FAST EXPONENTIATION

6 Mark

Problem:- Given integers, a, n, m where $n \geq 0$ & $0 \leq a < m$.

Find $a^n (\mod m)$.

Eg:- Find ~~5~~ $2^5 (\mod 6)$.

$\Rightarrow 32 \% 6 = 2$ //

(or)

$2^5 (\mod 6) = [2^2 \times 2^2 \times 2] \mod 6$

$\Rightarrow 2^1 (\mod 6) = 2$

$2^2 (\mod 6) = (2^1 \times 2^1) \mod 6$

$= 4 (\mod 6) = 4.$

$2^4 (\mod 6) = (2^2 \times 2^2) \mod 6$

$= (4 \times 4) \mod 6$

$= 16 (\mod 6) = 4.$

$2^5 (\mod 6) = (2^4 \times 2) \mod 6$

$= (4 \times 2) \mod 6$

$= 8 (\mod 6) = 2$ //

We get same answer Either ways.

If n is a power of 2,

$n = 2^K$.

=> Simply square 'a' for K times & take modulus each time.

Suppose, find $a^{128} \pmod m$.

$128 = 2^7 \Rightarrow a^{2^7} \pmod m$.

$\therefore 128 = n \quad \therefore K = 7 \quad (\because 128 = 2^7)$.

Only 7 Modular Multiplication will give result.

$$a^2 = a^2 \pmod m.$$

$$(a^2)^2 = (a^2)^2 \pmod m$$

$$(a^2)^3 = (a^2)^2 . a^2 \pmod m$$

$$(a^2)^4 = (a^2)^3 . a^2 \pmod m$$

"

"

"

$$(a^2)^7 = (a^2)^6 . a^2 \pmod m \text{ .//}$$

Suppose it is not a power of 2,

Eg:- $n = 205$

$(205)_{10} = (11001101)_2$

$\Rightarrow 2^7 + 2^6 + 2^3 + 2^2 + 2^0$

→

P.T.O

From this $n = (\beta_k . \beta_{k-1} \dots \beta_1 . \beta_0)_2$

Where $\beta_k \neq 0$ & $k = 0$.

$\Rightarrow 2^k \leq n < 2^{k+1}$ (Take Log)

$\Rightarrow K = \lfloor \ln(n) \rfloor$

So compute 'K' modular Multiplications,

$a^n \pmod m = a^{2^i}$ $(i \leq K)$.

Algorithm :-

```
Integer_Fast_Expo(int a, int n, int m)
{
    if (n==0)
        return 1;
  int y = a;
  for (int i = K-1; i ≥ 0; i--)
  {  if ($\beta_i$ == 0)
         y = $y^2$(mod m);
     else
         y = ($y^2$.a)(mod m);
  }
  return y;
}
```

Time Complexity :-

$O(\lg(m)^3)$.

Eg:- Compute 240^{265} mod 14.

$a = 240$ $\quad n = (265)_{10} = (100000110)_2$.

1st	2nd	3rd	4th	5th	6th	7th	8th	9th
1	0	0	0	0	0	1	1	0
240	4	2	4	2	4	4	4	$\boxed{2}$

$2^{nd} = (240)^2 \bmod 14 = 4$

$3^{rd} = (4)^2 \bmod 14 = 2$

$4^{th} = (2)^2 \bmod 14 = 4$

$5^{th} = (4)^2 \bmod 14 = 2$

$6^{th} = (2)^2 \bmod 14 = 4$

$7^{th} = (4)^2 \bmod 14 = (2 \times 240) \bmod 14 = 4$

$8^{th} = (4)^2 \bmod 14 = (2 \times 240) \bmod 14 = 4$

$9^{th} = (4)^2 \bmod 14 = 2.$ $\Rightarrow$ Answer.