UNIT-IV

Diophantine Equations and Congruences.

Linear Diophantine Equations: (LDE)

A linear diophantine equation in two variables x and y is an equation of the form

$ax+by=c.$

Diophantine Equation.
An Equ, is solvable.
that solu is integers.

Theorem:

The LDE $ax+by=c$ is solvable iff $d|c$, where $d=(a,b)$. If x_0, y_0 is a particular solution of the LDE, then all its solutions are given by,

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

where t is an arbitrary integer.

1. $\overset{a}{2}x+\overset{b}{3}y=\overset{c}{4}$
$d=\text{Gcd}(2,3)=1$
$\Rightarrow d|c \Rightarrow 1|4 \Rightarrow$ Solvable.

2. $2x+4y=7$
$d=(2,4)=2$
$2\nmid 7.$

Proof: The proof consists of four parts:

part: I If the LDE is solvable then $d|c$.

Assume that LDE is solvable.

Let $x=\alpha$ and $y=\beta$ be a solution.

Then $a\alpha+b\beta=c \rightarrow ①$

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

$\Rightarrow d|(a\alpha+b\beta)$

$\Rightarrow d|c.$

part: II Assume that $d|c$.

To prove that LDE is solvable.

suppose $d|c \Rightarrow$ there exists an integer e such that $c = de$.

since $d = (a,b)$, then there exist integers r and S such that $d = ra + Sb$.

$$\Rightarrow rae + Sbe = de.$$

$$\Rightarrow a(re) + b(Se) = c$$

Hence, $x = re$ and $y = Se$ are the solutions of LDE

$\Rightarrow$ the LDE is solvable.

part iii : To show that $x = x_0 + \left(\frac{b}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$ is a solution.

Now $ax + by = a\left[x_0 + \left(\frac{b}{d}\right)t\right] + b\left[y_0 - \left(\frac{a}{b}\right)t\right]$

$$= (ax_0 + by_0) + \frac{ab}{d}t - \frac{ab}{d}t$$

$$= ax_0 + by_0$$

$$ax + by = c$$

part iv : To show that if x', y' are solutions then they are of the form, $x_0 + \left(\frac{b}{d}\right)t$ and $y_0 - \left(\frac{a}{d}\right)t$.

we have, $ax_0 + by_0 = c$ and $ax' + by' = c$.

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

$$\Rightarrow a(x' - x_0) = b(y_0 - y') \rightarrow ②$$

$$\div d \Rightarrow \left(\frac{a}{d}\right)(x' - x_0) = \frac{b}{d}(y_0 - y') \rightarrow ③$$

since $d = (a,b) \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1 \rightarrow ④$

Now, ③ $\Rightarrow \left(\frac{b}{d}\right) \Big| (x'-x_0)\frac{a}{d}$

$\Rightarrow \left(\frac{b}{d}\right) \Big| (x'-x_0)$ [by ④]

$\Rightarrow x'-x_0 = \left(\frac{b}{d}\right)t$, for some integer t.

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

② $\Rightarrow a\left(\frac{b}{d}\right)t = b(y_0-y')$

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

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

Hence, $x' = x_0 + \left(\frac{b}{d}\right)t$ and $y' = y_0 - \left(\frac{a}{d}\right)t \rightarrow$ ⑤.

Hence every solution of the LDE is of the desired form.

Corollary:

If $(a,b)=1$, then the LDE $ax+by=c$ is solvable and the general solution is given by, $x = x_0+bt$, $y = y_0-at$, where x_0, y_0 is a particular Solution

Proof: Given: $(a,b)=1$, Here $d=1$.

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

$\Rightarrow x = x_0 + bt$ and $y = y_0 - at$

where x_0, y_0 is a particular Solution.

1. Determine whether the LDE'S $12x + 8y = 30$, $2x + 3y = 4$ and $6x + 8y = 25$. are solvable.

Solution:

1) $12x + 8y = 30$.

$a = 12, \quad b = 8, \quad c = 30.$

$\therefore d = (a,b) = (12,8) = 4$

$d|c = 4 \nmid 30$

$\Rightarrow 12x + 8y = 30$ is not solvable.

2) $2x + 3y = 4$.

$d = (2,3) = 1$

$d|c = 1|4$

$\Rightarrow 2x + 3y = 4$ is solvable.

3) $6x + 8y = 25$

$d = (6,8) = 2$

$d|c = 2 \nmid 25$

$\Rightarrow 6x + 8y = 25$ is not solvable.

2. Mahavira puzzle problem:

Twenty three weary travellers entered the outskirts of a lush and beautiful forest. They found 63 equal heaps ([illegible]) of plantains and seven single fruits and divided them equally. Find the number of fruits in each heap.

Solution:

Let x denote the number of plantains in each heap and y be the share for each one.

Then LDE is, $63x + 7 = 23y$

$\Rightarrow 63x - 23y = -7$

$d = (a,b) = (63, -23) = 1 \mid (-7) = c$

$\Rightarrow$ The LDE is solvable.

By Euclidean algorithm, $63 = 2 \cdot 23 + 17$

$23 = 1 \cdot 17 + 6$

$17 = 2 \cdot 6 + 5$

$6 = 1 \cdot 5 + 1$

$5 = 5 \, 1 + 0$

$23 \overline{)63}$ 2, 46, 17

$17 \overline{)23}$ 1, 17, 6

$6 \overline{)17}$ 2, 12, 5

$5 \overline{)6}$ 1, 5, 1

$1 \overline{)5}$ 5, 5, 0

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

$= 1 \cdot 6 - 1 \cdot (17 - 2 \cdot 6)$

$= 1 \cdot 6 - 1 \cdot 17 + 2 \cdot 6 = 3 \cdot 6 - 1 \cdot 17$

$= 3 \cdot (23 - 1 \cdot 17) - 17 = 3 \cdot 23 - 4 \cdot 17.$

$= 3 \cdot 23 - 4(63 - 2 \cdot 23)$

$1 = (-4) 63 + 11 \cdot 23$

$63 \times 28 = 1764$, $+7$, 1771

$23 \times 77 = 1771$

$\Rightarrow -7 = (28)(63) + (-77) \cdot 23$

$\Rightarrow 63(28) - 23(77) = -7.$

$\Rightarrow x = 28$ and $y = 77$ are particular solutions of the LDE $63x - 23y = -7$.

The general solutions are,

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

$\Rightarrow x = 28 + \left(\frac{-23}{1}\right)t, \quad y = 77 - \left(\frac{63}{1}\right)t$

$x = 28 - 23t, \quad y = 77 - 63t.$

3. Hundred Fowls puzzle:

If a cock is worth 5 coins, a hen 3 coins and 3 chicks together one coin, how many cocks, hens and chicks, totalling 100, can be bought for 100 coins?

Solution:

Let x, y, z denotes the number of cocks, the number of hens and the number of chicks respectively. Then $x + y + z = 100 \rightarrow ①$

and $5x + 3y + \frac{1}{3}z = 100 \rightarrow ②$

Eliminating z from ① & ② weget,

$$5x + 3y + \frac{1}{3}(100 - x - y) = 100 \quad (\text{by } ①)$$

$$\Rightarrow 14x + 8y = 200$$

$$\Rightarrow 7x + 4y = 100$$

4 ⟌ 7 (1)
4
3

3 ⟌ 4 (1)
3
1

1 ⟌ 3 (3)
3
0

Here $d = (7, 4) = 1$.

$7 = 1.4 + 3$
$4 = 1.3 + 1$
$3 = 3.1 + 0$

By trial and error, $1 = (-1).7 + 2(4)$

$$\Rightarrow 100 = 7(-100) + 4(200)$$

$1 = 4 - 1.3$
$= 4 - 1.(7 - 1.4)$

$\Rightarrow x_0 = -100,\ y_0 = 200$ are particular solutions of $7x + 4y = 100$.

$1 = 1.4 - 1.7 + 1.4$
$100 = 2.4 - 1.7$
$100 = 4(200) + 7(-100)$

The general solution is,

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

$\Rightarrow 7(-100) + 4(200)$
$= 100.$

$$= -100 + 4t' \qquad = 200 - 7t'$$

$$z = 100 - x - y = 100 - (-100 + 4t') - (200 - 7t') = 3t'.$$

t = 25
x = 4 ✓
y = 18 ✓
z = 78
100

Euler's Method for solving LDE'S

4. Solve the LDE $1076x + 2076y = 3076$, by Euler's Method.

Solution:

$$\text{Given: } 1076\overset{\substack{x \text{ is smaller} \\ \text{solve for } x.}}{\overset{\Uparrow}{x}} + 2076y = 3076.$$

Here $(1076, 2076) = 4$ and $4 \mid 3076$.

$$
\begin{array}{r|l}
 & -y+2 \\ \hline
1076 & -2076y+3076 \\
 & -1076y \\ \hline
 & -1000y+3076 \\
 & \qquad\quad +2152 \\
 & \qquad\quad (-) \\ \hline
 & -1000y+924
\end{array}
$$

$$x = \frac{-2076y+3076}{1076}$$

$$= (-y+2) + \frac{-1000y+924}{1076} \rightarrow ①$$

Let $u = \dfrac{-1000y+924}{1076}$

$$\Rightarrow 1076u + 1000\overset{\substack{y \text{ is smaller, then solve} \\ \text{for } y}}{\overset{\Uparrow}{y}} = 924$$

$$\Rightarrow y = \frac{-1076u+924}{1000}$$

$$= -u + \frac{924-76u}{1000} \longrightarrow ②$$

$$
\begin{array}{r|l}
 & -u \\ \hline
1000 & 924-1076u \\
 & \qquad -1000u \\
 & \qquad (+) \\ \hline
 & 924-76u
\end{array}
$$

Let $v = \dfrac{-76u+924}{1000}$, Then $76u + 1000v = 924$.

$$\Rightarrow u = \frac{924-1000v}{76}$$

$$= (-13v+12) + \frac{12-12v}{76} \rightarrow ③$$

$$
\begin{array}{r|l}
 & -13v+12 \\ \hline
76 & 924-1000v \\
 & \qquad -988v \\
 & \qquad (+) \\ \hline
 & 924-12v \\
 & 912 \\ \hline
 & 12-120
\end{array}
$$

Let $w = \dfrac{-12v+12}{76}$, so $12v + 76w = 12$

$$\Rightarrow v = \frac{-76w+12}{12} = \underline{-6w+1} - \frac{w}{3} \rightarrow ④$$

$w/3 = t \rightarrow$ ⑤

$$\begin{array}{r|l} & -6w+1 \\ \hline 12 & 12-76w \\ & \quad -72w \\ \hline & 12-4w \\ & 12 \\ \hline & \quad -4w \end{array}$$

To obtain a particular solution, weget $t=0$, when $w=0$.

④ $\Rightarrow$ $V = -6w+1-\frac{w}{3}$

$= -6(0)+1-\frac{0}{3}$

$-\frac{4w}{12} \quad -\frac{w}{3}$

$V = 1$

③ $\Rightarrow$ $u = \frac{-1000V+924}{76} = \frac{-1000+924}{76}$

$u = -1$

② $\Rightarrow$ $y = \frac{-1076u+924}{1000} = \frac{1076+924}{1000}$

$y = 2$

① $\Rightarrow$ $x = -\frac{2076y+3076}{1076} = -\frac{4152+3076}{1076} = -1$

$x = -1.$

To verify that $x_0 = -1$, $y_0 = 2$ is in fact a solution of the LDE.

To find the general Solution:

⑤ $\Rightarrow$ $w = 3t$

④ $\Rightarrow$ $V = -6w+1-\frac{w}{3} = -19t+1$

③ $\Rightarrow$ $u = -13V+12+w = 250t-1$

② $\Rightarrow$ $y = -u+V = -269t+2$

① $\Rightarrow$ $x = -y+2+u = 519t-1$

Hence the general Solution is, $x = 519t-1$,

$y = -269t+2.$

Fibonacci Numbers and LDE's.

Consider the LDE $F_{n+1}\, x + F_n\, y = c$.

where $(F_{n+1}, F_n) = 1$, so the LDE is solvable.

By Cassini's formula, $F_{n+1} F_{n-1} - F_n^2 = (-1)^n$.

Case (i) Let n be even. Then $F_{n+1} F_{n-1} - F_n^2 = 1$

we get, $x_0 = c F_{n-1}$, $y_0 = -c F_n$.

Case (ii) Let n be odd. Then $F_{n+1} F_{n-1} - F_n^2 = -1$

we get, $x_0 = -c F_{n-1}$, $y_0 = c F_n$.

NOTE: Fibonacci series,

1	1	2	3	5	8	13	21	34	55	
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	
1	2	3	4	5	6	7	8	9	10	...

1. Solve the LDE $13x + 8y = 4$ by treating 8 and 13 as consecutive Fibonacci numbers.

Solution:

Given: $13x + 8y = 4$.

Here $a = 13$, $b = 8$ and $c = 4$.

Here, $F_6 = 8$ and $F_7 = 13$.

Hence $n = 6$ is even.

The particular solution is,

$$x_0 = c F_{n-1} = 4(F_5) = 4(5) = 20$$
$$y_0 = -c F_n = -4(F_6) = -4(8) = -32.$$

Here $d = (F_{n+1}, F_n) = (13, 8) = 1$

The general solution is,

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

$$\Rightarrow \quad x = x_0 + \left(\frac{8}{1}\right)t, \quad y = y_0 - \left(\frac{13}{1}\right)t.$$

$\Rightarrow x = 20 + 8t \ , \ y = -32 - 13t.$

where t is an arbitrary integer.

2. Solve Fibonacci LDE $34x + 21y = 17$. ($n=8$ even).

Ans: $x = 221 + 21t \ , \ y = -357 - 34t.$

Congruences:

Congruence Modulo m:

Let m be a positive integer. Then an integer 'a' is congruent to an integer 'b' Modulo m if $m|(a-b)$. ie, $a \equiv b \pmod{m}$, m is the modulus of the congruence relation.

Ex: 1. $5|(23-3) \Rightarrow 23 \equiv 3 (\text{Mod } 5)$.

2. $16| 28-(-4) \Rightarrow 16|32 \Rightarrow 28 \equiv -4 (\text{Mod } 16)$

3. $7 \nmid 18+6 \Rightarrow 7 \nmid 24 \Rightarrow 18 \not\equiv -6 (\text{Mod } 7)$.

Congruence classes:

A congruence class Modulo 5 is the class of all integers leaving the same remainder and the possible remainders are 0, 1, 2, 3, 4.

$[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$

$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$

$[2] = \{\ldots, -8, -3, 2, 7, 12 \ldots\}$

$[3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$

$[4] = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$

are the only 5 congruence classes.

A complete set of Residues Modulo m:

The set of integers $\{a_1, a_2, \dots, a_m\}$ is a complete set of residues Modulo m, If they are congruent Modulo m to the least residues $0, 1, 2, \dots, (m-1)$ in some order.

EX: The set $\{-12, 9, 6, 23\}$ is a complete set of residues Modulo 4.

$$-12 \equiv 0 \pmod 4$$
$$9 \equiv 1 \pmod 4$$
$$6 \equiv 2 \pmod 4$$
$$23 \equiv 3 \pmod 4.$$

Theorem: 1

$a \equiv b \pmod m \iff a = b + km$ for some integer m.

Proof: Assume that $a \equiv b \pmod m$.

Then $m \mid (a-b) \Rightarrow a - b = m(t)$, where t is an integer.

$\Rightarrow a = b + mt$, "

conversely, assume that $a = b + mt$, where t is an integer.

Then $a - b = mt \Rightarrow m \mid (a-b) \Rightarrow a \equiv b \pmod m$.

Theorem: 2

Congruence Relation '$\equiv$' is an equivalence relation.

1) $a \equiv a \pmod m$ (Reflexive (OR) Property).

2) If $a \equiv b \pmod m$ then $b \equiv a \pmod m$ [symmetric property]

3) If $a \equiv b \pmod m$ and $b \equiv c \pmod m$ then $a \equiv c \pmod m$ [Transitive Property].

Proof:

Reflexive: since $0|m \Rightarrow (a-a)|m, \forall a \in Z$

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

Symmetric: Let $a \equiv b \pmod m$.

Then $m|(a-b) \Rightarrow m|-(b-a) \Rightarrow m|(b-a)$

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

Transitive: Let $a \equiv b \pmod m$ and

$b \equiv c \pmod m$.

Then $m|(a-b)$ and $m|(b-c)$

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

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

$\therefore$ '$\equiv$' is an equivalence relation.

Theorem: 3

$a \equiv b \pmod m$ iff a and b leave the same remainder when divided by m.

proof: Assume that $a \equiv b \pmod m$.

Then $m|(a-b) \Rightarrow (a-b) = km$, where k is an integer.

$\Rightarrow a = b+km \rightarrow$ ①

By division algorithm, given integers b and m, there exists integers q and r such that,

$b = mq+r$ (or) when $0 \le r < m$. $\rightarrow$ ②

using ② in ①, $a = b+km$

$= (mq+r)+km$

$a = (mq)+r+km = m(q+k)+r. \rightarrow$ ③

③&② ⇒ conversely let both a and b leave the same remainder r when divided by m.

Then by the division algorithm,

$$a = mq + r \text{ and } b = mq' + r, \quad 0 \leq r < m.$$

Then $a-b = (mq+r) - (mq'+r)$

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

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

Hence, $a \equiv b \pmod{m}$.

Corollary:

1. The integer r is the remainder when a is divided by m iff $a \equiv r \pmod{m}$, where $0 \leq r < m$.

2. Every integer is congruent to exactly one of the least residues $0, 1, 2, \ldots, (m-1)$.

3. Every integer a is congruent to its remainder r modulo m, r is called the least residue of a modulo m.

4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a-c \equiv b-d \pmod{m}$.

5. If $a \equiv b \pmod{m}$ and C is any integer then.

i) $a+b = b+C \pmod{m}$

ii) $a-c = b-c \pmod{m}$

iii) $ac \equiv bc \pmod{m}$.

iv) $a^2 \equiv b^2 \pmod{m}$.

Theorem: 4.

Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

Then i) $a+c \equiv b+d \pmod{m}$ and ii) $ac \equiv bd \pmod{m}$.

Proof: Given: $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$

$a \equiv b \pmod{m}$
$m | a-b \Rightarrow$
$a-b = ml$
$a = b+lm$

i)

$a \equiv b \pmod{m} \Rightarrow a = b+lm$

$c \equiv d \pmod{m} \Rightarrow c = d+km$, for some integer l and k.

$\Rightarrow a+c = (b+d)+(l+k)m$

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

ii) $ac = (b+lm)(d+km) = bd + bkm + ldm + lkm^2$

$\Rightarrow ac = bd + m(bk+dl+lkm)$.

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

Theorem: 5

If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$, for any positive integer n.

Proof: The proof is by induction on n.

when $n=1$, the result is same as the hypothesis.

Assume that the result is true for $n=k$.

i.e., $a^k \equiv b^k \pmod{m}$

we have, $a \equiv b \pmod{m}$

$\Rightarrow a^k . a \equiv b^k . b \pmod{m}$

$\Rightarrow a^{k+1} \equiv b^{k+1} \pmod{m}$.

$\therefore$ The result is true for any integer n.

By induction.

1. Prove that no prime of the form $4n+3$ can be expressed as the sum of two squares.

Solution: Let $N = 4n+3$ be a prime.

Then to prove that N cannot be expressed as the sum of 2 squares.

To prove this assume the contrary that,

$$N = A^2+B^2 \longrightarrow ①$$

$$4\overset{1}{\overline{)7}}$$
$$\underline{4}$$
$$3$$

$$\overset{\overset{\to odd}{7}}{}$$

$N = 4n+3 \Rightarrow N$ is odd and $N \equiv 3 \pmod 4$)

N is odd $\Rightarrow$ one of A^2, B^2 is odd and the other is $\xrightarrow{}$ ② even.

Let A^2 be odd and B^2 be even.

Then. A^2 odd $\Rightarrow A$ is odd

B^2 even $\Rightarrow B$ is even.

$a = b+mk$
$a \equiv b \pmod m$
$N = 3+4n$
$N \equiv 3 \pmod 4$

Let $A = 2a+1$ and $B = 2b$ for some integers a and b.

Then from ①, $N = (2a+1)^2+(2b)^2$

$= 4a^2+4a+1+4b^2$

$= 4(a^2+b^2+a)+1$

A^2+B^2
1^2+2^2
$=1+4=5=N$
$A^2=A=1$
$B^2=4 \Rightarrow B=2.$

$\Rightarrow N \equiv 1 \pmod 4$), a contradiction to ②.

Hence, No prime of the form $4n+3$ can be expressed as the sum of 2 squares.

2. prove that no integer of the form $8n+7$ can be expressed as a sum of three squares.

Solution: Let $N = 8n+7$.

Then $N \equiv 7 \pmod 8) \longrightarrow ①$

Assume the contrary that $N = x^2 + y^2 + z^2$, where x, y, z are integers.

W.k.T any integer (x) is congruent Modulo 8 to 0, 1, 2, 3, 4, 5, 6 or 7.

$5 \equiv -3 \pmod 8$, $6 \equiv -2 \pmod 8$, $7 \equiv -1 \pmod 8$.

$\Rightarrow$ x is congruent Modulo 8 to 0, 1, 2, 3, 4, -3, -2 or -1.

$\Rightarrow$ x^2 is congruent Modulo 8 to $0^2, 1^2, 2^2, 3^2$ or 4^2.

$\Rightarrow$ x^2 is congruent Modulo 8 to 0, 1, 4, 1 or 0.

$\Rightarrow$ x^2 is congruent Modulo 8 to 0, 1 or 4.

Illy both y^2 and $z^2 \equiv 0, 1,$ or $4 \pmod 8$.

$N = x^2 + y^2 + z^2 \equiv 0 \pmod 8$ or $1 \pmod 8$ or $2 \pmod 8$ or $3 \pmod 8$ or $4 \pmod 8$ or $5 \pmod 8$ or $6 \pmod 8$

This contradicts ①, Hence the result.

3. Find the remainder when $1! + 2! + \cdots + 100!$ is divided by 15.

Solution: For $k \geq 5$, $k!$ contains both 3 and 5.

$\therefore$ $5!, 6!, 7!, \ldots, 100!$ are all divisible by 15.

$\Rightarrow$ $5! \equiv 0 \pmod{15}$, $6! \equiv 0 \pmod{15}$, $\ldots$, $100! \equiv 0 \pmod{15}$.

$\Rightarrow$ $1! + 2! + \cdots + 100! = 1! + 2! + 3! + 4! + 0 + 0 + \cdots + 0 \pmod{15}$

$\equiv 1 + 2 + 6 + 24 \pmod{15}$

$\equiv 3 \pmod{15}$, since $30 \equiv 0 \pmod{15}$.

$\Rightarrow$ The required remainder is 3.

4. Find the positive integers n for which, $\sum_{k=1}^{n} k! = 1! + 2! + \cdots + n!$ is a square.

Solution: Let For $n \geq 5$, $n! \equiv 0 \pmod{10}$.

Thus $1! + 2! + \cdots 4! + 5! + \cdots + n! \equiv 1 + 2 + 6 + 24 + 0 + \cdots + 0 \pmod{10}$

$\equiv 3 \pmod{10}$.

For $n \geq 5$, $1! + 2! + \cdots + n!$ has 3 in its unit place.

No integer exists whose square ends in 3.

$\Rightarrow$ For $n \geq 5$, $1! + 2! + \cdots + n!$ is not a square.

When $n = 1$, $1! + \cdots + n! = 1! = 1$, a square

When $n = 3$, $1! + \cdots + n! = 1! + 2! + 3! = 1 + 2 + 6$

$= 9$, a square.

When $n = 2$, $1! + \cdots + n! = 1! + 2! = 1 + 2 = 3$, not a square.

When $n = 4$, $1! + \cdots + n! = 1! + 2! + 3! + 4!$

$= 1 + 2 + 6 + 24$

$= 33$, not a square.

$\therefore$ $1! + 2! + \cdots + n!$ is a square only for $n = 1$ and $n = 3$.

5. Find the remainder when 16^{53} is divided by 7.

Solution:

$16 \equiv 2 \pmod{7} \rightarrow ①$

$16^{53} \equiv 2^{53} \pmod{7}. \rightarrow ②$

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

$$\Rightarrow (2^3)^{17} \equiv 1^{17} \ (\text{mod } 7)$$

$$\Rightarrow 2^{51} \equiv 1 \ (\text{mod } 7)$$

$$\Rightarrow 2^{53} = 2^{51} \cdot 2^2 \equiv 1 \cdot 4 \ (\text{mod } 7) \equiv 4 \ (\text{mod } 7)$$

→ From ① ⇒ $16^{53} \equiv 4 \ (\text{mod } 7)$.

∴ The remainder is 4.

6. Find the remainder when 13^{218} is divided by 17.

Solution:

$$13^2 = 169 \equiv -1 \ (\text{mod } 17)$$

$$(13^2)^{109} \equiv (-1)^{109} \ (\text{mod } 17)$$

$$\equiv -1 \ (\text{mod } 17).$$

$$\equiv 16 \ (\text{mod } 17)$$

∴ The remainder is 16.

7. Find the remainder when 3^{247} is divided by 17.

Solution:

$$3^3 = 27 \equiv 10 \ (\text{mod } 17)$$

$(3^3)^2 \Rightarrow 3^6 \equiv 10^2 \ (\text{mod } 17) \equiv -2 \ (\text{mod } 17)$. $17 \times 6 = 102$

$\Rightarrow (3^6)^4 \equiv (-2)^4 (\text{mod } 17) \Rightarrow (3^6)^4 \equiv 16 \ (\text{mod } 17)$.

$$\Rightarrow 3^{24} \equiv (-1) \ (\text{mod } 17)$$

$$3^{247} = 3^{(24)(10)+7} = (3^{24})^{10} \ 3^6 \cdot 3$$

$$\equiv (-1)^{10} (-2)(3) \ (\text{mod } 17)$$

$$\equiv -6 \ (\text{mod } 17)$$

$$\equiv 11 \ (\text{mod } 17).$$

∴ The remainder is 11.

8. compute the remainder when 3^{247} is divided 25.

Solution: $3 \equiv 3 \pmod{25}$.

$$3^2 \equiv 9 \pmod{25}$$

$$(3^2)^2 \equiv 9^2 \pmod{25} \Rightarrow 3^4 \equiv 6 \pmod{25}$$

$$(3^4)^2 \equiv 6^2 \pmod{25} \Rightarrow 3^8 \equiv 11 \pmod{25}$$

$$(3^8)^2 \equiv 11^2 \pmod{25} \Rightarrow 3^{16} \equiv 21 \pmod{25}$$

$$(3^{16})^2 \equiv 21^2 \pmod{25} \Rightarrow 3^{32} \equiv 16 \pmod{25}$$

$$(3^{32})^2 \equiv 16^2 \pmod{25} \Rightarrow 3^{64} \equiv 6 \pmod{25}$$

$$(3^{64})^2 \equiv 6^2 \pmod{25} \Rightarrow 3^{128} \equiv 11 \pmod{25}$$

(128 is the largest power of 2 contained in 247)

$$3^{247} = 3^{128+64+32+16+4+2+1}$$

$$= 3^{128}\, 3^{64}\, 3^{32}\, 3^{16}\, 3^{4}\, 3^{2}\, 3$$

$$\equiv (11)(6)(16)(21)(6)(9)(3) \pmod{25}$$

$$\equiv 11\,(6.16)(21)(6.9)(3) \pmod{25}$$

$$\equiv [11(-4)][(-4)(-4)](3) \pmod{25}$$

$$\equiv (6)(9)(3) \pmod{25}$$

$$\equiv (4)(3) \pmod{25}$$

$$\equiv 12 \pmod{25}.$$

Hence the remainder is 12.

9. Find the remainder when 3^{181} is divided by 17.

Solution: $3^1 \equiv 3 \pmod{17}$.

$$3^2 \equiv 9 \pmod{17}.$$

$3^4 \equiv -4 \pmod{17}$

$3^8 \equiv -1 \pmod{17}$ ×

$3^{16} \equiv 1 \pmod{17}$

$3^{32} \equiv 1 \pmod{17}$

$3^{64} \equiv 1 \pmod{17}$

$3^{128} \equiv 1 \pmod{17}$.

$3^{181} = 3^{128}\ 3^{32}\ 3^{16}\ 3^{4}\ 3^{1}$

$\equiv 1 \cdot 1 \cdot 1 \cdot \overset{-4}{\cancel{13}} \cdot 3 \pmod{17}$.

$3^{181} \equiv 5 \pmod{17}$

The remainder is 5.

Linear Congruence:

A congruence is of the form $ax \equiv b \pmod{m}$, where m is a positive integer and a, b are integers and x is a variable is called a linear congruence.

A linear congruence $ax \equiv b \pmod{m} \Leftrightarrow$ $ax = my + b$ for some integer. y.

$\therefore$ $ax \equiv b \pmod{m}$ is solvable $\Leftrightarrow$ the LDE $ax - my = b$ is solvable.

Ex:

1. The congruence $4x \equiv 7 \pmod{5}$ has unique solution modulo 5, since $(4,5) = 1$.
2. The congruence $2x \equiv 3 \pmod{4}$ has no solution since $(2,4) = 2 = d$ and $d \nmid 3$.

3. The congruence $8x \equiv 10 \pmod{6}$ is solvable since $(8,6) = 2$ and $2|10$.

Theorem:

1. The linear congruence $ax \equiv b \pmod{m}$ is solvable iff $d|b$ where $d = (a, m)$.
2. The linear congruence $ax \equiv b \pmod{m}$ has a unique Solution iff $(a, m) = 1$.
3. The linear congruence $ax \equiv b \pmod{m}$. Then $d = (a, m)$ and the general solution is,

$$x = x_0 + \left(\frac{m}{d}\right)t, \quad 0 \leq t < d.$$

1. Solve the congruence relation $12x \equiv 48 \pmod{18}$.

Solution: $d = (a, m) = (12, 18) = 6$ and $d|48 \rightarrow 6|48$

$\Rightarrow$ The relation is solvable.

Since $d = 6$, the congruence has 6 incongruent solutions Modulo 6.

$$12x = 48 \pmod{18} \Leftrightarrow 12x \equiv 12 \pmod{18}.$$

By trial error, $x_0 = 1$ is a particular Solution.

The 6 incongruent solutions are:

$$x = x_0 + \left(\frac{m}{d}\right)t, \quad 0 \leq t < 6 = d$$

$$= 1 + \left(\frac{18}{6}\right)t, \quad 0 \leq t < 6$$

$$= 1 + 3t, \quad 0 \leq t < 6.$$

$\Rightarrow x = 1, 4, 7, 10, 13, 16.$

Modular Inverses:

Theorem: The unique solution of $ax \equiv b \pmod{m}$, where $(a,m)=1$, is the least residue of $a^{-1}b \pmod{m}$.

Proof: Given: $ax \equiv b \pmod{m}$

$$\Rightarrow a^{-1}ax \equiv a^{-1}b \pmod{m}$$

$$\Rightarrow 1.x \equiv a^{-1}b \pmod{m}$$

$$\Rightarrow x \equiv a^{-1}b \pmod{m}.$$

Ex: $7 \equiv 8^{-1}1 \pmod{11}$

1. Let $7.8 \equiv 1 \pmod{11}$, 7 is invertible and an inverse of 7 modulo 11 is 8.
   $8 \equiv 7^{-1}1 \pmod{11}$

2. Since $10.10 \equiv 1 \pmod{11}$ inverse of 10 modulo 10 is 10. ie, 10 is self-invertible.

$31 = 3\times10+1$

$1 = 31 - 3\times10$

1. Solve for x the linear congruence

   i) $3x \equiv 7 \pmod{31}$ (ii) $5x \equiv 8 \pmod{37}$.

$77-62$
31
93

$x \equiv 11.7 \pmod{31}$

77
62
15

Solution:

① $3x \equiv 7 \pmod{31} \Rightarrow x \equiv 3^{-1}7 \pmod{31} \longrightarrow$ ①

Given integers 31 and 3 by division algorithm.

$$31 = 10\times3+1$$

$$\Rightarrow 1 = 31 - 10\times3 \Rightarrow 1 = 31 + 21.3 \pmod{31}$$

$$\Rightarrow 1 \equiv 21.3 \pmod{31}$$

$$\Rightarrow 3^{-1} = 21$$

From ①, $x \equiv 21.7 \pmod{31} \Rightarrow x \equiv 147 \pmod{31}$

$$\Rightarrow x \equiv 23 \pmod{31}.$$

$31 = 10\times3+1$
$3 = 2.1+1$
$1 = 3 - 2.1$
$= 3 - 2(31 - 10.3)$
$= 3 - 2.31 + 10.3 \Rightarrow$
$= 3 -$

$1 = 11.3 - 2.31$
$11.3 = 1 + 2.31 \pmod{31}$
$11.3 \equiv 1 \pmod{31}$
$11 = 3^{-1}$
$x = 11.7 \pmod{31}$

(ii) $5x \equiv 8 \pmod{37}$

$\Rightarrow x = \boxed{5^{-1}} 8 \pmod{37}$. ①

By division algorithm,

$$\left.\begin{aligned} 37 &= 7.5 + 2 \\ 5 &= 2.2 + 1 \end{aligned}\right\} \Rightarrow \begin{aligned} 1 &= 5 - 2.2 \\ &= 5 - 2(37 - 7.5) \\ &= 15.5 - 2.37 \end{aligned}$$

$15.5 \equiv 1 + 2.37 \pmod{37}$

$\Rightarrow 15.5 \equiv 1 \pmod{37}$.

$\Rightarrow 5^{-1} = 15$

From ①, $x \equiv 15.8 \pmod{37}$

$\equiv 120 \pmod{37}$

$x \equiv 9 \pmod{37}$.

$$\begin{array}{r} 62 \\ 62 \\ \hline 124 \\ 31 \\ \hline 155 \end{array}$$

$3x \equiv 7 \pmod{31}$

$\rightarrow$ ① $x \equiv 3^{-1} 7 \pmod{31}$.

$31 = 10 \times 3 + 1$

$3 = 2.1 + 1$

$1 = 3 - 2.1$

$= 3 - (2(31 - 10.3)$

$= 1.3 - 2.31 + 20.3$

$= 1.3 - 2.31 + 20.3$

$= 21.3 - 2.31$

~~$1 \equiv 21.3 \pmod{37}$~~

$21.3 \equiv 1 \pmod{31}$

$3^{-1} = 21$

$x \equiv 21.7 \pmod{31}$

$\equiv 147 \pmod{31}$.

$\equiv 23 \pmod{31}$

$$\begin{array}{r} 147 \\ 124 \\ \hline 23 \\ \hline \end{array}$$

2x2 Linear System:

A 2x2 linear system is of the form

$ax + by \equiv e \pmod{m}$

$cx + dy \equiv f \pmod{m}$.

There are 2 Methods to solve this system,

1. Elimination Method.
2. Cramer's Rule.

1. Elimination Method:

1. Using the method of elimination, solve the linear system:

$2x + 3y \equiv 4 \pmod{13}$

$3x + 4y \equiv 5 \pmod{13}$.

Solution:

Given: $2x + 3y \equiv 4 \pmod{13} \rightarrow ①$

$3x + 4y \equiv 5 \pmod{13} \rightarrow ②$

$4 \times ① \Rightarrow 8x + 12y \equiv 16 \pmod{13} \equiv 3 \pmod{13} \rightarrow ③$

$3 \times ② \Rightarrow 9x + 12y \equiv 15 \pmod{13} \equiv 2 \pmod{13} \rightarrow ④$

$④ - ③ \Rightarrow x \equiv -1 \pmod{13}$

$\equiv 12 \pmod{13}.$

$8x \equiv 3 \pmod{13}$
$9x \equiv 2 \pmod{13}$
$x \equiv -1 \pmod{13}$
$\equiv 12 \pmod{13}$

from ① $\Rightarrow 2.12 + 3y \equiv 4 \pmod{13}$

$\Rightarrow 3y \equiv 4 - 11 \pmod{13}$

$\Rightarrow 3y \equiv -7 \pmod{13} \equiv 6 \pmod{13}$

$\Rightarrow y \equiv 2 \pmod{13}.$

2. **Cramer's Rule:**

1. The linear system,

$$ax + by \equiv e \pmod{m}$$
$$cx + dy \equiv f \pmod{m}.$$

has a unique solution iff $(\Delta, m) = 1$, where $\Delta \equiv (ad - bc) \pmod{m}$

2. When the linear system has unique solution mod m, it is given by,

$$x_0 \equiv \Delta^{-1} \begin{vmatrix} e & b \\ f & d \end{vmatrix} \pmod{m}$$

$$y_0 \equiv \Delta^{-1} \begin{vmatrix} a & e \\ c & f \end{vmatrix} \pmod{m}$$

$$\Delta \equiv \begin{vmatrix} a & b \\ c & d \end{vmatrix} \pmod{m}.$$

1. verify that the linear System:

$$2x + 3y \equiv 4 \pmod{13}$$
$$3x + 4y \equiv 5 \pmod{13}.$$

has a unique Solution Mod 13.

Solution: $\Delta \equiv (ad-bc) \pmod{13}$

$\equiv (8-9) \pmod{13}$

$\Delta \equiv -1 \pmod{13};$

$\Delta \equiv 12 \pmod{13}$

$\Rightarrow (\Delta, m) = (12, 13) = 1.$

⇒ The given System has unique Solution.

2. Solve the linear system:

$$\overset{a}{3}x + \overset{b}{13}y \equiv \overset{e}{8} \pmod{55}$$
$$\overset{c}{5}x + \overset{d}{21}y \equiv \underline{\overset{f}{34}} \pmod{55}.$$

Solution:

Given: $a = 3,\ b = 13,\ c = 5,\ d = 21$

$\Delta \equiv (ad - bc) \bmod 55$

$\equiv (63-65) \pmod{55}$

$\Delta \equiv -2 \pmod{55}. \equiv 53 \pmod{55}$

$\Rightarrow (\Delta, m) = (53, 55) = 1$

⇒ The system has a unique Solution.

The unique Solution is given by,

$$x_0 \equiv \Delta^{-1} \begin{vmatrix} 8 & 13 \\ 34 & 21 \end{vmatrix} \pmod{55}$$

$\equiv 27\,(168 - 442) \pmod{55}$

$= 27\,(-274) \pmod{55}.$

$\equiv 27(1) \pmod{55}$

$x_0 \equiv 27 \pmod{55}$

$y_0 \equiv \Delta^{-1} \begin{vmatrix} 3 & 8 \\ 5 & 34 \end{vmatrix} \pmod{55}$

$\equiv 27(102-40) \pmod{55}$

$\equiv 27(62) \pmod{55}$

$\equiv 27(7) \pmod{55}$

$\equiv 189 \pmod{55}$

$y_0 \equiv 24 \pmod{55}$

Since:

$\Delta = 53 \pmod{55}$

$\equiv -2 \pmod{55}$

and $(-2 \times 27) = -54$

$\equiv 1 \pmod{55}$

$\Rightarrow \Delta^{-1} = 27.$

$\equiv -2 \pmod{55}$

$\equiv \Delta \, 2 \times 27 (\quad)$

$\equiv -54 (\quad)$

$\Delta \equiv 1 \pmod{55}$

$1 \equiv \Delta^{-1} . 1 \pmod{55}$

Divisibility TESTS:

Divisibility Test for 10:

An integer is divisible by 10 iff its unit's digit is ~~10.~~ 0

Divisibility Test for 5:

An integer is divisible by 5 iff it ends in a 0 or 5.

Divisibility Test of 2

An integer n is divisible by 2^i iff the number formed by the last i digits in n is divisible by 2^i.

4886

$\frac{816}{8}$ 102

Divisibility Test for 3 and 9.

An integer is divisible by 3 iff sum of the digit is divisible by 3.

435 $4+3+5 = \frac{12}{3}$

An integer is divisible by 9 iff the sum of the digit is divisible by 9. 513

Divisibility Test for 11:

An integer is divisible by 11 iff the sum of the digits in the even positions minus the sum of the digits in the odd positions is divisible by 11.

$n_{2k-1} \; n_0$
231132
654321

5677765

Theorem: A palindrome with an even number of digits is divisible by 11.

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

Proof: Let $n = n_{2k-1} n_{2k-2} \cdots n_1 n_0$ be a palindrome, with even number of digits.

Then $n_{2k-1} = n_0, \; n_{2k-2} = n_1, \ldots, n_k = n_{k-1}$

$\therefore \; (n_0 + n_2 + \cdots + n_{2k-2}) - (n_1 + n_3 + \cdots + n_{2k-1}) = 0,$ divisible by 11.

$\Rightarrow n$ is divisible by 11.

11) 4224 (384
33
92
88
44
44
0

4+2+2+4 = 12
4+2+2+4 = 12
12 − 12 = 0.

Example:

1331 is a palindrome consisting even number of digits $\Rightarrow$ 1331 is divisible by 11.

Solution:

563365 is a palindrome with even number of digits => 563365 is divisible by 11.

The Chinese Remainder Theorem:

The linear system of congruences $x \equiv a_1 (\mod m_1)$, $x \equiv a_2 (\mod m_2), \ldots, x \equiv a_k (\mod m_k)$, where $m_1, m_2, \ldots, m_k$ are pairwise relatively prime, has a unique solution Modulo $m_1 m_2 \ldots m_k$.

$(M_1, m_1) = 1$ $(M_2, m_2) = 1$

$M = 4 \times 3 \times 5 \times 7$

Proof: Let $M = m_1 m_2 \ldots m_k$ and

$$M_1 = \frac{M}{m_1}, \quad M_2 = \frac{M}{m_2}, \ldots, M_k = \frac{M}{m_k}.$$

$M_1 = \frac{M}{4} = 3 \times 5 \times 7$

$M_2 = \frac{M}{m_2} = 4 \times 5 \times 7$

Then $(M_1, m_1) = 1 = (M_2, m_2) = \ldots = (M_k, m_k)$.

(For if $(M_1, m_1) \neq 1$, then let p be a prime factor of both m_1 and M_1.

$p | M_1 \Rightarrow p | (m_2 \ldots m_k)$ with $m_2, \ldots, m_k$ are pairwise relatively prime.

$\Rightarrow p | m_i$ for some i with $2 \leq i \leq k$.

$\therefore p | m_1$ and $p | m_i$ for some i with $2 \leq i \leq k$.

This is a contradiction, since $(m_1, m_i) = 1$.)

$M = 2, 4, 3, 6$

$M_1 = \frac{2 \times 4 \times 3}{2} = 12$

$(M_1, m_1) = (12, 2) = 2 = p$

$M = 2, 3, 5$

$M_1 = \frac{2 \times 3 \times 5}{2} = 15$

$(2, 15) = 1$

$M = 2, 3, 4, 5, 6$

$m_1 = \frac{M}{m_1} = \frac{\cancel{2} \times 3 \times 4 \times 5 \times 6}{\cancel{2}}$

$3 \times 4 \times 5 = 60$

$(60, 2) = 2$

$\frac{\cancel{2} \times 3 \times 5}{\cancel{2}}$

$(15, 2) = 1$

Also $M_i \equiv 0 (\mod m_j)$, if $i \neq j$. $\longrightarrow$ ①

(since for $i \neq j$, $m_j | M_i$ which implies $M_i \equiv 0 (\mod m_j)$)

Since $(M_i, m_i) = 1$, the congruence $M_i y \equiv 1 (\mod m_i)$ has a unique solution y_i, for $i = 1$ to k

$m_1 y_1 \equiv 1 (\mod m_1)$

i.e., $M_i y_i \equiv 1 (\mod m_i)$ for $i = 1$ to k. $\longrightarrow$ ②

Let $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_k M_k y_k$.

Claim: x is a solution of the given system of congruence.

For $1 \leq j \leq k$.

$$x = (a_1 M_1 y_1 + \dots + a_{j-1} M_{j-1} y_{j-1} + a_{j+1} M_{j+1} y_{j+1} + \dots + a_k M_k y_k) + a_j M_j y_j .$$

$$\equiv a_1 . 0 . y_1 + \dots + a_{j-1} . 0 . y_{j-1} + a_{j+1} . 0 . y_{j+1} + \dots + a_k . 0 . y_k + a_j . 1 \pmod{m_j} \text{ by ① and ②.}$$

$$\equiv 0 + a_j \pmod{m_j}$$

$$x \equiv a_j \pmod{m_j}$$

Thus 'x' Satisfies every congruence in the given System.

Uniqueness part:

To prove the uniqueness of the Solution, we need to prove that, for $1 \le j \le k$,

$x_0 \equiv a_j \pmod{m_j}$ and $x_1 \equiv a_j \pmod{m_j} \Rightarrow x_0 \equiv x_1 \pmod{M}$.

We know that,

$$x_1 \equiv a_j \pmod{m_j} \text{ and } x_0 \equiv a_j \pmod{m_j}$$

$$\Rightarrow x_1 - x_0 \equiv a_j - a_j \pmod{m_j} \equiv 0 \pmod{m_j}$$

$$\Rightarrow \overset{2\times3\times5}{m_j} \mid \overset{60}{(x_1 - x_0)} \text{ for every } j$$

$2 \times 3 \times 5 = 30 \mid 60$

$2 \mid 60, 3 \mid 60, 5 \mid 60.$

$$\Rightarrow \operatorname{lcm}(m_1, m_2, \dots, m_k) \mid (x_1 - x_0)$$

$\Rightarrow M \mid (x_1 - x_0)$, since $m_1, m_2, \dots, m_k$ are pairwise relatively prime.

$$\Rightarrow \operatorname{lcm}(m_1, m_2, \dots, m_k) = M$$

$$60 \overline{\smash{)}\, 120} \quad \begin{matrix} 2 \\ 120 \end{matrix}$$

$$\Rightarrow \overset{60}{x_0} \equiv \overset{120}{x_1} \pmod{\overset{60}{M}}$$

$120 - 60 \pmod{60}$

60

This prove the uniqueness part.

$60 \mid 120 - 60$

$60 \mid 60$

1. Solve Sun-Tsu's Puzzle by iteration Method.

$x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$.

Solution:

Given: $x \equiv 1 \pmod 3 \rightarrow ①$

$x \equiv 2 \pmod 5 \rightarrow ②$

$x \equiv 3 \pmod 7 \rightarrow ③$

Since $x \equiv 1 \pmod 3 \Rightarrow x = 1 + 3t_1$ where t_1 is an integer.

② $\Rightarrow \; 1 + 3t_1 \equiv 2 \pmod 5$

$\Rightarrow 3t_1 \equiv 1 \pmod 5$ $\Rightarrow 3^{-1} 3t_1 \equiv 3^{-1} \pmod 5$

$1 t_1 \equiv 3^{-1} \pmod 5$

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

$\equiv 2 \pmod 5$

$\Rightarrow t_1 \equiv 2 \pmod 5$

$\Rightarrow t_1 = 2 + 5t_2$, where t_2 is an integer.

$\therefore x = 1 + 3t_1 = 1 + 3(2 + 5t_2)$

$x = 7 + 15t_2$.

$10 \cdot 10 \equiv 1 \pmod{11}$

$10 = 10^{-1}$

③ $\Rightarrow \; 7 + 15t_2 \equiv 3 \pmod 7$

$\Rightarrow 15t_2 \equiv 3 \pmod 7$

$\Rightarrow t_2 \equiv 3 \pmod 7$

$\Rightarrow t_2 = 3 + 7t$, where t is an integer.

$\therefore x = 7 + 15t_2 = 7 + 15(3 + 7t)$

$x = 52 + 105t$

Hence any integer of the form $x = 52 + 105t$ is a solution of Sun-Tsu's Puzzle.

Taking $t = 0$, $x = 52$ is one of the solutions.

2. Using the CRT, Solve Sun-Tsu's Puzzle:

$x \equiv \overset{a_1}{1} \pmod{3}$, $x \equiv \overset{a_2}{2} \pmod{5}$, $x \equiv \overset{a_3}{3} \pmod{7}$.

Solution:

Given: $x \equiv 1 \pmod{\overset{m_1}{3}}$, $x \equiv 2 \pmod{\overset{m_2}{5}}$, $x \equiv 3 \pmod{\overset{m_3}{7}}$.

Here $m_1 = 3$, $m_2 = 5$, $m_3 = 7$.

They are pairwise disjoint and $M = m_1 m_2 m_3$

$= 3.5.7 = 105$.

$$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35, \quad M_2 = \frac{M}{m_2} = \frac{105}{5} = 21,$$

$$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15.$$

To find y_1 such that $M_1 y_1 \equiv 1 \pmod{m_1}$

ie, $35 y_1 \equiv 1 \pmod{3} \Rightarrow 2 y_1 \equiv 1 \pmod{3}$

$\Rightarrow y_1 \equiv 2^{-1} \pmod{3} \Rightarrow y_1 \equiv 2 \pmod{3}$.

To find y_2 such that $M_2 y_2 \equiv 1 \pmod{m_2}$

$\Rightarrow 21 y_2 \equiv 1 \pmod{5} \Rightarrow 1 y_2 \equiv 1 \pmod{5}$

$\Rightarrow y_2 \equiv 1 \pmod{5}$.

To find y_3 such that $M_2 y_3 \equiv 1 \pmod{m_3}$

i, $15 y_3 \equiv 1 \pmod{7} \Rightarrow 1 . y_3 \equiv 1 \pmod{7}$

$\Rightarrow y_3 \equiv 1 \pmod{7}$

By the CRT, the required solution is given by,

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{M}$

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

$\equiv (70 + 42 + 45) \pmod{105}$.

$$\equiv 157 \pmod{105}$$
$$\equiv 52 \pmod{105}$$

52 is the unique solution of the linear system Modulo 105. The general solution is,

$$x = 52 + 105t.$$

Towers of powers Modulo m:

1. Find the last digit in the decimal value of $1997^{(1998^{1999})}$.

Solution:

The last digit in the given number is equal to the least residue of the given number modulo 10. We have,

$$1997 \equiv 7 \pmod{10}. \longrightarrow ①$$

Further, $7^1 \equiv 7 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $7^3 \equiv 3 \pmod{10}$

$7^4 \equiv 1 \pmod{10}$; $7^5 \equiv 7 \pmod{10}$, $7^6 \equiv 9 \pmod{10}$

$7^7 \equiv 3 \pmod{10}$, $7^8 \equiv 1 \pmod{10}$, $7^9 \equiv 7 \pmod{10}$ etc.

Thus,
$$7^a \equiv \begin{cases} 7 \pmod{10}, & \text{if } a \equiv 1 \pmod 4 \\ 9 \pmod{10}, & \text{if } a \equiv 2 \pmod 4 \\ 3 \pmod{10}, & \text{if } a \equiv 3 \pmod 4 \\ 1 \pmod{10}, & \text{if } a \equiv 0 \pmod 4 \end{cases} \longrightarrow ②$$

498
4 | 1998
1996
2

we have, $1998 \equiv 2 \pmod 4$ $\longrightarrow$ ③

$\Rightarrow 1998^2 \equiv 0 \pmod 4$

$\Rightarrow (1998^2)^{999} \equiv 0 \pmod 4$

$\Rightarrow 1998^{1998} \equiv 0 \pmod 4$ $\longrightarrow$ ④

From ③ & ④, $1998^1 . 1998^{1998} \equiv 2 \times 0 \pmod 4$

$\Rightarrow 1998^{1999} \equiv 0 \pmod 4$ $\longrightarrow$ ⑤

Take $a = 1998^{1999}$. Then ⑤ $\Rightarrow a \equiv 0 \pmod 4$

(i) From ①, $1997^a \equiv 7^a \pmod{10} \equiv 1 \pmod{10}$ by ⑥

Hence, the last digit is 1.

2. Show that $11.14^n + 1$ is a composite number.

Solution:

Let $N = 11.14^n + 1$.

Then N is an odd integer.

To prove N is composite, we prove that some odd prime p divides N.

Case (i): Let n be even.

we try with $p = 3$. Note that $14 \equiv -1 \pmod 3$.

$\Rightarrow 14^n \equiv 1 \pmod 3$, since n is even.

$\Rightarrow 11.14^n \equiv 11 \pmod 3$

$\Rightarrow 11.14^n + 1 \equiv 12 \pmod 3$

$\Rightarrow 11.14^n + 1 \equiv 0 \pmod 3$.

$\Rightarrow 3 | N \Rightarrow N$ is composite.

Case (ii): Let N be odd.

we try with $p=5$.

Note that $14 \equiv -1 \pmod{5}$

$\Rightarrow 14^n \equiv -1 \pmod{5}$, since n is odd.

$\Rightarrow 11 \cdot 14^n \equiv -11 \pmod{5} \Rightarrow 11 \cdot 14^n + 1 \equiv -10 \pmod{5}$

$\Rightarrow N \equiv 0 \pmod{5}$.

$\Rightarrow 5 | N$

$\Rightarrow N$ is composite.

3. Find the remainder when $(n^2+n+41)^2$ is divided by 12.

Solution: Given: $(n^2+n+41)^2$ is divided by 12.

$$(n^2+n+41)^2 \equiv (n^2+n+5)^2 \pmod{12}.$$

$$\equiv (n^4+n^2+25+2n^3+10n+10n^2) \pmod{12}$$

$n^4+2n^3+11n^2+n^2-n^2+10n+2n-2n+25$

$$\equiv (n^4+2n^3+\cancel{12n^2}-n^2+\cancel{12n}-2n+1) \pmod{12}$$

$$\equiv (n^4+2n^3-n^2-2n+1) \pmod{12}$$

$$\equiv [n^3(n+2) - n(n+2)] + 1 \pmod{12}$$

$$\equiv (n^3-n)(n+2)+1 \pmod{12}.$$

$$\equiv n(n^2-1)(n+2)+1 \pmod{12}.$$

$n=2$ $1 \times 2 \times 3 \times 4 + 1 = 25/12 = 1$

$$\equiv \underbrace{(n-1)n(n+1)(n+2)}_{\text{product of 4 consecutive integers which is divisible by 12.}} + 1 \pmod{12}$$

$$\equiv 1 \pmod{12}$$

$\therefore$ The remainder is 1.

4. Show that the Fermat number $f_5 = 2^{2^5}+1$ is divisible by 641.

Solution: Given: $f_5 = 2^{2^5}+1$ is divisible by 641.

$640 \equiv -1 \ (\text{mod } 641)$

$\Rightarrow 5 \times 2^7 \equiv -1 \ (\text{mod } 641)$

$\Rightarrow (5 \times 2^7)^4 \equiv 1 \ (\text{mod } 641)$

$\Rightarrow 5^4 \times 2^{28} \equiv 1 \ (\text{mod } 641). \longrightarrow$ ①

Further, $5^4 = 625 \equiv -16 \ (\text{mod } 641) \longrightarrow$ ②

using ② in ①, $-16 \times 2^{28} \equiv 1 \ (\text{mod } 641)$

$\Rightarrow -2^4 \times 2^{28} \equiv 1 \ (\text{mod } 641)$

$\Rightarrow 2^{32} \equiv -1 \ (\text{mod } 641)$

$\Rightarrow 2^{2^5}+1 \equiv -1+1 \ (\text{mod } 641)$
$\equiv 0 \ (\text{mod } 641)$

$\Rightarrow 2^{2^5}+1$ is divisible by 641.

Casting out Nines:

"Every integer is congruent to the sum of its digits Modulo 9"

1. Using casting out nines, check if the sum of the numbers 3569, 24, 387 and 49, 508 is 78, 464.

Solution:

we have, $3569 \equiv 3+5+6+9 \equiv 5 \pmod 9$

$24,387 \equiv 2+4+3+8+7 \equiv 6 \pmod 9$

$49,508 \equiv 4+9+5+0+8 \equiv 8 \pmod 9$.

Their sum is, $\equiv 5+6+8 \pmod 9$

$\equiv 1 \pmod 9$. → ①

Given Sum $= 78,464$

$\equiv 7+8+4+6+4 \pmod 9$

$\equiv 2 \pmod 9$ → ②

① and ② ⇒ The answer is wrong.

Digital Root:

Let N be a given positive integer. Let S be the sum of the digits in N. Then find the sum of the digits in S. Continue the procedure until a single digit d is obtained. Then d is called the digital root of N.

1. Find the digital roots of square numbers.

Solution: Let n^2 be a given square number and let d its digital root.

By division algorithm,

$n \equiv r \pmod 9$, where $0 \le r < 9$.

$\Rightarrow n^2 \equiv r^2 \pmod 9$, where $0 \le r < 9$.

$r = 0 \Rightarrow r^2 = 0 \pmod 9$

$r = \pm 1 \Rightarrow r^2 \equiv 1 \pmod{9}$ ✓

$r = \pm 2 \Rightarrow r^2 \equiv 4 \pmod{9}$ ✓

$r = \pm 3 \Rightarrow r^2 = 9 \equiv 0 \pmod{9}$

$r = \pm 4 \Rightarrow r^2 = 16 \equiv 7 \pmod{9}$ ✓

$r = \pm 5 \Rightarrow r^2 = 25 \equiv 7 \pmod{9}$

⊗ $r = \pm 6 \Rightarrow r^2 = 36 \equiv 0 \pmod{9}$.

$r = \pm 5 \Rightarrow r^2 \equiv 1 \pmod{9}$

$r = \pm 7 \Rightarrow r^2 \equiv 4 \pmod{9}$

$r = \pm 7 \Rightarrow r^2 = 1 + 9 \equiv 4 \pmod{9}$.

$r = \pm 8 \Rightarrow r^2 = 64 \equiv 1 \pmod{9}$.

∴ For a square number, the digital root is one of 1, 4, 7, 9.