Selin Eyupoglu
21090

CS411 HOMEWORK 2

1.

Since quadratic equation $x^2 \equiv y \bmod n$ has 4 solutions, which is maximum number of solutions We let $n = p \times q$ be the product of two primes and we know the four solutions $x = \pm a, \pm b$ of $x^2 \equiv y \bmod n$. We proved in class that gcd(a-b,n)=p. In the code that I have written I have tried to understand which roots correspond to a's and which ones correspond to b by printing the gcd.r1 and r2 correspond to positive and negative a's whereas r3 and r4 correspond to b's. Thus, by simply calculating the gcd(r1-r3,n), I calculated the values as:

p=567212110818670791663976397722940564089534874688541547718209830933168388711124
61299104488217120802796794576188273840266714113231912409701860720560329365 39

q=132564129365365393206400621084095865029710745968804560670356527115126543297980
2461634305729042115298555854621627235748648240514441092401984224168417165312

n=pxq

2.

a. There are $\phi(58)$ elements in Z^*_{58}. Since 58=29.2, we can write $\phi(58)= \phi(2).\ \phi(29)=28$
Elements of the group: [1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57]

b. [3, 11, 15, 19, 21, 27, 31, 37, 39, 43, 47, 55] generate Z^*_{58}.

c. There are 14 elements in Q^*_{58}.
Elements of the Q^*_{58} : [1, 5, 7, 9, 13, 23, 25, 33, 35, 45, 49, 51, 53, 57]

d. [5, 9, 13, 33, 35, 51] generate Q^*_{58}.

3.

a. $\phi(n)=(p-1)*(q-1)$ since p and q are primes. I have calculated e's inverse in mod n to be 7743867766120419573468358460657148278606034607307382366256503635478073271990169 1
6822915115927210157393366505558453060406762540801133262149000567030327964134161 4
8833362595440786497153368536316168591266370065259003784679241855131283268931114 9
28617984398145991814429351420749556577775600558625278145271493713499. Then the result of pow(c,d,n) is
1181536904587981110384299120140438317909275252305837351710997006040867026519764 4
0240122162327375827736767204747423718009010398297866191614260790597794306151654 7
8180474538387103825825869238918158573611634139093792075110464245862323591770790 2
986884290087944996461920310795766251029133927666157562413018911828577.

Selin Eyupoglu
21090

b.

c_p=9320236508526392792501441624496343093490984989515385109388485454771276014346729475206520055944899268185138158163982736950910716898663264013744937241871742

c_q=7154575998388489651430394446626793038680924462041395960268426802608476072603948069377497281619866003658824193808814594532335865678247666058454289078788934

d_p=1508418563766902153705462288612197333702615905284262541900133782026782516026028158881223099778956686561949872471198567487253281063219132811047984214183843

d_q=8448217877722436208324303757299862201346942960023193625210296828379546370076667024122566735202062152931140475986264091178346112454699881857438649841071927

p^{-1}(modq)=5540070944604488232025655370794179865648000434577918451099278009045667427758464910608984628240418851219300479714812653318434232406140386012202938913288823

q^{-1}(modp)=5852962088339347258249186909229013255151679519566173824577075192807290287713751681325336920406338922004660026872402227478824406248376619284204607230985131

(c_p)^d_p(modp)=9343237457335060991354827507674878243798465388639625217049605210440938460361815753531931859732405537215889346940296196638338045615321567444568182453514041

(c_q)^d_q(modq)=3984521728701913962541086420105180309215160716356785093441790766549301662850741989820843331145280631598383997249458484238211911588985195408960379153483924

Result using CRT is:
118153690458798111038429912014043831790927525230583735171099700604086702651976440240122162327375827736767204747423718009010398297866191614260790597794306151654781804745383871038258258692389181585736116341390937920751104642458623235917707902986884290087944996461920310795766251029133927666157562413018911828577.

c.

This is the output of average time that these two approaches take after 100 iterations:
avg time that regular computation takes 0.277678017616272 s
avg time that crt takes 0.000002760887146 s

CRT is definitely much faster.

4.

a. gcd(a,n)=1, thus there exists only one solution.
x≡ba^{-1} (modn) First, a^{-1} should be calculated. It is 195271140381831409138894386045.

Then the unique solution is x ≡ 717219225411236668249702421766 (modn)

b. gcd(a,n)=2, there may be one solution or more. 2 divides b, so we proceed to check if gcd(a/2,n/2) = 1, since this holds:

1st solution : 409986093653961733346127330802 (modn)

Selin Eyupoglu
21090

2nd solution : 848364686422710508066971521240 (modn)

c. gcd(a,n)=2, there may be exactly two solutions. Since 2 does not divide b (which is odd), there is no solution.

5.

$f(x) = x^5 + x + 1$ is a irreducible polynomial over GF(2). To find the linear complexity, we have to determine the smallest m so that f(x) divides $x^m + 1$. Clearly, m > 5, the period divides $2^5 - 1 = 31$. Since 31 is prime, f(x) is a primitive polynomial. The states start to repeat themselves once in each 21 states.

$f(x) = x^4 + x^3 + 1$ is a irreducible polynomial over GF(2). To find the linear complexity, we have to determine the smallest m so that f(x) divides $x^m + 1$. Clearly, m > 4, the period divides $2^4 - 1 = 15$, thus it must be either 5 or 15. By trying the possibilities we get

$$x^5 + 1 = (x+1)(x^4 + x^3 + 1) + (x^3 + x)$$
$$x^{15} + 1 = (x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1)(x^4 + x^3 + 1)$$

Thus, f(x) has period 15 and so, is a primitive polynomial. States repeat themselves in each 15 state, thus length of LFSR is 15.

gcsd(21,15) is not 1, it is 3. Thus they do not generate a maximum period sequence.