18CA314-Cryptography and Network Security

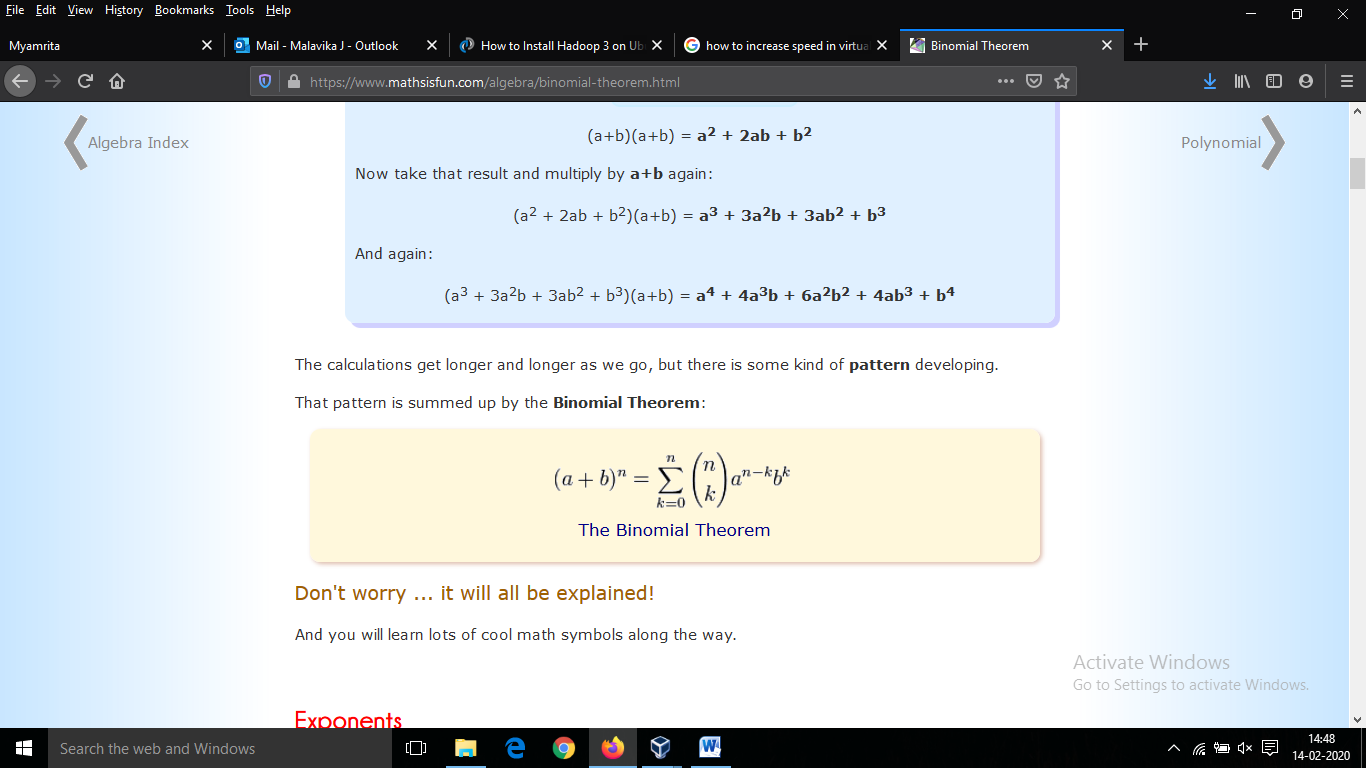
Assignment 1

Anjali m.s(AM.SC.P2CSC19009)

PART:A

**1.a belongs to Zp. Prove that (a + p)n(mod p) =an(mod p)**

Ans: Using binomial theorem,



On applying this to (a + p)n ( mod p)=an+pn  mod p

rest of the terms becomes 0 since (p mod p=0)

(a + p)n(mod p) = an+pn  mod p

=an mod p + pn mod p

=an  mod p + 0

=an  mod p

Then it is proved

2:Find the multiplicative inverse of all the elements in Z5 and Z11

Ans : a) Multiplication inverse Z5 : 1 2 3 4

1 3 2 4

b)multiplication inverse of Z11: 1 2 3 4 5 6 7 8 9 10

1 6 4 3 9 2 8 7 5 10

**3: Determine the gcd of 56245 and 43159**

**Ans:it will solve using Eucledian algorithm,**

**Gcd(56245,43159)**

**56245=1\*43159+13086**

**43159=3\*13086+3901**

**13086=3\*3901+1383**

**3901=2\*1383+1135**

**1383=1\*1135+248**

**1135=4\*248+143**

**248=1\*143+105**

**143=1\*105+38**

**105=2\*38+29**

**38=1\*29+9**

**29=3\*9+2**

**9=4\*2+1**

**2=2\*1+0**

**Hence we obtain gcd(56245,43159)=1**

**Then it is prime**

4: Compute Φ(n) for 34 and 210

Ans:here we use Eulers product formula

Φ(n)=n-(1-1/p)

1. Φn for 34

81(1-1/3)=81(3-1/3)

=54

b)Φn for 210

1024(1-1/2)=1024/2

=512

5. Compute 3100 mod(31319)

Ans) 30 mod 31319=3

32 mod 31319=9

34mod 31319=81

38mod 31319=6561

316mod 31319=14418

332mod 31319=21979

364mod 31319=12185

12185\*21979\*81 mod 31319

267814115 mod 31319

5346\*81 mod 31319

433026 mod 31319

2587

Part b)

1. Write a program to implement Extended Euclidean Algorithm and find multiplicative inverse for following values.

program:

#include<iostream>

using namespace std;

int Exeu(int a, int b, int \*x, int \*y)

{

if (a == 0)

{

\*x = 0, \*y = 1;

return b;

}

int x1, y1;

int gcd = Exeu(b%a, a, &x1, &y1);

\*x = y1 - (b/a) \* x1;

\*y = x1;

return gcd;

}

int main()

{

int a, m;

cin>>a>>m;

int x, y;

int g = Exeu(a, m, &x, &y);

if (g != 1)

cout<< "\n Inverse does not exist. ";

else

{

int res = (x%m + m) % m;

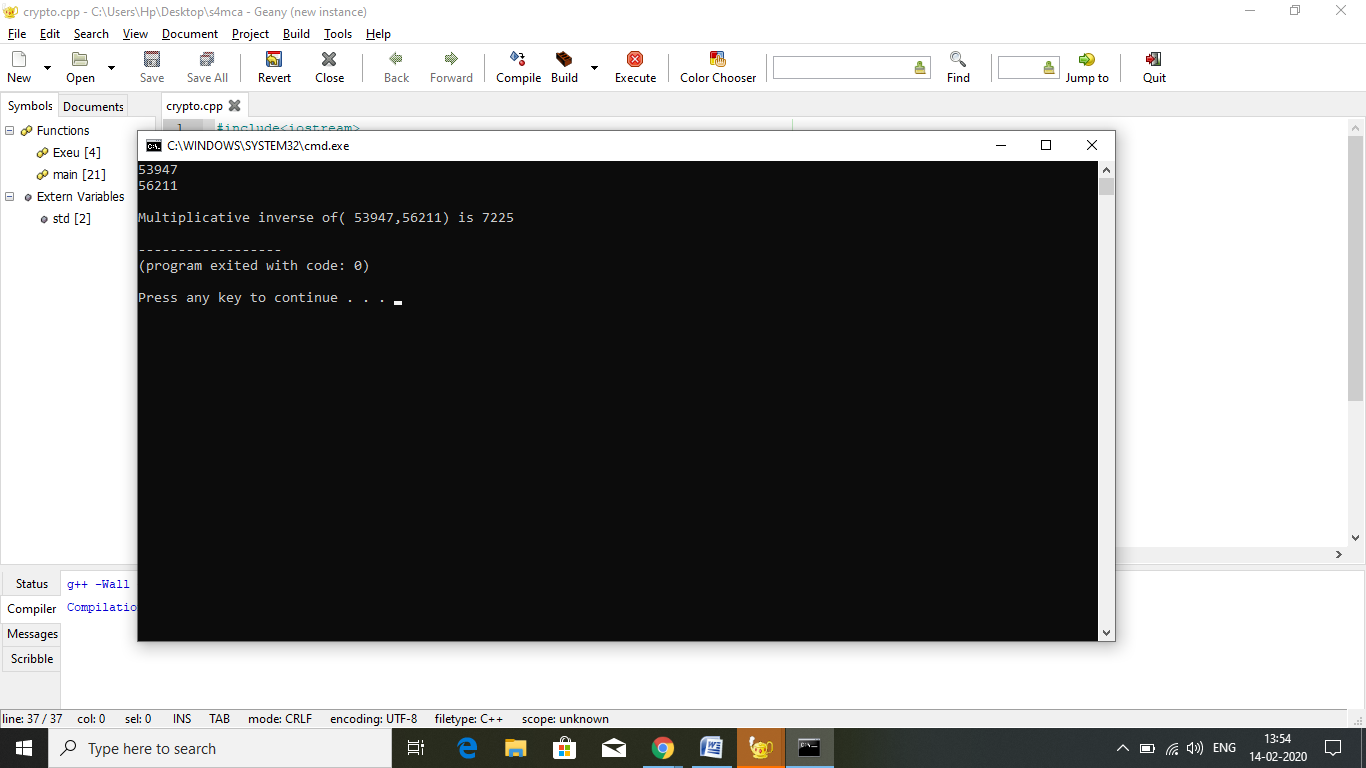
cout<< "\nMultiplicative inverse of( "<<a<<","<<m<<") is "<< res;

}

return 0;

}

1. 53947-1 mod 56211



B)19385-1 mod 431592.

