Sri Eshwar College of Engineering
An Autonomous Institution
Affiliated to Anna University, Chennai

U19MA203

DISCRETE MATHEMATICS

MODULE 5

DIOPHANTINE EQUATIONS AND CONGRUENCE'S

Prepared by Dr.N.Murugavalli, ASP/
Mathematics, SECE

MODULE V
NUMBER THEORY

Division algorithm- Base-b representations- Number patterns- Linear Diophantine equations – Congruences- Simultaneous linear congruences - Chinese Remainder Theorem (statement only) - Wilson's Theorem - Fermat's Theorem- Euler's Theorem.

Definition: Divisibility :

Let $a, b \in Z$. we say b divides a and write $b \mid a$ if $a = bc$ for some integer c.

We also say that b is a factor of a or **b is a divisor of a** or **a is a multiple of b**.

If b does not divide a, we write $b \nmid a$.

Theorem :

If $a, b, c \in Z$, then

(i) $a \mid a \; \forall \; a \neq 0 \in Z$ **(reflectivity)**

(ii) $a \mid b$ **and** $b \mid c \Rightarrow a \mid c \; \forall \; a, b \neq 0, c \neq 0 \in Z$ **(transitively)**

(iii) $a \mid b \Rightarrow a \mid bc, \forall \; a \neq 0, b \in Z$

(iv) $a \mid b$ **and** $a \mid c \Rightarrow a \mid xb + yc \;\; \forall \;\; x, y \in Z, a \neq 0 \in Z$ **(linearity)**

Definition: Divisibility :

Let a , $b \in Z$. we say b divides a and write b/a if a = bc for some integer c. we also say that b is a factor of a or b is a divisor of a or a is a multiple of b. If b does not divide a, we write $b \nmid a$.

Theorem :

If $a, b, c \in Z$, then

(i) $a \mid a \; \forall \; a \neq 0 \in Z$ **(reflectivity)**

(ii) $a \mid b$ **and** $b \mid c \Rightarrow a \mid c \; \forall \; a, b \neq 0, c \neq 0 \in Z$ **(transitively)**

(iii) $a \mid b \Rightarrow a \mid bc, \forall \; a \neq 0, b \in Z$

(iv) $a \mid b$ **and** $a \mid c \Rightarrow a \mid xb + yc \;\; \forall \;\; x, y \in Z, a \neq 0 \in Z$ **(linearity)**

Theorem : The Division algorithm.

Let a be any integer and b be a positive integer.

Then there exist unique integers q and r such that $a = q\,b + r$, where $0 \leq r < b$.

Proof:

First we prove existence and then uniqueness.

Existence is usually proved by suitable construction.

Consider the set $S = \{a - nb \mid n \in Z, a - nb \geq 0\}$

Clearly $S \subseteq W$.

Given a is any integer. Then $a < 0$ or $a \geq 0$.

If $a \geq 0$, then $a = a - 0 \cdot b \in S$ and so $a \in S$.

Hence S is non-empty.

Now let $a < 0$.

Since b is a positive integer, $b \geq 1$.

Multiplying by a, we get $ab \leq a$.

$\Rightarrow -ab \geq -a$ [as $a < 0$, in equality will reverse]

$\Rightarrow a - ab \geq a - a = 0$

$a - ab \in S \Rightarrow S$ is non empty

So, we find S is non-empty if $a \geq 0$ or $a < 0$.

Since S is a set of non-negative integers (by its construction), by well-ordering principle

S contains a least integer r.

As $r \in S$, we can find an integer q such that $r = a - q\,b$, where $r \geq 0$.

We shall now prove $r < b$.

We prove by contradiction.

Suppose $r \geq b$, then $r - b \geq 0$ and hence $r - b \in S$.
Since $r \geq 0$ and $b > 0$, $r - b < r$.

Now $r - b \in S$ and $r - b < r$, which contradicts the choice of r (as the least number in S)

$\therefore \quad r < b$

Thus there exist integers q and r such that

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

To prove the uniqueness.

Suppose we also have $a = q_1 b + r_1, 0 \le r_1 < b$

Then $q b + r = q_1 b + r_1$

$\Rightarrow (q - q_1) b = r_1 - r$

$\Rightarrow b \mid r_1 - r$

If $r_1 - r \neq 0$, then $b \mid r_1 - r$, which is a contradiction ($\because |r_1 - r| < b$)

$\therefore \quad r_1 - r = 0 \Rightarrow r_1 = r$

Hence $(q - q_1) b = 0 \quad \Rightarrow \quad q - q_1 = 0 \ (\because \ b > 0)$

$\Rightarrow q = q_1$

$\therefore$ the expression $a = qb + r, 0 \le r < b$ is unique, which is the division algorithm.

Note : In the expression $a = qb + r$, $0 \le r < b$. q is called the quotient and r is called the remainder.

If $r = 0$, then $a = q\,b \Rightarrow b \mid a$. i.e., if $r = 0$, then b is a factor of a. Though the theorem is called division algorithm, it does not give an algorithm (i.e., a sequence of steps that leads to the answer) to find q and r.

We find q and r by using the usual long division method.

Problem: Find *q* and *r* when

(i) 207 is divided by 15

(ii) –23 is divided by 5.

Solution:

(i) We have , $207 = 13(15) + 12, \quad 0 < 12 < 15$

$\therefore \quad q = 13$ and $r = 12$.

(ii) We have, $-23 = -5(5) + 2, \quad 0 < 2 < 5$

$\therefore \quad q = -5$ and $r = 2$.

Definition:

For any real number x,

1. **Absolute value** or **modulus function**

$$|x| = \begin{cases} x \ if \ x \geq 0 \\ -x \ if \ x \leq 0 \end{cases}$$

2. **Greatest integer function**

$[x]$= the greatest integer $\leq x$.

For Example: $[3.4]$= the greatest integer ≤ 3.4 *is* 3.

Base - b Representations

Base – *b* representations

We are familiar with the use of decimal notation, base 10, to express any integer or real number. We use it every day.

For example,

$$352 = 3(10^2) + 5(10) + 2(10^0)$$

$$= 3(10^2) + 5(10) + 2.1$$

This is called the decimal expansion of 352.

and $35.23 = 3(10^1) + 5\,(10^0) + 2\,(10^{-1}) + 3(10^{-2})$

Theorem :

Let b be an integer ≥ 2. If n is a positive integer, then it can be uniquely expressed in the form $n + a_k\, b^k + a_{k-1}\, b^{k-1} + \ldots + a_1\, b + a_0$, where $a_0, a_1, \ldots, a_k$ are non negative integers less than b and $a_k \neq 0$.

This theorem enables us to define the following representation.

Definition : If n is a positive integer and $b \geq 2$ and

$$n = a_k\, b^k + a_{k-1}\, b^{k-1} + \ldots + a_1 b + a_0, \qquad (1)$$

where $a_0, a_1, \ldots, a_k$ are non negative integers then the expression in (1) is called the **base *b*** expansion of the integer n.

We can write $n = (a_k\, a_{k-1} \ldots a_1 a_0)_b$.

For example,

$$(345)_{10} = 3(10^2) + 4\,(10) + 5\,(10^0)$$

$$(345)_8 = 3(8^2) + 4(8) + 5 = 165$$

Binary expansions

When base is 2, then the expansion is called the binary expansion when $b = 2$, each coefficient is 0 or 1 The digits 0 and 1 are called binary digits or bits. So, the binary expansion of an integer is just a bit string. Binary expansions are used by computers to represent and do arithmetic with integers.

Note :

1. The number system with base 10 is called the decimal system because the latin word **decem** means 10.

   The decimal system uses the 10 digits 0, 1, 2, 3,…, 9.
2. If the base $b > 10$, we use the letters A, B, C, … to represent the digits 10, 11, 12, … respectively in decimal notation.

Hexadecimal expansion

Another base used in computer science is 16. The base 16 expansion of an integer is called its hexadecimal expansion. Hexadecimal expansion uses the sixteen digits 0, 1, 2, …9, A, B, C, D, E and F where the letters A to F represent the digits 10 to 15 respectively (in decimal notation).

Problems:

1. **Express $(101011111)_2$ in base 10.**

Solution.

$$(101011111)_2 = 1(2^8) + 0(2^7) + 1(2^6) + 0(2^5) + 1(2^4) + 1(2^3) + 1(2^2) + 1(2) + 1(2^0)$$
$$= 256 + 64 + 16 + 8 + 4 + 2 + 1$$
$$= 351$$

2. **Express $(3\ AB0E)_{16}$ in base ten.**

Solution.

We know $A = 10, B = 11, E = 14$

$$\therefore \quad (3AB0E)_{16} = 3(16^4) + A(16^3) + B(16^2) + 0(16) + E(16^0)$$
$$= 3(16^4) + 10(16^3) + 11(16)^2 + 14$$
$$= 196608 + 40960 + 2816 + 14$$
$$= 240398$$

Express $(3\ ABC)_{16}$ in base 10.

Solution:

We know $A = 10, B = 11, C = 12$

$$(3ABC)_{16} = 3(16^3) + A(16^2) + B(16) + C$$

$$= 3(16^3) + 10(16)^2 + 11(16) + 12$$

$$= 12{,}288 + 2560 + 176 + 12$$

$$= 15036$$

Base conversion algorithm – decimal to base *b*

We shall now consider the converse problem of writing a decimal integer n into base b integer.

First divide n by b and obtain the quotient and remainder.

i.e., $n = q_0(b) + r_0, \quad 0 \le r_0 < b.$

Next we divide q_0 by b

i.e., $q_0 = q_1\, b + r_1, \quad 0 \le r_1 < b$

Next divide q_1

by b, i.e., $q_1 = q_2\, b + r_2, \quad 0 \le r_2 < b$

Proceed in this way until we get zero quotient.

Then the remainders in the reverse order gives the b representation of n.

Express 1076 in the binary system.

Solution.

$$
\begin{aligned}
1076 &= 538\,(2) + 0\\
538 &= 269\,(2) + 0\\
269 &= 134\,(2) + 1\\
134 &= 67\,(2) + 0\\
67 &= 33\,(2) + 1\\
33 &= 16\,(2) + 1\\
16 &= 8\,(2) + 0\\
8 &= 4\,(2) + 0\\
4 &= 2\,(2) + 0\\
2 &= 1\,(2) + 0\\
1 &= 0\,(2) + 1
\end{aligned}
$$

$$
\begin{array}{r|l}
2 & 1076 \\
 & 10 \\
\hline
 & 7 \\
 & 6 \\
\hline
 & 16 \\
 & 16 \\
\hline
 & 0
\end{array}
\qquad
538
$$

$$
\begin{array}{r|l}
2 & 538 \\
 & 4 \\
\hline
 & 13 \\
 & 12 \\
\hline
 & 18 \\
 & 18 \\
\hline
 & 0
\end{array}
\qquad
269
$$

$$
\begin{array}{r|l}
2 & 269 \\
 & 2 \\
\hline
 & 6 \\
 & 6 \\
\hline
 & 9 \\
 & 8 \\
\hline
 & 1
\end{array}
\qquad
134
$$

$$
\begin{array}{r|l}
2 & 134 \\
 & 12 \\
\hline
 & 14 \\
 & 14 \\
\hline
 & 0
\end{array}
\qquad
67
$$

$$
\begin{array}{r|l}
2 & 67 \\
 & 6 \\
\hline
 & 7 \\
 & 6 \\
\hline
 & 1
\end{array}
\qquad
33
$$

$$
\begin{array}{r|l}
2 & 33 \\
 & 2 \\
\hline
 & 13 \\
 & 12 \\
\hline
 & 1
\end{array}
\qquad
16
$$

$\therefore \quad 1076 = (10000110100)_2$

Express 12345 in the octal system.

Solution.

We have to write the decimal integer into base 8 system.

$$12345 = 1543\,(8) + 1$$
$$1543 = 192\,(8) + 7$$
$$192 = 24\,(8) + 0$$
$$24 = 3\,(8) + 0$$
$$3 = 0\,(8) + 3$$

$$\begin{array}{r|l} 8 & 12345 \\ \hline & 8 \\ \hline & 43 \\ & 40 \\ \hline & 34 \\ & 32 \\ \hline & 25 \\ & 24 \\ \hline & 1 \end{array} \qquad \begin{array}{r|l} 8 & 1543 \\ \hline & 8 \\ \hline & 74 \\ & 72 \\ \hline & 23 \\ & 16 \\ \hline & 7 \end{array} \qquad \begin{array}{r|l} 8 & 192 \\ \hline & 16 \\ \hline & 32 \\ & 32 \\ \hline & 0 \end{array} \qquad \begin{array}{r|l} 8 & 24 \\ \hline & 24 \\ \hline & 0 \end{array} \qquad \begin{array}{r} 3 \end{array}$$

$\therefore \quad 12345 = (30071)_8$

Base conversion from binary to octal:

To convert a binary system number to octal system, we group the binary digits into blocks of three bits from right to left and adding if necessary initial zero at the left most block and replace each group with the corresponding octal digit.

Convert the binary number $(11110011)_2$ into octal digit.

Solution:

Given 11 110 011

We group the digits in blocks of three digits from right to left.

Here the blocks are 011, 110, 011 (adding 0 to the left most block to get 3 digits).

Now, $011 = 0(2^2) + 1(2) + 1 = 3$

$110 = 1\,(2^2) + 1(2) + 0 = 6$

$011 = 0(2^2) + 1(2) + 1 = 3$

$(11110011)_2 = (363)_8$

Write 111010_{two} as an octal integer.

Solution:

Given $(111010)_2$

We rewrite, 111010 = 111, 010

Now, $111 = 1(2^2) + 1(2) + 1 = 7$

$010 = 0(2^2) + 1(2) + 0 = 2$

$(111010)_2 = (72)_8$

Base conversion from binary to hexadecimal

We group the binary digits into block of four bits from right to left, adding if necessary initial zero at the left most block to get a block of four bits. Replace each block by a hexadecimal number.

Write $(11111010111100)_2$ as a hexadecimal digit.

Solution:

Given $(111110110111100)_2$

We rewrite, 11 1110 1011 1100 as 0011, 1110, 1011, 1100

Now, $0011 = 0(2^3) + 0(2^2) + 1(2) + 1 = 3$

$1110 = 1(2^3) + 1(2^2) + 1(2) + 0 = 8 + 4 + 2 = 14(= E)$

$1011 = 1(2^3) + 0(2^2) + 1(2) + 1 = 8 + 2 + 1 = 11(= B)$

$1100 = 1(2^3) + 1(2^2) + 0(2) + 0 = 8 + 4 = 12(= C)$

$\therefore\ (11111010111100)_2 = (3EBC)_{16}$

Write $(3\ AD)_{16}$ as a binary number.

Solution:

Given $(3AD)_{16}$

We rewrite each digits as block of four bits.

$\therefore$ we write, $3 = 0(2^3) + 0(2^2) + 1(2) + 1 = 0011$

$$A = 10 = 1\,(2^3) + 0(2^2) + 1(2) + 0 = 1010$$

$$D = 13 = 1\,(2^3) + 1(2^2) + 0(2) + 1 = 1101$$

$\therefore$ $(3\ AD)_{16} = (001110101101)_2$

$= (1110101101)_2$

Convert $(237)_8$ as a binary number.

Solution:

Given: $(237)_8$

We rewrite each digit as blocks of three bits.

$\therefore$ we write, $2 = 0(2^2) + 1(2) + 0 = 010$

$$3 = 0(2^2) + 1(2) + 1 = 011$$

$$7 = 1(2^2) + 1(2) + 1 = 111$$

$$\therefore \quad (237)_8 = (010011111)_2$$

$$= (10011111)_2$$

Arrange the binary numbers 1011, 110, 11011, 10110 and 101010 in increasing order of magnitude.

Solution:

Given, 1011, 110, 11011, 10110.

We will convert these binary numbers into decimal numbers for comparison.

$\therefore$ we write, $1011 = 1(2^3) + 0(2^2) + 1(2) + 1 = 11$

$$110 = 1(2^2) + 1(2) + 0 = 6$$

$$11011 = 1(2^4) + 1(2^3) + 0(2^2) + 1(2) + 1 = 27$$

$$10110 = 1(2^4) + 0(2^3) + 1(2^2) + 1(2) + 0 = 22$$

and $$101010 = 1(2^5) + 0(2^4) + 1(2^3) + 0(2^2) + 1(2) + 0 = 42$$

$\therefore$ The binary numbers in increasing order are 110, 1011, 10110, 101010.

Find the value of the base b if $1001_b = 9$.

Solution:

Given : $1001_b = 9$

Since the digits are binary, we expect $b = 2$.

We shall now workout

Now, $1001_b = 9$

$$\Rightarrow 1(b^3) + 0(b^2) + 0(b) + 1 = 9$$

$$\Rightarrow b^3 + 1 = 9 \Rightarrow b^3 = 8 = 2^3 \Rightarrow b = 2$$

If $144_b = 49$, find the base b.

Solution:

Given: $(144)_b = 49$

$\Rightarrow 1(b^2) + 4(b) + 4 = 49$

$\Rightarrow b^2 + 4b - 45 = 0$

$\Rightarrow (b + 9)(b - 5) = 0$

Since base b is ≥ 2, $b + 9 \neq 0$.

$\therefore b - 5 = 0 \Rightarrow b = 5$

Try This!

(i) Write $(1010111)_2$ in hexadecimal system

(ii) Express 15036 in the hexadecimal system

(iii) Write 6137 in the octal system

(iv) Write 527 in binary system.

(v) Write $(A13F)_{16}$ in the binary system

NUMBER PATTERNS

In drawing scientific conclusions, there are two fundamental processes of reasoning that are commonly used.

One is the process of deduction, which is the process of reasoning from general to particular.

The other process of reasoning is the process of induction, which is the process of reasoning from particular to general. This process may lead to true or false conclusion. To succeed in the art of inductive reasoning one must be good at studying pattern. Observing particular cases or pattern a general statement is usually made. Such a statement is called a **conjecture or educated guess**.

A conjecture remains a conjecture until it is proved or disproved.

Inductive reasoning ends with the conjecture. Then the difficult task of proving it begins, one of the methods of proof is by mathematical induction.

We now consider some of the famous conjectures.

1. The great French mathematician Fermat (1601–1605) observed

$$2^{2^1} + 1 = 5, \text{ a prime}$$

$$2^{2^2} + 1 = 17, \text{ a prime}$$

$$2^{2^3} + 1 = 257, \text{ a prime}$$

On the basis of these particular cases Fermat conjectured that $2^{2^n} + 1$ is a prime for any positive integer n and he challenged the mathematicians of his days to disprove it. **After nearly 100 years, the great Swiss mathematician Euler** (1707–1783) **showed that $2^{2^5} + 1 = 4294967297$ is not a prime** because **it is divisible by 641**. Thus the conjecture is disproved

2. The great German mathematician G.W. Leibnitz (1646–1716) noticed that for any positive integer n.

$n^3 - n$ is divisible by 3

$n^5 - n$ is divisible by 5

$n^7 - n$ is divisible by 7

Observing this pattern, he was on the verge of conjecturing that for any odd integer r, $n^r - n$ is divisible by r.

But soon he noticed that $2^9 - 2 = 510$ is not divisible by 9.

This counter example disproved the conjecture.

From the pattern.

$$1.9+2=11$$
$$12.9+3=111$$
$$123.9+4=1111$$
$$1234.9+5=11111$$
$$\vdots$$

Write down the n^{th} row and prove the validity of the number pattern.

Solution.

From the given pattern we find the n^{th} row is $1\cdot2\cdot3\cdot4\cdot5\ldots n\cdot9+(n+1)=\underbrace{1111\ldots1}_{n+1\text{ ones}}$

$$\begin{aligned}
\text{L.H.S} &= 1\cdot2\cdot3\cdot4\ldots n\cdot9+(n+1)\\
&= 9\left[1(10^{n-1})+2(10^{n-2})+\ldots+(n-1)\cdot10+n\cdot1\right]+(n+1)\\
&= (10-1)[10^{n-1}+2\cdot10^{n-2}\ldots+(n-1)\cdot10+n]+(n+1)\\
&= 10^n+2\cdot10^{n-1}+3\cdot10^{n-2}+\ldots+(n-1)\cdot10^2+n\cdot10\\
&\qquad -\left(10^{n-1}+2\cdot10^{n-2}+\ldots+(n-1)\cdot10+n\right)+(n+1)\\
&= 10^n+10^{n-1}+10^{n-2}+\ldots+10-n+n+1\\
&= 10^n+10^{n-1}+10^{n-2}+\ldots+10+1\\
&= \underbrace{111\ldots1}_{(n+1)\text{ ones}} = \text{R.H.S} \qquad \text{(using place value)}
\end{aligned}$$

Sol: n^{th} row is

$$[9.8.7\ldots(10-n)].9+(8-n) = 8.8\ldots8 \quad (n+1) \text{ eight}$$

$1 \le n \le 8$.

$$LHS = 9.8.7\ldots(10-n).9+(8-n)$$

$$= 9\{9\times10^{n-1}+8\times10^{n-2}+\ldots+[10-(n-1)]\times10+(10-n).1\}+(8-n)$$

$$= 9[9.10^{n-1}+8.10^{n-2}+\ldots+(11-n).10+(10-n).1]+(8-n)$$

$$=(10-1)[9.10^{n-1}+8.10^{n-2}+\ldots+(11-n).10+(10-n).1]+(8-n)$$

$$= 9.10^n+8.10^{n-1}+7.10^{n-2}+\ldots+(11-n).10^2+(10-n).10-9.10^{n-1}-8.10^{n-2}-\ldots-(11-n).10-(10-n)+8-n.$$

$$= 9.10^n-10^{n-1}-10^{n-2}-\ldots-10-(10-n)+8-n$$

$$= 9.10^n-[10^{n-1}+10^{n-2}+\ldots+10]-2$$

(2) Given pattern

$9.9 + 7 = 88$

$98.9 + 6 = 888$

$987.9 + 5 = 8888$ ....

Find the formula for n^{th} row & prove it.

Sol: n^{th} row is

$[9.8.7 \ldots (10-n)] \cdot 9 + (8-n) = 8.8 \ldots 8$ ($n+1$) eight

$1 \le n \le 8$.

$LHS = 9.8.7 \ldots (10-n) \cdot 9 + (8-n)$

$= 9\{9 \times 10^{n-1} + 8 \times 10^{n-2} + \ldots + [10-(n-1)] \times 10 + (10-n) \cdot 1\} + (8-n)$

$$= 9\left[9.10^{n-1} + 8.10^{n-2} + \cdots + (11-n).10 + (10-n).1\right] + (8-n)$$

$$= (10-1)\left[9.10^{n-1} + 8.10^{n-2} + \cdots + (11-n).10 + (10-n).1\right] + (8-n)$$

$$= 9.10^{n} + 8.10^{n-1} + 7.10^{n-2} + \cdots + (11-n).10^{2} + (10-n).10 - 9.10^{n-1} - 8.10^{n-2} - \cdots - (11-n).10 - (10-n) + 8 - n.$$

$$= 9.10^{n} - 10^{n-1} - 10^{n-2} - \cdots - 10 - (10-n) + 8 - n$$

$$= 9.10^{n} - \left[10^{n-1} + 10^{n-2} + \cdots + 10\right] - 2$$

$$\left[(10-n) - (11-n)\right]10$$

$$(10-11)\,10 = -1 \times 10$$

$$= 9.10^n + 10^n - 10^n - [10^{n-1} + 10^{n-2} + \cdots + 10] - 1 - 1$$

$$= 10.10^n - [10^n + 10^{n-1} + \cdots + 10 + 1] - 1$$

$$= 10^{n+1} - \left[\frac{10^{n+1} - 1}{10 - 1}\right] - 1$$

$$= 10^{n+1} - \left[\frac{10^{n+1} - 1}{9}\right] - 1$$

$$= \frac{9.10^{n+1} - 10^{n+1} + 1 - 9}{9}$$

$$= \frac{1}{9}\left[8.10^{n+1} - 8\right]$$

$$\text{LHS} = \frac{8}{9}\left[10^{n+1} - 1\right]$$

$$LHS = \frac{8}{9}\left[10^{n+1} - 1\right]$$

$$RHS = \underbrace{8.8\ldots8}_{(n+1)\text{ eights}}.$$

$$= 8 \times 10^{n} + 8 \times 10^{n-1} + \ldots + 8 \times 10^{2} + 8 \times 10 + 8$$

$$= 8\left[10^{n} + 10^{n-1} + \ldots + 1\right]$$

$$= 8\left[\frac{10^{n+1} - 1}{10 - 1}\right]$$

$$RHS = \frac{8}{9}\left[10^{n+1} - 1\right]$$

$$LHS = RHS.$$

Hence the proof.

Linear Diophantine Equations

Introduction:

Equations with integer coefficients which are to be solved in integers are called Diophantine equations.

This type of equation was first investigated by the Greek algebraist Diophantus of Alexandria in the third century AD.

For example the equations

$$2x+3y=4, \qquad x^2+y^2=4, \qquad x^2+y^2=z^2$$

are called Diophantine equations if we restrict their solution to be integers.

The Diophantine equation $2x+3y=4$ is linear where as the other two Diophantine equations are nonlinear.

The equation $2x + 3y = 4$ has $(-1, 2)$ as a solution.

In fact it has infinitely many solutions $(2 + 3t, -2t)$, where t is an arbitrary integer.

Geometrically, Such solutions are points in the plane with integer coordinates and they are called lattice points.

Linear Diophantine Equations(LDE):

The linear Diophantine equations are the simplest class of Diophantine equations. The general form of a linear Diophantine equation (LDE) in two variables x and y is

$$ax + by = c$$

where a,b,c are integers

Theorem 4.1 :

The linear Diophantine equation a x + b y = c

Is solvable if and only if d/c, where d=(a,b). If x_0,y_0 is a particular solution of the linear Diophantine equation, then all its solutions are given by

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

Where a, b,c are integer.

Proof :

Assume the linear Diophantine equation $ax + by = c$ is solvable.

To prove d/c

If $x = \alpha$, $y = \beta$ is a solution, then

$$a\alpha + b\beta = c \qquad (1)$$

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

Implies $d/\ a\alpha + b\beta$

Implies $d/\ c$

Conversely , Assume d/c.

To prove the linear Diophantine

equation $ax + by = c$ is solvable

Since d/ c, c = dm for some integer m.

Since d = (a , b), then there exist integers r and s such that

d = r a + s b

Multiplying by m, we get

$$dm = (r\ a)\ m + (s\ b)\ m$$

$$c = (r\ m)\ a + (s\ m)\ b$$

This shows that $x_0 = r\ m$ and $y_0 = s\ m$ is a solution of the linear Diophantine equation .

So it is solvable.

Next we shall prove that if (x_0, y_0)is a solution of a x + b y= c, then

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

Is a solution for any integer t.

Now

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

$$= [a x_0 + b y_0] + (a b/d)t - (a b/d)t$$

$$= a x_0 + b y_0$$

$$= c$$

Therefore, $x = x_0 + \left(\frac{b}{d}\right) t \; and \; y = y_0 - \left(\frac{a}{d}\right) t$ is a solution for any t.

Finally , we prove that every solution x_1, y_1 is of this form.

Since x_0, y_0 and x_1, y_1 are solutions of the linear Diophantine equation $ax + by = c$.

We have , $ax_0 + by_0 = c$ and $ax_1 + by_1 = c$

Therefore , $ax_0 + by_0 = ax_1 + by_1$

$$a(x_1 - x_0) = b(y_0 - y_1) \qquad (2)$$

Dividing by d, we get

$$(a/d)\,(x_1 - x_0) = (b/d)\,(y_0 - y_1)$$

Since , $(a, b) = d$, $((a/d), (b/d)) = 1$

Hence (b / d) divides $(x_1 - x_0)$

Implies, $(x_1 - x_0) = (b / d)\, t$

for some integer t,

$$x_1 = x_0 + (b / d)\, t$$

Substituting in (2), we get

$$a(b / d)t = b(y_0 - y_1)$$

$$a((1/ d)t) = (y_0 - y_1)$$

$$(a / d)t = (y_0 - y_1)$$

$$y_1 = y_0 - (a / d) t.$$

Thus every solution is of the form

$x = x_0 + (b / d) t$ $y = y_0 - (a / d) t$, t is an arbitrary integer.

This solution is called the general solution of $ax + by = c$.

Corollary :

If (a,b)=1, then the LDE $ax + by=c$ is solvable and the general solution is

$$x = x_0 + b\,t$$

$$y = y_0 - a\,t$$

where x_0, y_0 is a particular solution and t is an arbitrary integer.

Theorem:

The linear Diophantine equation is solvable

$$a_1x_1+a_2x_2+\ldots+a_nx_n= c$$

iff $(a_1 ,a_2, \ \ldots, a_n)/c$.

When it is Solvable, it has infinitely many solutions.

Problem 1:

Determine if the linear Diophantine equation $12x+18y=30$ is solvable. If so, find the solutions.

Solution:

Given the LDE is $12x+18y=30$ (1)

Here $a=12, b=18, c=30$

$\therefore$ $(a, b) = (12, 18) = 6$

So, $d = (a, b) = 6$

Since $6 \mid 30$, we have $d \mid c$

So, the LDE is solvable.

Clearly, $x_0=1$, $y_0=1$ is a solution of (1)

Therefore the general solution is given by

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

$$\Rightarrow \quad x = 1 + \frac{18}{16} t \quad and \quad y = 1 - \frac{12}{6} t$$

$$\Rightarrow \quad x = 1 + 3t \quad and \quad y = 1 - 2t, \ \ t \in Z$$

Problem 2:

Examine whether the LDE $12x + 16y = 18$ is solvable. Write the general solution is solvable.

Solution:

Given the LDE is $12x + 16y = 18$ (1)

Here $a = 12$, $b = 16$, $c = 18$

$\therefore$ $(a, b) = (12, 16) = 4$

$\therefore$ $d = 4$

Since $4 \neq 18$, $d \neq c$

Hence the given LDE is not solvable.

Problem 3:

Prove that LDE ax + by = c is solvable if and only if $d \mid c$, where d=(a, b). Further obtain the general solution of 15x +21y = 39.

Solution:

For the first part refer theorem 4.1

Given the LDE is $15x + 21y = 39$ (1)

Here $a = 15$, $b = 21$, $c = 39$

$\therefore$ $(a, b) = (15, 21) = 3$ 3 15, 21

$\therefore$ $d = (a, b) = 3$ 5, 7

Since $3 \mid 39$, we have $d \mid c$

Hence the LDE is solvable.

By inspection (or trial and error), we find one solution of (1) is

$$x_0 = -3 \quad \text{and} \quad y_0 = 4$$

Then the general solution is given by

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

$$\Rightarrow \qquad x = -3 + \frac{21}{3}t \qquad and \qquad y = 4 - \frac{15}{3}t$$

$$\Rightarrow \qquad x = -3 + 7t \qquad and \qquad y = 4 - 5t, \qquad t \in Z$$

Congruence modulo m:

Let m be a positive integer. An integer a is congruent to an integer b modulo m if m $|$a-b.

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

If a is not congruent to b modulo m, we say a is in congruent to b mod m.

Example:

(i) Congruence mod 12 to tell the time of the day.

(ii) Congruence mod 7 to tell the day of the week.

Theorem 4.3

$a \equiv b \pmod{m}$ if and only if $a = b + km$

for some integer k.

Proof:

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

Then $a - b = mk$ for some integer k

$\Rightarrow$ $a = b + mk$

Conversely, let $a = b + km$

Then $a - b = km$

$\Rightarrow m \mid a - b$

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

Theorem 4.4

Properties of congruence relation

1. Reflexive property:

$$a \equiv a \pmod{m} \ \forall \ a \in Z.$$

2. Symmetric property:

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

3. Transitive property:

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

$a \equiv c \pmod{m}$.

Proof of (i)

Reflexive property:$a \equiv a \pmod{m}\ \forall\ a \in Z$

Proof:

Since $m \mid a - a = 0\ \forall\ a \in Z$

$a \equiv a \pmod{m} \forall\ a \in Z$

Symmetric property:

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

Proof:

If $a \equiv b \pmod{m}$, then $m \mid a - b$

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

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

Transitive property:

If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

Proof:

If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then

$$m \mid a - b \text{ and } m \mid b - c$$

$$\therefore \quad m \mid (a - b) + (b - c) \Rightarrow a \equiv c \pmod m$$

This theorem says congruence relation is an equivalence relation.

Theorem 4.5

$a \equiv b \pmod{m}$ if and only if a and b have the same remainder when divided by m.

Proof

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

Then $m \mid a - b$

$\Rightarrow$ $a - b = m k$ for some integer k.

$\Rightarrow$ $a = b + km$

Now consider b and m . By division algorithm

$$b = qm + r,\ 0 \leq r < m$$

Then $a = qm + r + km$

$\Rightarrow$ $= (q + k)m + r, \quad 0 \leq r < m$

$\therefore$ a leaves remainder r on division by m.

Thus a and b have the same remainder r when divided by m

Conversely, let a and b have the same remainder r when divided by m.

$\therefore \quad a = qm + r$

and $\quad b = q' m + r, \qquad 0 \le r < m$

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

$\Rightarrow \quad m \mid a - b$

$\Rightarrow \quad a \equiv b \pmod{m}.$

Theorem 4.6

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

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

(ii) $a \cdot c \equiv b \cdot d \pmod{m}$

Proof:

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

$\therefore \quad a = b + k\,m$

and $\quad c = d + k'\,m$

for some integers k , k'.

$\therefore \quad a + c = b + d + (k + k')\,m$

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

Hence (i) is proved

Now $ac = (b + km)(d + km)$

$= bd + (k k' + dk) m + k k' m^2$

$\Rightarrow \quad ac - bd = m [b k' + dk + k k' m]$

$\Rightarrow \quad m \mid ac - bd$

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

Hence (ii) is proved

Corollary:

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

(i) $a - c \equiv b - d \pmod{m}$

(ii) $ac \equiv bc \pmod{m}$

(iii) $a^2 \equiv b^2 \pmod{m}$

More generally $a^r \equiv b^r \pmod{m}$ for any positive integer r.

EXAMPLE 1

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

Solution.

We know $n! = 1 \cdot 2 \cdot 3 \ldots (n-1) \cdot n$

For divisibility by 15, we consider mod 15.

$5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$ is divisible by 15. (but $4! = 1 \cdot 2 \cdot 3 \cdot 4$ is not divisible by 15)

$\therefore \quad 5! \equiv 0 \pmod{15}$

All higher factorials are divisible by 15.

So, for $r \geq 5$, $r! \equiv 0 \pmod{15}$

$\therefore 1! + 2! + 3! + 4! + 5! + \ldots + 100!$

$\equiv 1! + 2! + 3! + 4! + 0 + 0 + \ldots + 0 \pmod{15}$

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

$\equiv 1 + 2 + 30 \pmod{15}$

$\equiv 3 + 0 \pmod{15}$ $[\because 30 \equiv 0 \pmod{15}]$

$\equiv 3 \pmod{15}$

$\therefore$ when $1! + 2! + 3! + \ldots + 100!$ is divided by 15, the remainder is 3.

EXAMPLE 2

Find the remainder when $1! + 2! + 3! + 4! + \ldots + 300!$ is divided by 13.

Solution.

For divisibility by 13, we consider mod 13.

For $r \geq 13$, $r!$ will contain 13 as a factor.

$\therefore$ $$r! \equiv 0 \pmod{13}$$

$$\therefore\ 1! + 2! + 3! + 4! + \ldots + 12! + \ldots + 300!$$

$$\equiv 1! + 2! + 3! + 4! + \ldots + 12! + 0 + 0 + \ldots + 0 \pmod{13}$$

$$\equiv 1! + 2! + 3! + 4! + 5! + \ldots + 12! \pmod{13}$$

$$= 1 + 2 + 6 + 24 + 120 + \ldots + 12! \pmod{13}$$

$2 + 24 = 26 \equiv 0 \pmod{13}$

$5! = 120 \equiv 3 \pmod{13}$

$6! = 5!\,6 \equiv 3 \times 6 \pmod{13}$

$\equiv 18 \pmod{13}$

$\equiv 5 \pmod{13}$

$7! = 6!\,7 \equiv 5 \times 7 \pmod{13}$

$\equiv 35 \pmod{13}$

$\equiv 9 \pmod{13}$

$8! = 7!\,8 \equiv 9 \times 8 \pmod{13}$

$\equiv 72 \pmod{13}$

$\equiv 7 \pmod{13}$

$9! = 8!\,9 \equiv 7 \times 9 \pmod{13}$

$\equiv 63 \pmod{13}$

$\equiv 11 \pmod{13}$

$$\begin{array}{r} 9 \\ 13\overline{)\,120} \\ 117 \\ \hline 3 \end{array} \qquad \begin{array}{r} 2 \\ 13\overline{)\,35} \\ 26 \\ \hline 9 \end{array}$$

$$\begin{array}{r} 5 \\ 13\overline{)\,72} \\ 65 \\ \hline 7 \end{array} \qquad \begin{array}{r} 4 \\ 13\overline{)\,63} \\ 52 \\ \hline 11 \end{array}$$

$$\begin{array}{r} 8 \\ 13\overline{)\,110} \\ 104 \\ \hline 6 \end{array} \qquad \begin{array}{r} 5 \\ 13\overline{)\,66} \\ 65 \\ \hline 1 \end{array}$$

$$10! = 9!\ 10 \equiv 11 \times 10 \pmod{13}$$

$$\equiv 110 \pmod{13}$$

$$\equiv 6 \pmod{13}$$

$$11! = 10!\ 11 \equiv 6 \times 11 \pmod{13}$$

$$\equiv 66 \pmod{13}$$

$$\equiv 1 \pmod{13}$$

$$12! = 11!\ 12 \equiv 1 \times 12 \pmod{13}$$

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

$$\therefore \quad 1! + 2! + 3! + \ldots + 300! \equiv 1 + 6 + 0 + 3 + 5 + 9 + 7 + 11 + 6 + 1 + 12 \pmod{13}$$

$$\equiv 61 \pmod{13} \equiv 9 \pmod{13}$$

$\therefore$ the remainder is 9 when $1! + 2! + 3! + \ldots + 300!$ is divided by 13.

Compute the remainder 3^{181} is divided by 17.

Solution.

We have to find the remainder when 3^{181} is divided by 17.

We have $3^2 \equiv 9 \pmod{17}$

$3^4 \equiv 9^2 = 81 \pmod{17}$

$\equiv 13 \pmod{17}$

$\equiv -4 \pmod{17}$

$3^8 \equiv (-4)^2 \pmod{17}$

$\equiv 16 \pmod{17}$

$\equiv -1 \pmod{17}$

$$\begin{array}{r|l} & 4 \\ 17 & 81 \\ & 68 \\ \hline & 13 \\ \hline \end{array} \qquad \begin{array}{r|l} & 2 \\ 17 & 39 \\ & 34 \\ \hline & 5 \\ \hline \end{array}$$

$\therefore \quad 3^{16} \equiv (-1)^2 \equiv 1 \pmod{17}$

$\therefore \quad (3^{16})^9 \equiv 1^9 \equiv 1 \pmod{17}$

$\Rightarrow \quad 3^{144} \equiv 1 \pmod{17}$

$3^{181} = 3^{144+32+4+1} = 3^{144} \cdot 3^{32} \cdot 3^4 \cdot 3^1$

But $(3^{16})^2 \equiv 1 \pmod{17}$

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

$\therefore \quad 3^{181} \equiv 1 \cdot 1 \cdot 13 \cdot 3 \pmod{17}$

$\equiv 39 \pmod{17}$

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

$\therefore$ the remainder when 3^{181} is divided by 17 is **5**.

EXAMPLE 8

Find the remainder when 193^{183} is divided by 19.

Solution.

We have to find the remainder when 193^{183} is divisible by 19.

We have $193 \equiv 3 \pmod{19}$

$193^2 \equiv 9 \pmod{19}$

$193^4 \equiv 81 \equiv 5 \pmod{19}$

$193^8 \equiv 5^2 \equiv 6 \pmod{19}$

$193^{16} \equiv 36 \equiv -2 \pmod{19}$

$\therefore \quad (193^{16})^4 \equiv (-2)^4 \pmod{19}$

$\Rightarrow \quad 193^{64} \equiv 16 \pmod{19}$

$\equiv -3 \pmod{19}$

$$\therefore \quad (193^{64})^2 \equiv 9 \pmod{19}$$

$$\Rightarrow \quad 193^{128} \equiv 9 \pmod{19}$$

$$\therefore \quad 193^{128} \cdot 193^{16} \equiv 9 \cdot (-2) \pmod{19}$$

$$\equiv -18 \pmod{19}$$

$$193^{144} \equiv 1 \pmod{19}$$

$$\Rightarrow \quad 193^{144} \cdot 193^{16} \equiv 1 \cdot (-2) \pmod{19}$$

$$\therefore \quad 193^{160} \equiv -2 \pmod{19}$$

$$\Rightarrow \quad 193^{183} = 193^{160+16+4+2+1}$$

$$\therefore \quad = 193^{160} \cdot 193^{16} \cdot 193^{4} \cdot 193^{2} \cdot 193$$

$$\equiv (-2) \cdot (-2) \cdot 5 \cdot 9 \cdot 3 \pmod{19}$$

$$\equiv (4 \times 5) \cdot (9 \times 3) \pmod{19}$$

$$\equiv 1 \cdot 8 \pmod{19}$$

$$\equiv 8 \pmod{19}$$

$[\because 4 \times 5 = 20 \equiv 1 \pmod{19}$ and $9 \times 3 = 27 \equiv 8 \pmod{19}]$

$\therefore$ the remainder is 8 when 193^{183} is divided by 19.

EXAMPLE 9

Find the last two digits in the decimal value of 1776^{1776}.

Solution.

The last two digits is the remainder when a number is divided by 100.

$$1776 \equiv 76 \pmod{100}$$

We shall now study the powers of 76.

$$76^2 \equiv 5776 \equiv 76 \pmod{100}$$

$$76^3 \equiv 76 \cdot 76 \equiv 76 \pmod{100}$$

and so on. We find

$$76^n \equiv 76 \pmod{100} \ \forall \ n \geq 1$$

$$1776^n \equiv 76 \pmod{100} \ \forall \ n \geq 1$$

$\therefore$

$$1776^{1776} \equiv 76 \pmod{100}$$

$\Rightarrow$

Hence the last two digits is 76.

Prove that $2^{2^5}+1$ is divisible by 641.

Solution.

We observe that $640 \equiv -1 \pmod{641}$ $[\because 640 = 64 \cdot 10 = 2^6 \cdot 2 \cdot 5]$

$\Rightarrow$ $5 \cdot 2^7 \equiv -1 \pmod{641}$

$\therefore$ $5^4 \cdot (2^7)^4 \equiv (-1)^4 \equiv 1 \pmod{641}$ (1)

But $5^4 = 625 \equiv -16 \pmod{641}$

$= -2^4 \pmod{641}$

$$-2^4 \cdot 2^{28} \equiv 1 \pmod{641}$$

$$-2^{32} \equiv 1 \pmod{641}$$

$$2^{32} \equiv -1 \pmod{641}$$

$$2^{2^5} + 1 \equiv 0 \pmod{641}$$

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

Theorem 4.7

If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $a \equiv b \pmod{m_3}$ … $a \equiv b \pmod{m_r}$. Then $a \equiv b \pmod{[m_1, m_2, \ldots m_r]}$.

Proof:

Given $a \equiv b \pmod{m_i}$, $i = 1, 2, 3, \ldots, r$

Then $m_i \mid a - b$, $i = 1, 2, 3, \ldots, r$

Since $m_1 \mid a - b$, $m_2 \mid a - b$, … $m_r \mid a - b$,

then, their LCM $[m_1, m_2, \ldots m_r] \mid a - b$

$\Rightarrow$ $a \equiv b \pmod{[m_1, m_2, \ldots m_r]}$.

Corollary:

If $a \equiv b \pmod{m_i}$, $i = 1, 2, 3, \ldots, r$ and

$m_1, m_2, \ldots m_r$ are pairwise relatively prime

then $a \equiv b \pmod{m_1, m_2, \ldots m_r}$

Note:

The above result says that congruence of two numbers with different moduli can be combined into a single congruence.

Theorem 4.8:

If ac≡ b c (mod m) and (c, m) = d, then $a \equiv b \left(\bmod \frac{m}{d} \right)$

Proof:

Given ac≡ b c (mod m) and (c, m) = d

$\Rightarrow$ m | ac – b c

$\Rightarrow$ m | c (a – b) and $\left(\frac{c}{d}, \frac{m}{d}\right)$ = 1

$\Rightarrow$ c (a – b) = km ----------(1)

Dividing (1) by d , we get $\frac{c}{d}(a-b) = k\frac{m}{d}$

$Since \ \frac{c}{d} \ and \ \frac{m}{d} \ are \ relatively \ prime, we \ get$

$\frac{m}{d} \ divides \ (a-b)$

$\Rightarrow \quad a \equiv b \left(\bmod \frac{m}{d} \right)$

For Example,

$$14 \equiv 8 \pmod 6$$

$$\Rightarrow \quad 2 \,.\, 7 \equiv 2 \,.\, 4 \pmod 6$$

and $(2 , 6) = 2$

$$\therefore \quad 7 \equiv 4 \left(\mod \frac{6}{2} \right)$$

$$7 \equiv 4 \pmod 3$$

Inverse of a modulo m:

Definition 4.2

When (a, m) = 1, there is unique least residue x such that $ax \equiv 1 \pmod{m}$. Then a is said to be invertible and x is called an inverse of a modulo m, denoted by a^{-1}.

$\therefore \quad a\,a^{-1} \equiv 1 \pmod{m}$

If $a^{-1} = a$, then a is said to be self invertible.

Theorem 4.9:

The unique solution of the linear congruence

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

Proof:

Given the linear congruence

$$ax \equiv b \pmod{m}, \text{ where } (a, m) = 1$$

Since $(a, m) = 1$, then a has inverse a^{-1} modulo m

Multiplying by a^{-1}

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

$$\Rightarrow (a^{-1} a)\, x \equiv a^{-1} b \pmod{m}$$

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

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

$\therefore$the solution is the least residue of $a^{-1} . b \pmod{m}$.

For example,

Since $2 \cdot 3 \equiv 1 \pmod 5$

$\therefore$ 2 is invertible and 3 is the inverse of 2 (mod 5)

i.e., $2^{-1} = 3 \pmod 5$

Since $4 \cdot 4 \equiv \pmod 5$, the inverse of 4 is 4 (mod 5) and so 4 is self reciprocal.

LINEAR CONGRUENCE

Definition 4.3:

A congruence 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**.

Necessary and sufficient condition for a linear congruence to be solvable.

Theorem 4.10:

The linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if $d \mid b$, where $d=(a,m)$.

If $d \mid b$, then it has *d* incongruent solutions.

Proof:

Given the linear congruence

$ax \equiv b \pmod{m}$, where $m \in Z^+$ and $a, b \in Z$.

$ax \equiv b \pmod{m}$ if and only if $m \mid ax - b$ (1)

$\Leftrightarrow$ $ax - b = my$ (by definition of divisibility)

$\Leftrightarrow$ $ax - my = b$ (2)

which is a linear Diophantine equation.

Thus, the linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if the linear Diophantine equation $ax - my = b$ is solvable.

Let $d = (a, m)$.

Then (by theorem 4.1) the linear Diophantine equation is solvable if $d \mid b$.

When $d \mid b$, there are infinitely many solutions, which are given by

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

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

$$x = x_0 + \frac{m}{d}t' \quad and \quad y = y_0 - \frac{a}{d}t', \; where\; t' = -t \in Z$$

Where (x_0, y_0) is a particular solution of (2).

Hence the congruence $ax \equiv b \pmod{m}$ has infinitely many solutions given by where x_0 is a particular solution if the congruence *t* is an arbitrary integer.

When $d \mid b$, we shall now prove that there are only *d* incongruent solutions.

Suppose $x_1 = x_0 + \left(\frac{m}{d}\right)t_1 \quad and \quad x_2 = x_0 + \left(\frac{m}{d}\right)t$

are two solutions of the congruence

Suppose $x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2 \pmod{m}, \ then \left(\frac{m}{d}\right)t_1 \equiv \left(\frac{m}{d}\right)t_2 \pmod{m}$

Since $\frac{m}{d}$ | m, we get $t_1 \equiv t_2 \pmod{d}$ [by theorem 4.6]

Thus x_1 and x_2 are congruent iff $t_1 \equiv t_2 \pmod{d}$.

$\therefore$ x_1 and x_2 are incongruent solutions iff t_1, t_2 belong to different congruence classes mod d.

But we know that there are only *d* congruence classes modulo *d*.

So, the number of incongruent solutions is *d* and they are given by

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

This is the general solution of the congruence.

Corollary :

The linear congruence $ax \equiv b \pmod{m}$ has unique solution if and only if $(a, m)=1$.

Problem 1 :

Determine whether the congruence $12x \equiv 48 \pmod{18}$ is solvable and also find all the solutions if solvable.

Solution:

Given the linear congruence equation

$$12x \equiv 48 \pmod{18} \quad \text{----------(1)}$$

Here $a = 12,\ b = 48,\ m = 18$

$\therefore \quad (a,m) = (12, 18) = 6$

$\therefore \quad d = 6$

Since $6 \mid 48$, we have $d \mid b$

$\therefore$ the equation (1) is solvable

Hence the general solution is $x = x_0 + \frac{m}{d}t, \ \ t \in Z$

We find, when x= 1, 12 = 48 (mod 18)

$\therefore$ x_0 = 1 is particular solution

$\therefore$ x= 1+(18/6)t

The incongruent solutions are

x = 1+ 3t, where 0≤ t <6.

When t= 0,1,2,3,4,5 we get the incongruent solution 1,4,7,10,13 and 16.

Problem 2 :

Determine the number of incongruent solution of $48x \equiv 119 \pmod{91}$.

Solution:

Given the congruence

$48x \equiv 144 \pmod{84}$

Here $a = 48$, $b = 144$, $m = 84$

Now $(a, m) = (48, 84) = 12$

$\therefore d = 12$

Since $12 \mid 144$, $d \mid b$ and show the congruence is solvable.

It has 12 incongruent solution.

SYSTEM OF LINEAR CONGRUENCES

When we consider a set of two or more linear congruences in the same number of variables, we call it a system of linear congruences.

For example,

$x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$ is a system of linear congruences.

Problem 1:

Solve the system of congruences $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$

Solution:

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

We solve this system by iteration. We start with $x \equiv 1 \pmod 3$

Here $a=1$, $b=1$, $m=3$

$\therefore (a, m) = (1, 3) = 1$

$\therefore d=1$ and so $d \mid b$

So, the equation has a solution $x_0=1$

$\therefore$ the general solution is $x = x_0 + \frac{m}{d}t$

$\Rightarrow$ $x= 1+3t_1$, $t_1 \in Z$ (1)

Substituting in (1) in $x \equiv 2(\text{mod}5)$, we get

$\therefore \quad 1 + 3\,t_1 \equiv 2(\text{mod}5)$

$\Rightarrow \quad 3\,t_1 \equiv 1(\text{mod}5)$

We find $t_1 = 2$ is clearly a solution, since $6 \equiv 1(\text{mod}\,5)$

$\therefore \quad t_1 \equiv 2(\text{mod}5)$ is a particular solution

Here $a=1$, $b=2$, $m=5$ and $(a, b) = (1, 2) = 1$.

So, the general solution is

$$t_1 = 2 + 5\,t_2,\ t_2 \in Z$$

$$\therefore \quad x = 1 + 3 + (2 + 5t_2) = 7 + 15\,t_2 \qquad (2)$$

Substituting in (2) $x \equiv 3 \pmod 7$, we get

$\therefore \quad 7 + 15\, t_2 \equiv 3 \pmod 7$

$\Rightarrow \quad 15\, t_2 \equiv -4 \pmod 7$

$\Rightarrow \quad 15\, t_2 \equiv 3 \pmod 7 \quad [\because -4 \equiv 3 \bmod 7]$

We find $t_2 = 3$ is a solution, since $45 \equiv 3 \pmod 7$

$\therefore \quad t_2 = 3 \pmod 7$ is a particular solution

Here $a=15, b=3, \ m=7$ and $(a, m) = (15, 7) = 1$

$\therefore \quad t_2 = 3 + 7t, t \in Z$

$\therefore \quad x = 7 + 15\,(3 + 7t) = 52 + 105t, t \in Z$

$\therefore$ the general solution of the system is $x = 52 + 105t, t \in Z$

Theorem 4.11 Chinese Remainder Theorem

The system of linear congruences $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$,… $x \equiv a_k \pmod{m_k}$, where $m_1, m_2, \ldots m_k$ are pair wise relatively prime positive integers and $a_1, a_2, \ldots a_k$ are given integers, has unique solution modulo

$m_1 . m_2 . m_3 . \ldots . m_k$..

Working Rule:

Let $n = m_1 m_2 \ldots m_k$ and $n_i = n / m_i$

Step 1: Find the solutions $y_1, y_2, \ldots y_k$, where

$n_i y_i \equiv 1 \pmod{m_i}$, $i = 1, 2, \ldots k$,

Step 2: $x = a_1 n_1 y_1 + a_2 n_2 y_2 + \ldots + a_k n_k y_k$ is the solution $\pmod{n}$

Problem 2:

Solve the system $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, $x \equiv 3 \pmod 5$.

Solution:

Given system is $x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 4$

$x \equiv 3 \pmod 5$

Here $a_1 = 1$, $a_2 = 2$, $a_3 = 3$

$m_1 = 3$, $m_2 = 4$, $m_3 = 5$

We find m_1, m_2, m_3 are pairwise relatively prime

Let $n = m_1\, m_2\, m_3 = 3 \cdot 4 \cdot 5 = 60$

$$n_1 = \frac{n}{m_1} = \frac{3.4.5}{3} = 20$$

$$n_2 = \frac{n}{m_2} = \frac{3.4.5}{4} = 15$$

and

$$n_3 = \frac{n}{m_3} = \frac{3.4.5}{5} = 12$$

1. We find y_1, y_2, y_3 from the congruences

$$n_1 y_1 \equiv 1 (\text{mod } m1)$$

$$n_2 y_2 \equiv 1 (\text{mod } m2)$$

$$n_3 y_3 \equiv 1 (\text{mod } m3)$$

We have $n_1 y_1 \equiv 1 (\text{mod } m1)$

$\Rightarrow$ $20 y_1 \equiv 1 (\text{mod } 3)$ $[\because n_1 = 0, \quad m_1 = 8]$

Since $20 \,.\, 2 \equiv 40 \equiv 1 (\text{mod } 3)$, we see $y_1 = 2$ is a solution

We have $n_2 y_2 \equiv 1 (\text{mod } m_2)$

$\Rightarrow$ $15 y_2 \equiv 1 (\text{mod } 4)$

Since $15 \,.\, 3 \equiv 1 (\text{mod } 4)$, we see $y_2 = 3$ is a solution

We have $n_3 y_3 \equiv 1 (\text{mod } m3)$

$\Rightarrow$ $12 y_3 \equiv 1 (\text{mod } 5)$

Since $12 \,.\, 3 \equiv 36 \equiv 1 (\text{mod } 5)$, we see $y_3 = 3$ is a solution

Then solution is $x \equiv a_1n_1y_1 + a_2n_2y_2 + a_3n_3y_3 \pmod{n}$

$\therefore \quad x \equiv 1 \,.\, 20 \,.\, 2 + 2 \,.\, 15 \,.\, 3 + 3 \,.\, 12 \,.\, 3 \pmod{60}$

$\Rightarrow \quad x \equiv 40 + 90 + 72 \pmod{60}$

$\Rightarrow \quad x \equiv 238 \pmod{60}$

$\Rightarrow \quad x \equiv 58 \pmod{60}$

$$
\begin{array}{r|l}
 & 3 \\
\hline
60 & 238 \\
 & 180 \\
\hline
 & 58
\end{array}
$$

$\therefore$ 58 is the unique solution (mod 60).

$\therefore$ The solution of the system is $x \equiv 58 \pmod{60}$ and it is the unique solution.

Problem 3:

Solve the linear system $x \equiv 3 (\mod 7)$, $x \equiv 4 (\mod 9)$, $x \equiv 8 (\mod 11)$

Solution:

Given linear system is $x \equiv 3 (\mod 7)$, $x \equiv 4 (\mod 9)$, $x \equiv 8 (\mod 11)$

Here $a_1 = 3$, $a_2 = 4$, $a_3 = 8$

and $m_1 = 7$, $m_2 = 9$, $m_3 = 11$

We find m_1, m_2, m_3 are pair wise relatively prime

Let $n = m_1 m_2 m_3 = 7 . 9 . 11 = 693$

$$n_1 = \frac{n}{m_1} = \frac{7.9.11}{7} = 99$$

$$n_2 = \frac{n}{m_2} = \frac{7.9.11}{9} = 77$$

and

$$n_3 = \frac{n}{m_3} = \frac{7.9.11}{11} = 63$$

1. We find y_1, y_2, y_3 from the congruences

$n_1y_1 \equiv 1 \pmod{m1}$

$n_2y_2 \equiv 1 \pmod{m2}$

$n_3y_3 \equiv 1 \pmod{m3}$

We have $n_1y_1 \equiv 1 \pmod{m1}$

$\Rightarrow$ $99y_1 \equiv 1 \pmod{7}$

We know $99 \cdot 1 = 99 \equiv 1 \pmod{7}$.

$\therefore$ $y_1 = 1$ is a solution

We have $n_2y_2 \equiv 1 \pmod{m_2}$

$\Rightarrow$ $77y_2 \equiv 1 \pmod{9}$

We know $77 \cdot 2 = 154 \equiv 1 \pmod{9}$

$$\begin{array}{r} 14 \\ 7\overline{)\,99} \\ 7 \\ \hline 29 \\ 28 \\ \hline 1 \end{array} \qquad \begin{array}{r} 17 \\ 9\overline{)\,154} \\ 9 \\ \hline 64 \\ 63 \\ \hline 1 \end{array} \qquad \begin{array}{r} 40 \\ 11\overline{)\,441} \\ 440 \\ \hline 1 \end{array}$$

$\therefore \quad y_2 = 2$ is a solution

We have $n_3 y_3 \equiv 1 (\text{mod } m_3)$

$\Rightarrow \quad 63 y_3 \equiv 1 (\text{mod } 11)$

We know $63 \cdot 7 = 441 \equiv 1 (\text{mod } 11)$

$\therefore \quad y_3 = 7$ is a solution

2. Then Solution is $x \equiv a_1 n_1 y_1 + a_2 n_2 y_2 + a_3 n_3 y_3 \pmod{n}$

$\therefore \quad x \equiv 3 \cdot 99 \cdot 1 + 4 \cdot 77 \cdot 2 + 8 \cdot 63 \cdot 7 \pmod{693}$

$\Rightarrow \quad x \equiv 297 + 616 + 3528 \pmod{693}$

$\Rightarrow \quad x \equiv 4441 \pmod{693}$

$\Rightarrow \quad x \equiv 283 \pmod{493}$

$\therefore$ 283 is the unique solution (mod 493)

Problem 4:

Sun – Tsu's puzzle given in the introduction page 4.26 can be translated as a system of congruences. If x is the number of things then

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

Solution:

Given linear system is $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

Here $a_1 = 2$, $a_2 = 3$, $a_3 = 2$

$m_1 = 3$ $m_2 = 5$ $m_3 = 7$

We find m_1, m_2, m_3 are pair wise relatively prime

Let $n = m_1 m_2 m_3 = 3 . 5 . 7 = 105$

$$n_1 = \frac{n}{m_1} = \frac{3.5.7}{3} = 35$$

$$n_2 = \frac{n}{m_2} = \frac{3.5.7}{5} = 21$$

and

$$n_3 = \frac{n}{m_3} = \frac{3.5.7}{7} = 15$$

1. We find y_1, y_2, y_3 from the congruences

$$n_1y_1 \equiv 1 \pmod{m_1}$$

$$n_2y_2 \equiv 1 \pmod{m_2}$$

$$n_3y_3 \equiv 1 \pmod{m_3}$$

We have $n_1y_1 \equiv 1 \pmod{m_1}$

$\Rightarrow$ $35y_1 \equiv 1 \pmod 3$

Since $35 \cdot 2 = 70 \equiv 1 \pmod 3$, we see $y_1 = 2$ is the solution

We have $n_2y_2 \equiv 1 \pmod{m2}$

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

Since $21 \cdot 1 = 21 \equiv 1 \pmod 5$ we see $y_2 = 1$ is the solution

We have $n_3y_3 \equiv 1 (\text{mod } m3)$

$\Rightarrow \quad 15y_3 \equiv 1 (\text{mod } 7)$

Since $15 . 1 = 15 \equiv 1 (\text{mod } 7)$ we see $y_3 = 1$ is the solution

2. Then solution is $x \equiv a_1n_1y_1 + a_2n_2y_2 + a_3n_3y_3 \ (\text{mod } n)$ is the solution

$\therefore \quad x \equiv 2 . 35 . 2 + 3 . 21 . 1 + 2 . 15 . 1 \ (\text{mod } 105)$

$\Rightarrow \quad x \equiv 140 + 63 + 30 \ (\text{mod } 105)$

$\Rightarrow \quad x \equiv 233 \ (\text{mod } 105)$

$\Rightarrow \quad x \equiv 23 \ (\text{mod } 105)$

$\therefore$ 23 is the smallest number satisfying the system.

Classical Theorems
&
Multiplicative Functions

- ***Wilson's Theorem***
- ***Fermat's Little Theorem***
- ***Euler's Theorem***

Theorem 5.1 Wilson's theorem

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof :

We have to prove $(p-1)! \equiv -1 \pmod{p}$

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

So, the theorem is true when p = 2.

Now let $p > 2$ and let a be a positive integer such that $1 \leq a \leq p-1$.

Since p is a prime and $a < p$, $(a, p) = 1$

Then the congruence $ax \equiv 1 \pmod{p}$ has a solution a' congruence modulo p.

$\therefore$ $aa' \equiv 1 \pmod{p}$, where $1 \leq a' \leq p-1$

$\therefore$ a, a' are inverses of each other modulo p.

If a'=a then $a \cdot a \equiv 1 \pmod{p}$

$\Rightarrow a^2 - 1 \equiv 0 \pmod{p}$

$\therefore$ $p \mid a^2 - 1 \Rightarrow p \mid (a-1)(a+1) \Rightarrow p \mid a-1$ or $p \mid a+1$

Since $a < p$, if $p \mid a+1$ then $a = p-1$

If $p \mid a-1$, then $a - 1 = 0 \Rightarrow a = 1$

$\therefore \quad a = 1$ or $p - 1$ if $a = a'$

ie., 1 and $p - 1$ are their own inverses.

If $a' \neq a$, excluding, 1 and $p - 1$, the remaining $p - 3$ residues $2, 3, 4 \ldots, (p - 3), (p - 2)$ can be grouped into $(p - 3) / 2$ pairs of the type a, a' such that $aa' \equiv 1 \pmod{p}$

Multiplying all these pairs together we get

$$2 . 3 . 4 \ldots (p - 3)(p - 2) \equiv 1 \pmod{p}$$

$$\Rightarrow \quad 1 . 2 . 3 . 4 \ldots (p - 2)(p - 1) \equiv p - 1 \pmod{p}$$

$$\Rightarrow \quad (p - 1)! \equiv -1 \pmod{p} \qquad (\because p - 1 \equiv -1 \pmod{p})$$

This can be rewritten as $(p - 1)! + 1 \equiv 0 \pmod{p}$

$$\Rightarrow \quad p \mid (p - 1)! + 1,$$

Which is the result suggested by Wilson.

Problem 1 :

Show that $18! + 1$ is divisible by 437

Solution:

Wilson's theorem is $(p - 1)! + 1$ is divisible by a prime p.

Here 437 is not a prime

$437 = 19.23$, where 19 and 23 are primes.

Since 19 is a prime $(19 - 1)! + 1 = 18! + 1$ is divisible by 19

$\Rightarrow$ $18! + 1 \equiv 0 \pmod{19}$

Since 23 is a prime $(23 - 1)! + 1 = 22! + 1$ is divisible by 23.

$\Rightarrow$ $22! + 1 \equiv 0 \pmod{23}$

$\Rightarrow$ $22.21.20.19.18! + 1 \equiv 0 \pmod{23}$

But $22 \equiv -1 \pmod{23}, \quad 21 \equiv -2 \pmod{23}$

$20 \equiv -3 \pmod{23}, 19 \equiv -4 \pmod{23}$

$\therefore \quad 22.21.20.19 \equiv (-1)(-2)(-3)(-4) \pmod{23}$

$\equiv 24 \pmod{23}$

$\equiv 1 \pmod{23}$

Multiplying by 18!, we get

$$22.21.20.19.18! \equiv 18! \pmod{23}$$

$$\Rightarrow \quad 22.21.20.19.18! + 1 \equiv 18! + 1 \pmod{23}$$

But LHS is $22! + 1 \equiv 0 \pmod{23}$

Hence $18! + 1 \equiv 0 \pmod{23}$

$\therefore$ $18! + 1$ is divisible by 19 and 23

$\Rightarrow$ $18! + 1$ is divisible by lcm $[19, 23] = 19 \cdot 23 = 437$

$\Rightarrow$ $18! + 1 \equiv 0 \pmod{437}$

Problem 2 :

If p is a prime number of the form $4m + 1$, where m is a positive integer, prove that $(2m!)^2 + 1 \equiv 0 \pmod{p}$.

Solution:

Given the prime number p is of the form $4m + 1$, where m is a positive integer

To prove $(2m!)^2 + 1 \equiv 0 \pmod{p}$.

Since $p = 4m + 1$ is a prime, Wilson's theorem

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

$$\Rightarrow (p - 1)! + 1 \equiv 0 \pmod{p}$$

$$\Rightarrow (4m + 1 - 1)! + 1 \equiv 0 \pmod{p}$$

$$\Rightarrow 4m! + 1 \equiv 0 \pmod{p} \qquad (1)$$

$$\Rightarrow 4m(4m - 1)(4m - 2) \ldots (4m - (2m - 1)) \cdot 2m! + 1 \equiv 0 \pmod{p} \qquad (1)$$

But

$$4m + 1 = p$$

$$4m = p - 1 \equiv -1 \pmod{p}$$

$$4m - 1 = p - 2 \equiv (-2) \pmod{p}$$

$$4m - 2 = p - 3 \equiv (-3) \pmod{p}$$

$$4m - (2m - 1) = p - 2m \equiv -2m \pmod{p}$$

Multiplying together we get

$$4m(4m - 1)(4m - 2)\ldots(4m - (2m - 1))$$

$$\equiv (-1)(-2)(-3)\ldots(-2m) \pmod{p}$$

$$\equiv 2m! \pmod{p}$$

Multiplying both sides by $(2m)!$ we get

$$4m(4m-1)(4m-2)\ldots(4m-(2m-1))(2m!)$$

$$\equiv (2m!)(2m!) \pmod{p}$$

$$\Rightarrow \quad 4m! \equiv (2m!)^2 \pmod{p}$$

$$\Rightarrow \quad 4m!+1 \equiv (2m!)^2+1 \pmod{p} \quad [\text{using } (1)]$$

$$\Rightarrow \quad 0 \equiv (2m!)^2+1 \pmod{p}$$

$$\therefore \quad (2m!)^2+1 \equiv 0 \pmod{p}$$

Problem 3 :

If n is a positive integer such that $(n-1)! \equiv -1 \pmod{n}$, then prove that n is a prime.

Solution :

Given n is a positive integer such that

$$(n-1)! \equiv -1 \pmod{n} \Rightarrow (n-1)! \equiv 0 \pmod{n} \qquad (1)$$

To prove n is a prime.

Suppose n is not a prime, then n is a composite number.

$\therefore$ $n = a\,b$, where a, b are integers between 1 and n

ie., $1 < a, b < n$.

Since $a \mid ab$, $a \mid n$ by (1)

$$n \mid [(n-1)! + 1]$$

$\therefore$ $$a \mid [(n-1)! + 1]$$

But $1 < a < n$, so, a is one of the integers $2, 3, 4, \ldots, (n-1)$

$\therefore$ a divides the product $2 \cdot 3 \cdot 4 \ldots (n-1) = (n-1)!$

Thus, $a \mid [(n-1)! + 1]$ and $a \mid (n-1)!$

$\Rightarrow$ $$a \mid [(n-1)! + 1 - (n-1)!] \Rightarrow a \mid 1$$

Which is a contradiction, since $1 < a$.

$\therefore$ Our assumption n is composite is wrong

Hence n is a prime.

Problem 6:

If $x = 1 . 3 . 5 \ldots (p-2)$, where p is an odd prime, show that $x^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$

Solution :

Given $x = 1 . 3 . 5 \ldots (p-2)$, where p is an odd prime.

Since p is a prime, by Wilson's theorem

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

$$\Rightarrow \quad 1 . 2 . 3 . 4 . 5 \ldots (p-2)(p-1) \equiv -1 \pmod{p}$$

$$\Rightarrow \quad (1 . 3 . 5 \ldots (p-2))(2 . 4 . 6 \ldots (p-1)) \equiv -1 \pmod{p}$$

$$\Rightarrow \quad x(2 . 4 . 6 \ldots (p-1)) \equiv -1 \pmod{p}$$

$$\Rightarrow \quad x[p-(p-2)]\,[p-(p-4)]\ldots(p-1) \equiv -1 \pmod{p} \qquad (1)$$

Now

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

$$p-(p-4) \equiv -(p-4) \pmod{p}$$

$$\vdots$$

$$p-3 \equiv -3 \pmod{p}$$

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

The number of equations is $\frac{p-1}{2}$

Multiplying together, we get

$$[p-(p-2)]\,[p-(p-4)]\ldots(p-3)\,(p-1)$$

$$\equiv (-1)^{\frac{p-1}{2}} \cdot (p-2)\,(p-4)\ldots 3 \,.\, 1 (\text{mod } p)$$

$$= (-1)^{\frac{p-1}{2}} \,.\, x \,.\, (\text{mod } p)$$

Substitute in (1) *we get*

$$x \,.\, x(-1)^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$$

$$\Rightarrow \qquad x^2 \equiv (-1)^{\frac{p-1}{2}+1} \pmod{p}$$

Theorem 5. 2 Fermat's Little Theorem

If p is a prime and a is any integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof:

Given p is a prime and a is any integer not divisible by p, ie., $p \nmid a$.

When an integer is divided by p, the set of possible remainders are $0, 1, 2, 3, \ldots, p-1$.

Consider the set of integers

$$1 . a, 2 . a, 3 . a, \ldots . (p-1) a$$

Suppose $ia \equiv 0 \pmod{p}$, then $p \mid ia$.

But $p \nmid a$ $\therefore$ $p \mid i$, which is impossible, since $i < p$.

$\therefore$ $ia \not\equiv 0 \pmod{p}$ for $i = 1,2,\ldots,p-1$.

So, no term of (1) is zero.

Next we prove they are all distinct

Suppose $ia \equiv ja \pmod{p}$, where $1 \leq i, \quad j \leq p-1$.

$\therefore \quad i - j = 0 \Rightarrow i \equiv j \pmod{p}$

$\therefore \quad i \neq j \Rightarrow ia \neq ja$.

This means, no two of the integers in (1) are congruent modulo p.

$\therefore$ The least residues (or remainders) of the integers a, 2a, 3a, …., (p – 1) a modulo p are the same as integers 1, 2, 3, …., p -1 in some order.

So, their products congruent modulo p.

$$\therefore \quad a \cdot 2a \cdot 3a \cdot \ldots (p-1)\, a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod{p}$$

$$\Rightarrow \quad 1 \cdot 2 \cdot 3 \ldots (p-1) \cdot a^{p-1} \equiv (p-1)! \pmod{p}$$

$$\Rightarrow \quad (p-1)!\, a^{p+1} \equiv (p-1)! \pmod{p}$$

$$\Rightarrow \quad a^{p-1} \equiv 1 \pmod{p} \qquad (\because p \nmid (p-1))$$

Problem 1:

Find the remainder when 193^{183} is divided by 19.

Solution:

We have to find the remainder when 193^{183} is divided by 19.

19 is a prime and $19 \nmid 193$.

$\therefore$ by Fermat's little theorem

$$193^{19-1} \equiv 1 \pmod{19}$$

$$\Rightarrow \quad 193^{18} \equiv 1 \pmod{19}$$

$$\therefore \quad (193^{18})^{10} \equiv 1^{10} \pmod{19}$$

$$\Rightarrow \quad 193^{180} \equiv 1 \pmod{19}$$

Now $193^{183} = 193^{180+2+1}$

$$= 193^{180} \cdot 193^{2} \cdot 193$$

$$\begin{array}{r} 10 \\ 18\overline{)\,183} \\ 18 \\ \hline 3 \end{array} \qquad \begin{array}{r} 10 \\ 19\overline{)\,193} \\ 190 \\ \hline 3 \end{array}$$

But $193 \equiv 3 \pmod{19}$

$\therefore$ $1932 \equiv 32 \pmod{19} \Rightarrow 1932 \equiv 9 \pmod{19}$

$\therefore$ $193^{183} \equiv 1 \cdot 9 \cdot 3 \pmod{19}$

$\equiv 27 \pmod{19}$

$\equiv 8 \pmod{19}$

$\therefore$ The remainder is 8, When 193^{183} is divided by 19.

$$
\begin{array}{r}
1 \\
19 \overline{)\,27} \\
19 \\
\hline
8
\end{array}
$$

5.3 EULER'S THEOREM

Fermats theorem is $a^{p-1} \equiv 1 (\text{mod } p)$, which is of the form $a^{f(p)} \equiv 1 (\text{mod } p)$, where p is a prime.

It is natural to extend to the form $a^{f(m)} \equiv 1 (\text{mod } m)$, where m is not a prime and $(a, m) = 1$.

Definition 5.1 Arithmetical Function or Number Theoretic Function.

A real (or complex) valued function defined on the set of positive integers N is called an **arithmetical function** or **number theoretic function**.

We shall now define a special number theoretic function called **Euler's Phi function** or **Euler totient function** ϕ, named after one of the all time **great mathematicians Euler**.

Definition 5.2 Let $\phi : N \to N$ be a function defined by $\phi(1) = 1$ and for $n > 1$.

$\phi(n)$ = the number of positive integers $\leq n$ and relatively prime to n.

This function is called **Euler's ϕ-function.**

$\phi(2) = 1$, since 1 is the only integer ≤ 2 and prime to it.

$\phi(3) = 2$, since 1, 2 are the only integers ≤ 3 and prime to 3.

$\phi(4) = 2$, since 1, 3 are the integers ≤ 4 and prime to it.

$\phi(5) = 4$, since 1, 2, 3, 4 are the integers ≤ 5 and prime to 5.

$\phi(6) = 2$, since 1, 5 are the integers ≤ 6 and prime to 6.

$\phi(7) = 6$, since 1, 2, 3, 4, 5, 6 are the integers ≤ 7 and prime to 7.

Note that $\phi(5) = 5 - 1 = 4$

$\phi(7) = 7 - 1 = 6$

It is true for any prime p, since $1, 2, 3, \ldots, p - 1$ are the positive integers $\leq p$ and prime to p.

$\therefore \quad \phi(p) = p - 1.$

Theorem 5.4 Euler's theorem

Let m be a positive integer and a be any integer such that $(a, m) = 1$.

Then $$a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m).$$

Definition 5.3 Multiplicative function.

A number theoretic function f is **multiplicative** if f is not identically zero and if $f(mn) = f(m)\,f(n)$ whenever $(m, n) = 1$.

A multiplicative function is called **completely multiplicative** if we also have

$$f(mn) = f(m)f(n) \qquad \text{for all } m, n \in \mathrm{N}.$$

Theorem 5.5 Let f be a multiplicative function and n be a positive integer with canonical decomposition $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

Then
$$f(n) = f\left(p_1^{\alpha_1}\right) \cdot f\left(p_2^{\alpha_2}\right) \cdots f\left(p_k^{\alpha_k}\right).$$

Theorem 5.7 **Let p be a prime and α is a positive integer.**

Then $$\phi\left(p^{\alpha}\right) = p^{\alpha} - p^{\alpha-1} = p^{\alpha}\left(1-\frac{1}{p}\right).$$ **[AU 2018]**

Proof $\phi\left(p^{\alpha}\right)$ = number of positive integers $\leq p^{\alpha}$ and relatively prime to it

= number of positive integers $\leq p^{\alpha}$

– number of positive integers $\leq p^{\alpha}$ and not relatively prime to it.

The number of positive integers $\leq p^{\alpha}$ is p^{α} (because they are 1, 2, 3, …, p^{α})

The number of positive integers $\leq p^{\alpha}$ and not prime to it are the various multiples of p.

They are $1p, 2p, 3p, \ldots, p^{\alpha-1}\,p$

$\therefore$ The number of such numbers $= p^{\alpha-1}$.

Hence $$\phi\left(p^{\alpha}\right) = p^{\alpha} - p^{\alpha-1} = p^{\alpha}\left(1-\frac{1}{p}\right)$$ ■

Theorem 5.8 **Let $n = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ be the canonical decomposition of the positive integer n.**

Then $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)$.

Compute $\phi(6860)$.

Solution.

We have $6860 = 2^2 \cdot 5 \cdot 7^3$

$\therefore$ $\phi(6860) = \phi(2^2) \cdot \phi(5) \cdot \phi(7^3)$

$$= 2^2\left(1-\frac{1}{2}\right)\cdot(4)\cdot 7^3\left(1-\frac{1}{7}\right)$$

$$= 2 \cdot 4 \cdot 7^2 \cdot 6$$

$$= 2352$$

2	6860
2	3430
5	1715
7	343
7	49
	7

Find the positive integers n such that $\phi(n) = 6$.

Solution.

Given $\phi(n) = 6$

We have to find possible n by trial and error

$$\phi(6) = \phi(2 \cdot 3) = \phi(2) \cdot \phi(3) = 1 \cdot 2 = 2 \neq 6$$

$$\phi(7) = 7 - 1 = 6. \qquad \therefore \ n = 7$$

$$\phi(8) = \phi\left(2^3\right) = 2^3\left(1 - \frac{1}{2}\right) = 4 \neq 6$$

$$\phi(9) = \phi\left(3^2\right) = 3^2\left(1 - \frac{1}{3}\right) = 6 \qquad \therefore \ n = 9$$

$$\phi(10) = \phi(2 \cdot 5) = \phi(2) \cdot \phi(15) = 1.4 \neq 6$$

$$\phi(11) = 10 \neq 6$$

$$\phi(12) = \phi\left(2^2 \cdot 3\right) = \phi\left(2^2\right) \cdot \phi(3) = 2^2\left(1 - \frac{1}{2}\right) \cdot 2 = 4 \neq 6$$

$$\phi(13) = 12 \neq 6$$

$$\phi(14) = \phi(2 \cdot 7) = \phi(2) \cdot \phi(7) = 1 \cdot 6 = 6 \qquad \therefore n = 14$$

$$\phi(15) = \phi(3 \cdot 5) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8 \neq 6$$

$$\phi(16) = \phi(2^4) = 2^4\left(1 - \frac{1}{2}\right) = 8 \neq 6$$

$$\phi(17) = 16$$

$$\phi(18) = \phi\left(3^2 \cdot 2\right) = \phi\left(3^2\right) \cdot \phi(2)$$

$$= 3^2\left(1 - \frac{1}{3}\right) \cdot 1 = 3 \cdot 2 = 6 \qquad \therefore n = 18$$

the only possible values of n are 7, 9, 14, 18.

Show that $\phi(n) = \frac{n}{2}$ if $n = 2^k$.

Solution.

Given $n = 2^k$

$\therefore$

$$\phi(n) = \phi(2^k) = 2^k\left(1 - \frac{1}{2}\right)$$

$$= 2^k \cdot \frac{1}{2} = \frac{n}{2}$$

Using Eulers theorem find the remainder when 245^{1040} is divided by 18.

Solution.

We have to find the remainder when 245^{1040} is divided by 18.

Here $a = 245 = 5 \cdot 7^2$ and $m = 18 = 3^2 \cdot 2$

$\therefore$ $(a, m) = 1$

Hence by Euler's theorem,

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

$\Rightarrow$ $$245^{\phi(18)} \equiv 1 \pmod{18}$$

But $$\phi(18) \equiv \phi(3^2 \cdot 2) = \phi(3^2) \cdot \phi(2)$$

$$= 3^2\left(1 - \frac{1}{3}\right) \cdot 1 = 6$$

Using Eulers theorem find the remainder when 245^{1040} is divided by 18.

Solution.

We have to find the remainder when 245^{1040} is divided by 18.

Here $a = 245 = 5 \cdot 7^2$ and $m = 18 = 3^2 \cdot 2$

$\therefore$ $(a, m) = 1$

Hence by Euler's theorem,

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

$\Rightarrow$ $$245^{\phi(18)} \equiv 1 \pmod{18}$$

But $$\phi(18) \equiv \phi(3^2 \cdot 2) = \phi(3^2) \cdot \phi(2)$$

$$= 3^2\left(1 - \frac{1}{3}\right) \cdot 1 = 6$$

$\therefore$ By Eulers theorem

$$73^{40} \equiv 1 \pmod{100}$$

$\therefore$ $$(73^{40})^{49} \equiv 1^{49} \pmod{100}$$

$\Rightarrow$ $$73^{1960} \equiv 1 \pmod{100}$$

$\Rightarrow$ $$73^{1960} \cdot 73 \equiv 73 \pmod{100}$$

$\Rightarrow$ $$73^{1961} \equiv 73 \pmod{100}$$

$\Rightarrow$ $$273^{1961} \equiv 73 \pmod{100}$$

Hence the remainder is 73, when 273^{1961} is divided by 100.

$$
\begin{array}{r}
49 \\
40\overline{)\,1961} \\
160 \\
\hline
361 \\
360 \\
\hline
1 \\
\hline
\end{array}
$$

Verify the theorem $\sum_{d|n} \phi(d) = n$ for $n = 28$.

Solution.

Given $n = 28$

The positive divisors of 28 are 1, 2, 4, 7, 14, 28

$$\therefore \quad \sum_{d|n} \phi(d) = \phi(1) + \phi(2) + \phi(4) + \phi(7) + \phi(14) + \phi(28)$$

But

$$\phi(1) = 1, \qquad \phi(2) = 1,$$

$$\phi(4) = \phi(2^2) = 2^2\left(1 - \frac{1}{2}\right) = 2$$

$$\phi(7) = 7 - 1 = 6,$$

$$\phi(14) = \phi(2 \cdot 7) = \phi(2) \cdot \phi(7) = 1 \cdot 6 = 6$$

$$\phi(28) = \phi(2^2 \cdot 7) = \phi(2^2) \cdot \phi(7)$$

$$= 2^2\left(1 - \frac{1}{2}\right) \cdot 6 = 2 \cdot 6 = 12$$

$$\therefore \quad \sum_{d|n} \phi(d) = 1 + 1 + 2 + 6 + 6 + 12$$

$$= 28$$

Part A
Q & A

1. Compute the remainder when 3^{302} is divided by 5.

Ans. We have $3^4 = 81 \equiv 1 \pmod 5$

$$\therefore \quad (3^4)^{75} \equiv 1^{75} \pmod 5$$

$$\Rightarrow \quad 3^{300} = 1 \pmod 5$$

$$3^{302} = 3^{300+2} = 3^{300} \cdot 3^2$$

But $3^2 = 9 \equiv 4 \pmod 5$

$$\therefore \quad 3^{302} \equiv 1 \cdot 4 \pmod 5$$

$$\equiv 4 \pmod 5$$

So, the remainder is 4.

$$
\begin{array}{r}
75 \\
4\overline{)\,302} \\
28 \\
\hline
22 \\
20 \\
\hline
2 \\
\hline
\end{array}
$$

2. Find the remainder when 100! Is divided by 101. **[AU 2013, 2017]**

Ans. We know 101 is a prime.

$\therefore$ by Wilson's theorem

$$(101 - 1)! \equiv -1 \pmod{101}$$

$$\Rightarrow \quad 100! \equiv 100 \pmod{101} \qquad [\because -1 \equiv 100 \pmod{101}]$$

$\therefore$ the remainder is 100.

3. Find the remainder when 18! Is divided by 19.

Ans. We know 19 is a prime.

$\therefore$ by Wilson's theorem

$$(19-1)! \equiv -1 \pmod{19}$$

$\Rightarrow$

$$18! \equiv -1 \pmod{19}$$

$$\equiv 18 \pmod{19}$$

$\therefore$ The remainder is 18.

1. Find the remainder when 3^{247} is divided by 17 using Fermat's little theorem.

2. Compute the remainder. When 3^{247} is divided by 25 using Euler's theorem.


Thank
You