CS1802 Week5: Inverse, Extended Euclid, RSA

Extended Euclid

i. What does it mean for two numbers to be relatively prime (also known as co-prime)?

Solution:
1. Both numbers a,b satisfy gcd(a, b) = 1

ii. Circle each pair that is relatively prime.
1. 17 and 35

2. 75 and 25

3. 423 and 23

Solution:
1. circled
2. not circled (gcd(75, 25) = 25)
3. circled

i. Previously, we computed used the Euclidean Algorithm (in week 4) to compute the gcd of two numbers. Now, compute using the Extended Euclidean Algorithm.

1. Compute by hand using the Extended Euclidean Algorithm the gcd(384, 42). You will find coefficients a and b (ax + by = gcd(a, b)) at the end of the problem. These will be useful when computing RSA.

Solution:
(a) $384 = 42(9) + 6$
(b) $42 = 6(7) + 0$ We can stop here, and look at the above line to find our gcd of 6.

(a) The backwards substitution goes as following.
(b) $6 = 384 - 42(9)$
(c) $6 = 384 + 42(-9)$
(d) $6 = 384 + (6(7) + 0)(-9)$
(e) $6 = 384 + (6(7))(-9)$
(f) $6 = 384 + 42(-9)$
(g) $6 = 384(1) + 42(-9)$
Inverses mod n For the following examples \((a, n)\) compute the inverse of \(a\) mod \(n\) in 3 ways:

A) by computing \(a^k\) powers up to the the order \(v\) s.t. \(a^v = 1\); the inverse \(a^{v-1} \mod n\)

B) compute gcd coeff \(x, y\) s.t. \(ax + ny = 1\) with Extended Euclid; then the inverse is \(x \mod n\)

C) factorize \(n\) then compute \(\varphi(n)\) with the formula below; the inverse is \(a^{\varphi(n)-1} \mod n\)

\[n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots \cdot p_t^{e_t}\]

\[\varphi(n) = p_1^{e_1-1}(p_1 - 1) \cdot p_2^{e_2-1}(p_2 - 1) \cdot p_3^{e_3-1}(p_3 - 1) \cdots \cdot p_t^{e_t-1}(p_t - 1)\]

1. \(a = 8\) mod \(n = 11\) (You may read this as “Find the multiplicative inverse of 8 mod 11”)

   **Solution:**

   \[8^2 = 64 = -2 = 9\]
   \[8^3 = 64 = -16 = -5 = 6\]
   \[8^4 = 4\]
   \[8^5 = 32 = -1\]
   \[8^{10} = 1\]

   order=10; inverse is \(8^9 = 4 \cdot -1 = -4 = 7\)

   \(n\) prime means \(\varphi(n) = n - 1 = 10\); same as the order in this case.

   **EXT EUCLID**

   \[
   \begin{array}{cccccc}
   a_i & b_i & q_i & r_i & x_i & y_i \\
   11 & 8 & 1 & 3 & 3 & -4 \\
   8 & 3 & 2 & 2 & -1 & 3 \\
   3 & 2 & 1 & 1 & 1 & -1 \\
   2 & 1 & 2 & 0 & 0 & 1 \\
   \end{array}
   \]

   GCD is 1

   -4=7 is the multiplicative inverse of 8 (mod 11)
2. \(a = 3 \mod n = 26\)

**Solution:**
\[
\varphi(26) = (2 - 1)(13 - 1) = 12 \text{ so } 3^{11} = 9 \text{ is the inverse}
\]
\[3^3 = 1; \text{ order}=3; \text{ inverse is } 3^2 = 9\]

**EXT EUCLID**

\[
\begin{array}{cccccc}
a_i & b_i & q_i & r_i & x_i & y_i \\
26 & 3 & 8 & 2 & -1 & 9 \\
3 & 2 & 1 & 1 & 1 & -1 \\
2 & 1 & 2 & 0 & 0 & 1 \\
\end{array}
\]

\GCD\ is 1. 9 is the multiplicative inverse of 3 (mod 26)

3. \(a = 28 \mod n = 36.\) Why there is no inverse here? Compute coef \((x, y)\) with Extended Euclid.

**Solution:**

**EXT EUCLID**

\[
\begin{array}{cccccc}
a_i & b_i & q_i & r_i & x_i & y_i \\
36 & 28 & 1 & 8 & -3 & 4 \\
28 & 8 & 3 & 4 & 1 & -3 \\
8 & 4 & 2 & 0 & 0 & 1 \\
\end{array}
\]

\GCD\=4
4. $a = 10 \mod n = 21$

**Solution:**
\[\varphi(21) = (3 - 1)(7 - 1) = 12\] so $10^{11} = 19$ is the inverse

$10^6 = 1; \text{order}=6; \text{inverse is } 10^5 = 19$

EXT EUCLID

\[
\begin{array}{ccccccc}
a_i & b_i & q_i & r_i & x_i & y_i \\
21 & 10 & 2 & 1 & 1 & -2 \\
10 & 1 & 10 & 0 & 0 & 1 \\
\end{array}
\]

GCD is 1

-2 is the multiplicative inverse of 10 (mod 21). Note: -2 = 19 (mod 21)
5. \(a = 100 \mod n = 143\)

**Solution:**
\[
\varphi(143) = (11 - 1)(13 - 1) = 120 \text{ so } 10^{119} = 133 \text{ is the inverse}
\]

\(100^3 = 1; \text{ order}=3; \text{ inverse is } 100^2 = 133\)

**EXT EUCLID**

\[
\begin{array}{cccccc}
a_i & b_i & q_i & r_i & x_i & y_i \\
143 & 100 & 1 & 43 & 7 & -10 \\
100 & 43 & 2 & 14 & -3 & 7 \\
43 & 14 & 3 & 1 & 1 & -3 \\
14 & 1 & 14 & 0 & 0 & 1 \\
\end{array}
\]

GCD is 1

-10 is the multiplicative inverse of 100 (mod 143). Note: -10 = 133 (mod 143)

---

**RSA**

i. Let us assume Alice is a bank and there is no such field of public key cryptography. If Alice has \(N\) vaults filled with money for her customers, how many keys does Alice need to keep track of for \(N\) customer who wants to withdraw or deposit from their vault when they send Alice a message?
**Solution:**

1. **N** keys total, one per person

ii. Now let us use make use of public key cryptography. Let us assume Alice can have any number of public and a private keys to access any of the bank vaults based on messages she retrieves. How many keys does Alice need to access a vault? Which key should she send out to her customers to communicate with the bank?

**Solution:**

1. Alice needs 1 public key and 1 private key. Alice should make her public key known for anyone whom wants to communicate with her bank. Anyone can use Alice’s public key to send a message (withdraw money, deposit, etc), and Alice uses her private key to decrypt the message and unlock the proper vault and perform a transaction.

iii. List the order of the steps for Alice to compute RSA below (Taken from your RSA notes!):

1. Alice stores the pair \((d, n)\) as the secret key, with \(DECODE_A(Y) = Y^d \mod n\).
2. Alice selects at random two large primes \(p\) and \(q\).
3. Alice publish the pair \((e, n)\) as the public key, with \(ENCODE_A(X) = X^e \mod n\).
4. Alice selects a small odd integer as public key \(e\) that is relatively prime to \(\varphi(n)\).
5. Alice computes \(\varphi(n) = \varphi(pq) = (p - 1)(q - 1)\).
6. Alice sets private key \(d\) so that \(de \mod (p - 1)(q - 1)\) equals 1.
7. Alice computes \(n = pq\)

**Solution:**

1. Alice selects at random two large primes \(p\) and \(q\).
2. Alice computes \(n = pq\).
3. Alice computes \(\varphi(n) = \varphi(pq) = (p - 1)(q - 1)\)
4. Alice selects a small odd integer \( e \) that is relatively prime to \((p - 1)(q - 1)\)

5. Alice sets \( d \) so that \( de \mod (p - 1)(q - 1) = 1 \)

6. Alice publish the pair \((e, n)\) as the public key, with \( P_A(M) = M^e \mod n \).

7. Alice stores the pair \((d, n)\) as the secret key, with \( S_A(E) = E^d \mod n \).

**iv.** What is at least one way we can be sure that RSA is secure? What strategies do we use to make it more secure?

**Solution:**

1. Generate sufficiently large random primes. The intuition provided to a student may be to choose two small primes \((p, q)\) and multiply them together (to get \( n \)). Then repeat with two large primes, and ask them which would take longer to find the prime factorization of \( n \). (Explain that a computer may take hundreds of years for a sufficiently large value of \( n \))

2. Do not make \( n \) (in the RSA public and private key) easily factored into primes \( p \) and \( q \).

3. Encode plain text messages with fixed-size random pad to encrypt the message (suggestion from text on p. 83)
v. Set up RSA for \( p = 5 \) and \( q = 13 \). Try \( e = 7, e = 3, e = 5 \) and see which one is most suitable as public key, then compute the private key \( d \).

For \( e = 5 \) encode and decode \( x = 2, x = 12, x = 16, x = 61 \).

Solution: \( n = 5 \times 13 = 65 ; \varphi(n) = (p - 1)(q - 1) = 48 \)

\( e = 7 \) is math-correct but gives \( d = 7 \) which is unfortunate, for a secret key to be the same as the public key makes it easy to guess.

\( e = 3 \) doesn’t work mathwise because \( \gcd(3, \varphi(pq)) = \gcd(3, (p - 1)(q - 1)) = \gcd(3, 48) \neq 1 \).

\( e = 5 \) works best, \( d = e^{-1} \mod{48} = 29 \)

\( y = encode(x = 2) = 2^5 \mod{65} = 32 \)
\( x = decode(y = 32) = 32^{29} \mod{65} = 2 \)

\( y = encode(x = 16) = 16^5 \mod{65} = 61 \)
\( x = decode(y = 61) = 61^{29} \mod{65} = 16 \)
**Primality test** for \( n \) using Fermats Theorem Converse (not always true, but often enough): pick several \( a \in \mathbb{Z}_n \) and compute \( a^{n-1} \mod n \)

- if any result is \( \neq 1 \) then declare "\( n \) is not prime for sure"
- if all results are 1 then declare "\( n \) is probably prime"

Use this primality test for the following examples. You can use a calculator.

A) \( n = 823 \), \( a \in \{2, 5, 10, 20, 100\} \)

**Solution:** \( 2^{822} = 2^9 \cdot 2^6 \cdot 2^4 \cdot 2^2 \cdot 2^1 = 1 \mod 823 \) etc; all calculations give 1. So the test gives "yes, prime" which is correct.

B) \( n = 307 \), \( a \in \{2, 7, 19, 20\} \)

**Solution:** \( 2^{306} = (2^{102})^3 = ((2^{17})^6)^3 = (290^6)^3 = 1^3 = 1 \mod 307 \) etc; all calculations give 1. So the test gives "yes, prime" which is correct.

C) \( n = 35 \), \( a \in \{6, 29, 34\} \)

**Solution:** \( 6^{34} = 1 \mod 35 \)
\( 29^{34} = 1 \mod 35 \)
\( 34^{34} = 1 \mod 35 \)
All calculations give 1. So the test gives "yes, prime" which is incorrect. If we were to try \( a = 5 \) or \( a = 7 \) obviously we would not get 1, why?

D) \( n = 45 \), \( a \in \{8, 19, 37, 17, 4\} \)
EXTRA : 10 wise men
10 wise men leave in a village; each man has a color dot on the forehead either R or B not known to him; knowing his color means immediate death. But everyone knows the other men’s colors, so B person sees 5R and 4B.

The men don’t speak/communicate to each other, but each morning they meet in a circle and they can see if anyone died. They are extremely smart (can infer anything) and know when someone dies its because he must have figured out his color.

For quite a few days this goes unchanged, until one day a stranger passes to the village and remarks ”the number of B colors is not 20”. Prove that eventually everyone in the village will figure out his color and die.

**hint1.** Put yourself in the shoes of a B wise man. He knows there are 5R and 4B, so what an R person sees?
- If you have B, the R person sees 5B and 4R : that implies a total 5B+5R
- If you have R, the R person sees 5R and 4B : that implies a total 4B+6R

An R person would kill himself the moment he figure out his color (R), and thats equivalent with figuring out which one of the two cases above is correct, or equivalent with figuring out that there are not a total of 6R.

How can an R person tell there are not 6R+4B total ? Well suppose there are 6R+4B (from his point of view that is possible). What would happen then ? What a different R person sees?

Let’s change the stranger statement to ”the number of B colors is not 10”. Show that the next morning everyone knows that ”the number of B colors is not 9”.

That first stranger statement ”the number of B colors is not 20” is not useful for reasoning. But this one ”the number of B colors is not 10” is. What is the difference?

**EXTRA** : implement Extended Euclid Algorithm in your favorite language. Easy choices: Python, Perl, Matlab.