Lab Notes 2 24 12

I. Euclidian Algorithm

a. Purpose: to find greatest common divisor

b. General equation: $r_{i-1} = r_i q_I + r_{i+1}$,

i. where $r_{i+1}$ is in the bounds $0 <= r_{i+1} < r_i$

Ex: a = 80, b= 35

Step 1:

Automatically, $r_0 = a$ and $r_1 = b$. Therefore, $r_0 = 80$ and $r_1 = 35$.

Variable track: $r_0 = 80$, r1 = 35

Step 2:

To find $r_2$, use $r_{i-1} = r_i q_I + r_{i+1}$.

$r_0 = r_1 q_1 + r_2$ where $r_0 = 80$, r1 = 35

$80 = 35q_1 + r_2$

$80 = 35(2) + 10$

$q_1 = 2$, $r_2 = 10$

Variable track: $r_0 = 80$, $r_1 = 35$, $r_2 = 10$, $q_1 = 2$

Step 3:

To find $r_3$, use use $r_{i-1} = r_i q_I + r_{i+1}$.

$r_1 = r_2 q_2 + r_3$

$35 = 10q_2 + r_3$

$35 = 10(3) + 5$

$q_2 = 3$, $r_3 = 5$

Variable track: $r_0 = 80$, $r_1 = 35$, $r_2 = 10$ $r_3 = 5$, $q_1 = 2$, $q_2 = 3$

Step 4:

To find $r_4$, use use $r_{i-1} = r_i q_I + r_{i+1}$.

$r_2 = r_3q_3 + r_4$

$10 = 5q_3 + r_4$

$10 = 5(2) + 0$

$q_3 = 2, r_4 = 0$

Variable track: $r_0 = 80, r_1 = 35, r_2 = 10, r_3 = 5, r_4 = 0, q_1 = 2, q_2 = 3, q_3 = 2$

However, once $r_i$ reaches 0, EA stops and returns the GCD of a and b, which is the $r_i$ *before* $r_i = 0$. In this case the gcd(80, 35) = $r_3 = 5$.
These two $r_i$'s, the 0 and the gcd, have special names in the EA. When you have reached 0, that $r_i$ is called $r_{\lambda+1}$ and the r that is the GCD is $r_\lambda$ . In fact, EA loops through different sets of $r_{i-1}$–$r_{i+1}$'s until it finds $r_{\lambda+1}$ , which is an $r_{i+1}$ that is 0. In this case, $r_\lambda = r_3 = 5$.

Ex2: a/d = 80/5 = 16, b/d = 35/5 = 7

Step 1:

$r_0 = 16, r_1 = 7$

Variable Track: $r_0 = 16, r_1 = 7$

Step 2:

Find $r_2$

$r_{i-1} = r_iq_I + r_{i+1}$

$r_0 = r_1q_1 + r_2$

$16 = 7q_1 + r_2$

$16 = 7(2) + 2$

$q_1 = 2, r_2 = 2$

Variable track: $r_0 = 16, r_1 = 7, r_2 = 2, q_1 = 2$

Step 3:

Find $r_3$

$r_{i-1} = r_i q_i + r_{i+1}$

$r_1 = r_2 q_2 + r_3$

$7 = 2q_2 + r_3$

$7 = 2(3) + 1$

$q_2 = 3, r_3 = 1$

Variable track: $r_0 = 16, r_1 = 7, r_2 = 2, r_3 = 1, q_1 = 2, q_2 = 3$

Step 4:

Find $r_4$

$r_{i-1} = r_i q_i + r_{i+1}$

$r_2 = r_3 q_3 + r_4$

$2 = 1q_3 + r_4$

$2 = 1(2) + 0$

$q_3 = 2, r_4 = 0$

Since $r_4 = 0$, $(\lambda + 1)$ is set to 4

$\lambda = 3$

Return $r_\lambda = r_3 = 1$

Variable track: $r_0 = 16, r_1 = 7, r_2 = 2, r_3 = 1, r_4 = 0, q_1 = 2, q_2 = 3, q_3 = 2$

As can be seen from this example, when a and b from the previous example are divided by their GCD and put again into EA some interesting things happen

1. $\lambda$ does not change, meaning EA performs the same amount of steps or operations
2. the set of $\{q\}_i^\lambda$ does not change
3. the set of remainders $\{r\}_i^\lambda$ from the first example goes to $\{r/d\}_i^\lambda$ in the second example
4. the $r_\lambda$ of the second equation is $(r_{\lambda/}\ r_\lambda)$ of the first equation

II. RSA Encryption

a. RSA is used because it is very hard to break

b. This is due to the fact that to break it, factoring large primes would be necessary.

   i. This is thought to be impossible or near impossible to do efficiently, although it has not been proven

c. How it works

   i. Take p and q, such that p and q are 2 distinct large primes
   $p = 61 \quad q = 153$

   ii. Then multiply them to attain n
   $n = p*q = 61*153 = 3233$

   iii. Then calculate $\phi(n) = (p-1)(q-1)$
   $\phi(n) = (p-1)(q-1) = 60*152 = 3120$
   (Note:This will always be an even number)

   iv. Choose an encryption key(called encryption exponent in the book) $e$, such that $0 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$
   $e = 17$

   v. Compute the decryption key(called decryption exponent in the book) $d$ such that $de \equiv 1 \pmod{\phi(n)}$

      1. This means $d$ is the multiplicative inverse of $e$ in the ring of residues mod $\phi(n)$ and as such, $d$ is unique

   $d = 2735$

   vi. Now the public key and the private key are as follows:
   Public Key ($n = 3233$, $e = 17$)
   Private Key($n = 3233$, $d = 2753$)

vii. How to encrypt a message m

1. Raise the message to the encryption key and take it mod n. Assign it to a variable c that will store the encrypted message

$c = m^e \pmod{n} = m^{17} \pmod{3233}$

viii. To Decrypt an encrypted message c

1. Raise c to $d$ and take it mod n

$m = c^d \pmod{n} = c^{2753} \pmod{3233}$

Ex:

$m = 65$

$c = 65^{17} \pmod{3233} = 2790$

$m = 2790^{2735} \pmod{3233} = 65$

$c^d \pmod{n} = (m^e)^d \pmod{n} = m \pmod{n}$ because $\gcd(n, \phi(n)) = 1$