**Cryptography Assignment - 5**

**Pramod Aravind Byakod**

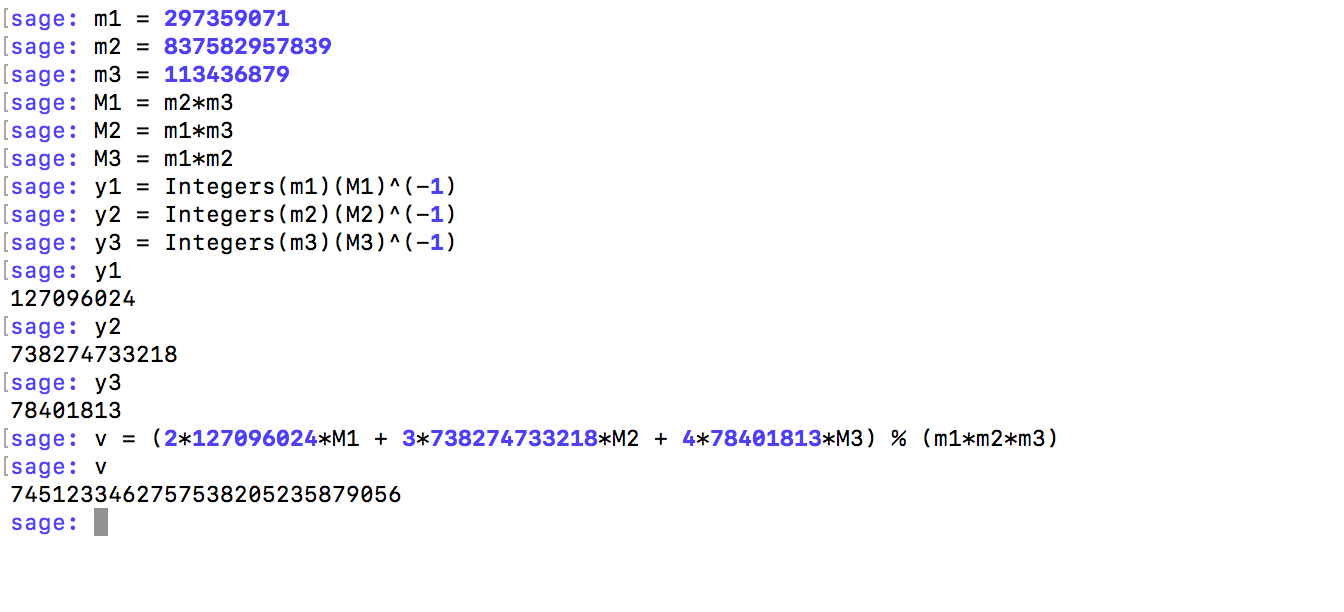
**1. Let id be your student id number. Solve the simultaneous congruences:**

**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.**

Output – **7451233462757538205235879056**

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

11 mod 5 = 1, 24 mod 5 = 1, 34 mod 5 = 1, 42 mod 5 = 1

11 mod 8 = 1, 32 mod 8 = 1, 52 mod 8 = 1, 72 mod 8 = 1

11 mod 10 = 1, 34 mod 10 = 1, 92 mod 10 = 1, 74 mod 10 = 1

11 mod 12 = 1, 112 mod 12 = 1, 52 mod 12 = 1, 72 mod 12 = 1

Values of m are **5,8,10,12**

**2. Let id be your student id number, p be the prime number  
93935935937584760927320853927657, and q be the prime number 20395358947549853439147504976967820947509174847. Find an integer x such that    x^37 = id (mod n ),  
where n = p\* q.**

Id = 113436879, n=p\*q=1915857131521089184784710083109923630468542490987591340737045841149703102043479

x^37 = 113436879 (mod n)

According to Fermat’s Theorem if gcd(x,m)=1, then xphi(m) = 1 mod m.

By extending the same, xphi(m) +1 = x mod m.

Let’s find u such that 37u = phi(m) +1

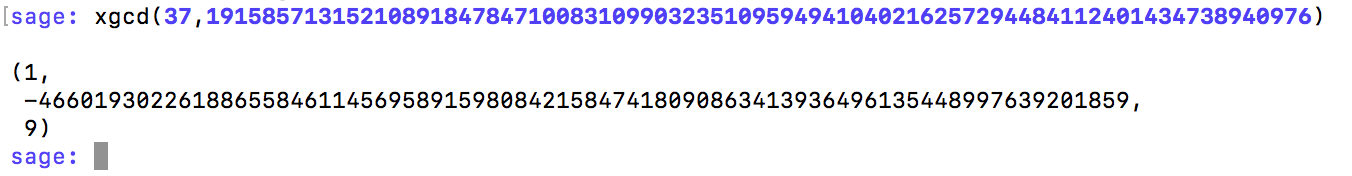
In our case m is value of n.

phi(n) = phi(p) \* phi(q)

phi(n) = (p-1) \* (q-1)

phi(n)=1915857131521089184784710083109903235109594941040216257294484112401434738940976

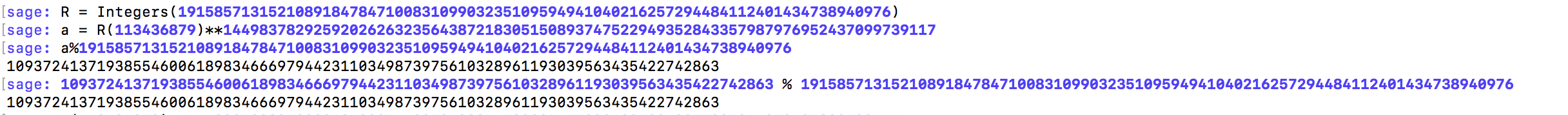
xgcd(37,phi(n)) will give you 1 = 37\*u+phi(n)\*v



So, v = 9 and u = 1449837829259202626323564387218305150893747522949352843357987976952437099739117

Now it can be transformed to x^37^u = id^u mod m

The same is equal to x^(phi(m)+1) => x



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 a6 = 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**