Module - 4

Modular Arithmetic

Congruence

Let a & b be any two integers with m being +ve integer, then a is congruent to b modulo m if

* $m \mid (a-b)$ i.e. m divides $a-b$

or

* a & b have the same remainder when divided by m

or

* $\exists$ an integer k $\ni$ $a-b = km$.

And it is denoted by $a \equiv b \pmod m$, with $0 \leq |b| < m$

Ex: $2023 \equiv -1 \pmod 4$, $2023 \equiv 3 \pmod 5$

Properties

1. $a \equiv a \pmod m$ — reflexive
2. $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ — symmetric
3. $a \equiv b \pmod m$ & $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ — transitive
4. $a \equiv b \pmod m \Rightarrow a+c \equiv b+c \pmod m$ &
   $ac \equiv bc \pmod m$
5. $a_1 \equiv b_1 \pmod m$ & $a_2 \equiv b_2 \pmod m$
   $\Rightarrow a_1+a_2 \equiv b_1+b_2 \pmod m$ &
   $a_1 a_2 \equiv b_1 b_2 \pmod m$
6. $a \equiv b \pmod m$ & $k \geq 1 \Rightarrow a^k \equiv b^k \pmod m$
7. If $P(x)$ be a polynomial with integer coefficients & $a \equiv b \pmod m$, then $P(a) \equiv P(b) \pmod m$

Ex: $3x^2 + x + 1 = 5$ & $5 \equiv 2 \pmod 3$

then $3 \cdot 5^2 + 5 + 1 = 81$, $3 \cdot 2^2 + 2 + 1 = 15$

$81 \equiv 15 \pmod 3$.

8. $a \equiv b \pmod m \Rightarrow \gcd(a,m) = \gcd(b,m)$

9. $a \equiv b \pmod m$ & $n/m \Rightarrow a \equiv b \pmod n$

Ex: $39 \equiv 3 \pmod{12}$ & $4/12 \Rightarrow 39 \equiv 3 \pmod 4$

10. $a \equiv b \pmod m$, $a \equiv b \pmod n$ & $\gcd(m,n) = 1$

[m & n are relatively prime or coprime]

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

Ex: $16 \equiv 1 \pmod 3$, $16 \equiv 1 \pmod 5$ & $\gcd(3,5) = 1$

$\therefore 16 \equiv 1 \pmod{15}$

11. If $a \equiv b \pmod m$ & c is a +ve integer, then $ca \equiv cb \pmod{cm}$

12. If $ab \equiv ac \pmod m$ & $\gcd(a,m) = 1$, then $b \equiv c \pmod m$.

Linear congruence

If a, b & n are integers such that $a \not\equiv 0 \pmod{n}$ & x is some unknown, then the congruence $ax \equiv b \pmod{n}$ is called linear congruence.

Thm: The linear congruence $ax \equiv b \pmod{n}$ has a soln iff $d \mid b$ where $d = \gcd(a, n)$.

* If $d \mid b$, then it has d mutually incongruent solns modulo n.
* If $\gcd(a, n) = 1$, then the congruence has a unique soln modulo n.

To solve $ax \equiv b \pmod{n}$ for unique soln

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

step 1: Find $\gcd(a, n)$.

step 2: If $\gcd(a, n) = 1$ then $ax \equiv b \pmod{n}$ has an unique soln

step 3: Express $1 = au + nv$ $\therefore nv = 1 - au = -(au - 1)$

$n \mid -(au-1)$ or $n \mid au-1$

step 4: $au \equiv 1 \pmod{n}$

step 5: Multiply both the sides by b

$\therefore a(bu) \equiv b \pmod{n}$

Now $x \equiv bu \pmod{n}$ is the required soln.

Note: If $d \nmid b$ (d does not divide b), then the congruence $ax \equiv b \pmod{n}$ has no soln, where $d = \gcd(a, n)$.

Find the no. of solns exist w.r.t. following:

1. $8x \equiv 12 \pmod{20}$

   $\gcd(8,20) = 4$ & $4 \mid 12$

   $\therefore$ $\exists$ 4 solns.

2. $9x \equiv 15 \pmod{27}$

   $\gcd(9,27) = 9$ & $9 \nmid 15$

   No soln.

3. $7x \equiv 2 \pmod{37}$

   $\gcd(7,37) = 1 \implies$ unique soln.

To find GCD of two numbers (Euclid's algorithm).

1. GCD of 32 & 54

$32)54(1$ $\quad 32$ $\quad 22$

$22)32(1$ $\quad 22$ $\quad 10$

$10)22(2$ $\quad 20$ $\quad 2$

$2)10(5$ $\quad 10$ $\quad 0$

$22 = 54 - 1(32)$ $\qquad 10 = 32 - 1(22)$ $\qquad 2 = 22 - 2(10)$

The last non-zero remainder is 2 $\quad \therefore \gcd(32, 54) = 2$

To express $\gcd(32, 54)$ in the form $32u + 54v$.

$$2 = 22 - 2(10)$$
$$= [54 - 1(32)] - 2[32 - 1(22)]$$
$$= 54 - 3(32) + 2(22)$$
$$= 54 - 3(32) + 2[54 - 1(32)]$$
$$= 3(54) - 5(32)$$
$$= 54(3) + 32(-5) \qquad \therefore u = -5, \; v = 3.$$

2. GCD of 25520 & 19314

$19314)25520(1$ $\quad 19314$ $\quad 6206$

$6206)19314(3$ $\quad 18618$ $\quad 696$

$696)6206(8$ $\quad 5568$ $\quad 638$

$638)696(1$ $\quad 638$ $\quad 58$

$58)638(11$ $\quad 638$ $\quad 0$

$\therefore$ The last non-zero remainder is 58

$\gcd(25520, 19314) = 58$

$58 = 696 - 1(638)$

$638 = 6206 - 8(696)$

$696 = 19314 - 3(6206)$

$6206 = 25520 - 1(19314)$

$$58 = 696 - 1(638)$$
$$= 696 - 1[6206 - 8(696)]$$
$$= 9(696) - 6206$$
$$= 9[19314 - 3(6206)] - 6206$$
$$= 9(19314) - 28(6206)$$
$$= 9(19314) - 28[25520 - 1(19314)]$$
$$= 25520(-28) + 19314(37)$$

$u = -28, \; v = 37$

Solve the following linear congruences:

1. $7x \equiv 2 \pmod{37}$

Here $a = 7$, $b = 2$, $n = 37$

$\gcd(7, 37) = 1 = d \Rightarrow$ unique soln

To express $d = au + nv$.

1) $37 = 7(5) + 2$	2) $7 = 3(2) + 1$
$\frac{35}{2}$	$\frac{6}{1}$
$2 = 37 - 5(7)$	$1 = 7 - 3(2)$

$\therefore 1 = 7 - 3[37 - 5(7)]$

$= 7(16) + 37(-3)$

i.e $u = 16$, $v = -3$

$\therefore au \equiv 1 \pmod{n} \Rightarrow 7 \times 16 \equiv 1 \pmod{37}$

Multiply by $b = 2$

$7(2 \times 16) \equiv 2 \pmod{37}$

$7(32) \equiv 2 \pmod{37}$

$\therefore x \equiv 32 \pmod{37}$

Verify $37 \mid (7 \times 32) - 2$

2. Solve $11x \equiv 4 \pmod{25}$

Here $a = 11$, $b = 4$, $n = 25$

$\gcd(11, 25) = 1 \Rightarrow$ unique soln.

To express $d = au + nv$

1) $25 = 2(11) + 3$	3) $11 = 3(3) + 2$	2) $3 = 1(2) + 1$
$\frac{22}{3}$	$\frac{9}{2}$	$\frac{2}{1}$
$3 = 25 - 2(11)$	$2 = 11 - 3(3)$	$1 = 3 - 1(2)$

$\therefore 1 = 3 - 1(2)$

$= [25 - 2(11)] - 1[11 - 3(3)]$

$= 25 - 3(11) + 3[25 - 2(11)] = 25(4) + 11(-9)$ $u = -9$, $v = 4$

Now $au \equiv 1 \pmod{n} \Rightarrow 11(-9) \equiv 1 \pmod{25}$

Multiply by $b = 4$

$11(-9 \times 4) \equiv 4 \pmod{25}$

$11(-36) \equiv 4 \pmod{25}$

i.e $11x \equiv 4 \pmod{25}$

$\Rightarrow x \equiv -36 \pmod{25}$

$\therefore x \equiv 14 \pmod{25}$ as $25 \mid x+36$, the least $x = 14$.

3. $5x \equiv 1 \pmod{4}$

$\gcd(5,4) = 1$ $a = 5, b = 1, n = 4$

4) 5 (1 $\quad 1 = 5 - 1 \cdot 4 = 5(1) + 4(-1)$: $u = 1, v = -1$

1

Now $au \equiv 1 \pmod{n} \Rightarrow 5(1) \equiv 1 \pmod{4}$

Multiply by $b = 1$

$5(1) \equiv 1 \pmod{4}$

$\therefore x \equiv 1 \pmod{4}$

4. $3x \equiv 2 \pmod{23}$

$\gcd(3,23) = 1$ $a = 3, b = 2, n = 23$

3) 23 (7 $\quad$ 2) 3 (1 $\quad 2 = 23 - 7 \cdot 3$

21 $\quad$ 2 $\quad 1 = 3 - 1 \cdot 2$

2 $\quad$ 1

$\therefore 1 = 3 - 1[23 - 7 \cdot 3] = 3(8) + 23(-1)$ $u = 8, v = -1$

Now $au \equiv 1 \pmod{n} \Rightarrow 3(8) \equiv 1 \pmod{23}$

Multiply by $b = 2$, $3(8 \times 2) \equiv 2 \pmod{23}$

$\therefore x \equiv 16 \pmod{23}$

To solve $ax \equiv b \pmod{n}$ for $d > 1$ & $d \mid b$, where $d = \gcd(a, n)$.

Given $ax \equiv b \pmod{n}$ —①

step 1 : Find $d = \gcd(a, n)$

If $d > 1$, check $d \mid b$.

step 2 : To find d solutions : Divide ① by d

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

Now, $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1 \Rightarrow$ unique soln

Let $x \equiv t \pmod{n/d}$

Step 3 : Soln of $ax \equiv b \pmod{n}$ is

$$x_k \equiv \left[t + (k-1)\left(\frac{n}{d}\right)\right] \pmod{n}$$

where $k = 1, 2, 3, \ldots, d$.

Here each x_k is distinct.

Solve the following congruences :

1. Solve $12x \equiv 6 \pmod{21}$ —①

Here $a = 12$, $b = 6$, $n = 21$. $\gcd(12, 21) = 3 = d$

$3 \mid 6 \Rightarrow$ ① has 3 solns.

Divide ① by $d = 3$

$$\frac{12}{3}x \equiv \frac{6}{3} \pmod{\frac{21}{3}}$$

$$4x \equiv 2 \pmod{7} \quad —②$$

Now $\gcd(4, 7) = 1$

4) 7 (1 , $\frac{4}{3}$ 3) 4 (1 , $\frac{3}{1}$ $1 = 4 - 1(3)$

$3 = 7 - 1(4)$

$\therefore 1 = 4 - 1(3)$

$= 4 - 1[7 - 1(4)] = 4(2) + 7(-1) : u = 2, v = -1$

Now $4(2) \equiv 1 \pmod 7$

Multiply by 2

$\therefore 4(4) \equiv 2 \pmod 7$

Unique soln of ② is $x \equiv 4 \pmod 7$

i.e. $x_1 \equiv 4 \pmod 7$ i.e $x \equiv t \pmod{n/d}$

To find other solns

$x_k \equiv [t + (k-1)\frac{n}{d}] \pmod n$

$k = 1, 2, 3$, $t = 4$, $n = 21$, $d = 3$

$\therefore x_1 \equiv 4 \pmod{21}$

$x_2 \equiv [4 + (2-1)\frac{21}{3}] \pmod{21}$

$\therefore x_2 \equiv 11 \pmod{21}$

$x_3 \equiv [4 + (3-1)\frac{21}{3}] \pmod{21}$

$\therefore x_3 \equiv 18 \pmod{21}$

2. Solve $8x \equiv 6 \pmod{10}$ —①

$a = 8, \quad b = 6, \quad n = 10$

$\gcd(8, 10) = 2 = d \quad \& \quad 2 \mid 10$

$\therefore$ ① has 2 solns.

Divide ① by $d = 2$.

$$4x \equiv 3 \pmod{5} \quad —②$$

$\gcd(4, 5) = 1$

$4) 5 (1$

$\frac{4}{1}$

$1 = 5 - 1 \cdot 4 = 4(-1) + 5(1) \quad \therefore u = -1, v = 1$

$4(-1) \equiv 1 \pmod{5}$

Multiply by 3

$$4(-3) \equiv 3 \pmod{5}$$

$\therefore \quad x \equiv -3 \pmod{5}$

i.e $x \equiv 2 \pmod{5}$ is the soln of ②

$x \equiv t \pmod{n/d}$

Here $t = 2, \quad n = 10, \quad a = 8, \quad d = 2$

$\therefore$ Solns are given by

$$x_k = \left[t + (k-1)\frac{n}{d}\right] \pmod{n}$$

$k = 1, 2$

$k = 1, \quad x_1 \equiv \left[2 + (0)\frac{10}{2}\right] \pmod{10}$

$\therefore x_1 \equiv 2 \pmod{10}$

$k = 2, \quad x_2 \equiv \left(2 + 1 \cdot \frac{10}{2}\right) \pmod{10}$

$\therefore x_2 \equiv 7 \pmod{10}.$

3. $28x \equiv 56 \pmod{49}$ — ①

$\gcd(28, 49) = 7 = d$ & $7 \mid 49$

$\Rightarrow$ ① has 7 distinct solns.

Divide ① by $d = 7$

$4x \equiv 8 \pmod{7}$ — ②

Now $\gcd(4, 7) = 1$

4) 7 (1 $\quad$ 3) 4 (1 $\quad$ $3 = 7 - 1 \cdot 4$

$\frac{4}{3}$ $\quad$ $\frac{3}{1}$ $\quad$ $1 = 4 - 1 \cdot 3$

$\therefore 1 = 4 - 1 \cdot [7 - 1 \cdot 4] = 4(2) + 7(-1)$: $u = 2, v = -1$

Now $4(2) \equiv 1 \pmod{7}$

Multiply by 8,

$4(16) \equiv 8 \pmod{7}$

$\therefore x \equiv 16 \pmod{7}$

$x \equiv 2 \pmod{7}$ is the soln of ②.

$x \equiv t \pmod{n/d}$

$\therefore$ Solns of ① are given by

$$x_k \equiv \left[t + (k-1)\frac{n}{d}\right] \pmod{n}$$

$t = 2, \quad k = 1, 2, 3, 4, 5, 6, 7, \quad d = 7, \quad n = 49$

$k = 1, \quad x_1 \equiv 2 \pmod{49}$

$k = 2, \quad x_2 \equiv 9 \pmod{49}$

$k = 3, \quad x_3 \equiv 16 \pmod{49}$

$k = 4, \quad x_4 \equiv 23 \pmod{49}$

$k = 5, \quad x_5 \equiv 30 \pmod{49}$

$k = 6, \quad x_6 \equiv 37 \pmod{49}$

$k = 7, \quad x_7 \equiv 44 \pmod{49}$

H.W 4. Solve $3x \equiv 12 \pmod 6$ —①

$\gcd(3,6) = 3$ & $3 \mid 12$ $\Rightarrow$ ① has 3 distinct solns

Divide ① by 3,

$$x \equiv 4 \pmod 2$$

i.e. $x \equiv 0 \pmod 2$

$\therefore t = 0$

$\therefore$ Solns of ① are given by $x_k \equiv t + (k-1)\frac{n}{d} \pmod n$

$k = 1, 2, 3$, $n = 6$, $d = 3$

$k = 1$, $x_1 \equiv 0 \pmod 6$

$k = 2$, $x_2 \equiv 2 \pmod 6$

$k = 3$, $x_3 \equiv 4 \pmod 6$.

Problems

1. Solve $5x \equiv 4 \pmod{13}$

Alt. $13 \mid 5x-4$

$\therefore \quad 5x-4 = 13k \quad , k \in Z$

$5x = 13k+4 \quad \Rightarrow x = \frac{13k+4}{5}$

By inspection $k=2$ gives the integral value of x.

i.e. $x = \frac{13(2)+4}{5} = 6$

$\therefore \quad x \equiv 6 \pmod{13}$.

2. Solve $7x \equiv 9 \pmod{15}$

Alt. $15 \mid 7x-9$

$\therefore \quad 7x-9 = 15k \quad , k \in Z$

$7x = 15k+9 \quad \Rightarrow x = \frac{15k+9}{7}$

By inspection $k=5$ gives the integral value of x

i.e $x = \frac{15(5)+9}{7} = 12$

$\therefore \quad x \equiv 12 \pmod{15}$

3. If $2^8 \equiv a \pmod{13}$, find a.

$2^8 = (2^4)^2 = 256$

$256 \equiv 9 \pmod{13}$

i.e $2^8 \equiv 9 \pmod{13}$

$\therefore \quad a = 9$

$$
\begin{array}{r}
19 \\
13 \overline{)256} \\
13 \\
\hline
126 \\
117 \\
\hline
9
\end{array}
$$

4. Find the least +ve values of x such that

MQP (i) $71 \equiv x \pmod 8$

MQP (ii) $78 + x \equiv 3 \pmod 5$

MQP (iii) $89 \equiv (x+3) \pmod 4$

(iv) $96 \equiv {}^{x}/_{7} \pmod 5$

(v) $5x \equiv 4 \pmod 6$

(i) $8)71(8$ $\quad \therefore x = 7$

$\frac{64}{7}$

(ii) $78 + x - 3 = 5k \quad , \quad k \in Z$

$\therefore 75 + x = 5k$

Let $x = 5$, then $75 + 5 = 80$ is divisible by 5.

$\therefore$ the least value of x is 5.

(iii) $89 - x - 3 = 4k, \quad k \in Z$

$86 - x = 4k$

Let $x = 2$, then $86 - 2 = 84$ is divisible by 4.

$\therefore$ the least value of x is 2

(iv) $96 - \frac{x}{7} = 5k, \quad k \in Z$

$\frac{96(7) - x}{7} = 5k \quad \Rightarrow \quad 672 - x = 35k$

Let $x = 7$, then $672 - 7 = 665$ is divisible by 35.

$\therefore$ the least value of x is 7.

(v) $5x - 4 = 6k \quad , \quad k \in Z$

$5x = 6k + 4 \quad \Rightarrow \quad x = \frac{6k+4}{5}$

If $k = 1, 6, 11, 16 \ldots$ then $x = 2, 8, 14, 20 \ldots$ respectively.

$\therefore$ the least value of x is 2.

5. If $2x \equiv 3 \pmod 7$ find x such that $9 \leq x \leq 30$.

$x = 5$ satisfies the congruence.

$\therefore \quad x \equiv 5 \pmod 7$ is the soln.

Soln set $= \{ \ldots\ldots -9, -2, 5, 12, 19, 26, 33, \ldots \}$

$\therefore$ the required values of x are $12, 19, 26$.

6. Find the least +ve remainder when 2^{301} is divided by 5.

$2^4 = 16 \equiv 1 \pmod 5$

$(2^4)^{75} \equiv (1)^{75} \pmod 5$

$2^{300} \equiv 1 \pmod 5$

$2^{300} \cdot 2 \equiv 1 \cdot 2 \pmod 5$

$\therefore \quad 2^{301} \equiv 2 \pmod 5$

$\therefore$ remainder is 2.

4) 301 (75
28
21
20
1

$2^2 = 4$

$2^3 = 8$

$2^4 = 16$

$301 = 4(75) + 1$

$\therefore 2^{301} = 2^{(4 \times 75) + 1}$

$= (2^4)^{75} \cdot 2$

7. Find the unit digit in the number 7^{289}.

$7^2 \equiv 9 \pmod{10}$

$(7^2)^2 \equiv 9^2 (= 81) \equiv 1 \pmod{10}$

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

$(7^4)^{72} \equiv (1)^{72} \pmod{10}$

$7^{288} \equiv 1 \pmod{10}$

$7^{288} \cdot 7 \equiv 1 \cdot 7 \pmod{10}$

$\therefore 7^{289} \equiv 7 \pmod{10}$ i.e unit digit in 7^{289} is 7.

4) 289 (72
28
09
8
1

H.W. & MBP

Find the last digit of 7^{2013}

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

$(7^4)^{503} \equiv 1^{503} \pmod{10}$

$7^{2012} \equiv 1 \pmod{10}$

$7^{2012} \cdot 7 \equiv 1 \cdot 7 \pmod{10}$

$\therefore 7^{2013} \equiv 7 \pmod{10}$

$\therefore$ unit digit in 7^{2013} is 7.

4) 2013 (503
20
13
12
1

9. Find the last digit in the number 7^{126}

$7^2 \equiv 9 \pmod{10}$

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

$(7^4)^{31} \equiv 1^{31} \pmod{10}$

$7^{124} \equiv 1 \pmod{10}$

$7^{124} \cdot 7^2 \equiv 1 \cdot 9 \pmod{10}$

$\therefore 7^{126} \equiv 9 \pmod{10}$

$\therefore$ the last digit in 7^{126} is 9.

4) 126 (31
12
6
4
2

10. Find the unit digit in 13^{37}

$13 \equiv 3 \pmod{10}$

$13^2 \equiv 3^2 \pmod{10}$

$13^2 \equiv 9 \pmod{10}$

$13^2 \equiv -1 \pmod{10}$

$(13)^4 \equiv (-1)^2 \pmod{10}$

$13^4 \equiv 1 \pmod{10}$

$4) 37 (9$
$\underline{36}$
1

$(13^4)^9 \equiv 1^9 \pmod{10}$

$13^{36} \equiv 1 \pmod{10}$

$13^{36} \cdot 13 \equiv 1 \cdot 13 \pmod{10}$

$13^{37} \equiv 3 \pmod{10}$

∴ the unit digit in 13^{37} is 3.

11. What is the remainder in the division of 2^{50} by 7?

$2^3 = 8 \equiv 1 \pmod{7}$

$(2^3)^{16} \equiv 1 \pmod{7}$

$2^{48} \cdot 2^2 \equiv 1 \cdot 4 \pmod{7}$

$2^{50} \equiv 4 \pmod{7}$

∴ the remainder is 4.

Imp

12. Find the remainder when 2^{23} is divided by 47.

$2^8 = 256 \equiv 21 \pmod{47}$

47) 256 (5
235
21

$(2^8)^2 \equiv (21)^2 \pmod{47}$

$2^{16} \equiv 18 \pmod{47}$

47) 441 (9
423
18

$2^7 = 128 \equiv 34 \pmod{47}$

47) 128 (2
94
34

$\therefore 2^{16} \times 2^7 \equiv 18 \times 34 \pmod{47}$

$2^{23} \equiv 612 \pmod{47}$

47) 612 (13
47
142
141
1

$2^3 \equiv 1 \pmod{47}$

$\therefore$ the remainder is 1.

Imp

13. Find the remainder when $135 \times 74 \times 48$ is divided by 7.

7) 135 (19
7
65
63
2

$135 \equiv 2 \pmod{7}$

7) 74 (10
70
4

$74 \equiv 4 \pmod{7}$

7) 48 (6
42
6

$48 \equiv 6 \pmod{7}$

$\therefore 135 \times 74 \times 48 \equiv 2 \times 4 \times 6 \pmod{7}$

$\equiv 48 \pmod{7} \equiv 6 \pmod{7} \Rightarrow 6$ is the remainder

H.W.

14. Find the remainder when $349 \times 74 \times 36$ is divided by 3

The remainder when 349 is divided by 3 is 1.

(digit sum method)

Or. $3)\overline{349}\ (116$

3

4

3

19

18

1

The remainder when 74 is divided by 3 is 2.

Or. $3)\overline{74}\ (24$

6

14

12

2

The remainder when 36 is divided by 3 is 0.

$3)\overline{36}\ (12$

3

6

6

0

$\therefore 349 \times 74 \times 36 \equiv 0 \pmod 3 \Rightarrow$ the remainder is 0.

15. Find the remainder obtained when $64 \times 65 \times 66$ is divided by 67.

$64 \equiv -3 \pmod{67}$

$65 \equiv -2 \pmod{67}$

$66 \equiv -1 \pmod{67}$

$\therefore 64 \times 65 \times 66 \equiv -6 \pmod{67}$

i.e $64 \times 65 \times 66 \equiv 61 \pmod{67}$

$\therefore$ the remainder is 61.

MQP 16. Find the remainder when $175 \times 113 \times 53$ is divided by 11.

$11) 175 (15$, $\quad 11$, $\quad 65$, $\quad 55$, $\quad 10$ $\qquad 175 \equiv 10 \pmod{11}$

$11) 113 (10$, $\quad 110$, $\quad 3$ $\qquad 113 \equiv 3 \pmod{11}$

$11) 53 (4$, $\quad 44$, $\quad 9$ $\qquad 53 \equiv 9 \pmod{11}$

$\therefore 175 \times 113 \times 53 \equiv 10 \times 3 \times 9 \pmod{11}$

$\equiv 270 \pmod{11}$

$\equiv 6 \pmod{11}$.

$11) 270 (24$, $\quad 22$, $\quad 50$, $\quad 44$, $\quad 6$

$\therefore$ the remainder is 6.

IMP. 17. Find the remainder when 2^{1000} is divided by 13.

$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 \equiv 3 \pmod{13}$, $2^5 = 32$,

$2^6 = 64 \equiv -1 \pmod{13}$

$\therefore$ choose 6.

$6) 1000 (166$, $\quad 6$, $\quad 40$, $\quad 36$, $\quad 40$, $\quad 36$, $\quad 4$

$\therefore 1000 = 166(6) + 4$

$2^{1000} = 2^{166(6)+4}$

$= (2^6)^{166} \cdot 2^4$

$2^{1000} = (2^6)^{166} \cdot 2^4$

$\therefore 2^{1000} \equiv (-1)^{166} \cdot 3 \pmod{13}$

$\equiv 3 \pmod{13}$

$\therefore$ the remainder is 3.

The Chinese remainder theorem
(The remainder theorem)

The Chinese remainder thm (CTR) is used to solve a set of different congruent eqns with one variable but different moduli which are relatively prime.

Statement :

If $m_1, m_2, m_3, \ldots, m_n$ are pairwise relatively prime +ve integers & if $a_1, a_2, a_3, \ldots a_n$ are any integers, then the simultaneous congruences

$x \equiv a_1 \pmod{m_1}$ $\quad x \equiv a_2 \pmod{m_2}$ $\quad \ldots\ldots$ $\quad x \equiv a_n \pmod{m_n}$

have a soln, & the soln is unique modulo m, where

$m = m_1 \cdot m_2 \cdot m_3 \cdots m_n$

The soln is $x \equiv a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1} \pmod{m}$.

where $M_1 = \frac{m}{m_1} = m_2 m_3 \cdots m_n$

$M_2 = \frac{m}{m_2} = m_1 m_3 \cdots m_n$ & so on.

M_i^{-1} is a modular multiplicative inverse of M_i modulo m_i, $i = 1, 2, \ldots n$

$\therefore$ $M_i \equiv 0 \pmod{m_i}$ for $i = 2, 3, \ldots\ldots$ $(i \neq 1)$

$\gcd(m_1, M_1) = 1$

$M_i \times M_i^{-1} \equiv 1 \pmod{m_i}$

Modular multiplicative inverse

Given two integers a & m, the modular multiplicative inverse of a is an integer b such that

$$ab \equiv 1 \pmod{m}.$$

Note: * The value of b should be in the range $\{1, 2, \ldots, m-1\}$.

* $b \neq 0$ as $a \cdot 0 \bmod m$ will never be 1.

* The multiplicative inverse of $a \bmod m$ exists iff $\gcd(a, m) = 1$

Problems

1. Solve the following congruences using CRT

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Here 3, 5, 7 are relatively prime numbers.

$m = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$

$M_1 = m_2 m_3 = 35$

$M_2 = m_1 m_3 = 21$

$M_3 = m_1 m_2 = 15$

Given		To Calculate		
$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$	$m = 105$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$	
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$	

We have $M_i \times M_i^{-1} \equiv 1 \pmod{m_i}$

$35 \times M_1^{-1} \equiv 1 \pmod 3$

$35 \times 2 \equiv 1 \pmod 3$

$\therefore M_1^{-1} = 2$

$21 \times M_2^{-1} \equiv 1 \pmod 5$

$21 \times 1 \equiv 1 \pmod 5$

$\therefore M_2^{-1} = 1$

$15 \times M_3^{-1} \equiv 1 \pmod 7$

$15 \times 1 \equiv 1 \pmod 7$

$\therefore M_3^{-1} = 1$

We have $x \equiv a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} \pmod m$

$x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \pmod{105}$

$\therefore x \equiv 233 \pmod{105}$

$\Rightarrow x \equiv 23 \pmod{105}$

$105) \overline{233} (2$

$\underline{210}$

23

2. Solve the following congruences using CRT

$4x \equiv 5 \pmod 9$ Multiply by 4^{-1}. $x \equiv 4^{-1} \times 5 \pmod 9 \Rightarrow x \equiv 8 \pmod 9$

$2x \equiv 6 \pmod{20} \Rightarrow x \equiv 3 \pmod{10}$

Given		To calculate		
$a_1 = 8$	$m_1 = 9$	$M_1 = 10$	$M_1^{-1} = 1$	$m = 90$
$a_2 = 3$	$m_2 = 10$	$M_2 = 9$	$M_2^{-1} = 9$	

$m = m_1 \times m_2 = 9 \times 10 = 90$

$M_1 = m_2 = 10$ $\quad M_2 = m_1 = 9$

$M_1 \times M_1^{-1} \equiv 1 \pmod{m_1}$

$10 \times 1 \equiv 1 \pmod 9$

$\therefore M_1^{-1} \equiv 1$

$M_2 \times M_2^{-1} \equiv 1 \pmod{m_2}$

$9 \times 9 \equiv 1 \pmod{10}$

$M_2^{-1} = 9$

Now, $x \equiv a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} \pmod m$

$\equiv 8 \times 10 \times 1 + 3 \times 9 \times 9 \pmod{90}$

$\equiv 323 \pmod{90}$

$\therefore x \equiv 53 \pmod{90}$

90) 323 (3
270
53

[Multiplicative inverse of 4 i.e. 4^{-1} modulo 9 is 7.

$y \times 4^{-1} \equiv 1 \pmod 9$

$\therefore y = 7$]

$7 \times 5 = 35 \equiv 8 \pmod 9$

3. Solve the following using CRT.

$x \equiv 5 \pmod 3$ $\quad x \equiv 2 \pmod 5$ $\quad x \equiv 1 \pmod{11}$

Given

$a_1 = 5 \quad m_1 = 3$

$a_2 = 2 \quad m_2 = 5$

$a_3 = 1 \quad m_3 = 11$

To calculate

$M_1 = 55 \quad M_1^{-1} = 1$

$M_2 = 33 \quad M_2^{-1} = 2$

$M_3 = 15 \quad M_3^{-1} = 3$

$m = 165$

$M_1 = m_2 m_3 = 55$

$M_2 = m_1 m_3 = 33$

$M_3 = m_1 m_2 = 15$

$M_1 \times M_1^{-1} \equiv 1 \pmod{m_1}$

$55 \times M_1^{-1} \equiv 1 \pmod 3$

$55 \times 1 \equiv 1 \pmod 3$

$\therefore M_1^{-1} = 1$

$M_2 \times M_2^{-1} \equiv 1 \pmod{m_2}$

$33 \times M_2^{-1} \equiv 1 \pmod 5$

$33 \times 2 \equiv 1 \pmod 5$

$\therefore M_2^{-1} = 2$

$M_3 \times M_3^{-1} \equiv 1 \pmod{m_3}$

$15 \times M_3^{-1} \equiv 1 \pmod{11}$

$15 \times 3 \equiv 1 \pmod{11}$

$\therefore M_3^{-1} = 3$

$$x \equiv [a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}] \pmod m$$

$$\equiv [5 \times 55 \times 1 + 2 \times 33 \times 2 + 1 \times 15 \times 3] \pmod{165}$$

$\equiv 452 \pmod{165}$

$\equiv 122 \pmod{165}$

$165) 452 (2$

330

122

H.W : $x \equiv 5 \pmod 3$ $\quad x \equiv 2 \pmod 5$

Ans : $x \equiv 2 \pmod{15}$

4. Solve $3^{302} \mod 5005$ using CRT

$\therefore 5005 = 5 \times 7 \times 11 \times 13$

5	5005
7	1001
11	143
13	13
	1

Prime factorization

$m_1 = 5 \quad m_2 = 7$

$m_3 = 11 \quad m_4 = 13$

$M_1 = m_2 m_3 m_4 = 1001$

$M_2 = m_1 m_3 m_4 = 715$

$M_3 = m_1 m_2 m_4 = 455$

$M_4 = m_1 m_2 m_3 = 385$

To find a_i's values: $a_i \equiv 3^{302} \pmod{m_i}$

* $a_1 \equiv 3^{302} \pmod 5$

$302 = (60 \times 5) + 2$

$\therefore 3^{302} = (3^{60})^5 \cdot 3^2$

5) 302 (60
300
2

$3^4 \equiv 1 \pmod 5$

$(3^4)^{65} \equiv 1 \pmod 5$

$(3^{60})^5 \equiv 1 \pmod 5$

$3^{300} \cdot 3^2 \equiv 4 \pmod 5$

$3^1 = 3$
$3^2 = 9$
$3^3 = 27$
$3^4 = 81$
$3^5 = 243$

Or take $3^4 \equiv 1 \pmod 5$

$\therefore \boxed{a_1 = 4}$

* $a_2 \equiv 3^{302} \pmod 7$

7) 302 (43
28
22
21
1

$\therefore 302 = (43 \times 7) + 1.$

$3^{302} = (3^{43})^7 \cdot 3^1$

$3^3 \equiv -1 \pmod 7$

$(3^3)^{14} = 3^{42} \equiv 1 \pmod 7$

$3^{42} \cdot 3 = 3^{43} \equiv 3 \pmod 7$

$(3^{43})^7 \equiv 3^7 \pmod 7$ $\quad \because 3^7 = 3^3 \cdot 3^3 \cdot 3$

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

$\therefore 3^{301} \equiv 3 \pmod 7$

$3^{301} \cdot 3 = 3^{302} \equiv 3 \cdot 3 \pmod 7$

$\equiv 2 \pmod 7$

$\therefore \boxed{a_2 = 2}$

* $a_3 \equiv 3^{302} \pmod{11}$

$3^5 = 243 \equiv 1 \pmod{11}$ $\quad \therefore$ $5)\overline{302}\,(60$
 $\underline{300}$
 2

$302 = (60 \times 5) + 2$

$(3^5)^{60} \equiv 1 \pmod{11}$

$3^{300} \cdot 3^2 \equiv 3^2 \pmod{11}$

$\equiv 9 \pmod{11}$

$\therefore \boxed{a_3 = 9}$

* $a_4 \equiv 3^{302} \pmod{13}$

$302 = (3 \times 100) + 2$ $\quad$ & $3^3 \equiv 1 \pmod{13}$

$\therefore (3^3)^{100} \equiv 1 \pmod{13}$

$3^{300} \cdot 3^2 \equiv 9 \pmod{13}$

$\therefore \boxed{a_4 = 9}$

Now, $x \equiv a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} + a_4 M_4 M_4^{-1} \pmod{m}$

$M_1 \times M_1^{-1} \equiv 1 \pmod{m_1}$

$1001 \times 1 \equiv 1 \pmod{5}$

$\therefore M_1^{-1} = 1$

$M_2 \times M_2^{-1} \equiv 1 \pmod{m_2}$

$715 \times 1 \equiv 1 \pmod{7}$

$\therefore M_2^{-1} = 1$

7) 715 (102
7
015
14
1

$M_3 \times M_3^{-1} \equiv 1 \pmod{m_3}$

$455 \times 3 \equiv 1 \pmod{11}$

$\therefore M_3^{-1} = 3$

Calculate $[(455 \times 3) - 1] \div 11 = 124$

$\Rightarrow 11 / (455 \times 3) - 1$

$M_4 \times M_4^{-1} \equiv 1 \pmod{m_4}$

$385 \times 5 \equiv 1 \pmod{13}$

$\therefore M_4^{-1} = 5$

$\therefore x \equiv [4 \times 1 \times 1001 + 2 \times 1 \times 715 + 9 \times 3 \times 455 + 9 \times 5 \times 385] \bmod 5005$

$\equiv 35044 \pmod{5005}$

$\equiv 9 \pmod{5005}$

5005) 35044 (7
35035
9

Linear Diophantine Eqns

A linear Diophantine eqn (LDE) is an eqn with 2 or more more integer unknowns & the integer unknowns are each to at most degree of 1.

LDE in two variables takes the form of $ax+by=c$ where $x,y \in \mathbb{Z}$ & a,b,c are integer constants. Here x & y are unknown variables.

A homogeneous LDE is $ax+by=0$, $x,y \in \mathbb{Z}$.

Note that $x=0$ & $y=0$ is a soln, called the trivial soln

Ex: $5x+3y=0$, $x,y \in \mathbb{Z}$

Here $x=0$, $y=0$ is the trivial soln

$x=3$, $y=-5$ is a soln

$x=6$, $y=-10$ is a soln

In general, $x=3t$ & $y=-5t$, $t \in \mathbb{Z}$ is the soln.

Thm: Let $ax+by=0$ —(1), $x,y \in \mathbb{Z}$ be a homogeneous LDE. If $\gcd(a,b)=d$, then the family of solns to (1) is given by $\left\{x=\frac{b}{d}t,\ y=\frac{-a}{d}t : t \in \mathbb{Z}\right\}$

Ex: Solve $6x+9y=0$, $x,y \in \mathbb{Z}$

$\gcd(6,9)=3$

$\therefore$ Solns are $x=\frac{9}{3}k=3t$

$y=\frac{-6}{3}k=-2t$

where $t \in \mathbb{Z}$.

Thm: Let $a, b, c \in \mathbb{Z}$. Consider the Diophantine eqn

$$ax + by = c$$

* If $\gcd(a,b) \nmid c$, there are no solns
* If $\gcd(a,b) \mid c$, there are infinitely many solns of the form

$$x = x_0 + \frac{b}{d}t \quad , \quad y = y_0 - \frac{a}{d}t$$

where (x_0, y_0) is a particular soln & $t \in \mathbb{Z}$

Problems

1. Which of the following Diophantine eqns cannot be solved:

(i) $6x + 51y = 22$ (ii) $33x + 14y = 115$ (iii) $54x + 21y = 906$

(i)
$$\begin{array}{r|l} 6 & 51 \ (8 \\ \underline{48} & \\ 3 & \end{array} \qquad \begin{array}{r|l} 3 & 6 \ (2 \\ \underline{6} & \\ 0 & \end{array}$$

$\therefore \gcd(6, 51) = 3$ & $3 \nmid 22$

$\therefore$ (i) is not solvable

(ii)
$$\begin{array}{r|l} 14 & 33 \ (2 \\ \underline{28} & \\ 5 & \end{array} \qquad \begin{array}{r|l} 5 & 14 \ (2 \\ \underline{10} & \\ 4 & \end{array} \qquad \begin{array}{r|l} 4 & 5 \ (1 \\ \underline{4} & \\ 1 & \end{array}$$

$\therefore \gcd(33, 14) = 1$ & $1 \mid 115$

$\therefore$ (ii) is solvable.

(iii)
$$\begin{array}{r|l} 21 & 54 \ (2 \\ \underline{42} & \\ 12 & \end{array} \qquad \begin{array}{r|l} 12 & 21 \ (1 \\ \underline{12} & \\ 9 & \end{array} \qquad \begin{array}{r|l} 9 & 12 \ (1 \\ \underline{9} & \\ 3 & \end{array} \qquad \begin{array}{r|l} 3 & 9 \ (3 \\ \underline{9} & \\ 0 & \end{array}$$

$\therefore \gcd(54, 21) = 3$ & $3 \mid 906$ $\therefore$ (iii) is solvable.

Algorithm to solve non-homogeneous Diophantine eqn.

$ax+by = c$ —①, $x, y \in Z$

step 1: Find $d = \gcd(a,b)$

step 2: If d/c, ∃ infinitely many solns

Let $\frac{c}{d} = k$ & goto step 3.

Otherwise, no soln.

step 3: Express $d = au+bv$ —②

step 4: $d = au+bv \quad \times k$ i.e. Multiply ② by k.

$\therefore dxk = a(uk) + b(vk)$

i.e. $c = ax_0 + by_0$ & (x_0, y_0) is a particular soln of ①

step 5: Gen. soln of $ax+by=c$ is given by

$x = x_0 + \frac{b}{d}t \qquad y = y_0 - \frac{a}{d}t, \quad t \in Z$

2. Solve $6x + 9y = 21$ — ①

$\gcd(6, 9) = 3$ & $3 \mid 21$, $a = 6,\ b = 9,\ d = 3$

∴ ① has infinite solns

Dividing ① by 3, $2x + 3y = 7$

By inspection $x_0 = 2,\ y_0 = 1$ is a particular soln. i.e. $2(2) + 3(1) = 7$

∴ Gen. soln is $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$

$x = 2 + 3t$, $y = 1 - 2t$, $t \in \mathbb{Z}$

3. Find the general soln of $70x + 112y = 168$ — ①

$a = 70,\ b = 112,\ c = 168$

$70)\ 112\ (1$ $\quad$ $42)\ 70\ (1$ $\quad$ $28)\ 42\ (1$ $\quad$ $14)\ 28\ (2$

$\underline{70}$ $\quad$ $\underline{42}$ $\quad$ $\underline{28}$ $\quad$ $\underline{28}$

42 $\quad$ 28 $\quad$ 14 $\quad$ 0

∴ $\gcd(70, 112) = 14 = d$

$42 = 112 - 1 \cdot 70$

$28 = 70 - 1 \cdot 42$

$14 = 42 - 1 \cdot 28$

$14 = 42 - 1 \cdot 28$

$= 42 - 70 + 42$

$= 2(42) - 70$

$= 2(112 - 70) - 70$

Express d as $d = au + bv$

∴ $14 = 70(-3) + 112(2)$ — ②

Also $14 \mid 168$ ∴ ① has soln. Let $k = \frac{168}{14} = 12$

Multiply ② by $k = 12$

$d \times k = a(uk) + b(vk)$

$14 \times 12 = 70(-3)(12) + 112(2)(12)$

$168 = 70(-36) + 112(24)$ i.e. $c = ax_0 + by_0$

∴ $x_0 = -36$, $y_0 = 24$ is a particular soln of ①.

$a = 70$, $b = 112$, $d = 14$

$\therefore$ Gen. soln is. $x = x_0 + \frac{b}{d}t \quad , \quad y = y_0 - \frac{a}{d}t$

$x = -36 + \left(\frac{112}{14}\right)t \quad , \quad y = 24 - \left(\frac{70}{14}\right)t$

$\therefore \; x = -36 + 8t \quad , \quad y = 24 - 5t \quad , t \in Z$

[Verify by taking $t = 1$: $70(-28) + 112(19) = 168$]

4. Solve $39x - 56y = 11$ —①

$a = 39 \; , \quad b = -56 \; , \quad c = 11$

To find gcd of 39 & 56

$39)\,56\,(1$	$17)\,39\,(2$	$5)\,17\,(3$	$2)\,5\,(2$	$1)\,2\,(2$
$\underline{39}$	$\underline{34}$	$\underline{15}$	$\underline{4}$	$\underline{2}$
17	5	2	1	0

$\therefore \; \gcd(39, 56) = 1 = d$

& $1 / 11$. $\Rightarrow$ ① has soln

Let $k = \frac{11}{1} = 11$

To express d as $d = au + bv$

$1 = 5 - 2(2)$

$= 5 - 2[17 - 3(5)]$

$= 7(5) - 2(17)$

$= 7[39 - 2(17)] - 2[56 - 1(39)]$

$= 39(9) + (-56)(2) - 14[56 - 1(39)]$

$1 = 39(23) + (-56)(16)$ —②

$1 = 5 - 2(2)$

$2 = 17 - 3(5)$

$5 = 39 - 2(17)$

$17 = 56 - 1(39)$

Multiply ② by $k = 11$

$1 \times 11 = 39(23 \times 11) + (-56)(16 \times 11)$

$11 = 39(253) + (-56)(176)$

i.e. $c = ax_0 + by_0$

$\therefore x_0 = 253$, $y_0 = 176$ is a particular soln of ①.

Gen. soln. of ① is

$x = x_0 + \frac{b}{d}t$ $\qquad$ $y = y_0 - \frac{a}{d}t$, $t \in Z$

$= 253 + \left(\frac{-56}{1}\right)t$ $\qquad$ $= 176 - \left(\frac{39}{1}\right)t$

$= 253 - 56t$ $\qquad$ $= 176 - 39t$

[Verify by taking $t = 1$]

5. Solve $7x + 18y = 208$ — ①

$a = 7$, $b = 18$, $c = 208$

To find gcd of 7 & 18

7) 18 (2 $\quad$ 4) 7 (1 $\quad$ 3) 4 (1

14 $\quad$ 4 $\quad$ 3

4 $\quad$ 3 $\quad$ 1

$4 = 18 - 2(7)$

$3 = 7 - 1(4)$

$1 = 4 - 1(3)$

$\therefore$ gcd $(7, 18) = 1 = d$ & $1 / 208 \Rightarrow$ ① has soln.

Let $k = \frac{208}{1} = 208$

To express d as $d = au + bv$

$1 = 4 - 1(3)$

$= 4 - 1[7 - 1(4)]$

$= 2(4) + 7(-1)$

$= 2[18 - 2(7)] + 7(1)$

$1 = 7(-5) + 18(2)$ — ②

Multiply ② by $k = 208$

$1 \times 208 = 7(-5 \times 208) + 18(2 \times 208)$

$208 = 7(-1040) + 18(416)$

i.e $c = a x_0 + b y_0$

$\therefore x_0 = -1040$, $y_0 = 416$ is a particular soln.

Gen. soln of ① is

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

$= -1040 + 18t$

$y = y_0 - \frac{a}{d}t \quad , t \in Z$

$= 416 - 7t$

6. Solve $56x + 72y = 40$ — ①

$a = 56$, $b = 72$, $c = 40$

To find gcd of 56, 72

56) 72 (1 — 56

16

16) 56 (3 — 48

8

8) 16 (2 — 16

0

$8 = 56 - 3(16)$

$16 = 72 - 1(56)$

$\therefore$ gcd $(56, 72) = 8$

& $8 / 40 \Rightarrow$ ① has soln.

Let $k = \frac{40}{8} = 5$

To express d as $d = au + bv$

$8 = 56 - 3(16)$

$= 56 - 3[72 - 1(56)]$

$8 = 56(4) + 72(-3)$ — ②

Multiply ② by $k = 5$.

$8 \times 5 = 56(4 \times 5) + 72(-3 \times 5)$

$40 = 56(20) + 72(-15)$

i.e. $c = ax_0 + by_0$

$\therefore x_0 = 20$, $y_0 = -15$ is a particular soln.

Gen. soln of ① is

$x = x_0 + \frac{b}{d}t = 20 + \frac{72}{8}t = 20 + 9t$

$t \in Z$.

$y = y_0 - \frac{a}{d}t = -15 - \frac{56}{8}t = -15 - 7t$

7. Solve $172x + 20y = 1000$ —①

$a = 172$, $b = 20$, $c = 1000$

To find gcd of 172 , 20

$20)\overline{172}\,(8$ $\quad 160$ $\quad 12$

$12)\overline{20}\,(1$ $\quad 12$ $\quad 8$

$8)\overline{12}\,(1$ $\quad 8$ $\quad 4$

$4)\overline{8}\,(2$ $\quad 8$ $\quad 0$

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

& $4 / 1000 \Rightarrow$ ① has soln.

Let $k = \frac{1000}{4} = 250$

To express d as $d = au + bv$

$4 = 12 - 1(8)$

$= 12 - 1[20 - 1(12)]$

$= 2(12) + 20(-1)$

$= 2[172 - 8(20)] + 20(-1)$

$4 = 172(2) + 20(-17)$ —②

$4 = 12 - 1(8)$

$8 = 20 - 1(12)$

$12 = 172 - 8(20)$

Multiply ② by 250

$4 \times 250 = 172(2 \times 250) + 20(-17 \times 250)$

$1000 = 172(500) + 20(-4250)$

i.e $c = ax_0 + by_0$

$\therefore x_0 = 500$, $y_0 = -4250$ is a particular soln

Gen. soln of ① is

$x = x_0 + \frac{b}{d}t = 500 + \frac{20}{4}t = 500 + 5t$

$t \in Z$

$y = y_0 - \frac{a}{d}t = -4250 - \frac{172}{4}t = -4250 - 43t$

[Verify by taking $t = 1$

$172(505) + 20(-4293) = 1000$]

System of linear congruences

Thm: The system of linear congruences

$$ax+by \equiv r \pmod n$$
$$cx+dy \equiv s \pmod n$$

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

1. Solve $7x+3y \equiv 10 \pmod{16}$ — ①
$2x+5y \equiv 9 \pmod{16}$ — ②

$a=7$, $b=3$, $c=2$, $d=5$, $n=16$

$\gcd(ad-bc, n) = \gcd(35-6, 16) = \gcd(29, 16) = 1$

∴ system has unique soln modulo 16.

$7x+3y \equiv 10 \pmod{16}$ ×5
$2x+5y \equiv 9 \pmod{16}$ ×3

$35x+15y \equiv 50 \pmod{16}$
$6x+15y \equiv 27 \pmod{16}$
(−) (−) (−)
$29x \equiv 23 \pmod{16}$

$13x \equiv 7 \pmod{16}$

∵ Remainders of 29 & 23 are resp. 13 & 7 when they are divided by 16

Multiplicative inverse of 13 modulo 16 is 5.

i.e. $13 \times 5 \equiv 1 \pmod{16}$

∴ $13x \equiv 7 \pmod{16}$ ×5

$x \equiv 35 \pmod{16}$

∴ $\boxed{x \equiv 3 \pmod{16}}$

From ②, $2(3)+5y \equiv 9 \pmod{16}$ ⇒ $5y \equiv 3 \pmod{16}$ ×13

$(5 \times 13)y \equiv 13 \times 3 \pmod{16}$

∴ $\boxed{y \equiv 7 \pmod{16}}$

Verify by taking $x=3$ & $y=7$ in ① & ②.

2. Solve $5x+3y \equiv 2 \pmod{14}$ —①

$-3x+4y \equiv 7 \pmod{14}$ —②

$a=5,\ b=3,\ c=-3,\ d=4,\ n=14$

$\gcd(ad-bc, n) = \gcd(29, 14) = 1$

∴ the system has unique soln modulo 14.

$5x+3y \equiv 2 \pmod{14}$ $\times 3$

$-3x+4y \equiv 7 \pmod{14}$ $\times 5$

$15x+9y \equiv 6 \pmod{14}$

$-15x+20y \equiv 35 \pmod{14}$

$29y \equiv 41 \pmod{14}$

∴ $\boxed{y \equiv 13 \pmod{14}}$

From ②, $-3x \equiv -45 \pmod{14}$

$3x \equiv 45 \pmod{14}$

Since 5 is the multiplicative inverse of 3 modulo 14,

$3 \times 5 \equiv 1 \pmod{14}$.

∴ $3x \equiv 45 \pmod{14}$ $\times 5$

$x \equiv 225 \pmod{14}$

∴ $\boxed{x \equiv 1 \pmod{14}}$

OR from ①,

$5x \equiv -37 \pmod{14}$ $\times 3$

$x \equiv -111 \pmod{14}$

$\equiv -13 \pmod{14}$

$14)225(16$

14

85

84

1

Verification:

From ①, $14/42$

From ②, $14/42$

MQP

3. Solve $2x + 6y \equiv 1 \pmod 7$ —①

$4x + 3y \equiv 2 \pmod 7$ —②

$a = 2, \quad b = 6, \quad c = 4, \quad d = 3, \quad n = 7$

$\gcd(ad - bc, n) = \gcd(-18, 7) = 1$.

$\therefore$ the system has unique soln modulo 7.

$2x + 6y \equiv 1 \pmod 7 \quad \times 4$

$4x + 3y \equiv 2 \pmod 7 \quad \times 2$

$$8x + 24y \equiv 4 \pmod 7$$

$$(-)\ 8x + (-)\ 6y \equiv (-)\ 4 \pmod 7$$

$$18y \equiv 0 \pmod 7$$

$$\therefore \boxed{y \equiv 0 \pmod 7}$$

From ①, $2x \equiv 1 \pmod 7$

4 is the multiplicative inverse of 2 modulo 7.

$\therefore \quad 2x \equiv 1 \pmod 7 \quad \times 4$

$\therefore \quad \boxed{x \equiv 4 \pmod 7}$

Verification:

From ①, $7 / 8 - 1 = 1$

From ②, $7 / 16 - 2$

Euler's totient / phi function

It counts the number of +ve integers upto a given integer $n (\geq 2)$ that are relatively prime to n.

It is denoted by $\phi(n)$.

i.e. $$\phi(n) = n \prod_{p|n} (1 - 1/p)$$

where product is over distinct primes p dividing n.

n	invertible elements mod n	$\phi(n)$
2	1	1
3	1, 2	2
4	1, 3	2
5	1, 2, 3, 4	4
6	1, 5	2
7	1, 2, 3, 4, 5, 6	6
8	1, 3, 5, 7	4
9	1, 2, 4, 5, 7, 8	6
10	1, 3, 7, 9	4
12	1, 5, 7, 11	4

Note: If n is prime, then $\phi(n) = n - 1$

Euler's thm

If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$

Problems

1. Find the last digit of 3^{30} by using Euler's thm.

$a=3,\ n=10$, $\phi(n) = n\prod_{p/n}(1-1/p) = 10(1-1/2)(1-1/5) = 4$

By Euler's thm,

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

$3^{\phi(10)} \equiv 1 \pmod{10}$

$3^4 \equiv 1 \pmod{10}$

$(3^4)^7 \cdot 3^2 \equiv (1)^7 \cdot 9 \pmod{10}$

$\therefore 3^{30} \equiv 9 \pmod{10}$

$\therefore$ last digit is 9.

2. Find the last two digits of 11^{84}.

To find last two digits take mod 100. $\therefore a=11, n=100.$

$\phi(n) = n\prod_{p/n}(1-1/p)$ by Euler's totient function.

$\phi(100) = 100(1-1/2)(1-1/5) = 40$

$a^{\phi(n)} \equiv 1 \pmod{n}$ by Euler's thm

$11^{40} \equiv 1 \pmod{100}$

$(11^{40})^2 \cdot 11^4 \equiv 1^2 \cdot 11^4 \pmod{100}$

$11^{84} \equiv 14641 \pmod{100}$

$\therefore$ last two digits are 4,1. respectively.

3. Find the remainder when 2^{10} is divided by 11.

Or find b, $2^{10} \equiv b \pmod{11}$. by Euler's thm

$a = 2, \quad n = 11.$

$$\phi(n) = n \prod_{p/n} (1 - 1/p)$$

$$\phi(11) = 11 \left(1 - \tfrac{1}{11}\right) = 10$$

Now, $a^{\phi(n)} \equiv 1 \pmod{n}$ by Euler's thm

$$2^{10} \equiv 1 \pmod{11}$$

$\therefore$ remainder is 1 or $b = 1$.

4. Find the remainder when 2^{2003} is divided by 11.

By above ex. $2^{10} \equiv 1 \pmod{11}$

$$(2^{10})^{200} \cdot 2^3 \equiv 1^{200} \cdot 2^3 \pmod{11}$$

$$2^{2003} \equiv 8 \pmod{11}.$$

$\therefore$ remainder is 8.

Wilson's thm

If p is a prime number then $\boxed{(p-1)! \equiv -1 \pmod{p}}$

or $\boxed{(p-1)! \equiv p-1 \pmod{p}}$

Note:

$(p-1)(p-2)! \equiv p-1 \pmod{p}$

W.k.t. if $ab \equiv ac \pmod{m}$ & $\gcd(a,m) = 1$, then $b \equiv c \pmod{m}$.

$\therefore \boxed{(p-2)! \equiv 1 \pmod{p}}$

Also, $\boxed{(p-3)! \equiv \frac{p-1}{2} \pmod{p}}$

Problems

1. What is the remainder in the division of 12! by 13.

By Wilson's thm, $(p-1)! \equiv p-1 \pmod{p}$

$\therefore 12! \equiv 12 \pmod{13}$

$\Rightarrow$ 12 is the remainder.

2. Illustrate the Wilson's thm for $p = 13$.

i.e. to show $12! \equiv -1 \pmod{13}$

$2^{-1} \pmod{13} = 7$ $\qquad$ $5^{-1} \pmod{13} = 8$

$3^{-1} \pmod{13} = 9$ $\qquad$ $6^{-1} \pmod{13} = 11$

$4^{-1} \pmod{13} = 10$

$12! = 12 \times 11 \times 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$

$\therefore 12! \equiv (1\times12)(2\times7)(3\times9)(4\times10)(5\times8)(6\times11) \pmod{13}$

$\equiv (-1)(1)(1)(1)(1)(1) \pmod{13}$

$\equiv -1 \pmod{13}$

or

$\equiv 12 \pmod{13}$

Fermat's little thm (Fermat's thm)

If p is prime & $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$

(It's a particular case of Euler's thm)

Note: If p is prime & $p \nmid a$ then $a^p \equiv a \pmod{p}$

Problems

1. Find the remainder of 50^{250} when it is divided by 83.

   Or. Reduce $50^{250} \pmod{83}$ to a number in the range $\{0, 1, 2, \ldots, 82\}$

   Since 83 is prime & $83 \nmid 50$, by Fermat's thm

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

   $50^{82} \equiv 1 \pmod{83}$

   $(50^{82})^3 \equiv 1^3 \pmod{83}$

   $50^{246} \equiv 1 \pmod{83}$

   $50^{246} \cdot 50^4 \equiv 50^4 \pmod{83}$

   $50^{250} \equiv 6250000 \pmod{83}$

   $\equiv 17 \pmod{83}$

   $\therefore$ remainder is 17.

   $82)\overline{250}\,(3$
   $\underline{246}$
   4

   $\therefore 250 = (3 \times 82) + 4$

2. Reduce $47^{222} \pmod{113}$ to a number in the range $\{0, 1, 2, \ldots, 112\}$

   Since 113 is prime & $113 \nmid 47$, by Fermat's thm

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

   $47^{112} \equiv 1 \pmod{113}$

   $112)\overline{222}\,(1$
   $\underline{112}$
   110

$47^{112} \cdot 47^{110} \equiv 1 \cdot 47^{110} \pmod{113} \Rightarrow 47^{222} \equiv 47^{110} \pmod{113}$

Now, $x \equiv 47^{110} \pmod{113}$

$47^2 \cdot x \equiv 47^2 \cdot 47^{110} \pmod{113}$

$2209\, x \equiv 47^{112} \pmod{113}$

$62x \equiv 1 \pmod{113}$ —①

To find the inverse of 62 mod 113 :

[gcd (62, 113)]

62) 113 (1
62
51

$51 = 113 - 1 \cdot 62$

51) 62 (1
51
11

$11 = 62 - 1 \cdot 51$

11) 51 (4
44
7

$7 = 51 - 4 \cdot 11$

7) 11 (1
7
4

$4 = 11 - 1 \cdot 7$

4) 7 (1
4
3

$3 = 7 - 1 \cdot 4$

3) 4 (1
3
1

$1 = 4 - 1 \cdot 3$

1) 3 (3
3
0

$\therefore$ gcd (62, 113) = 1.

To express $1 = 62u + 113v$:

$1 = 4 - 1 \cdot 3$

$= 4 - [7 - 1 \cdot 4]$

$= 2 \cdot 4 - 7$

$= 2[11 - 1 \cdot 7] - 7$

$= 2 \cdot 11 - 3 \cdot 7$

$= 2 \cdot 11 - 3[51 - 4 \cdot 11]$

$= 14 \cdot 11 - 3 \cdot 51$

$= 14[62 - 1 \cdot 51] - 3 \cdot 51$

$= 14 \cdot 62 - 17 \cdot 51$

$= 14 \cdot 62 - 17[113 - 1 \cdot 62]$

$\therefore 1 = 62(31) + 113(-17)$

i.e $62 \times 31 \equiv 1 \pmod{113}$

$\therefore$ Inverse of 62 mod 113 is 31

Multiply ① by 31,

$(62 \times 31)x \equiv 31 \pmod{113}$

$\therefore x \equiv 31 \pmod{113}$

$\therefore$ 31 is the ans.

3. Compute $12 \cdot 13 \cdot \cdots \cdot 20 \cdot 21 \pmod{11}$

The any ten consecutive numbers, none divisible by 11, reduce mod 11 to $\{1, 2, \cdots, 10\}$

$\therefore \quad 12 \cdot 13 \cdot \cdots \cdot 20 \cdot 21 = 10! \equiv -1 \pmod{11}$ by Wilson's thm

$\equiv 10 \pmod{11}$

4. Simplify $\frac{130!}{87} \pmod{131}$ to a number in the range $\{1, 2, \cdots, 130\}$

By Wilson's thm $130! \equiv -1 \pmod{131}$

Let $x \equiv \frac{130!}{87} \pmod{131}$

$87x \equiv 130! \pmod{131}$

$87x \equiv -1 \pmod{131}$ —①

To find $87^{-1} \bmod 131$.

$87)131(1$ $\quad$ $44)87(1$ $\quad$ $43)44(1$

$\underline{87}$ $\quad$ $\underline{44}$ $\quad$ $\underline{43}$

44 $\quad$ 43 $\quad$ 1

$44 = 131 - 1 \cdot 87$ $\quad$ $43 = 87 - 1 \cdot 44$ $\quad$ $1 = 44 - 1 \cdot 43$

To express $1 = 87u + 131v$

$1 = 44 - 1 \cdot 43$

$= 131 - 1 \cdot 87 - 87 + 1 \cdot 44$

$= 131 - 2 \cdot 87 + 1 \cdot 44$

$= 131 - 2 \cdot 87 + 131 - 1 \cdot 87$

$= 87(-3) + 131(2)$

i.e. $87(-3) \equiv 1 \pmod{131}$ $\quad$ But $-3 \equiv 128 \pmod{131}$

$\therefore$ Inverse of 87 mod 131 is 128

Multiply ① by 128.

$(87 \times 128)x \equiv -128 \pmod{131}$

$\therefore \quad x \equiv 3 \pmod{131}$

5. Find the remainder when 146! is divided by 149

By Wilson's thm, $148! \equiv -1 \pmod{149}$

Let $x \equiv 146! \pmod{149}$

$147 \cdot 148\, x \equiv 147 \cdot 148 \cdot 146! \pmod{149}$

$(-2)(-1)x \equiv 148! \pmod{149}$ $\quad \therefore 147 \equiv -2 \pmod{149}$

$148 \equiv -1 \pmod{149}$

$-2x \equiv 1 \pmod{149}$ —— ①

To find the inverse of $-2 \bmod 149$.

$$
\begin{array}{r|l}
2 & 149 \\
 & \underline{14} \\
 & 9 \\
 & \underline{8} \\
 & 1
\end{array}
\quad 74
$$

$\therefore 1 = 149 - 2 \cdot 74$

$\therefore (-2)(74) \equiv 1 \pmod{149}$

$\therefore$ Inverse of $-2 \bmod 149$ is 74.

Multiply ① by 74.

$(-2 \times 74)x \equiv 74 \pmod{149}$

$\therefore \quad x \equiv 74 \pmod{149}$

$\therefore$ the remainder is 74.

6. Find the remainder when $14!$ is divided by 17.

By Wilson's thm, $16! \equiv -1 \pmod{17}$

Let $x \equiv 14! \pmod{17}$

$16 \cdot 15\, x \equiv 16 \cdot 15 \cdot 14! \pmod{17}$

$(-1)(-2)\, x \equiv 16! \pmod{17}$

$2x \equiv -1 \pmod{17}$

$\therefore -2x \equiv 1 \pmod{17}$ —— (1)

To find the inverse of $-2 \bmod 17$.

$2)\ 17\ (8$

$\frac{16}{1}$

$\therefore 1 = 17 - 8 \cdot 2$

$\therefore (-2)(8) \equiv 1 \pmod{17}$

$\therefore$ Inverse of $-2 \bmod 17$ is 8.

Multiply (1) by 8

$(-2)(8)\, x \equiv (1)(8) \pmod{17}$

$\therefore x \equiv 8 \pmod{17}$

$\therefore$ the remainder is 8.

7. Solve $f(x) = x^3 + 5x + 1 \equiv 0 \pmod{27}$

$x^3 + 5x + 1 \equiv 0 \pmod{3^3}$

$x^3 + 5x + 1 \equiv 0 \pmod{3}$

$\therefore$ possible values of x are $0, 1, 2$.

$f(0) = 1 \not\equiv 0 \pmod{3}$

$f(1) = 7 \not\equiv 0 \pmod{3}$

$f(2) = 19 \not\equiv 0 \pmod{3}$.

$\therefore f(x) = x^3 + 5x + 1 \equiv 0 \pmod{27}$ has no soln.

8. Find the remainder when 14! is divided by 17

Don't follow this method

By Wilson's thm,

$$(p-1)! \equiv -1 \equiv p-1 \pmod{p} \quad \text{—①}$$

$$(p-2)! \equiv 1 \pmod{p} \quad \text{—②}$$

$$(p-3)! \equiv \frac{p-1}{2} \pmod{p} \quad \text{—③}$$

From ③, $14! \equiv \frac{17-1}{2} = 8 \pmod{17}$

$\therefore$ 8 is the remainder.

9. What is the remainder when $(14!)^{38}$ is divided by 17.

$$(14!)^{38} \equiv 8^{38} \pmod{17}$$

$$\equiv 2^{3\times 38} \pmod{17}$$

$$\equiv 2^{114} \pmod{17}$$

$$\equiv 2^{4\times 28} \cdot 2^2 \pmod{17}$$

$$\equiv (-1)^{28} \cdot 2^2 \pmod{17}$$

$$\equiv 4 \pmod{17}$$

$\therefore$ 4 is the remainder.

$2^2 = 4$

$2^3 = 8$

$2^4 = 16 \equiv -1 \pmod{17}$

$$4)\,114\,(28$$
$$\underline{8}$$
$$34$$
$$\underline{32}$$
$$2$$

$\therefore 114 = (4\times 28) + 2$

10. What is the remainder when $1! + 2! + 3! + \cdots + 2021!$ is divided by 21.

All the factorials greater than or equal to $7!$ will be divisible by 21 as they contain 3 & 7.

$\Rightarrow$ remainder will be zero when the factorials greater than or equal to $7!$ are divided by 21.

$\therefore$ we have to find the remainder when

$1! + 2! + \cdots + 6!$ is divided by 21.

$1! = 1$, $\quad 1! \equiv 1 \pmod{21}$

$2! = 2$, $\quad 2! \equiv 2 \pmod{21}$

$3! = 6$, $\quad 3! \equiv 6 \pmod{21}$

$4! = 24$, $\quad 4! \equiv 3 \pmod{21}$

$5! = 120$, $\quad 5! \equiv 15 \pmod{21}$

$6! = 720$, $\quad 6! \equiv 6 \pmod{21}$

$$21) \begin{array}{r} 120 \,(5 \\ 105 \\ \hline 15 \end{array}$$

$$21) \begin{array}{r} 720 \,(34 \\ 63 \\ \hline 90 \\ 84 \\ \hline 6 \end{array}$$

$\therefore 1! + 2! + \cdots + 6!$

$\equiv 1 + 2 + 6 + 3 + 15 + 6 \pmod{21}$

$\equiv 33 \pmod{21}$

$\equiv 12 \pmod{21}$

$\therefore$ 12 is the remainder.

11. Using Fermat' Little thm, show that $8^{30} - 1$ is divisible by 31.

Let $p = 31$ & $a = 8$.

Since p is prime & $p \nmid a$, by Fermat's Little thm

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

$$\therefore 8^{30} \equiv 1 \pmod{31}$$

$$\Rightarrow 8^{30} - 1 \text{ is divisible by } 31.$$

12. Find the (smallest integer) remainder when 11^{104} is divided by 17.

Let $p = 17$, $a = 11$. Since p is prime & $p \nmid a$, by Fermat's little thm,

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

$$11^{16} \equiv 1 \pmod{17}$$

$$(11^{16})^6 \equiv 1^6 \pmod{17}$$

$$11^{96} \equiv 1 \pmod{17}$$

$$11^{96} \cdot 11^8 \equiv 11^8 \pmod{17}$$

$$\therefore 11^{104} \equiv 16 \pmod{17}$$

$\therefore$ remainder is 16.

$$16 \overline{)104} \ (6$$
$$\underline{96}$$
$$8$$

$\therefore 104 = (16 \times 6) + 8$

$$11^2 = 121 \equiv 2 \pmod{17}$$

$$(11^2)^4 \equiv 2^4 \pmod{17}$$

$$11^8 \equiv 16 \pmod{17}$$

H.W.

13. $2^{53} \pmod{11}$

By FLT, $2^{10} \equiv 1 \pmod{11}$

$$(2^{10})^5 \cdot 2^3 \equiv 8 \pmod{11}.$$

14. Find the remainder of 67! when divided by 71.

By Wilson's thm, $(p-1)! \equiv -1 \pmod{p}$

$\therefore 70! \equiv -1 \pmod{71}$

$70 \times 69 \times 68 \times 67! \equiv -1 \pmod{71}$

$(-1)(-2)(-3)\,67! \equiv -1 \pmod{71}$

$(6)\,67! \equiv 1 \pmod{71}$ —①

To find multiplicative inverse of 6 mod 71 (or to find $6^{-1} \bmod 71$)

$6)\,71\,(11$ $\quad$ $5)\,6\,(1$

$\begin{array}{r} 6 \\ \hline 11 \\ 6 \\ \hline 5 \end{array}$ $\quad$ $\begin{array}{r} 5 \\ \hline 1 \end{array}$

$5 = 71 - 6 \cdot 11$ $\quad$ $1 = 6 - 1 \cdot 5$

$\therefore 1 = 6 - 1 \cdot 5$

$= 6 - 71 + 6 \cdot 11$

$= 6(12) + 71(-1)$

$\therefore$ inverse of 6 mod 71 is 12

Multiply ① by 12

$(6 \times 12)\,67! \equiv 1 \times 12 \pmod{71}$

$67! \equiv 12 \pmod{71}$

$\therefore$ remainder is 12.

H.W.

15. Find the remainder of 97! when divided by 101.

$100! \equiv -1 \pmod{101}$

$100 \times 99 \times 98 \times 97! \equiv -1 \pmod{101}$

$(-1)(-2)(-3)\,97! \equiv -1 \pmod{101}$

$(6)\,97! \equiv 1 \pmod{101}$

Inverse of 6 mod 101 is 17

$\therefore 97! \equiv 17 \pmod{101}$

$\Rightarrow$ remainder is 17.

16. Find the remainder of 149! when divided by 139.

By Wilson's thm, $(p-1)! \equiv -1 \pmod{p}$

$\therefore 138! \equiv -1 \pmod{139}$

Now, $149! = 149 \times 148 \times 147 \times 146 \times 145 \times 144 \times 143 \times 142 \times 140 \times 139 \times 138!$

$\equiv 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 \times 0 \times (-1) \pmod{139}$

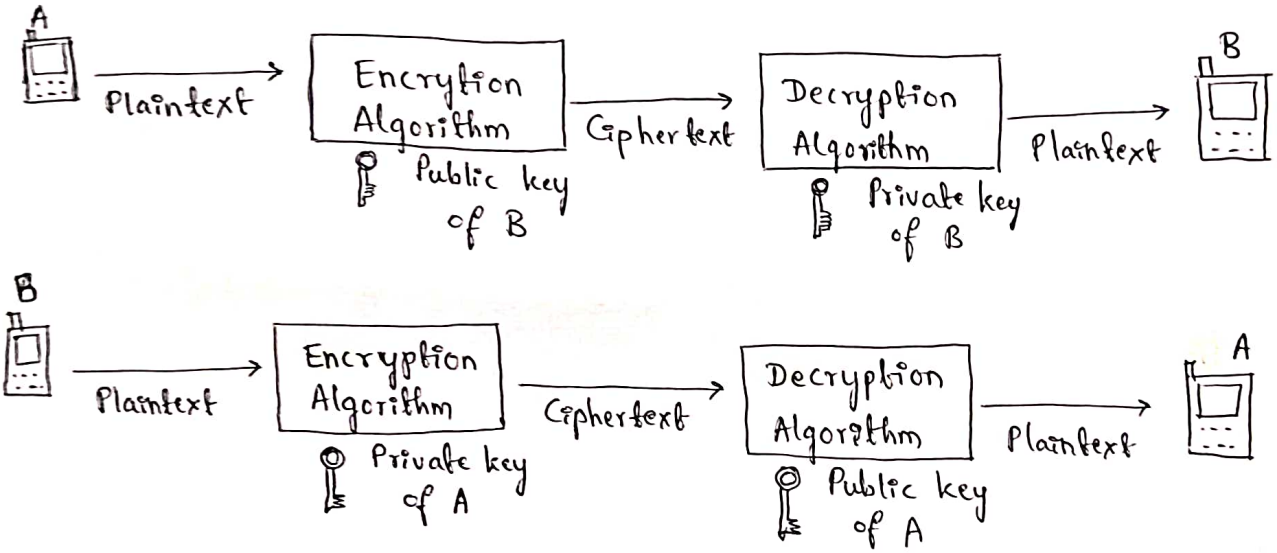
$\equiv 0 \pmod{139}$

$\therefore$ remainder is 0.

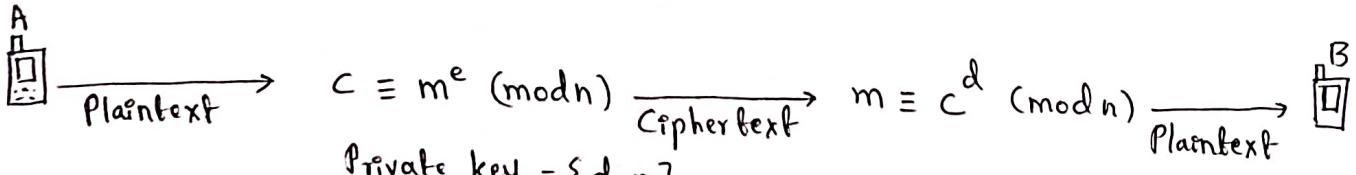
RSA Algorithm

(Rivest, Shamir, Adleman)

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys: Public key & Private key.
Public key is given to everyone & Private key is kept private.
i.e. in asymmetric algorithm, sender & receiver use different keys for encryption & decryption.



* The data to be sent is encrypted by sender A using the public key of the intended receiver B.
* B decrypts the received ciphertext using its private key, which is known only to B. *B replies to A encrypting its message using A's public key. * A decrypts the received ciphertext using its private key, which is known to only A.



Private key = {d, n}
Public key = {e, n}

I. Key generation :

1. Select two large prime numbers p & q
2. Calculate $n = p \times q$
3. Calculate Euler's totient function, $\phi(n) = (p-1)(q-1)$
4. Choose value of e such that
   $1 < e < \phi(n)$ & $\gcd(e, \phi(n)) = 1$.
5. Calculate $d \equiv e^{-1} \mod (\phi(n))$
   i.e. $de \equiv 1 \mod (\phi(n))$
   i.e. inverse of e modulo $\phi(n)$.
6. Public key = $\{e, n\}$ or $\{n, e\}$
   Private key = $\{d, n\}$

II. Encryption.

$c \equiv m^e \pmod n$, where m is plaintext & $m < n$.
c is ciphertext.

III. Decryption

$m \equiv c^d \pmod n$

Problems

1. Using RSA algorithm find public key & private key w.r.t. $p = 3$, $q = 11$ & $m = 31$.

$n = p \times q = 33$

$\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$

Let $e = 7$ as $1 < 7 < 20$ & $\gcd(7, 20) = 1$.

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

$d \times 7 \equiv 1 \pmod{20}$

$\therefore d = 3$

Now, public key = $\{e, n\} = \{7, 33\}$

private key = $\{d, n\} = \{3, 33\}$

Encryption : $C \equiv m^e \pmod{n}$

$\equiv 31^7 \pmod{33}$

$\equiv (-2)^7 \pmod{33}$

$\equiv -128 \pmod{33}$

$\equiv -29 \pmod{33}$

$\equiv 4 \pmod{33}$

$33)-128(3$
99
-29

$\therefore C = 04 = AE$

A	B	C	D	E	.....	Z
0	1	2	3	4	.....	25

Decryption : $m \equiv c^d \pmod{n}$

$\equiv 4^3 \pmod{33}$

$\equiv 31 \pmod{33}$

$\therefore m = 31 = DB.$

i.e. $m = 31 = \underset{\text{plaintext}}{DB}$ $\quad C = 04 = \underset{\text{ciphertext.}}{AE}$

2. In RSA algorithm if $p = 7$, $q = 11$ & $e = 13$, then what will be the value of d?

$n = p \times q = 7 \times 11 = 77$

$\phi(n) = (p-1)(q-1) = 6 \times 10 = 60$

Given $e = 13$.

To find d:

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

$d \times 13 \equiv 1 \pmod{60}$

13) 60 (4	8) 13 (1	5) 8 (1	3) 5 (1	2) 3 (1
52	8	5	3	2
8	5	3	2	1

$8 = 60 - 4(13)$ $\quad 5 = 13 - 1(8)$ $\quad 3 = 8 - 1(5)$ $\quad 2 = 5 - 1(3)$ $\quad 1 = 3 - 1(2)$

$1 = 3 - 1(2)$

$= 3 - 5 + 1 \cdot 3$

$= 2(3) - 5$

$= 2[8 - 1(5)] - 5$

$= 2(8) - 3(5)$

$= 2(8) - 3[13 - 1(8)]$

$= 5(8) - 3(13)$

$= 5[60 - 4(13)] - 3(13)$

$= 5(60) - 23(13)$

$= 60(5) + 13(-23)$

$\therefore (-23)13 \equiv 1 \pmod{60}$

$37 \times 13 \equiv 1 \pmod{60}$

$\therefore d = 37$

Public key $= \{e, n\} = \{13, 77\}$

Private key $= \{d, n\} = \{37, 77\}$

Imp
3.
MAP

Encode STOP using RSA algorithm with key (2537, 13) & $p = 43$, $q = 59$

Here $n = 2537$, $e = 13$, $p = 43$, $q = 59$

$\phi(n) = (p-1)(q-1) = 42 \times 58 = 2436$

Given $e = 13$, $1 < 13 < 2436$ & $\gcd(13, 2436) = 1$

m = STOP = 18191415

Let $m_1 = 1819$, $m_2 = 1415$

Encryption: $c \equiv m^e \pmod n$

$c_1 \equiv m_1^e \pmod n$

$\equiv (1819)^{13} \pmod{2537}$

$\equiv 2081 \pmod{2375}$

Using Calculator:

$1819^6 \equiv 1779 \pmod{2537}$

$1819^7 \equiv 1326 \pmod{2537}$

$1819^{13} \equiv 1779 \times 1326 \pmod{2537}$

$c_2 \equiv m_2^e \pmod n$

$\equiv (1415)^{13} \pmod{2537}$

$\equiv 2182 \pmod{2537}$

$1415^6 \equiv 355 \pmod{2537}$

$1415^7 \equiv 2536 \pmod{2537}$

$1415^{13} \equiv 355 \times 2536 \pmod{2537}$

$c = c_1 c_2 = 2081\,2182$ = UIBVIC

(Consider two numbers from left to right, if it is greater than 25, consider one number.)

0	1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M	N
14	15	16	17	18	19	20	21	22	23	24	25		
O	P	Q	R	S	T	U	V	W	X	Y	Z		

4. If $p=3$, $q=11$ & private key $d=7$, find the public key using RSA algorithm & hence encrypt the number 19.

$n = p \times q = 3 \times 11 = 33$

$\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$

Given $d = 7$.

To find e :

$de \equiv 1 \mod (\phi(n))$

$7 \times e \equiv 1 \pmod{20}$

$\therefore e = 3.$

Given $m = 19 = BJ$

Encryption: $c \equiv m^e \pmod n$

$\equiv 19^3 \pmod{33}$

$\equiv 28 \pmod{33}$ | by calculator

$\therefore c = 28 = cI$

5. Using RSA algorithm decrypt 09810461 using $d = 937$, $p = 43$, $q = 59$

$n = p \times q = 43 \times 59 = 2537$

$\phi(n) = (p-1)(q-1) = 42 \times 58 = 2436$

$c = \underline{0981}\ \underline{0461}$

Let $c_1 = 0981$, $c_2 = 0461$

To find plaintext m : $m \equiv c^d \pmod n$

$m_1 \equiv c_1^d \pmod n$

$\equiv (0981)^{937} \pmod{2537}$

$\equiv 0704 \pmod{2537}$

$(981)^6 \equiv 489 \pmod{2537}$

$(981)^{6 \times 50} \equiv (489)^{50} \pmod{2537}$

$(981)^{300} \equiv 1091 \pmod{2537}$

$[(981)^{300}]^3 \equiv (1091)^3 \pmod{2537}$

$(981)^{900} \equiv 140 \pmod{2537}$

$(981)^{900} \cdot 981^{37} \equiv 140 \times 150 \pmod{2537}$

$(981)^{937} \equiv 21000 \pmod{2537}$

$\equiv 704 \pmod{2537}$

$\therefore m_1 = 0704$

$m_2 \equiv c_2^{\,d} \pmod{n}$

$\equiv (0461)^{937} \pmod{2537}$

$\equiv 1115 \pmod{2537}$

$\therefore m_2 = 1115$

$m = \underline{07}\,\underline{04}\,\underline{11}\,\underline{15} = HELP$

$(461)^{100} \equiv 1185 \pmod{2537}$

$[(461)^{100}]^9 \equiv 1185^9 \pmod{2537}$

$(461)^{900} \equiv 2467 \pmod{2537}$

$(461)^{900} \cdot (461)^{37} \equiv 2467 \times 1615 \pmod{2537}$

$\equiv 1115 \pmod{2537}$

6. Encrypt the plaintext 9 using RSA algorithm using two prime numbers 7 & 11.

Here $m = 9$, $p = 7$, $q = 11$

$n = p \times q = 7 \times 11 = 77$

$\phi(n) = (p-1)(q-1) = 6 \times 10 = 60$

Let $e = 7$ $\therefore 1 < 7 < 20$ & $\gcd(7, 20) = 1$.

To find d:

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

$d \times 7 \equiv 1 \pmod{60}$

$7)\,60\,(8$
$\underline{56}$
4

$4)\,7\,(1$
$\underline{4}$
3

$3)\,4\,(1$
$\underline{3}$
1

$4 = 60 - 8(7)$ $\quad 3 = 7 - 1(4)$ $\quad 1 = 4 - 1(3)$

$1 = 4 - 1(3)$

$= 4 - 7 + 4$

$= 2(4) - 1(7)$

$= 2[60 - 8(7)] - 1(7)$

$= 2(60) - 17(7)$

$= 60(2) + 7(-17)$

$\therefore (-17) \times 7 \equiv 1 \pmod{60}$

$43 \times 7 \equiv 1 \pmod{60}$

$\therefore d = 43$

$(981)^{900} \equiv 140 \pmod{2537}$

$(981)^{900} \cdot 981^{37} \equiv 140 \times 150 \pmod{2537}$

$(981)^{937} \equiv 21000 \pmod{2537}$

$\equiv 704 \pmod{2537}$

$\therefore m_1 = 0704$

$m_2 \equiv c_2^{\,d} \pmod{n}$

$\equiv (0461)^{937} \pmod{2537}$

$\equiv 1115 \pmod{2537}$

$\therefore m_2 = 1115$

$m = \underline{0704}\,\underline{1115} = \text{HELP}$

$(461)^{100} \equiv 1185 \pmod{2537}$

$[(461)^{100}]^9 \equiv 1185^9 \pmod{2537}$

$(461)^{900} \equiv 2467 \pmod{2537}$

$(461)^{900} \cdot (461)^{37} \equiv 2467 \times 1615 \pmod{2537}$

$\equiv 1115 \pmod{2537}$

6. Encrypt the plaintext 9 using RSA algorithm using two prime numbers 7 & 11.

Here $m = 9$, $p = 7$, $q = 11$

$n = p \times q = 7 \times 11 = 77$

$\phi(n) = (p-1)(q-1) = 6 \times 10 = 60$

Let $e = 7$ $\therefore 1 < 7 < 20$ & $\gcd(7, 20) = 1$.

To find d:

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

$dx7 \equiv 1 \pmod{60}$

$7)60(8$ $\quad 56$ $\quad 4$

$4)7(1$ $\quad 4$ $\quad 3$

$3)4(1$ $\quad 3$ $\quad 1$

$4 = 60 - 8(7)$

$3 = 7 - 1(4)$

$1 = 4 - 1(3)$

$1 = 4 - 1(3)$

$= 4 - 7 + 4$

$= 2(4) - 1(7)$

$= 2[60 - 8(7)] - 1(7)$

$= 2(60) - 17(7)$

$= 60(2) + 7(-17)$

$\therefore (-17) \times 7 \equiv 1 \pmod{60}$

$43 \times 7 \equiv 1 \pmod{60}$

$\therefore d = 43$

Now, public key = $\{e, n\} = \{7, 77\}$

private key = $\{d, n\} = \{43, 77\}$

To find ciphertext c: $c \equiv m^e \pmod{n}$

$\equiv 9^7 \pmod{77}$

$\equiv 37 \pmod{77}$

$\therefore \quad c = 37$

7. In an RSA cryptosystem, a particular A uses two prime numbers 13 & 17 to generate the public & private keys. If the public of A is 35, what is the private key of A?

Here $p = 13$, $q = 17$, $e = 35$

$n = p \times q = 13 \times 17 = 221$

$\phi(n) = (p-1)(q-1) = 12 \times 16 = 192$

To find d:

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

$d \times 35 \equiv 1 \pmod{192}$

$35) 192 (5$ $\quad$ $17) 35 (2$

$\underline{175}$ $\quad$ $\underline{34}$

17 $\quad$ 1

$17 = 192 - 5(35)$ $\quad$ $1 = 35 - 2(17)$

$1 = 35 - 2(17)$

$= 35 - 2[192 - 5(35)]$

$= 35(11) + 192(-2)$

$\therefore \quad 11 \times 35 \equiv 1 \pmod{192}$

$\therefore d = 11$

$\Rightarrow$ private key of A is 11.

8. An RSA cryptosystem uses two prime numbers 3 & 13 to generate the public key = 3 & the private key = 7. What is the value of ciphertext for a plain text = 5?

$p = 3, \quad q = 13, \quad e = 3, m = 5, \quad d = 7, \quad c = ?$

$n = p \times q = 3 \times 13 = 39$

To find c:

$c \equiv m^e \pmod{n}$

$\equiv 5^3 \pmod{39}$

$\equiv 125 \pmod{39}$

$\equiv 8 \pmod{39}$

$\therefore \quad c = 8.$

An RSA algorithm uses two prime numbers 3 & 11 to generate private key = 7. What is the value of ciphertext for a plain text 5 using RSA public-key encryption algorithm?

$p = 3, \quad q = 11, \quad d = 7, \quad m = 5, \quad e = ?$

$n = p \times q = 3 \times 11 = 33$

$\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$

To find e:

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

$7 \times 3 \equiv 1 \pmod{20}$

$\therefore e = 3.$

$\therefore$ public key $= \{e, n\} = \{3, 33\}$

or public key, $e = 3.$

Solving polynomials

Thm: Let p be prime & $f(x)$ be a polynomial with integer coefficients & degree n modulo p. Then $f(x) \equiv 0 \pmod{p}$ has at most n distinct roots.

Thm: Let $f(x)$ be a polynomial with integer coefficients modulo n, & $\exists\ c \in \mathbb{Z}$ such that $f(c) \equiv 0 \pmod{n}$, then $\exists\ q(x)$ such that $f(x) \equiv (x-c)\,q(x) \pmod{n}$.

Problems

1. Solve $x^2 + x + 1 \equiv 0 \pmod{2}$.

Here $0 \le x < 2$. Let $f(x) = x^2 + x + 1$

$\therefore$ possible values of x are : 0, 1.

$f(0) = 1 \not\equiv 0 \pmod{2}$

$f(1) = 3 \not\equiv 0 \pmod{2}$

$\therefore$ $f(x)$ has no soln modulo 2.

2. Solve $x^3 + x + 2 \equiv 0 \pmod{36}$

$36 = 4 \times 9$, where 4 & 9 are relatively prime.

$\therefore$ $x^3 + x + 2 \equiv 0 \pmod{4}$ — ①

$x^3 + x + 2 \equiv 0 \pmod{9}$ — ②

Now, possible residues in ① are : 0, 1, 2, 3.

possible residues in ② are : 0, 1, 2, ..., 8.

Solns are :

$x \equiv 1, 2, 3 \pmod{4}$ to ①

$x \equiv 8 \pmod{9}$ to ②

Now, by applying CRT :

	case(i)	(ii)			
$a_1 = 2$	1	3	$m_1 = 4$	$M_1 = 9$	$M_1^{-1} = 1$
$a_2 = 8$	8	8	$m_2 = 9$	$M_2 = 4$	$M_2^{-1} = 7$

$m = 36$

Case (ii) $x \equiv a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} \pmod m$

$\equiv (2 \times 9 \times 1) + (8 \times 4 \times 7) \pmod{36}$

$\equiv 242 \pmod{36}$

$\equiv 26 \pmod{36}$.

Case (i)

$x \equiv (1 \times 9 \times 1)(8 \times 4 \times 7) \pmod{36}$

$\equiv 233 \pmod{36}$

$\equiv 17 \pmod{36}$

Case (iii)

$x \equiv$

3. Solve $x^2 \equiv 0 \pmod{12}$.

$x^2 \equiv 0 \pmod 3$ —①, $x^2 \equiv 0 \pmod 4$ —②

The possible solns are: $x \equiv 0 \pmod 3$ to ①

$x \equiv 0 \pmod 4$, $x \equiv 2 \pmod 4$ } to ②.

Now consider $x \equiv 0 \pmod 3$

$x \equiv 0 \pmod 4$

By CTR, $x \equiv 0 \pmod{12}$ is the soln

Now consider $x \equiv 0 \pmod 3$

$x \equiv 2 \pmod 4$

Applying CRT

$a_1 = 0$	$m_1 = 3$	$M_1 = 4$	$M_1^{-1} = 1$	$m = 12$
$a_2 = 2$	$m_2 = 4$	$M_2 = 3$	$M_2^{-1} = 3$	

$x \equiv a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} \pmod m$

$\equiv 0 + (2 \times 3 \times 3) \pmod{12}$

$\equiv 6 \pmod{12}$

$\therefore x \equiv 0, 6 \pmod{12}$ are the solns.

4. Solve $x^2 \equiv 1 \pmod{30}$

$30 = 2 \times 3 \times 5$.

$\therefore$ $x^2 \equiv 1 \pmod 2$ — ①

$x^2 \equiv 1 \pmod 3$ — ②

$x^2 \equiv 1 \pmod 5$ — ③

Possible residues in ① are : 0, 1

" " " ② " : 0, 1, 2

" " " ③ " : 0, 1, 2, 3, 4.

Solns are :

To ① : $x \equiv 1 \pmod 2$

To ② : $x \equiv 1, 2 \pmod 3$

To ③ : $x \equiv 1, 4 \pmod 5$

Case(i) Consider $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 5$

$a_1 = 1$ $m_1 = 2$ $M_1 = 15$ $M_1^{-1} = 1$

$a_2 = 1$ $m_2 = 3$ $M_2 = 10$ $M_2^{-1} = 1$ $m = 30$

$a_3 = 1$ $m_3 = 5$ $M_3 = 6$ $M_3^{-1} = 1$

$$x \equiv \sum_{i=1}^{3} a_i M_i M_i^{-1} \pmod m$$

$\equiv (1 \times 15 \times 1) + (1 \times 10 \times 1) + (1 \times 6 \times 1) \pmod{30}$

$\equiv 31 \pmod{30}$

$\equiv 1 \pmod{30}$

Case (ii) Consider $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 3$, $x \equiv 4 \pmod 5$

$a_1 = 1$ $m_1 = 2$ $M_1 = 15$ $M_1^{-1} = 1$

$a_2 = 1$ $m_2 = 3$ $M_2 = 10$ $M_2^{-1} = 1$ $m = 30$

$a_3 = 4$ $m_3 = 5$ $M_3 = 6$ $M_3^{-1} = 1$

$x \equiv (1 \times 15 \times 1) + (1 \times 10 \times 1) + (4 \times 6 \times 1) \pmod{30}$

$\equiv 49 \pmod{30}$

$\equiv 19 \pmod{30}$

Case (iii) Consider $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 5$

$a_1 = 1$ $m_1 = 2$ $M_1 = 15$ $M_1^{-1} = 1$

$a_2 = 2$ $m_2 = 3$ $M_2 = 10$ $M_2^{-1} = 1$ $m = 30$

$a_3 = 1$ $m_3 = 5$ $M_3 = 6$ $M_3^{-1} = 1$

$x \equiv (1 \times 15 \times 1) + (2 \times 10 \times 1) + (1 \times 6 \times 1) \pmod{30}$

$\equiv 41 \pmod{30}$

$\equiv 11 \pmod{30}$

Case (iv) Consider $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 4 \pmod 5$

$a_1 = 1$ $m_1 = 2$ $M_1 = 15$ $M_1^{-1} = 1$

$a_2 = 2$ $m_2 = 3$ $M_2 = 10$ $M_2^{-1} = 1$ $m = 30$

$a_3 = 4$ $m_3 = 5$ $M_3 = 6$ $M_3^{-1} = 1$

$x \equiv (1 \times 15 \times 1) + (2 \times 10 \times 1) + (4 \times 6 \times 1) \pmod{30}$

$\equiv 59 \pmod{30}$

$\equiv 29 \pmod{30}$.

$\therefore$ Solns are $x \equiv 1, 19, 11, 29 \pmod{30}$

5. Solve $x^3 + x + 3 \equiv 0 \pmod{25}$ —①

Since $25 = 5^2$, first solve the congruence modulo 5.

Let $q(x) = x^3 + x + 3$.

Now consider $q(x) \equiv 0 \pmod 5$

i.e $x^3 + x + 3 \equiv 0 \pmod 5$

∴ All possible residues are : 0, 1, 2, 3, 4.

The soln of $q(x) \equiv 0 \pmod 5$ is $x \equiv 1 \pmod 5$.

Let $x = 1 + 5a$ be the soln of $x^3 + x + 3 \equiv 0 \pmod{5^2}$.

From ①, $(1+5a)^3 + (1+5a) + 3 \equiv 0 \pmod{25}$

$1^3 + (5a)^3 + 3(1^2)(5a) + 3(1)(5a)^2 + (1+5a) + 3 \equiv 0 \pmod{25}$

$5 + \cancel{25}\overset{0}{(5a^3)} + \cancel{25}\overset{0}{(3a^2)} + 20a \equiv 0 \pmod{25}$

∴ $5 + 20a \equiv 0 \pmod{25}$

$20a \equiv -5 \pmod{25}$ ÷ by 5.

$4a \equiv -1 \pmod 5$

∴ $4a \equiv 4 \pmod 5$ $\Rightarrow a \equiv 1 \pmod 5$

As $4^{-1} \pmod 5 = 4$

∴ $x \equiv 1 + 5(1) \pmod{5^2}$

i.e $x \equiv 6 \pmod{5^2}$ is the soln.

6. Solve $x^3+4x \equiv 4 \pmod{343}$ —①

Since $343 = 7^3$, first solve the congruence modulo 7, then 7^2 & finally 7^3.

Consider $x^3+4x \equiv 4 \pmod 7$, $0 \le x < 7$.

Possible soln is $x \equiv 3 \pmod 7$. of $x^3+4x \equiv 4 \pmod 7$.

Let $x = 3+7a$ be the soln of $x^3+4x \equiv 4 \pmod{7^2}$ —②

$\therefore (3+7a)^3 + 4(3+7a) \equiv 4 \pmod{7^2}$

$3^3 + 7^2(7a^3) + (3\times 9 \times 7a) + (3\times 3 \times 7^2a^2) + 12 + 28a \equiv 4 \pmod{7^2}$

$39 + 217a \equiv 4 \pmod{7^2}$

$21a \equiv -35 \pmod{7^2}$

49) 217 (4
196
21

$\therefore 21a \equiv 14 \pmod{7^2}$ ÷ by 7.

$3a \equiv 2 \pmod 7$

Multiplicative inverse of $3 \pmod 7$ is 5.

$\therefore (3\times 5)a \equiv 2\times 5 \pmod 7$

$a \equiv 3 \pmod 7$

$\therefore x = 3+7(3) = 24$ i.e. $x \equiv 24 \pmod{49}$ is the soln of ②.

Let $x = 24+49b$ be the soln of ①.

$\therefore (24+49b)^3 + 4(24+49b) \equiv 4 \pmod{343}$

Or $(24+7^2b)^3 + 4(24+7^2b) \equiv 4 \pmod{7^3}$

$24^3 + 7^3(7^2b^3) + (3\times 24\times 7^3(7b^2)) + (3\times 24^2\times 7^2b) + (4\times 24) + (4\times 7^2b) \equiv 4 \pmod{7^3}$

$13920 + 84868b \equiv 4 \pmod{7^3}$

$200 + 147b \equiv 4 \pmod{7^3}$

$147b \equiv -196 \pmod{7^3}$

$147b \equiv 147 \pmod{7^3}$ ÷ by 7^2

$3b \equiv 3 \pmod 7$

Multiplicative inverse of $3 \pmod 7$ is 5

$(3\times 5)b \equiv 3\times 5 \pmod 7$

$b \equiv 1 \pmod 7$

$\therefore x = 24 + 49(1) = 73$

i.e $x \equiv 73 \pmod{7^3}$ is the soln of (1).