25 \pmod{35}$

Soln: Here $a = 15$, $b = 25$ and $m = 35$,

$(15, 35) = 5$, and $5 \mid 25$

$\therefore$ five solns exist.

To find solns:

$$15x \equiv 25 \pmod{35}$$

$$\Rightarrow 5 \cdot 3x \equiv 5 \cdot 5 \pmod{35}$$

$$\Rightarrow 3x \equiv 5 \pmod{\frac{35}{(5,35)}}$$

$$\Rightarrow 3x \equiv 5 \pmod 7 \quad \text{— (*)}$$

we have $ax \equiv ay \pmod m \Rightarrow x \equiv y \pmod{\frac{m}{(a,m)}}$

$6 \cdot 3x \equiv 30 \pmod{42}$

$6 \cdot 3x \equiv 6 \cdot 5 \pmod{42}$

$3x \equiv 5 \pmod{\frac{42}{(6,42)}}$

$3x \equiv 5 \pmod 7$

Let us find inverse of 3 modulo 7.

Consider $3y \equiv 1 \pmod 7$

inv. of 3, $\bar{3}$ is 5 ($\because 3 \cdot 5 \equiv 1 \pmod 7$ we found it by inspection, we can also use Euclidean alg)

(*),

$3x \equiv 5 \pmod 7$

$\Rightarrow \bar{3} \cdot 3x \equiv \bar{3} \cdot 5 \pmod 7$ (we have $x \equiv y \pmod m \Rightarrow ax \equiv ay \pmod m$)

$\Rightarrow x \equiv 25 \pmod 7$

$\Rightarrow x \equiv 4 \pmod 7$ ($\because 3 \cdot \bar{3} \equiv 1 \pmod 7$ and $25 \equiv 4 \pmod 7$)

Soln are

$4, 4+1\cdot 7, 4+2\cdot 7, 4+3\cdot 7, 4+4\cdot 7 \pmod{35}$

i.e, $4, 11, 18, 25, 32 \pmod{35}$.

b) $20x \equiv 4 \pmod{30}$.

Soln: Here $a=20$, $b=4$ and $m=30$

$(20, 30) = 10$. But $10 \nmid 4$. $\therefore$ it has no soln.

c) $3x \equiv 4 \pmod 7$.

Soln: Here $(3,7) = 1$ and $1 \mid 4$. $\therefore$ We have 1 soln.

From Ex a, we note that inverse of 3 mod 7, $\bar{3} = 5$.

Consider $3x \equiv 4 \pmod 7$

$\bar{3} \cdot 3x \equiv \bar{3} \cdot 4 \pmod 7$

$\Rightarrow x \equiv 20 \pmod 7$ ($\because \bar{3} \cdot 3 \equiv 1 \pmod 7$)

$\Rightarrow x \equiv 6 \pmod 7$ ($20 \equiv 6 \pmod 7$)

Thus, soln is $6 \pmod 7$.

The Chinese remainder theorem

Let $m_1, m_2, \dots, m_n$ be pairwise relatively prime positive integers (that is $(m_i, m_j) = 1$, $i \neq j$) and

$a_1, a_2, \dots, a_n$ arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique soln modulo $M = m_1 m_2 m_3 \cdots m_n$

(i.e There is a soln x with $0 \leq x < M$, and all other solns are congruent modulo M to this soln)

Ex 1: Find the positive integer x such that

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 2 \pmod 6 \\ x &\equiv 2 \pmod 7. \end{aligned}$$

Soln: Here no.s 5, 6, and 7 are pairwise relatively prime.

Because $(5,6)=1$, $(6,7)=1$, and $(5,7)=1$

Thus, the system has unique soln modulo $M = 5 \times 6 \times 7 = 210$.

Consider

$$\begin{aligned} & x \equiv 1 \pmod 5 \\ \Rightarrow\ & x - 1 = 5k_1, \quad \text{for some int. } k_1. \\ \Rightarrow\ & x = 1 + 5k_1 \quad \text{——} \ (1) \end{aligned}$$

Sub this in 2nd congruence

$$\begin{aligned} & x \equiv 2 \pmod 6 \\ \Rightarrow\ & 5k_1 + 1 \equiv 2 \pmod 6 \\ \Rightarrow\ & 5k_1 \equiv 1 \pmod 6 \end{aligned}$$

k_1 is inverse of 5, we find it by inspection.

Inverse of 5 modulo 6 is 5. $(\because 5 \cdot 5 \equiv 1 \pmod 6)$

$\therefore \quad k_1 \equiv 5 \pmod 6$

$\Rightarrow \quad k_1 - 5 = 6k_2$, for some $k_2 \in \mathbb{Z}$

$\Rightarrow \quad k_1 = 6k_2 + 5$ —— (2)

Sub (2) in (1),

$$x = 1 + 5(6k_2 + 5)$$

$\Rightarrow \quad x = 30k_2 + 26$ —— (3) (This satisfies 1st and 2nd congruence)

Sub (3) in 3rd congruence

$$x \equiv 2 \pmod 7$$

$\Rightarrow \quad 30k_2 + 26 \equiv 2 \pmod 7$

$\Rightarrow \quad 30k_2 \equiv -24 \pmod 7$ $\quad (-24 \equiv 4 \pmod 7,\ 30 \equiv 2 \pmod 7)$

$\Rightarrow \quad 2k_2 \equiv 4 \pmod 7$

By inspection, we see that

$\Rightarrow \quad k_2 \equiv 2 \pmod 7$

$\Rightarrow \quad k_2 - 2 = 7k_3$, for some $k_3 \in \mathbb{Z}$

$\Rightarrow \quad k_2 = 7k_3 + 2$ —— (4)

Sub (4) in (3)

$$x = 30(7k_3 + 2) + 26$$

$\Rightarrow \quad x = 210k_3 + 86$

$\Rightarrow \quad x \equiv 86 \pmod{210}$

Here 86 is least positive soln of the given system.

Ex2 : Find the least positive integer such that

$x \equiv 5 \pmod 7$
$x \equiv 7 \pmod{11}$
$x \equiv 3 \pmod{13}$

Soln: Here 7, 11, and 13 are pairwise relatively prime.

$\therefore$ The system has a unique soln modulo $M = 7 \times 11 \times 13 = 1001$

Consider

$$x \equiv 5 \pmod 7$$
$$\Rightarrow x - 5 = 7k_1, \quad \text{for some } k_1 \in \mathbb{Z}$$
$$\Rightarrow x = 7k_1 + 5 \quad \text{—— (1)}$$

Sub (1) in 2nd congruence

$$x \equiv 7 \pmod{11}$$
$$\Rightarrow 7k_1 + 5 \equiv 7 \pmod{11}$$
$$\Rightarrow 7k_1 \equiv 2 \pmod{11}$$

By inspection, we see that $(\because 7 \cdot 5 \equiv 2 \pmod{11})$

$$k_1 \equiv 5 \pmod{11}$$
$$\Rightarrow k_1 - 5 = 11k_2, \quad \text{for some } k_2 \in \mathbb{Z}$$
$$\Rightarrow k_1 = 11k_2 + 5 \quad \text{—— (2)}$$

Sub (2) in (1)

$$x = 7(11k_2 + 5) + 5$$
$$\Rightarrow x = 77k_2 + 40 \quad \text{—— (3)}$$

(It satisfies 1st and 2nd congruences)

Sub (3) in third congruence,

$$x \equiv 3 \pmod{13}$$
$$\Rightarrow 77k_2 + 40 \equiv 3 \pmod{13}$$

$\Rightarrow \quad 77k_2 \equiv -37 \pmod{13}$ $\quad \left(\because 77 \equiv 12 \pmod{13},\ -37 \equiv 2 \pmod{13}\right)$

$\Rightarrow \quad 12k_2 \equiv 2 \pmod{13}$

By inspection, we see that

$$k_2 \equiv 11 \pmod{13}$$

$\Rightarrow \quad k_2 - 11 = 13k_3$, for some $k_3 \in \mathbb{Z}$

or $\quad k_2 = 13k_3 + 11 \quad \text{—— (4)}$

(or Inverse of 12 is -1

$-12k_2 \equiv -2 \pmod{13}$

$\Rightarrow \quad k_2 \equiv -2 \pmod{13}$

$\Rightarrow \quad k_2 \equiv 11 \pmod{13}$)

Sub (4) in (3),

$$x = 77(13k_3 + 11) + 40$$

$$\Rightarrow \quad x = 1001k_3 + 887$$

$$\Rightarrow \quad x \equiv 887 \pmod{1001}$$

$\therefore$ Least +ve int. that satisfy system is 887.

Defn: A reduced residue system modulo m is a set of integers r_i such that $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ if $i \neq j$, and such that every x relatively prime to m is congruent modulo m to some member of r_i of the set.

Ex: $m = 8$

1, 3, 5, 7 is complete reduced residue system mod 8.

Also, 9, 11, 13, 15 is complete reduced residue system mod 8.

Ex: $m = 5$

1, 2, 3, 4 is complete reduced residue system modulo 5.

Defn [Euler function]: The number $\phi(m)$ is the number of positive integers less than or equal to m that are relatively prime to n.

Ex: $m = 8, \quad \phi(8) = 4$
$m = 5, \quad \phi(5) = 4$

($\because$ No. of +ve ints ≤ 8 and relatively prime to 8 are 1, 3, 5, and 7)

Note: 1) If $(m_1, m_2) = 1$, then $\phi(m_1 \cdot m_2) = \phi(m_1) \cdot \phi(m_2)$.

Ex: $m = 35 = 5 \cdot 7$

$\phi(35) = \phi(5 \cdot 7) = \phi(5)\phi(7) = 4 \cdot 6 = 24.$

2) If m is any positive integer,

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

Ex: $m = 8$. Here $8 = 2^3$

$\therefore \phi(8) = 8 \cdot \left(1 - \frac{1}{2}\right) = 4$

Ex: $m = 100$

Here $100 = 2^2 \cdot 5^2$

$\phi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right)$

$= 100 \cdot \frac{1}{2} \cdot \frac{4}{5}$

$= 40$

3) If p is any prime, then

$$\phi(p) = p - 1$$

Ex: $m = 101$ ($\because$ 101 is a prime)

$\phi(101) = 100$

Thm 15 [Fermat Little theorem]: Let p denote a prime. If $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}$$

For every integer a,

$$a^p \equiv a \pmod{p}$$

Ex: Let $p = 5$, $a = 4$. Then $4^4 \equiv 1 \pmod{5}$

Ex: Let $p=101$, $a=1542$. Then $1542^{100} \equiv 1 \pmod{101}$

Thm 16 [Euler's generalisation of Fermat's Little thm]:

If $(a,m)=1$, then

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

Ex: Let $m=8$, $a=15$.

$\phi(8)=4$ and $15^4 \equiv 1 \pmod{8}$

pf of thm 16 : Let $r_1, r_2, r_3, \cdots, r_{\phi(m)}$ be a reduced residue system modulo m.

Then $ar_1, ar_2, \cdots, ar_{\phi(m)}$ is also a reduced residue system modulo m.

Because if $ar_i \equiv ar_j \pmod{m}$ $(i \neq j)$

$\Rightarrow r_i \equiv r_j \pmod{m}$ $(\because (a,m)=1)$,

it contradicts the fact that $r_1, r_2, \cdots, r_{\phi(m)}$ is a reduced residue system modulo m.

$\therefore ar_i \not\equiv ar_j \pmod{m}$, $i \neq j$

Also, $(ar_i, m) = 1$

$\therefore$ corresponding to each r_i there is one and only one ar_j such that $r_i \equiv ar_j \pmod{m}$.

$$\Rightarrow ar_1 \cdot ar_2 \cdots ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \pmod{m}$$

$$\Rightarrow a^{\phi(m)} \cdot r_1 \cdot r_2 \cdots r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \pmod{m}$$

$$\Rightarrow a^{\phi(m)} \equiv 1 \pmod{m}. \quad (\because (r_i, m) = 1)$$

pf of thm 15 : If $p \nmid a$, then $(a,p)=1$ and

$a^{\phi(p)} \equiv 1 \pmod{p}$ (From thm 15)

$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$.

Ex: Find the remainder when 7^{222} is divided by 11.

Soln: We have to find $7^{222} \bmod 11$.

Here $m = 11$

$\phi(11) = 11 - 1 = 10$ $\quad ((11, 7) = 1)$

$\therefore$ By Euler's thm,

$7^{\phi(11)} \equiv 1 \pmod{11}$

$\Rightarrow 7^{10} \equiv 1 \pmod{11}$ ——— (1)

By division algorithm

$222 = 22 \cdot 10 + 2$

$\therefore 7^{222} = 7^{22 \cdot 10 + 2}$

$= (7^{10})^{22} \cdot 7^2$

$\equiv 1^{22} \cdot 49$ $\quad$ (From (1))

$\equiv 5 \pmod{11}$

Thus $7^{222} \bmod 11 = 5$.

$2^6 \equiv 1 \pmod{7}$

$100 = 16 \cdot 6 + 4$

$2^{100} = (2^6)^{16+4}$

$= (2^6)^{16} \cdot 2^4 \pmod{7}$

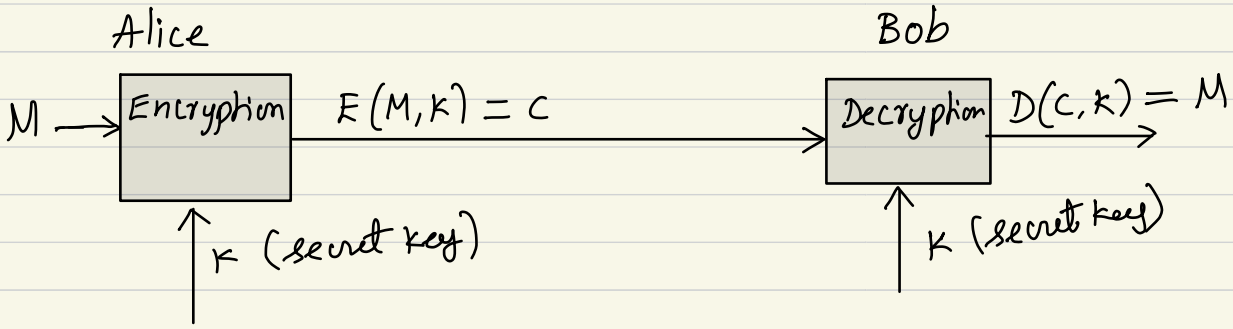
$2^{100} = 1 \cdot 16 \pmod{7}$

$2^{100} \equiv 2 \pmod{7}$

Cryptography

Symmetric cryptosystem.

K → is unknown to all



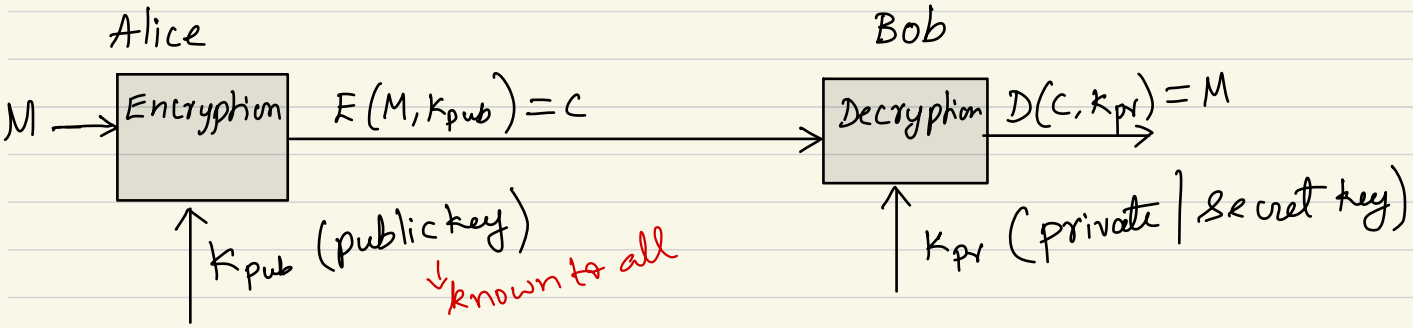
M — Message or plaintext to be sent.

C — Cipher text : (Message which is encrypted)

K — Secret key

In symmetric cryptosystem same key K (secret key) is used to encrypt and decrypt the message M.

Asymmetric cryptosystem (Public key cryptosystem)



Here we use different keys to encrypt and decrypt messages.

The key we use to encrypt the message is called public key.

and key to decrypt msg is kept secret.

Following are the popularly used Public-key cryptosystem.

1) RSA cryptosystem (Rivest – Shamir – Adleman)
2) Elliptic curve cryptosystem

RSA cryptosystem

a) Key generation

publickey K_{pub}, privatekey K_{pr}

It require computation of the pair (K_{pub}, K_{pr})

1) Choose large primes p, q (200 digits)

2) $n = p \cdot q$

3) $\phi(n) = \phi(p \cdot q) = \phi(p) \cdot \phi(q) = (p-1)(q-1)$

4) Choose $K_{pub} = (n, e)$

where $e \in \{1, 2, 3, \cdots, \phi(n)-1\}$

such that $(e, \phi(n)) = 1$.

5) Compute $K_{pr} = d$ such that

$d \cdot e \equiv 1 \pmod{\phi(n)}$

For instance
$n = 15 = 3 \cdot 5$
$\phi(15) = 2 \cdot 4 = 8$

Then $e=3$ or $e=5$, or $e=7$

b) Encryption and decryption

Enc:

Given $K_{pub} = (n, e)$, Let M be a message (plain text) (it is an integer belongs to $\mathbb{Z}_n$)

$C = E(M, K_{pub}) \equiv M^e \pmod{n}$. $(\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\})$

Dec:

Given $K_{pr} = d$, $C \in \mathbb{Z}_n$

$M = D(C, K_{pr}) = C^d \pmod{n}$.

Because $de \equiv 1 \pmod{\phi(n)}$

$\Rightarrow de - 1 = t\,\phi(n)$, for some int t

$\Rightarrow de = 1 + t\,\phi(n)$

and $M^{ed} = M^{1+t\phi(n)}$

$\Rightarrow (M^e)^d = M \cdot M^{t(\phi(n))}$

$\Rightarrow C^d \equiv M \cdot 1 \pmod n$ $\quad \left(\because C \equiv M^e \pmod n, \; M^{\phi(n)} \equiv 1 \pmod n \right)$

Ex: Suppose we need to send a msg

$M = 4$ (Any text msg should be first converted to an integer)

a) Key generation

1) Choose $p = 3$ and $q = 11$

2) $n = p \cdot q = 33$

3) $\phi(n) = (p-1)(q-1) = 20$

4) Choose e, let $e = 3$ $\quad (\because 3 < 20$ and $(3, 20) = 1)$

$\therefore K_{pub} = (n, e) = (33, 3)$.

5) Compute $K_{pr} = d$, such that

$de \equiv 1 \pmod{\phi(n)}$

$\Rightarrow 3d \equiv 1 \pmod{20}$

By inspection, $d \equiv 7 \pmod{20}$

b) Encryption:

Cipher text, $C = M^e \bmod n$

i.e $C = 4^3 \bmod 33$

$\therefore C = 31$.

The encrypted msg is now $C = 31$. The receiver can get the original msg M by below computation.

c) Decryption:

Original msg, $M \equiv c^d \bmod n$

$\equiv 31^7 \bmod 33$

That is M is the remainder when 31^7 is divided by 33.

The binary expansion of 7 is

$7 = 2^2 + 2 + 1 = 4 + 2 + 1$

To compute $31^7 \bmod 33$, we will proceed as follows:

$31^2 = 961 \equiv 4 \pmod{33}$

$31^4 \equiv 4^2 \pmod{33}$

$\Rightarrow 31^7 = 31^{4+2+1} = 31^4 \cdot 31^2 \cdot 31 \equiv 16 \cdot 4 \cdot 31 \bmod 33$

$\equiv 31 \cdot 31 \pmod{33}$

$= 4$

In this way we can recover the original msg M from the encrypted msg C.