Cryptography Assignment - 5
Pramod Aravind Byakod

1. Let id be your student id number. Solve the simultaneous congruences:
x = 2 mod 297359071
x = 3 mod 837582957839
x = 4 mod id
Follow the algorithm in the book. You may use Sage to help you in each step. You should not use Sage function "crt" directly.

```
[sage: m1 = 297359071
[sage: m2 = 837582957839
[sage: m3 = 113436879
[sage: M1 = m2*m3
[sage: M2 = m1*m3
[sage: M3 = m1*m2
[sage: y1 = Integers(m1)(M1)^(-1)
[sage: y2 = Integers(m2)(M2)^(-1)
[sage: y3 = Integers(m3)(M3)^(-1)
[sage: y1
127096024
[sage: y2
738274733218
[sage: y3
78401813
[sage: v = (2*127096024*M1 + 3*738274733218*M2 + 4*78401813*M3) % (m1*m2*m3)
[sage: v
7451233462757538205235879056
sage:
```

Output – **7451233462757538205235879056**

3. Find all the positive integers m such that (Z/m Z)^* has four elements.

1^1 mod 5 = 1, 2^4 mod 5 = 1, 3^4 mod 5 = 1, 4^2 mod 5 = 1
1^1 mod 8 = 1, 3^2 mod 8 = 1, 5^2 mod 8 = 1, 7^2 mod 8 = 1
1^1 mod 10 = 1, 3^4 mod 10 = 1, 9^2 mod 10 = 1, 7^4 mod 10 = 1
1^1 mod 12 = 1, 11^2 mod 12 = 1, 5^2 mod 12 = 1, 7^2 mod 12 = 1
Values of m are **5,8,10,12**

2. Let id be your student id number, p be the prime number 9393593593758476092732085392765\7, and q be the prime number 203953589475498534391475049769678209475091748\47. Find an integer x such that   x^37 = id (mod n), where n = p* q.

Id = 113436879,
n=p*q=19158571315210891847847100831099236304685424909875913407370458411497031020434\79
x^37 = 113436879 (mod n)
According to Fermat's Theorem if gcd(x,m)=1, then $x^{phi(m)}$ = 1 mod m.
By extending the same, $x^{phi(m)\ +1}$ = x mod m.
Let's find u such that 37u = phi(m) +1
In our case m is value of n.
phi(n) = phi(p) * phi(q)
phi(n) = (p-1) * (q-1)
phi(n)=19158571315210891847847100831099032351095949410402162572944841124014347389409\76
xgcd(37,phi(n)) will give you 1 = 37*u+phi(n)*v

```
sage: xgcd(37,1915857131521089184784710083109903235109594941040216257294484112401434738940976)

(1,
 -466019302261886558461145695891598084215847418090863413936496135448997639201859,
 9)
sage:
```

So, v = 9 and u =
14498378292592026263235643872183051508937475229493528433579879769524370997391\17

Now it can be transformed to x^37^u = id^u mod m
The same is equal to x^(phi(m)+1) => x

```
sage: R = Integers(1915857131521089184784710083109903235109594941040216257294484112401434738940976)
sage: a = R(113436879)**1449837829259202626323564387218305150893747522949352843357987976952437099739117
sage: a%1915857131521089184784710083109903235109594941040216257294484112401434738940976
1093724137193855460061898346669794423110349873975610328961193039563435422742863
sage: 1093724137193855460061898346669794423110349873975610328961193039563435422742863 % 1915857131521089184784710083109903235109594941040216257294484112401434738940976
1093724137193855460061898346669794423110349873975610328961193039563435422742863
```

Therefore using Sage we get the value of x as
1093724137193855460061898346669794423110349873975610328961193039563435422742863

4. Calculate by hand 31^{30^45} mod 35 using Chinese Remainder Theorem.

31^(30^45) mod 35
x = 31^(30^45) mod 7*5
a = 31^(30^45) mod 7 , b=31^(30^45) mod 5

a = 31^(30^45) mod 7
a = 3^(30^45) mod 7 (31 mod 7 = 3)
We know a^6 = 1 mod 7. And, (30^45) mod 6 = 0
a = 3^(0) mod 7
a = 1

b = 31^(30^45) mod 5
b = 1^(30^45) mod 5 (31 mod 5 =1)
b = 1 mod 5
b = 1

Value of x= a*b => 1*1 = 1
Therefore **31^(30^45) mod 35 = 1**