Basic concepts in Number Theory.

1. Divisibility and the Division Algorithm:

Divisibility:- we say that a non zero b divides a if $a = mb$ for some m, where a, b and m are integers. That is, b divides a if there is no remainder on division. The notation $b|a$ is commonly used to mean b divides a. Also, if $b|a$, we say that b is a divisor of a.

Ex: The +ve integers divisors of 24 are 1, 2, 3, 4, 6, 8, 12 and 24.

$-5|30$, $12|60$, $17|0$. etc..

Some simple properties of divisibility for integers are:

1) If $a|1$, then $a = \pm 1$.
2) If $a|b$ and $b|a$, then $a = \pm b$.
3) any $b \neq 0$ divides 0.
4) If $a|b$ and $b|c$, then $a|c$.

Ex: $2|6$ and $6|18$, then $2|18$.

5) If $b|g$ and $b|h$ then $b|(mg + nh)$ for arbitrary integers m and n.

Ex: $b=3$, $g=6$, $h=15$, $m=2$ and $n=3$.
Here $3|6$ and $3|15$. consider $a(mg+nh) = (2\cdot 6 + 3\cdot 15) = 12+45 = 57$.
Here $3|57$. Hence $b|(mg+nh)$.

The Division Algorithm:

Given any positive integer n and any non negative integer a, if we divide a by n, we get an integer quotient q and an integer remainder r that obey the following relationship:

$$a = qn + r, \quad 0 \leq r < n; \quad q = \lfloor a/n \rfloor$$

Ex: $a = 9$, and $n = 5$; $9 = 1\times 5 + 4$; $r = 4$, $q = 1$.
$a = -9$; $n = 5$; $-9 = (-2)\times 5 + 1$; $r = 1$, $q = -2$.

2. The Euclidean Algorithm:- This algorithm determines the greatest common divisor (gcd) of two positive integers.

Def:- Two integers are **relatively prime** if their only common positive integer factor is 1.

Ex:- 5 and 8;

Greatest common divisor :-

We know that a non zero b is a divisor of a if $a = mb$ for some m, where a, b and m are integers.

We denote gcd(a, b) = greatest common divisor of a and b.

The greatest common divisor of a and b is the largest integer that divides both a and b. We also define gcd(0, 0) = 0.

i.e., The positive integer c is said to be the greatest common divisor of a and b if

1. c is a divisor of a and of b.
2. Any divisor of a and b is a divisor of c.

i.e., $gcd(a, b) = \max\{K,$ such that $K|a$ and $K|b\}$.

Since gcd is positive, $gcd(a, b) = gcd(a, -b) = gcd(-a, b), gcd(-a, -b)$
$= gcd(|a|, |b|)$.

$$gcd(32, 24) = gcd(32, -24) = 8.$$

Since any non zero integer divid 0, we have $gcd(a, 0) = |a|$.

If a and b are relatively prime, then $gcd(a, b) = 1$.

Here 5 and 8 are relatively prime, $gcd(5, 8) = 1$.

Finding the greatest common divisor :-

Euclid's Algorithm for computation of gcd(a, b).

Result: If $a = bq + r$ then $gcd(a, b) = gcd(b, r)$.

Algorithm: Suppose $a > b > 0$, (otherwise interchange a and b).

we can write $a = bq_1 + r_1$, $0 \le r_1 < b$.

we apply division algorithm successively, Then we have:

Divide b by r_1 : $b = r_1 q_2 + r_2$; $0 \le r_2 < r_1$

Divide r_1 by r_2 : $r_1 = r_2 q_3 + r_3$, $0 \le r_3 < r_2$.

Divide r_2 by r_3 : $r_2 = r_3 q_4 + r_4$; $0 \le r_4 < r_3$.

Divide r_{n-2} by r_{n-1} : $r_{n-2} = r_{n-1} q_n + r_n$; $0 \le r_n < r_{n-1}$

Divide r_{n-1} by r_n : $r_{n-1} = r_n q_{n+1} + r_{n+1}$; $0 \le r_{n+1} < r_n$.

since $\{r_j\}$ form a decreasing set of non negative integers.

There must exist $r_{n+1} = 0$. Then from the above result:

$gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = \cdots = gcd(r_{n-1}, r_n) = gcd(r_n, 0)$
$= r_n$.

The gcd a and b is r_n which is the last non zero remainder

Ex: Find gcd of 2406 and 654.

Applying the division algorithm repeatedly,

$2406 = 3 \times 654 + 444$

$654 = 1 \times 444 + 210$

$444 = 2 \times 210 + 24$

$210 = 8 \times 24 + 18$

$24 = 1 \times 18 + 6$

$18 = 3 \times 6 + 0.$

Since the last non zero remainder is 6, the gcd $(2406, 654) = 6.$

---

3. Modular Arithmatic :

The Modulus :- If a is an integer and n is a +ve integer, we define $a \bmod n$ to be the remainder when a is divided by n. The integer n is called the modulus. Thus for any integer a, ~~we can write~~ we have

$$a = qn + r, \quad 0 \le r < n$$

i.e., $a = qn + (a \bmod n).$

Ex: (1) $a = 10$; $n = 3$, then $10 = 3 \times 3 + 1$
$= 3 \times 3 + (10 \bmod 3)$

$a = 13$, $n = 3$, then $13 = 4 \times 3 + 1 = 4 \times 3 + (13 \bmod 3).$

$\therefore (10 \bmod 3) = (13 \bmod 3)$. This can be written as

$10 \equiv 13 \pmod 3.$

$\because -11 = -2 \times 7 + 3$

Ex: $11 \bmod 7 = 4$; $-11 \bmod 7 = 3$

Two integers a and b are said to be congruent modulo n, if $(a \bmod n) = (b \bmod n)$. This can be written as $a \equiv b \pmod n.$

Note: Ex: If $a = 10$ and $n = 2$,

$10 \bmod 2 = 0 = 0 \bmod 2.$

$\therefore 10 \equiv 0 \pmod 2$

If $n \mid a$, then $a \equiv 0 \pmod a.$

properties of congruences:

1. $a \equiv b \pmod n$ if $n \mid (a-b)$.
2. $a \equiv b \pmod n$ implies $b \equiv a \pmod n$
3. $a \equiv b \pmod n$ and $b \equiv c \pmod n$ imply $a \equiv c \pmod n$.

Ex: $13 \equiv 10 \pmod 3$ because $13-10 = 3 = 1 \times 3$

Modular Arithmetic operations:-

Modular Arithmetic has the following properties:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$.
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$.
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$.

Ex:
L.H.S.
① $11 \bmod 8 = 3$, $15 \bmod 8 = 7$.
$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$.
R.H.S.
$(11+15) \bmod 8 = 26 \bmod 8 = 2$

② $[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = (3-7) \bmod 8 = -4 \bmod 8 = 4$.
$(11-15) \bmod 8 = -4 \bmod 8 = 4$.

③ $[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$.
$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$.

4. Exponentiation is performed by repeated multiplication.

To find $11^7 \bmod 13$:

$11^2 = 121 \equiv 4 \pmod{13}$
$11^4 = (11^2)^2 = 4^2 = 3 \pmod{13}$
$11^7 = 11 \times 11^2 \times (11^2)^2 = 11 \times 4 \times 3 = 132 = 2 \pmod{13}$

Consider Arithmetic Modulo 8.

+	0	1	2	3	4	5	6	7
0	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

addition 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

Multiplication Modulo 8

properties of Modular Arithmatic:

We define the set Z_n as the set of non-ve integers less than n.

i.e $Z_n = \{0, 1, 2, 3, \ldots, n-1\}$.

Here each integer in Z_n represents a residue class.

We label the residue classes (mod n) as $[0], [1] \ldots [n-1]$,

where $[r] = \{a / a \text{ is an integer}, a \equiv r \pmod n\}$

The residue classes (mod 4) are:

$[0] = \{a / a \text{ is an integer}, a \equiv 0 \pmod 4\}$

$= \{\ldots -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$

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

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

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

of all the integers in a residue class, the smallest non-ve integer is the one used to represent the residue class.

properties of Modular Arithmatic for integers in Z_n.

1. Commutative laws: $(w + x) \bmod n = (x + w) \bmod n$
   $(w \times x) \bmod n = (x \times w) \bmod n$
2. Associative laws: $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$
   $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$.
3. Distributive laws: $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
4. Identities: $(0 + w) \bmod n = w \bmod n$
   $(1 \times w) \bmod n = w \bmod n$.
5. Additive inverse $(-w)$: For each $w \in Z_n$ there exists a z s.t $w + z \equiv 0 \bmod n$

6. If $(a + b) \equiv (a + c) \pmod n$ then $b \equiv c \pmod n$.
   Adding the additive inverse of a to both sides of the above equation,
   we have $((-a) + a + b) \equiv ((-a) + a + c) \pmod n$
   i.e., $b \equiv c \pmod n$.

   Ex: $(5 + 23) \equiv (5 + 7) \pmod 8$; $23 \equiv 7 \bmod 8$.

7. If $(a \times b) \equiv (a \times c) \pmod n$ then $b \equiv c \pmod n$, if a is relatively prime to n.
   Ex. If we take $a = 5$ and $n = 8$, (relatively primes)

Z_8 :	0	1	2	3	4	5	6	7
Multiply by 5:	0	5	10	15	20	25	30	35
Residues:	0	5	2	7	4	1	6	3

The line of residues contains all the integers in Z_n in a different order.

Euclidean Algorithm revisited:

The Euclidean algorithm can be based on the following theorem:

For any integers a, b, with $a \geq b \geq 0$,

$$\gcd(a,b) = \gcd(b, a \bmod b). \rightarrow (1)$$

Ex: $\gcd(52,22) = \gcd(22, 55 \bmod 22)$
$= \gcd(22,11) = 11.$

(1) can be used repetitively to determine the gcd.

$\gcd(18,12) = \gcd(12,6) = \gcd(6,0) = 6$

$\gcd(11,10) = \gcd(10,1) = \gcd(1,0) = 1.$

The Extended Euclidean Algorithm:-

We now proceed to look at an extension to the Euclidean algorithm that will be important for later computations in the area of finite fields and in encryption algorithms, such as RSA.

For given integers a and b, the extended Euclidean algorithm not only calculates the greatest common divisor d but also two additional integers x and y that satisfy the following equation

$$ax + by = d = \gcd(a,b).$$ (x and y will have opposite signs)

Ex: Find gcd of 595 and 252 and express it in the form ϕ

$\gcd(595,252) = d = 595x + 252y.$

Applying division algorithm repeatedly, we have

$595 = 2 \cdot 252 + 91$

$252 = 2 \cdot 91 + 70$

$91 = 1 \cdot 70 + 21$

$70 = 3 \cdot 21 + 7$

$21 = 3 \cdot 7 + 0.$

Since the last non-zero remainder is 7, $\gcd(595, 252) = 7.$

Now we find x and y $\ni$ $7 = 595x + 252y.$

To find x and y, we begin with the last non zero remainder

$7 = 70 - 3 \cdot 21.$

$= 70 - 3(91 - 1 \cdot 70) = 4 \cdot 70 - 3 \cdot 91$

$= 4 \cdot (252 - 2 \cdot 91) - 3 \cdot 91 = -11 \cdot 91 + 4 \cdot 252$

$= -11(595 - 2 \cdot 252) + 4 \cdot 252$

$= 26 \cdot 252 + (-11) 595$

$\therefore x = -11, y = 26.$

More Number Theory:

1. **prime numbers**:- An integer $p > 1$ is a prime number if and only if its only divisors are ± 1 and $\pm p$.

Any integer $a > 1$ can be factored in a unique way as

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_n^{a_n}$$

where $p_1 < p_2 < \cdots < p_n$ are prime numbers and where each a_i is a positive integer. This is known as the fundamental theorem of arithmetic.

The unique expression for the integer $a \geq 2$ as a product of primes is called the prime factorization of, the product prime decomposition of a.

Ex. The prime factorization of 81, 100 and 289 are: $81 = 3 \times 3 \times 3 \times 3 = 3^4$.

$100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$,

$289 = 17 \times 17 = 17^2$.

Result:- Let $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$.

Then $\gcd(a, b) = \prod p^{\min(a_i, b_i)}$.

Ex. use prime factorization to find the gcd of 12 and 30.

prime factorization of 12 and 30 are:

$12 = 2^2 \times 3^1 \times 5^0$ and $30 = 2^1 \times 3^1 \times 5^1$.

Hence $\gcd(12, 30) = 2^{\min(2,1)} \cdot 3^{\min(1,1)} \times 5^{\min(1,0)} = 2 \times 3 \times 1 = 6$.

Ex. Find gcd of 18 and 300 using prime factorization.

We have $300 = 2^2 \times 3^1 \times 5^2$ and $18 = 2^1 \times 3^2$,

$\gcd(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$.

---

2. **Fermat's and Euler's Theorems**:

Fermat's th and Euler's th. play important roles in public-Key Cryptography.

Fermat's Theorem:- If p is prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

Ex:- Take $a = 7$, $p = 19$.

$7^2 = 49 \equiv 11 \pmod{19}$

$7^4 = 121 \equiv 7 \pmod{19}$

$7^8 \equiv 49 \equiv 11 \pmod{19}$

$7^{16} \equiv 121 \equiv 7 \pmod{19}$

$a^{p-1} = 7^{18} = 7^{16} \times 7^2 = 7 \times 11 = 1 \pmod{19}$.

An alternative form of Fermat's th is also useful:

If p is prime and a is a positive integer, then

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

Ex: $p = 5$; $a = 3$; $a^p = 3^5 = 243 \equiv 3 \pmod 5 = a \pmod p$

$p = 5, a = 10$; $a^p = 10^5 = 10000 = 10 \pmod 5 = 0 \pmod 5 = a \pmod p$

Euler's Totient Function:

Euler's totient function is denoted as $\phi(n)$ and defined as the number of positive integers less than n and relatively prime to n.

$\phi(1) = 1$.

Ex: Determine $\phi(37)$ and $\phi(35)$.

Since 37 is prime, all positive integers from 1 to 36 are relatively prime to 37. Thus $\phi(37) = 36$.

To find $\phi(35)$, we list all the +ve integers less than 35 that are relatively prime to 35.

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18,
19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

There are 24 numbers on the list, so $\phi(35) = 24$.

It is clear that, for a prime number p,

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

Result: If p and q are prime with $p \neq q$, then $\phi(pq) = \phi(p) \times \phi(q)$
$= (p-1) \times (q-1)$

Ex:

$\phi(21) = \phi(3) \times \phi(7) = (3-1) \times (7-1) = 2 \times 6 = 12$.

where 12 integers are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

Euler's Theorem:-

For every a and n that are relatively prime:

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

Ex: $a = 3$, $n = 10$, $\phi(10) = 4$; $a^{\phi(n)} = 3^{\phi(10)} = 3^4 = 81 = 1 \pmod{10} = 1 \pmod n$

$a = 2$; $n = 11$; $\phi(n) = \phi(11) = 10$; $a^{\phi(n)} = 2^{\phi(11)} = 2^{10} = 1024 = 1 \pmod{11} = 1 \pmod n$

alternative Euler's th: $a^{\phi(n)+1} = a \pmod n$.

3. Testing For primality:

For many cryptographic algorithms, it is necessary to select one or more very large prime numbers at random. Then we are faced with the task of determining whether a given large number is prime.

Miller-Rabin algorithm: The algorithm is typically used to test a large number for primality.

TEST (n):
1. Find integers k, q, with $k>0$, q odd, so that $(n-1) = 2^k q$.
2. select a random integer a, $1 < a < n-1$;
3. if $a^q \bmod n = 1$ then return "inconclusive".

Ex: Test the prime number $n = 29$. we have $(n-1) = 28 = 2^2(7) = 2^k q$.

First, Let us try $a = 10$. we compute $10^7 \bmod 29 = 17$, which is neither 1 or 28, so we continue the test.

The next calculation find that $(10)^{14} \bmod 29 = 28$, and Test returns inconclusive.

Let us try again with $a = 2$. we have the calculation:
$2^7 \bmod 29 = 12$; $2^{14} \bmod 29 = 28$: and Test again returns "inconclusive".

If we perform the test for all integers a in the range $1 < a < 29$, we get the same "inconclusive" result, which is compatible with n being a prime number.

primeTesting:

Theorem. If $n > 1$ is a composite integer then there exists a prime p such that $p | n$ (i.e., n has a prime divisor p) and $p \le \sqrt{n}$.

Then to check if a given integer n is prime, it is enough to see that it is not divisible by any prime less than or equal to its square root.

Ex: Show that 47 is prime.
Take $n = 47$. Since $6 < \sqrt{47} < 7$; and 2, 3 and 5 are the primes less than or equal to 6. But 47 is not divisible by 2, 3, 5.
So 47 must be prime.

It can be shown that given an odd number n that is not prime and a randomly chosen integer a with $1 < a < n-1$, the probability that Test will return "inconclusive" (i.e. fail to detect that n is not prime) is less than $\frac{1}{a}$. Then, if t different values of a are chosen, the probability that all of them will pass Test (return "inconclusive") for n is less than $\left(\frac{1}{a}\right)^t$. For example, for $t = 10$ the probability that a non prime number will pass all ten tests is less than 10^{-6}. Thus for a sufficiently large value of t, we can be confident that n is prime if Miller's Test always returns "inconclusive".

Repeatedly invoke Test(n) using randomly chosen values for a. If, at any point, Test returns composite, then n is determined to be non prime. If Test continues to return inconclusive" for t tests, then for a sufficiently large value of t, assume that n is prime.

4. The chinese Remainder Theorem:

Let $m_1, m_2, \ldots, m_k$ be integers that are pairwise relatively prime for $1 \le i, j \le k$, and $i \ne j$.

Define $M = m_1 \cdot m_2 \cdot m_3 \cdots \cdots m_k$. Let $a_1, a_2, \ldots, a_k$ be integers. Then the set of congruences:

$$x = a_1 \pmod{m_1}$$
$$x = a_2 \pmod{m_2}$$
$$\vdots$$
$$x = a_k \pmod{m_k}$$

has a unique solution modulo M.

Let $M = m_1 \cdot m_2 \cdots m_k$ and $M_1 = M/m_1$, $M_2 = M/m_2 \ldots M_k = M/m_k$.

Since m_i are pairwise prime, then $\gcd(M_i, m_i) = 1$.

Let $\Lambda_1, \Lambda_2 \ldots \Lambda_k$ be the solutions, respectively, of the congruences $M_1 x = 1 \pmod{m_1}$, $M_2 x = 1 \pmod{m_2}$, $\ldots M_k x = 1 \pmod{m_k}$.

Then $x = M_1 \Lambda_1 a_1 + M_2 \Lambda_2 a_2 + \cdots + M_k \Lambda_k a_k$ is a solution of the system.

Ex: Solve the following simultaneous congruences:

$x \equiv 3 \pmod 5$, $x \equiv 6 \pmod 7$.

Sol: Here $m_1 = 5$, $m_2 = 7$, $a_1 = 3$, $a_2 = 6$.

Since 5 and 7 are relatively prime there exists a unique sol.

Modulo $M = 5 \cdot 7 = 35$ and $M_1 = M/m_1 = \frac{35}{5} = 7$, $M_2 = \frac{35}{7} = 5$.

Consider $7x \equiv 1 \pmod 5$ and $5x \equiv 1 \pmod 7$ which are equivalent to

$2x \equiv 1 \pmod 5$ and $5x \equiv 1 \pmod 7$.

The solutions of these equations are $\Lambda_1 = 3$ and $\Lambda_2 = 3$.

The required solution of the given system of congruences is

$x = M_1 \Lambda_1 a_1 + M_2 \Lambda_2 a_2 = 7 \cdot 3 \cdot 5 + 5 \cdot 3 \cdot 5 \pmod{35}$

$\equiv 153 \pmod{35}$

$\equiv 13 \pmod{35}$.

The smallest +ve sol. which satisfies the two congruences is therefore $x = 13$.

Solve $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$

Here $m_1 = 3$, $m_2 = 5$, $m_3 = 7$. $a_1 = 2, a_2 = 3, a_3 = 2$.

Since 3, 5, 7 are pairwise relatively prime, there exists a unique sol.

Modulo $M = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$.

$M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$; $M_3 = \frac{105}{7} = 15$.

From CRT, we have

Consider $35x \equiv 1 \pmod 3$; $21x \equiv 1 \pmod 5$; $15x \equiv 1 \pmod 7$.

$\therefore \Lambda_1 = 2$, $\Lambda_2 = 1$, $\Lambda_3 = 1$

$x = M_1 \Lambda_1 a_1 + M_2 \Lambda_2 a_2 + M_3 \Lambda_3 a_3$

$= 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2$

$= 140 + 63 + 30$

$= 233 \pmod{105}$

$= 23 \pmod{105}$

$\therefore x = 23$

The smallest +ve sol. which satisfies the 3 congruences is

$x = 23$

5. Discrete Logarithms:

Discrete logarithms are fundamental to a number of public-key algorithms, including Diffie-Hellman key exchange and the digital signature algorithm (DSA).

From the Euler's th., we have, for every a and n that are relatively prime, $a^{\phi(n)} \equiv 1 \pmod n$

where $\phi(n)$, Euler's totient function, is the number of +ve integers less than n and relatively prime to n. Now consider

$$a^m \equiv 1 \pmod n. \rightarrow (1)$$

If a and n are relatively prime, then there is at least one integer m that satisfies (1), namely $m = \phi(n)$. The least +ve integer m that satisfies (1), namely the exponent m for which (1) holds is referred to in several ways:

1. The order of a (mod n).
2. The exponent to which a belongs (mod n)
3. The length of the period generated by a.

Ex. Consider the powers of 7, modulo 19.

$7^1 \equiv 7 \pmod{19}$

$7^2 = 49 = 2\times19+11 \equiv 11 \pmod{19}$

$7^3 = 343 = 18\times19+1 \equiv 1 \pmod{19}$

$7^4 = 2401 = 126\times19+7 \equiv 7 \pmod{19}$

$7^5 = 16807 = 884\times19+11 \equiv 11 \pmod{19}$

Here the sequence is repeating.

$7^3 \equiv 1 \pmod{19}$; $7^{3+3} = 7^3 7^3 \equiv 7^3 \pmod{19}$

and hence, any two powers of 7 whose exponents differ by 3 (a multiple of 3) are congruent to each other (mod 19).

In other words, the sequence is periodic, and the length of the period is the smallest +ve exponent m such that

$7^m \equiv 1 \pmod{19}$.

Logarithm for modular arithmatic :—

For ordinary +ve real numbers, the logarithm function is the inverse of exponentiation.

The logarithm of a number is defined to be the power to which some +ve base (except 1) must be raised in order to equal the number.

That is, for base x and for a value y, $y = \log_x(y)$.

properties are : 1) $\log_x(1) = 0$

2) $\log_x(x) = 1$

3) $\log_x(yz) = \log_x(y) + \log_x(z)$.

4) $\log_x(y^n) = n \cdot \log_x(y)$.

Any integer b satisfies $b \equiv r \pmod p$ for some r, where $0 \le r \le (p-1)$,

by the definition of modular Arithmatic. It follows that for any integer b and a primitive root a of prime number p, we can find a unique exponent i such that

$b \equiv a^i \pmod p$, where $0 \le i \le (p-1)$,

this exponent i is referred to as the discrete logarithm of the number b for the base $a \pmod p$.

We denote this value as $d\log_{a,p}(b)$.

Here discrete logarithm is also called as the index.

we have :

$d\log_{a,p}(1) = 0$ because $a^0 \bmod p = 1 \bmod p = 1$.

$d\log_{a,p}(a) = 1$ because $a^1 \bmod p = a$.

Ex: Consider a non prime modulus $n = 9$. Here $\phi(n) = 6$ and $a = 2$ is a primitive root. we compute

$2^0 = 1$	$2^4 \equiv 7 \pmod 9$
$2^1 = 2$	$2^5 \equiv 5 \pmod 9$
$2^2 = 4$	$2^6 \equiv 1 \pmod 9$.
$2^3 = 8$	

This gives the following table of the numbers with given discrete logarithms $\pmod 9$ for the root $a = 2$.

Logarithm :	0	1	2	3	4	5
Number :	1	2	4	8	7	5

To make it easy to obtain the discrete logarithm of a given number we rearrange the table :

Number	1	2	4	5	7	8
Logarithm	0	1	2	5	4	3

consider: $x = a^{d\log_{a,\beta}(x)} \bmod \beta$; $y = a^{d\log_{a,\beta}(y)} \bmod p$.

$$xy = a^{d\log_{a,\beta}(xy)} \bmod \beta.$$

Also $d\log_{a,\beta}(xy) = [d\log_{a,\beta}(x) + d\log_{a,\beta}(y)] \pmod p$

and $d\log_{a,\beta}(y^n) = [n \cdot d\log_{a,\beta}(y)] \pmod p$.