Prime Proofs

Karim El Shenawy

February 2021

Introduction

This course notebook is the collection of theorem proofs, exercises and answers from Unit 5 of the Number Theory Through Inquiry (Mathematical Association of America Textbooks).

Introduction to Cryptography

5.1 Theorem

If p and q are distinct prime numbers and W is a natural number with $(W, pq) = 1$, then $W^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

Proof. Given p and q are distinct prime numbers and W is a natural number with $(W, pq) = 1$, we can deduce that $(W, p) = (W, q) = 1$, by Theorem 4.29. With that we can apply the Fermat's Little Theorem to showcase that $W^{p-1} \equiv 1 \pmod{p}$ and $W^{q-1} \equiv 1 \pmod{q}$. This also implies that $W^{(p-1)(q-1)} \equiv 1 \pmod{p}$ and similarly for $W^{(p-1)(q-1)} \equiv 1 \pmod{q}$. Therefore, by the Chinese Remainder Theorem, we can conclude that $W^{(p-1)(q-1)} \equiv 1 \pmod{pq}$. □

5.2 Theorem

If p and q are distinct prime numbers, k be a natural number, and W be a natural number less than pq. Then,

$$W^{1+k(p-1)(q-1)} \equiv W \pmod{pq}.$$

Proof. By direct proof, given p and q are distinct prime numbers, k be a natural

number, and W be a natural number less than pq which implies that $(W, pq) = 1$;

$$\begin{aligned} W^{1+k(p-1)(q-1)} &\equiv W \pmod{pq} \\ W^1 W^{k(p-1)(q-1)} &\equiv W \pmod{pq} \\ W^1 (W^{(p-1)(q-1)})^k &\equiv W \pmod{pq} \\ W^1 \cdot 1^k &\equiv W \pmod{pq} \qquad \textbf{By Theorem 5.1} \\ W^1 &\equiv W \pmod{pq} \\ W &\equiv W \pmod{pq} \end{aligned}$$

□

5.3 Theorem

Let p and q be distinct primes and E be a natural number relatively to $(p-1)(q-1)$*. Then there exist natural numbers D and y such that*

$$ED = 1 + y(p-1)(q-1).$$

Proof. Let p and q be distinct primes and E be a natural number relatively to $(p-1)(q-1)$, thus $(E, (p-1)(q-1)) = 1$. By Theorem 1.40, we can express $(E, (p-1)(q-1)) = 1$ as $Ea + b(p-1)(q-1) = 1, \exists a, b \in \mathbf{Z}$. Now, since Natural numbers fall under integers, we can say that given natural number D and y where $a = D$ and $b = -y$, then;

$$\begin{aligned} Ea + b(p-1)(q-1) &= 1 \\ ED - y(p-1)(q-1) &= 1 \\ ED &= 1 + y(p-1)(q-1) \end{aligned}$$

Thus, there exist natural numbers D and y such that $ED = 1 + y(p-1)(q-1)$. □

5.4 Theorem

Let p and q be distinct primes, W be a natural number less than pq, and E, D, and y be natural numbers such that $ED = 1 + y(p-1)(q-1)$*. Then*

$$W^{ED} \equiv W \pmod{pq}.$$

Proof. Let p and q are distinct primes and $W, E, D, y \in \mathbf{N}$ with $W < pq$ such that $ED = 1 + y(p-1)(q-1)$. Now, suppose $W^{ED} \equiv W \pmod{pq}$. By direct proof, we can show that this holds,

$$\begin{aligned} W^{ED} &\equiv W \pmod{pq} \\ W^{1+y(p-1)(q-1)} &\equiv W \pmod{pq} \qquad \textbf{Since, } ED = 1 + y(p-1)(q-1) \\ W &\equiv W \pmod{pq} \qquad \textbf{By Theorem 5.2} \end{aligned}$$

Thus, $W^{ED} \equiv W \pmod{pq}$ holds. □

5.5 Exercise

Consider two distinct primes p and q. Describe every step of RSA Public Key Coding System. State what numbers you choose to make public, what message can be encoded, how messages should be encoded, and how messages are decoded. What number should be called the encoding exponent and what number should be called the decoding exponent?

The following are the steps of the RSA Public Key Coding System;

1. Consider two distinct primes p and q thus $p \neq q$. Both primes must remain private.
2. Calculate n $\implies n = p \times q$. The value of n will be made public.
3. Calculate the Euler Totient Function of n, $\implies \phi(n) = (p-1) \times (q-1)$.
4. Select an integer E such that $gcd(E, \phi(n)) = gcd(E, (p-1)(q-1)) = 1$ where $1 < E < \phi(n)$. E will be set to public, thus making the **Public key** $= \{n, E\}$.
5. Calculate integer D where $1 < D < \phi(n)$ such that $D \equiv E^{-1} \pmod{\phi(n)}$ or $ED \equiv 1 \pmod{\phi(n)}$. D will be set to private, thus making the **Private key** $= \{n, D\}$.
6. To Encode, we consider a plaintext P, $0 < P < n$, and we calculate the ciphertext C with **the encoding exponent E**. Therefore, $C \equiv P^E \pmod{n}$.
7. To Decode, we consider a ciphertext C and we calculate the plaintext P with **the decoding exponent D**. Therefore, $P \equiv C^D \pmod{n}$.

5.6 Exercise

Describe an RSA Public Key Code System based on the primes 11 and 17. Encode and decode several messages.

The following are the steps of the RSA Public Key Coding System with primes 11 and 17;

1. Consider two distinct primes p and q where $p = 11$ and $q = 17$.
2. Calculate n $\implies n = p \times q = 11 \times 17 = 187$.
3. Calculate the Euler Totient Function of n, $\implies \phi(n) = \phi(187) = (11-1) \times (17-1) = 10 \times 16 = 160$.
4. Select an integer E such that $gcd(E, \phi(n)) = gcd(E, 160) = 1$ where $1 < E < 160$. Possible E values $3, 7, 9, 11, 13, 17, .., 159$. For simplicity, let $E = 7$. **Public key** $= \{187, 7\}$.

5. Calculate integer D where $1 < D < 160$ such that $D \equiv E^{-1} \pmod{\phi(n)}$ or $ED \equiv 1 \pmod{\phi(n)}$. We can calculate D by $D = \frac{(\phi(n)\cdot i)+1}{E}, \exists i \in \mathbf{Z}$.

$$D = \frac{(160 \cdot 1) + 1}{7} = 23, D \in \mathbf{Z} \qquad \mathbf{i = 1}$$
$$D = \frac{(160 \cdot 2) + 1}{7} = 45.857, D \notin \mathbf{Z} \qquad \mathbf{i = 2}$$

Thus, $ED \equiv 7(23) \equiv 161 \equiv 1 \pmod{160}$. **Private key** $= \{187, 23\}$.

6. To Encode, we consider a plaintext P, $0 < P < n$ and we calculate the ciphertext C with **the encoding exponent E**. Therefore, $C \equiv P^7 \pmod{187}$. Let's try encoding with following examples, for simplicity we will mostly use numerical plaintexts. However, we can also use plaintext in the form of numbers;

   - $P = 4$, $C \equiv 4^7 \equiv 115 \pmod{187}$
   - $P = 9$, $C \equiv 9^7 \equiv 70 \pmod{187}$
   - $P = 17$, $C \equiv 17^7 \equiv 85 \pmod{187}$
   - $P = BEES = \{2, 5, 5, 19\}$, $C \equiv \{2, 5, 5, 19\}^7 \equiv \{2^7 \pmod{187}, 5^7 \pmod{187}, 5^7 \pmod{187}, 19^7 \pmod{187}\} \equiv \{128, 146, 146, 145\} \pmod{187}$

7. To Decode, we consider a ciphertext C and we calculate the plaintext P with **the decoding exponent D**. Therefore, $P \equiv C^{23} \pmod{187}$. We will use the values from the encoding step.

   - $C = 115$, $P \equiv 115^{23} \equiv 4 \pmod{187}$
   - $C = 70$, $P \equiv 70^{23} \equiv 9 \pmod{187}$
   - $C = 85$, $P \equiv 85^{23} \equiv 17 \pmod{187}$
   - $C = \{128, 146, 146, 145\}$, $P \equiv \{128, 146, 146, 145\}^{23} \equiv \{128^{23} \pmod{187}, 146^{23} \pmod{187}, 146^{23} \pmod{187}, 145^{23} \pmod{187}\}$ $\equiv \{2, 5, 5, 19\} \pmod{187}$ which is "BEES".

5.7 Exercise

You are a secret agent. An evil spy with shallow number theory skills uses the RSA Public Key Coding System in which the public modulus is n = 1537, and the encoding exponent is E = 47. You intercept one of the the encoded secret messages being sent to the evil spy, namely the number 570. Using your superior number theory skills, decode this message, thereby saving countless people from the fiendish plot of the evil spy.

To decode the message we must do the following,

1. Since n and E are known, we can attempt to find the primes p and q such that $n = pq$ and $gcd(E, \phi(n)) = gcd(E, (p-1)(q-1)) = 1$. This can be done by factoring out 1537, $1537 = 29 \times 53$. Thus, $p = 29$ and $q = 53$. And $gcd(E, (p-1)(q-1)) = gcd(47, (29-1)(53-1)) = gcd(47, 1456) = 1$ is true.

2. Now, we can attempt to calculate integer D since we know that $D \equiv E^{-1} \pmod{\phi(n)}$ or $ED \equiv 1 \pmod{\phi(n)}$. We can calculate D by $D = \frac{(\phi(n)\cdot i)+1}{E}, \exists i \in \mathbf{Z}$.

$$D = \frac{(1456 \cdot 1) + 1}{47} = 31, D \in \mathbf{Z} \qquad \mathbf{i = 1}$$
$$D = \frac{(1456 \cdot 2) + 1}{47} = 61.978, D \notin \mathbf{Z} \qquad \mathbf{i = 2}$$

Thus, $ED \equiv 47(31) \equiv 1457 \equiv 1 \pmod{1456}$. **Private key** $= \{31, 1537\}$.

3. Now we can decode the ciphertext 570, since $P \equiv C^D \pmod{n}$. Thus,

$$P \equiv 570^{31} \equiv 131 \pmod{1537}$$

Thus the decoded message is 131, which can possibly be "ACA" or "MA".

5.8 Exercise

Suppose an RSA Public Key Coding System publishes n (which is equal to the product of two undisclosed primes p and q) and E, with E relatively prime to (p-1)(q-1). Suppose someone wants to send a secret message and so encodes the message number W (less than n) by finding the number m less than n such that $m \equiv W^E \pmod{n}$. Suppose you intercept this number m and you are able to factor n. How can you figure out the original message W?

We know n, $\phi(n)$ and encoded exponent E. Also we are able to factor p and q from n. This also allows us to calculate the decoded exponent D since we know that $D \equiv E^{-1} \pmod{\phi(n)}$ or $ED \equiv 1 \pmod{\phi(n)}$. (We can use the same method used to find D in Exercise 5.7).
Now, since $m \equiv W^E \pmod{n}$ and we have m but we want to find W. We can obtain W by $m^D \pmod{n}$. By direct proof,

$$\begin{aligned} m &\equiv W^E \pmod{n} \\ m^{D \pmod{\phi(n)}} &\equiv W^{ED \pmod{\phi(n)}} \pmod{n} \\ m^D &\equiv W^1 \pmod{n} \qquad \textbf{Since } ED \equiv 1 \pmod{\phi(n)} \\ m^D &\equiv W \pmod{n} \end{aligned}$$

5.9 Application Exercise

You have seen the application of number theory to RSA cryptography. Find out all you can about the role of number theory in some other types of "codes" such as bar codes, ISBN codes, and credit card number "codes."

They are instances of Number Theory in many real world applications. Notably, in credit cards which use the Luhn Fromula to verify transactions. It

works as such; given a credit card number, it doubles each-other number starting from the right and sum the digits of those doubled numbers if they result into 2 digits. With this new string of numbers, sum all the numbers together, if the number is divisible by 10 then the credit card number is valid.

Furthermore, Number Theory is also used in ISBN codes for inventory tracking. ISBN codes consist of two types, ISBN-10 (10 digits) and ISBN-13 (13 digits). Both have similar digit structure. However, these codes use number theory to be verified. For ISBN-10, given a code of $x_1, ..x_10$, the verification theorem is

$$\sum 10i = 1ix_i \equiv 0 \pmod{11}$$

Now for ISBN-13, given a code with digits $x_1, .., x_i, x_13$ is verified by multiplying each odd i with 1 and each even i with 3 and then summing them to see if they come to 0 modulo 10,

$$x_1+3x_2+x_3+3x_4+x_5+3x_6+x_7+3x_8+x_9+3x_10+x_11+3x_12+x_13 \equiv 0 \pmod{10}$$

Letters and Numbers

5.1.1 Exercise

Can you find a method for representing an alphabetic message as a number? Note that this message must avoid ambiguity arising from use of the same number to represent different words. For example, as you can see from Table 5.1, the word YES (25, 5, 19) could be written as 25519, but this number could also be (2, 5, 5, 19) (BEES)[1]

There are multiple ways we can represent numbers. We can keep their numerical representation as a set, for instance $BEES = \{2, 5, 5, 19\}$. Another way would be to divide all numbers in each group. Then each letter representation would consist of 2 values, (n, p). n would be which group and p can be the number in that group. For instance let the first group be $\{A, B, C, D, E, F, G, H\}$, the second group would be $\{I, J, K, L, M, N, O, P\}$ and the third group would be the rest. Now, lets represent "GOOD", G = (1, 7), O = (2, 7) and D = (1, 4). Thus "GOOD" can be $(1, 7) + 2(2, 7) + (1, 4)$.

5.1.2 Exercise

Using nothing other than pencil, paper and pocket calculator, factor the numbers below

- $731 = 17 \times 43$
- 9,379 (Extremely without calculator)
- 19,493 (Extremely without calculator)
- 21,877 (Extremely without calculator)

5.1.3 Exercise

You have intercepted the following message encrypted using an RSA public key system. The public key is 21,877. The original message is given in terms of two numbers derived from the number-letter correspondences of Table 5.2. The encoded message is (13318, 12932).

From the public key 21,877, we know that n is 21877, thus p = 131, q = 167 and $\phi(n) = (130)(166) = 21580$. Also, we can calculate the encoding exponent, E, such that $gcd(E, \phi(n)) = gcd(E, 21580) = 1$ where $1 < E < 21580$. Possible E values $3, 7, 9, 11, 17, .., 21579$. For simplicity, let $E = 7$. **Public key =** $\{21877, 7\}$.

Now, we need to calculate the decoding exponent D where $1 < D < 21580$ such that $D \equiv E^{-1} \pmod{\phi(n)}$ or $ED \equiv 1 \pmod{\phi(n)}$. We can calculate D by $D = \frac{(\phi(n) \cdot i)+1}{E}, \exists i \in \mathbf{Z}$.

$$D = \frac{(21580 \cdot i) + 1}{7} = 3083, 1 < D < 21580 \qquad \mathbf{i = 1}$$

$$D = \frac{(12 \cdot 73) + 1}{7} = 6165.857, D \in \mathbf{Z} \qquad \mathbf{i = 2}$$

Thus, $ED \equiv 7(3083) \equiv 21581 \equiv 1 \pmod{21580}$. **Private key =** $\{187, 3083\}$.

Moreover, we can decode the encoded message,

- $13318^{3083} \equiv 11725 \pmod{21877}$
- $12932^{3083} \equiv 1948 \pmod{21877}$

Thus, the original message is (11725, 1948).

5.1.4 Exercise

In Exercise 5.6 on page 68 of the textbook, you devised a public key encryption system based on the prime numbers 11 and 17. Suppose that you use Table 5.2 to generate the numerical representation (8535, 1221) of the message HOME. What problem do you encounter in attempting to encrypt this message? Can you think of a way to resolve this problem?

From Exercise 5.6, we know that that n is 187, the encoding exponent E is 7 and the decoding exponent d is 23. Le's encrypt,

$$P = (8535, 1221), C \equiv (8535^7 \pmod{187}, 1221^7 \pmod{187}) \equiv (120, 176).$$

The issue is that we are unable to convert the encryption to letters. Since the table reference part of encoded message results to 176. Thus, we are unable to reference the last 2 digits of our encrypted message back to the table. A way top resolve this is by not encrypting the reference number. However, this will create a vulnerability in the system since an attacker knows from which table is each letter of the original message.