Unit-V

Elementary Number Theory and Cryptography

Divisibility

If a and b are integers such that $b \neq 0$, then we say that "b divides a" if there exists an integer k such that $a = kb$. And it is written as $b|a$.

Note: If b divides a, then we say that "b is a factor of a" or "a multiple of b"

Division Algorithm

If a and b are integers such that $b > 0$, then there exists unique integers q and r such that

$$a = bq + r, \text{ where } 0 \leq r < b$$

Note: q is called quotient and r is called remainder.

Congruence Relation

Let m be a positive integer. Then ~~two~~ an integer 'a' is said to be congruent to an integer b modulo m if "m divides $a-b$". Symbolically it is written as

$$a \equiv b \pmod{m} \text{ or } a \equiv b \text{ (modulo } m)$$

It is read as "'a' is congruent to 'b' modulo m".

Here m is called the modulus, and b is called residue of $a \pmod{m}$.

Note: If $a \equiv b \pmod{m}$, then $m|(a-b) \Rightarrow a-b = mk$
$\Rightarrow \boxed{a = mk + b.}$

Meaning: when a is divided by m remainder is b.

Properties of Congruence

1. $a \equiv b \pmod{m}$ if $m | a-b$.
2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
3. $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

Modular Arithmetic operations

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

1. $a+k \equiv b+k \pmod{m}$, $\forall\, k \in \mathbb{Z}$
2. $a-k \equiv b-k \pmod{m}$, $\forall\, k \in \mathbb{Z}$
3. $ak \equiv bk \pmod{m}$, $\forall\, k \in \mathbb{Z}$
4. $a^k \equiv b^k \pmod{m}$, $\forall\, k \in \mathbb{Z}$

For example

Modular addition and multiplication modulo 8 table is as follows:

Addition modulo 8

+	0	1	2	3	4	5	6	7
0	$\boxed{0}$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Multiplication modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Properties of Modular Arithmetic

1) Residue classes

Define the set $\mathbb{Z}_n$ as set of non-negative integers less than n

$$\mathbb{Z}_n = \{0, 1, 2, \dots (n-1)\}$$

This refered as the set of residues or residue classes (mod n).

To be more precise, each integer in $\mathbb{Z}_n$ represents a residue class. We denote the residue classes (mod n) as $[0], [1], [2] \dots [n-1]$,

where $[r] = \{a : a \in \mathbb{Z}, a \equiv r \pmod{n}\}$

For example:

The residue classes (mod 4) are

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$\therefore [0] = \{\dots -16, -12, -8, -4, 0, 4, 8, 12, 16 \dots\}$

$[1] = \{\dots -15, -11, -7, -3, 1, 5, 9, 13, 17, \dots\}$

$[2] = \{\dots -14, -10, -6, -2, 2, 6, 10, 14, 18 \dots\}$

$[3] = \{\dots -13, -9, -5, -1, 3, 7, 11, 15, 19 \dots\}$

Prime Numbers

Defn: An integer $P \geq 2$ is called prime number if it is divisible by 1 and itself. Otherwise a number is called compositile number.

For examples:

1) Prime numbers are: 2, 3, 5, 7, 11, 13, 17, 19, 23 ....
2) Composite numbers are: 4, 6, 8, 9, 10, 12 ...

Prime Factorization

Prime factorization of any composite number 'n', is expressing it as a product of prime numbers.

$$\therefore \; n = P_1 \cdot P_2 \cdot P_3 \cdots P_n$$

where $P_1, P_2, P_3 \ldots P_n$ are prime numbers

For example:
1) $20 = 5 \times 2 \times 2$
2) $50 = 5 \times 5 \times 2$
3) $100 = 5 \times 5 \times 2 \times 2$
4) $143 = 11 \times 13$

Relatively Prime numbers or Co-prime numbers

Defn: Two numbers are said to be relatively prime if they have no common divisors other than 1.

OR

Two numbers a and b are said to be relatively prime if GCD of a and b is 1.

i.e ~~Gta,b~~ $GCD(a,b) = 1$ or simply $(a,b) = 1$

For example:
1) 10 and 21 are relatively prime as $GCD(10, 21) = 1$
2) 15 and 17 are relatively prime as $GCD(15, 17) = 1$

Note: Every prime number is relatively prime to non-zero positive integers less than that prime.

For example: 5 is relatively prime to 1, 2, 3, 4

Theorem: Let m be the positive integer and $a \equiv b \pmod m$ and $c \equiv d \pmod m$. Then prove that $a+c \equiv b+d \pmod m$ and $ac \equiv bd \pmod m$.

Proof: Given that

$a \equiv b \pmod m$ and $c \equiv d \pmod m$

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

$\Rightarrow a-b = k_1 m$ and $c-d = k_2 m$, $\longrightarrow$ ①

where k_1 and k_2 are unique non-zero integers

$\Rightarrow a-b+c-d = k_1 m + k_2 m$

$\Rightarrow (a+c)-(b+d) = (k_1+k_2)m$

$\Rightarrow (a+c)-(b+d) = k'm$, where $k' = k_1+k_2 \in \mathbb{Z}$

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

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

Next, of ①.

Multiply c on both sides of $a-b = k_1 m$ and b on both sides of $c-d = k_2 m$, we get

$c(a-b) = c(k_1 m)$ and $b(c-d) = b(k_2 m)$

$\Rightarrow ac-bc = (k_1 c)m$ and $bc-bd = (k_2 b)m$

Adding above two relations, we get

$ac-\cancel{bc}+\cancel{bc}-bd = (k_1 c)m + (k_2 b)m$

$\Rightarrow ac-bd = (k_1 c + k_2 b)m$

$\Rightarrow ac-bd = k''m$ where $k'' = k_1 c + k_2 b \in \mathbb{Z}$

$\Rightarrow m \mid ac-bd$

$\therefore \boxed{ac \equiv bd \pmod m}$

Fermat's Theorem or Fermat's Little Theorem

Statement: Let p be prime and $p \nmid a$. Then

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

OR

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

Proof: Consider the set of reduced residue system mod p

$\{1, 2, 3, \ldots (p-1)\}$

$\Rightarrow 1 \equiv 1 \pmod{p}$; $2 \equiv 1 \pmod{p}$; ..... $(p-1) \equiv 1 \pmod{p}$

Other reduced residue system mod p is

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

$\Rightarrow a \equiv 1 \pmod{p}$; $2a \equiv 2 \pmod{p}$; $3a \equiv 3 \pmod{p}$ .... $(p-1)\overset{a}{\equiv} p-1 \pmod{p}$

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

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

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

OR

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

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

This proves the Fermat's thm.

Example:

1) $a = 10$, $p = 7$

$\therefore a^{p-1} \equiv 1 \pmod{p} \Rightarrow 10^{7-1} \equiv 1 \pmod{7}$

$\Rightarrow 10^{6} \equiv 1 \pmod{7}$

$\Rightarrow 1000000 \equiv 1 \pmod{7}$

as $7 \mid 1000000 - 1$