UNIT-7

Number Theoretic Algorithms:

Small easier unit so read everything instead of imp only

Number Theoretic Notations:

i) Divisibility and Divisors: The notation $d|a$ (read "d divides a") means that $a=kd$ for some integer k. If $d|a$, then we say that 'a' is a multiple of d. Every integer divides 0. If $a>0$ and $d|a$, then $|d| \leq |a|$. If $d|a$ and $d \geq 0$, we say that d is a divisor of a. A divisor of an integer 'a' is at least 1 but not greater than $|a|$.

For example: The divisors of 24 are 1, 2, 3, 4, 6, 8, 12 and 24.

trivial divisors of 24: 1 and 24 ← 1 and the no. itself

non-trivial divisors of 24: 2, 3, 4, 6, 8 and 12 ← other remaining ones than that of trivial

ii) Prime and Composite Numbers:

An integer $a>1$ whose only divisors are the trivial divisors (i.e, 1 and 'a' itself only) is said to be a prime number or simply prime.

An integer $a>1$ that is not prime is said to be a composite number. The integer 1 is said to be a unit and is neither prime nor composite. Similarly, the integer 0 and all negative integers are neither prime nor composite.

iii) Common Divisors and Greatest Common Divisors:

If 'd' is a divisor of 'a' and also divisor of 'b', then 'd' is a common divisor of 'a' and 'b'. Note that 1 is a common divisor of any two integers. An important property of common divisors is that:

→ if $d|a$ and $d|b$ then, $d|(a+b)$ and $d|(a-b)$.

→ if $d|a$ and $d|b$ then, $d|(ax+by)$

The greatest common divisor $\gcd(a,b)$ is the largest of the common divisors of a and b. We define $\gcd(0,0)$ to be 0.

→ For any integers a and b if $d|a$ and $d|b$ then, $d|\gcd(a,b)$.

→ For all integers a and b and any nonnegative integer n,

$$\gcd(an, bn) = n \gcd(a, b)$$

→ For all positive integers n, a, and b, if $n|ab$ and $\gcd(a,n)=1$, then $n|b$.

iv) Relatively Prime Integers:

Two integers a, b are said to be relatively prime if their only common divisor is 1, that is if $\gcd(a,b)=1$.

→ For any integers a, b, and p, if both $\gcd(a,p)=1$ and $\gcd(b,p)=1$ then, $\gcd(ab,p)=1$.

→ For all primes p and all integers a, b if $p|ab$, then $p|a$ or $p|b$ or both.

⊛. Euclid's Algorithm for solving Modular Linear Equations: [Imp]

Euclidean algorithm is an efficient method for computing the greatest common divisor of two numbers.

Algorithm:

```
EUCLID (a,b)
{ if b=0
      return a;
  else
      return EUCLID (b, a mod b)
}
```

Analysis: Since it is recursive algorithm so we need to find their recurrence relation, Since every time the problem is divided into two parts one is b and another is a mod b.

Thus the size of sub-problem $= \frac{n}{2}$

Dividing and merging time = constant = $O(1)$

Thus, recurrence relation is, $T(n) = T(n/2) + O(n)$

By, solving this we get, $T(n) = O(\log n)$.

Example: Find $\gcd(30,21)$ by Euclid's Algorithm.

Solution

EUCLID(30,21)

= EUCLID (21, 30 mod 21)

= EUCLID (21, 9)

= EUCLID (9, 21 mod 9)

= EUCLID (9, 3)

= EUCLID (3, 9 mod 3)

= EUCLID (3, 0)

Since b==0, so return a

= 3

∴ $\gcd(30,21) = 3$.

⊛. Extended Euclid's Algorithm for solving Modular Linear Equation: [Imp],

Extended Euclid's Algorithm is an extension to Euclid's algorithm which computes the coefficients of Bezout's identity, (which are integers x and y) in addition to the greatest common divisors of integers a and b such that:

$$d = gcd(a,b) = ax + by$$

where, x and y may be zero or **negative**.

Algorithm:

```
EXTENDED-EUCLID (a,b)
{
  if b=0
     return (a,1,0);
  (d',x',y') ← EXTENDED-EUCLID (b, a mod b)
  (d,x,y) ← (d',y',x' - floor (a/b) y')
  return (d,x,y);
}
```

Analysis: Same as Euclid's algorithm i.e, $T(n) = O(\log n)$.

Example: Find GCD (161, 28) and value of x and y by using extended Euclidean's algorithm.

Solution:

We have, $a = 161$, $b = 28$ and $GCD(a,b) = ax + by$.

Let's define following three equations;

$r = r_1 - q * r_2$

$x = x_1 - q * x_2$

& $y = y_1 - q * y_2$

formulas that will be used to calculate r, x, y in below table

Consider $a = r_1$ and $b = r_2$.

remainder

always initialize $x_1 = 1, x_2 = 0$ & $y_1 = 0, y_2 = 1$

r_1/r_2

q	r_1	r_2	r	x_1	x_2	x	y_1	y_2	y
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0	.	-1	4		6	-23	

पछिल्लो step मा $r=0$ so last step shift only

$x = -1, y = 6$

Since: $ax + by = gcd(a,b)$

or, $\{161 * (-1)\} + (28 * 6) = 7$

or, $7 = 7$

⊛. Miller–Rabin Randomized Primality Test:

This test algorithm test determines whether a given number is prime or not.

Algorithm:

/* It returns false if n is composite and returns true if n is probably prime. k is an input parameter that determines accuracy level. Higher value of k indicates more accuracy. */

bool IsPrime (int n, int k)

1) Handle base cases for n<3
2) If n is even, return false.
3) Find an odd number d such that n-1 can be written as d*2r.
   Note that since n is odd, (n-1) must be even and r must be greater than 0.
4) Do following k times
   if (millerTest (n,d)==false)
   return false
5) Return true.

bool millerTest (int n, int d)

1). Pick a random number 'a' in range [2, n-2]
2). Compute: x= pow (a,d)%n
3) If x==1 or x==n-1, return true.

//Below loop mainly runs 'r-1' times.

4). Do following while d doesn't become n-1.
   a) x=(x*x) % n.
   b) If (x==1) return false.
   c) If (x==n-1) return true.

<u>Example:</u> Input: $n=13, k=2$.

1). Compute d and r such that $d*2r = n-1$,

$d=3, r=2$.

2) Call millerTest k times.

<u>1st Iteration:</u>

1) Pick a random number 'a' in range [2, n-2]

Suppose $a=4$

2). Compute: $x = pow(a,d) \% n$

$x = 43 \% 13 = 12$

3). Since $x = (n-1)$, return true.

<u>2nd Iteration:</u>

1) Pick a random number 'a' in range [2, n-2]

Suppose $a=5$

2) Compute: $x = pow(a,d) \% n$

$x = 53 \% 13 = 8$

3) x neither 1 nor 12.

4) Do following $(r-1) = 1$ times

a) $x = (x*x) \% 13 = (8*8) \% 13 = 12$

b) Since $x = (n-1)$, return true.

Since both iterations return true, we return true.

⊛. Chinese Remainder Theorem:

The chinese remainder theorem states that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise co-prime.

Statement: If $m_1, m_2, \ldots, m_k$ are pairwise relatively prime positive integers, and if $a_1, a_2, \ldots, a_k$ are any integers, then the simultaneous congruences

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2}, \ldots$$
$$x \equiv a_k \pmod{m_k}$$ have a solution, and the solution is unique modulo m.

Here we need to calculate x with the help of following formulas:

$$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + \ldots + M_k x_k a_k) \pmod{M}$$
$$M = m_1 \cdot m_2 \ldots m_k$$
$$M_i = \frac{M}{m_i}$$
& $M_i x_i = 1 \pmod{m_i}$

Example: Solve following congruences by using Chinese remainder theorem.

$$x \equiv 1 \pmod 5$$
$$x \equiv 1 \pmod 7$$
$$x \equiv 3 \pmod{11}$$

Solution:
We have, $a_1 = 1, a_2 = 1, a_3 = 3$
$m_1 = 5, m_2 = 7, m_3 = 11$

$$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \pmod{M}$$
$$M = m_1 \cdot m_2 \cdot m_3 = 5 \times 7 \times 11 = 385$$
$$M_1 = \frac{M}{m_1} = \frac{385}{5} = 77$$
$$M_2 = \frac{M}{m_2} = \frac{385}{7} = 55$$

$$M_3 = \frac{M}{m_3} = \frac{385}{11} = 35$$

Now,
$M_1 x_1 = 1 \pmod 5$
or, $77 x_1 = 1 \pmod 5$
or, $2 x_1 = 1 \pmod 5$
or, $x_1 = 3$

Since we have to put value of x_1 in such a way that (product of 2 and x_1) (mod 5) becomes equal to 1.
for e.g. let we put 1 then, $(2\times1) \bmod 5 = 2$
Now we put 3 then, $2\times3 = 6 \bmod 5 = 1$ ✓
So, $x_1 = 3$

$M_2 x_2 = 1 \pmod 7$
or, $55 x_2 = 1 \pmod 7$
or, $6 x_2 = 1 \pmod 7$
or, $x_2 = 6$

random multiply	mod 7 value
$6\times1=6$	$6\ (\neq 1)$
$6\times2=12$	$5\ (\neq 1)$
$6\times3=18$	$4\ (\neq 1)$
$6\times4=24$	$3\ (\neq 1)$
$6\times5=30$	$2\ (\neq 1)$
$6\times6=36$	$1\ (=1)$

Hence, $x_2 = 6$. on putting 6 and doing mode we got 1

$M_3 x_3 = 1 \pmod{11}$
or, $35 x_3 = 1 \pmod{11}$
or, $2 x_3 = 1 \pmod{11}$
or, $x_3 = 6$

$\therefore\ x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \pmod M$
$= (77\times3\times1 + 55\times6\times1 + 35\times6\times3) \pmod{385}$
$= (231 + 330 + 630) \pmod{385}$
$= 1191 \pmod{385}$
$= 36$ Ans.

Also, we can test the solution as;
$36 \pmod 5 = 1$
$36 \pmod 7 = 1$
$36 \pmod{11} = 3$