

Design and Analysis of Algorithms Assignment - 5

Name: Dhanraj Kore

Div: TY B

Roll No: 60

Batch : B-3

Fast Modular Exponentiation

Approach 1: Using Divide n Conquer

CODE :

```
#include<bits/stdc++.h>
using namespace std;

int FME(int a,int b,int n)
{
    if(b==0)
        return 1;
    else if(b==1)
        return a;
    int pow = FME(a,b/2,n);
    if(b%2==0)
        return ((pow%n)*(pow%n))%n;
    else
        return ((pow%n)*a*(pow%n))%n;
}

int main()
{
    int a,b,n;

    cout<<"Enter the nos a,b & n : ";

    cin>>a>>b>>n;
```

```

    int ans = FME(a,b,n);

    cout<<"Fast Modular Expression is : "<<ans<<endl;
}

```

O/P:

```

mod_1.cpp
13     else
14         return ((pow(n)*a*(pow(n)))%n;
15     }
16 int main()
17 {
18     int a,b,n;
19     cout<<"Enter the nos a,b & n : ";
20     cin>>a>>b>>n;
21     int ans = FME(a,b,n);
22     cout<<"Fast Modular Expression is : "<<ans<<endl;
23 }

```

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Users\VASUS\Documents\TY SEM 2\DA\DA\ LAB\LAB 5> g++ mod_1.cpp
PS C:\Users\VASUS\Documents\TY SEM 2\DA\DA\ LAB\LAB 5> .\a.exe
Enter the nos a,b & n : 2 3 4
Fast Modular Expression is : 0
PS C:\Users\VASUS\Documents\TY SEM 2\DA\DA\ LAB\LAB 5> .\a.exe
Enter the nos a,b & n : 3 4 5
Fast Modular Expression is : 1
PS C:\Users\VASUS\Documents\TY SEM 2\DA\DA\ LAB\LAB 5> .\a.exe
Enter the nos a,b & n : 4 2 7
Fast Modular Expression is : 2
PS C:\Users\VASUS\Documents\TY SEM 2\DA\DA\ LAB\LAB 5>

```

Approach 2 : Using Bit Manipulation

CODE:

```

#include <bits/stdc++.h>

using namespace std;

long long FME(long long a, long long b, long long n)
{
    long long res = 1;

    while (b > 0)

```

```

{
    if (b & 1)
    {
        res = (res * a) % n;
    }

    a = (a * a) % n;

    b = b >> 1;
}

return res;
}

int main()
{
    long long a, b, n;

    cout << "Enter the nos a,b & n : ";

    cin >> a >> b >> n;

    long long ans = FME(a, b, n);

    cout << "Fast Modular Expression is : " << ans << endl;
}

```

O/P:

```

mod_2.cpp x  mod_1.cpp
mod_2.cpp > FME(long long, long long, long long)
3
4 long long FME(long long a, long long b, long long n)
5 {
6     long long res = 1;
7     while (b > 0)
8     {
9         if (b & 1)
10        {
11            res = (res * a) % n;
12        }
13        a = (a * a) % n;
14        b = b >> 1;
15    }
16    return res;
17 }

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Users\VASUS\Documents\TY SEM 2\DA\DA\ LAB\LAB 5> g++ mod_2.cpp
PS C:\Users\VASUS\Documents\TY SEM 2\DA\DA\ LAB\LAB 5> ./a.exe
Enter the nos a,b & n : 3 4 5
Fast Modular Expression is : 1
PS C:\Users\VASUS\Documents\TY SEM 2\DA\DA\ LAB\LAB 5> ./a.exe
Enter the nos a,b & n : 2 4 7
Fast Modular Expression is : 2
PS C:\Users\VASUS\Documents\TY SEM 2\DA\DA\ LAB\LAB 5>

```