Number Theory Basics

CHAPTER 2

Motivation

- Public key cryptography is based on large primes that have to be generated & tested using modular arithmetic.
- Fermat & Euler's work is used to prime or relatively prime numbers.
- Euclid's algorithm finds multiplicative inverses that are needed to find appropriate encryption keys in public key cryptography.

Divisibility

Definition 2.1.1

Let $a, b \in \mathbb{Z}$ and $a \neq 0$. We say a divides b if there exists $k \in \mathbb{Z}$ such that $b = ak$. This is denoted by $a|b$.

Example 2.1.1

3|15, -15|60, $7 \nmid 18$

Proposition 2.1.1

Let $a, b, c \in \mathbb{Z}$.

For every $a \neq 0$, $a|0$ and $a|a$. Also $1|b$ for every b.

If $a|b$ and $b|c$ then $a|c$.

If $a|b$ and $a|c$ then $a|(sb + tc)$ where $s, t \in \mathbb{Z}$.

Proof:

Divisibility

Q: Which of the following is true?

1. $77 \mid 7$
2. $7 \mid 77$
3. $24 \mid 24$
4. $0 \mid 24$
5. $24 \mid 0$

Greatest Common Divisor

Definition: The greatest common divisor (gcd) for two integers a and b is the largest integer dividing a and b.

<u>Example 2.1.2</u>

gcd(4,6) = 2, gcd(5,7) = 1, gcd(24,60) = 12

Definition 2.1.2

2 integers a and b are relative prime if gcd(a,b) = 1.

Euclidean algorithm

Definition

This is a method to find the gcd of 2 integers.

As an example , let’s say we want to find gcd(a,b) and a>b.

Step 1

Divide a by b. Determine the remainder. We will have

$$a = q_1 b + r_1$$

Step 2

If $r_1 = 0$ then

If $r_1 \neq 0$, continue by dividing b with r_1. We will have

$$b = q_2 r_1 + r_2$$

Step 3

If $r_2 = 0$,

$\gcd(a, b) = r$, else do

$$r_1 = q_3 r_2 + r_3$$
$$\vdots$$
$$r_{k-2} = q_k r_{k-1} + r_k$$
$$r_{k-1} = q_{k+1} r_k + 0$$

So, $\gcd(a, b) = r_k$.

Euclidean algorithm

Example 2.1.3

Compute $gcd(482,1180)$.

$$1180 = 2(482) + 216$$
$$482 = 2(216) + 50$$
$$216 = 4(50) + 16$$
$$50 = 3(16) + 2$$
$$16 = 8(2)$$

This is the gcd

That is, gcd(482,1180) = 2.

Example 2.1.4

Compute gcd(12345,11111).

Euclidean algorithm

Solving $\boldsymbol{ax + by = d}$.

In the above Euclidean algorithm we did not use the quotients q_i.

Theorem 2.1.2

Let $a, b \in \mathbb{Z}$ with at least one of the numbers is non-zero and let $\gcd(a, b) = d$.

Then there exists $x, y \in \mathbb{Z}$ such that $ax + by = d$ (x and y can be either positive or negative).

Example 2.1.5

$\gcd(4,6) = 2$. There exists $x = -1, y = 1$ such that $4x + 6y = 2$

Euclidean algorithm

Example 2.1.6

Determine $\gcd(748{,}2024)$ and find the two integers $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(748{,}2024)$.

To solve $ax + by = \gcd(a, b)$ where $a < b$. We need to use an algorithm called **extended Euclidean algorithm**.

Extended Euclidean algorithm

Solve $ax + by = \gcd(a, b)$ where $a < b$.

- **Step 1**

Divide a into b (i.e. $\frac{b}{a}$).

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\vdots$$
$$r_{k-2} = q_k r_{k-1} + r_k$$
$$r_{k-1} = q_{k+1} r_k + 0$$

- **Step 2**

  Set $x_0 = 0$, $x_1 = 1$ and $x_j = -q_{j-1} x_{j-1} + x_{j-2}$.

  Set $y_0 = 1$, $y_1 = 0$ and $y_j = -q_{j-1} y_{j-1} + y_{j-2}$

- **Step 3**

  Then $ax_n + by_n = \gcd(a, b)$.

Extended Euclidean algorithm

Example 2.1.7

Find

$$\gcd(4,6)$$

$$\gcd(6,21)$$

$$\gcd(748,2024)$$

Extended Euclidean algorithm

Remark 2.1.1

We will define the solution pair (x_n, y_n) as the initial solution for

$ax + by = \gcd(a, b)$. We re-denote as (X_0, Y_0).

We define the **general solution** for $ax + by = \gcd(a, b)$ as

$$X = X_0 + bt \text{ and } Y = Y_0 - at \text{ where } t \in \mathbb{Z}.$$

That is for any $t \in \mathbb{Z}$, (X, Y) will always satisfy $ax + by = \gcd(a, b)$.

Example 2.1.8

Try to find gcd(12345,11111) and solve 12345x + 11111y = gcd(12345,11111).

Modular Arithmetic

2.2.1 <u>Congruence</u>

<u>Definition 2.2.1</u>

Let $a, b, n \in \mathbb{Z}$ and $n \neq 0$. We say $a \equiv b (\text{mod } n)$ if $\frac{a-b}{n} = k \in \mathbb{Z}$.

<u>Example 2.2.1</u>

$$32 \equiv 7 (\text{mod } 5)$$

Modular Arithmetic

Proposition 2.2.1

Let $a, b, n \in \mathbb{Z}$ and $n \neq 0$.

i) $a \equiv a (\text{mod } n)$

ii) $a \equiv b (\text{mod } n)$ implies $b \equiv a (\text{mod } n)$

iii) If $a \equiv b (\text{mod } n)$ and $b \equiv c (\text{mod } n)$ then $a \equiv c (\text{mod } n)$.

Proof:

Modular Arithmetic

Arithmetic operations

i. [(a mod n) + (b mod n)] mod n = (a + b) mod n

ii. [(a mod n) - (b mod n)] mod n = (a - b) mod n

iii. [(a mod n) x (b mod n)] mod n = (a x b) mod n

Modular Arithmetic

Remark 2.2.1

Cryptography thought in this course will work with the integers modulo n. They are denoted by $\mathbb{Z}_n$ or also as $\mathbb{Z}/n\mathbb{Z}$.

$$\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$$

Example 2.2.2

Generate the addition and multiplication table modulo 10.

Modular Arithmetic

- **Rules for Addition, Modulo 10**

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Modular Arithmetic

2.2.1.1 <u>Division in modular arithmetic</u>

<u>Proposition 2.2.2</u>

Let $a, b, n \in \mathbb{Z}$ and $n \neq 0$ with $ab \equiv ac (\text{mod } n)$ then

$$b \equiv c (\text{mod } n).$$

<u>Proof</u>:

<u>Example 2.2.5</u>

Solve $2x + 7 \equiv 3 (\text{mod } 17)$. (Note: please observe gcd$(2,17)$)

Modular Arithmetic

Proposition 2.2.3

Suppose $\gcd(a, n) = 1$. Let $s, t \in \mathbb{Z}$ such that $as + nt = 1$ (s and t can be found using the extended Euclidean algorithm).

If $as \equiv 1 (\text{mod } n)$, then s is the multiplicative inverse for $a (\text{mod } n)$.

Proof:

Inverses

- When we are working in modular arithmetic, we often need to find the inverse of a number relative to an operation.
- We are normally looking for an additive inverse (relative to an addition operation) or a multiplicative inverse (relative to a multiplication operation).

Inverses - Additive Inverses

- In Z_n, two numbers a and b are additive inverses of each other if

$$a + b \equiv 0 \pmod{n}$$

Note

In modular arithmetic, each integer has an additive inverse. The sum of an integer and its additive inverse is congruent to 0 modulo n.

Inverses - Additive Inverses

- Example:

    Find all additive inverse pairs in Z10.

Solution

The six pairs of additive inverses are (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).

Inverses

- Multiplicative Inverse

In Z_n, two numbers a and b are the multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

Note

In modular arithmetic, an integer may or may not have a multiplicative inverse. When it does, the product of the integer and its multiplicative inverse is congruent to 1 modulo n.

Inverses - Multiplicative Inverses

- Example

  Find the multiplicative inverse of 8 in Z_{10}.

- Solution

  There is no multiplicative inverse because gcd (10, 8) = 2 ≠ 1. In other words, we cannot find any number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.

- Example:

  Find all multiplicative inverses in Z_{10}

- Solution

  There are only three pairs: (1, 1), (3, 7) and (9, 9). The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse.

Inverses in Cryptography

We will use one number to encrypt and its inverse to decrypt.

Consider an input string to be encrypted = 3692.

Add a constant mod 10 to map the string to a new string (character by character).

$(3 + 6) \bmod 10 = 9$

$(6 + 6) \bmod 10 = 2$

$(9 + 6) \bmod 10 = 5$

$(2 + 6) \bmod 10 = 8$

The encrypted string for 3692 = 9258

Inverses in Cryptography

Now use the additive inverse of 6; it is $6 + x = 0$; $x = 4$
to decrypt (inverse is taken from the table).

$(9 + 4) \bmod 10 = 3$
$(2 + 4) \bmod 10 = 6$
$(5 + 4) \bmod 10 = 9$
$(8 + 4) \bmod 10 = 2$ The encrypted string is decrypted!

This is a simple substitution cipher (e.g., Caesar). The only difference is numbers were used instead of letters.

But – easy to break – lets do something harder!

Inverses in Cryptography - Multiplicative

x	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

If this works like addition, we should be able to encrypt and decrypt. Trouble is, it only works part of the time.

We can encrypt/decrypt some, but not all, numbers.

Inverses in Cryptography - Multiplicative

Encrypt the string 8732 using a multiplicative constant of:
5 mod 10

(8 x 5) mod 10 = 0; (40/10 = 4, 0)
(7 x 5) mod 10 = 5; (35/10 = 3, 5)
(3 x 5) mod 10 = 5; (15/10 = 1, 5)
(2 x 5) mod 10 = 0; (10/10 = 1, 0)

So the encrypted string would be 0550.

Trouble is, half the characters mapped to 0 and half to 5.
We might guess this is a problem since results are not unique.

Inverses in Cryptography - Multiplicative

However, if we use 3 mod 10 we get unique results:

(8 x 3) mod 10 = 4; (24/10 = 2, 4)
(7 x 3) mod 10 = 1; (21/10 = 2, 1)
(3 x 3) mod 10 = 9; (9/10 = 0, 9)
(2 x 3) mod 10 = 6; (6/10 = 0, 6)

The result is 4196.

This looks better, but do inverses work?

Can we decrypt?

Inverses in Cryptography - Multiplicative

The multiplicative inverse of n is m, where (n x m) mod 10 = 1.

The multiplicative inverse of 3 is (3 x m) mod 10 = 1;
so m = 7. Decrypting 4196 (previous slide) using 7 :

(4 x 7) mod 10 = 8
(1 x 7) mod 10 = 7
(9 x 7) mod 10 = 3
(6 x 7) mod 10 = 2; So… the inverse decrypts the cipher!

What is the condition that makes 3 work and 5 not work?

Inverses in Cryptography - Multiplicative

Why 3 works.

If (a x b) $\equiv$ (a x c) mod n, then b $\equiv$ c mod n, if and only if (iff) a is relatively prime to n.

Because ((a^{-1}) x a x b) $\equiv$ ((a^{-1}) x a x c) mod n = b $\equiv$ c mod n

This is in accordance with Fermat's theorem.

That is, a mod n will not produce a complete & unique set of residues if a & n have any factors in common except 1!

Exercises

Example 2.2.3

Solve $x + 5 \equiv 9 (\text{mod } 20)$

Example 2.2.4

Solve $x + 7 \equiv 3 (\text{mod } 17)$

Example 2.2.6

Solve $5x + 6 \equiv 13 (\text{mod } 11)$

Example 2.2.7

Solve $11111x \equiv 4 (\text{mod } 12345)$

The Chinese Remainder Theorem

Let us examine the following congruence relation

$$x \equiv 25 (\text{mod } 42)$$

This means there exists $k \in \mathbb{Z}$ such that

$$x = 25 + 42k \tag{1}$$

Let us re-write $42 = 7 \cdot 6$. We can have equation (1) becoming

$$x = 25 + 7(6k) \tag{2}$$

OR

$$x = 25 + 6(7k) \tag{3}$$

From (2) we can have

$$x \equiv 25 \equiv 4 (\text{mod } 7)$$

From (3) we can have

$$x \equiv 25 \equiv 1 (\text{mod } 6)$$

The Chinese Remainder Theorem

Therefore we can say that

$$x \equiv 25 (\text{mod } 42) = \begin{cases} x \equiv 4 (\text{mod } 7) \\ x \equiv 1 (\text{mod } 6) \end{cases}$$

The Chinese Remainder Theorem will reverse this process.

That is, a system of congruences can be replaced by a single congruence (But under certain conditions).

The Chinese Remainder Theorem

<u>Theorem 2.3.1</u> (The Chinese Remainder Theorem)

Suppose $\gcd(m, n) = 1$ Given $a, b \in \mathbb{Z}$ there exists exactly one solution $x(\text{mod } mn)$ to the simultaneous congruence

$$x \equiv a(\text{mod } m)$$

$$x \equiv b(\text{mod } n)$$

<u>Proof:</u>

The Chinese Remainder Theorem

Example 2.3.1

Solve

$$x \equiv 3(\text{mod } 7)$$
$$x \equiv 5(\text{mod } 15)$$

Solution:

We can observe that $\gcd(7,15) = 1$ and $mn = 105$. What is x congruent to modulo 105????

List down numbers congruent $3(\text{mod } 7)$: 3, 10, 17, 24, 31, 38, 45, 52, 59, 66, 73, 80, 87, 94, 101,…

List down numbers congruent $5(\text{mod } 15)$: 5, 20, 35, 50, 65, 80, 95,…

Thus, $x \equiv 80(\text{mod } 105)$

The Chinese Remainder Theorem

THE BIG QUESTION IS:

WHAT ABOUT FOR LARGE NUMBERS???

MAKING A LIST LIKE THE ONE ABOVE WOULD BE IN-EFFICIENT!!!!

Let's look back at the question: Find a solution for

$$x \equiv a (\text{mod } m) \qquad (1)$$

$$x \equiv b (\text{mod } n) \qquad (2)$$

Such that

$$x \equiv y (\text{mod } mn)$$

(i.e. x is congruent to y modulo mn)

From (1)

$$x = a + mk \qquad (3)$$

The Chinese Remainder Theorem

(3) and (2) we have:

Solve

$$a + mk \equiv b (\text{mod } n)$$

That is,

$$mk \equiv b - a (\text{mod } n)$$

Since $\gcd(m, n) = 1$ there exists a multiplicative inverse i for $m(\text{mod } n)$.

So,

$$imk \equiv (b - a)i (\text{mod } n)$$

and

$$k \equiv (b - a)i (\text{mod } n)$$

All answers are obtained by adding and subtracting multiples of *mn* to the particular answer.

Substituting back into (3)

$$x = a + m(b - a)i \equiv a + m(b - a)i (\text{mod } mn)$$

$$x = \cdots, [a + m(b - a)i] - 2mn, \qquad [a + m(b - a)i] - mn,$$
$$[a + m(b - a)i] + mn, [a + m(b - a)i] + 2mn \ , \ldots \ \blacksquare$$

The Chinese Remainder Theorem

Example 2.3.2

Let us try for small numbers first. Solve

$$x \equiv 1 (\text{mod } 5) \qquad (1)$$

$$x \equiv 9 (\text{mod } 11) \qquad (2)$$

From (1)

$$x = 1 + 5k_1 \qquad (3)$$

(3) into (2)

$$1 + 5k_1 \equiv 9 (\text{mod } 11)$$

$$5k_1 \equiv 8 (\text{mod } 11) \qquad (4)$$

Multiply both sides of (4) with inverse of $5 (\text{mod } 11)$

Thus,

$$k_1 \equiv 72 \equiv 6 (\text{mod } 11)$$

and

$$x \quad = 1 + 5 \cdot 6 \equiv 31 (\text{mod } 55)$$

The Chinese Remainder Theorem

<u>Example 2.3.3</u>

Solve

$$x \equiv 7 (\text{mod } 563)$$
$$x \equiv 3 (\text{mod } 219)$$

<u>Solution:</u>

Try.

Assignment

The Chinese Remainder Theorem

Theorem 2.3.2 (The Chinese Remainder Theorem – General Form)

Let $m_1, \dots, m_k \in \mathbb{Z}$ with $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. Given $a_1, \dots, a_k \in \mathbb{Z}$ there exists exactly on solution $x \pmod{m_1 m_2 \cdots m_k}$ to the simultaneous congruences $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$,…, $x \equiv a_k \pmod{m_k}$.

Example 2.4.4

Solve

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{7}$$

$$x \equiv 4 \pmod{16}$$

The Chinese Remainder Theorem

Remark 2.3.1

How do you use the Chinese remainder theorem????

Suppose you want to solve $x^2 \equiv 1 (\text{mod } 35)$. Since

$$x^2 \equiv 1 (\text{mod } 35) = \begin{cases} x^2 \equiv 1 (\text{mod } 7) \\ x^2 \equiv 1 (\text{mod } 5) \end{cases}$$

Observe that $x^2 \equiv 1 (\text{mod } 7)$ has 2 solutions, $x \equiv \pm 1 (\text{mod } 7)$ and for $x^2 \equiv 1 (\text{mod } 5)$ we have $x \equiv \pm 1 (\text{mod } 5)$.

We can arrange them in 4 ways:

$$\begin{aligned} x &\equiv 1 (\text{mod } 5), & x &\equiv 1 (\text{mod } 7) \Rightarrow x \equiv 1 (\text{mod } 35) \\ x &\equiv 6 \equiv 1 (\text{mod } 5), & x &\equiv 6 \equiv -1 (\text{mod } 7) \Rightarrow x \equiv 6 (\text{mod } 35) \\ x &\equiv 29 \equiv -1 (\text{mod } 5), & x &\equiv 29 \equiv 1 (\text{mod } 7) \Rightarrow x \equiv 29 (\text{mod } 35) \\ x &\equiv 34 \equiv -1 (\text{mod } 5), & x &\equiv 34 \equiv -1 (\text{mod } 7) \Rightarrow x \equiv 34 (\text{mod } 35) \end{aligned}$$

So, solutions of $x^2 \equiv 1 (\text{mod } 35)$ are $x \equiv 1, 6, 29, 34$ (mod 35).

Square roots

Consider the following:

$$x^2 \equiv 71 (\text{mod } 77)$$

Or more generally

$$x^2 \equiv b (\text{mod } n)$$

Where $n = pq$ is the product of primes.

Remark 2.4.1

When we say $x^2 \equiv b (\text{mod } n)$ it means that x is a square root of b modulo n.

As in the "normal" situation such as $2^2 = 4$ means 2 is a square root of 4.

$6^2 = 36$ means 6 is a square root of 36

Square roots

<u>Proposition 2.4.1</u>

Let $p \equiv 3 (\text{mod } 4)$ be a prime and let $y \in \mathbb{Z}$. Let $x \equiv y^{\frac{(p+1)}{4}} (\text{mod } p)$.

If y has a square root mod p, then the square roots of y mod p are $\pm x$.

If y has a no square root mod p, then $-y$ has a square root mod p, then the square roots of $-y$ mod p are $\pm x$.

<u>Proof:</u>

Square roots

Example 2.4.1

Find square root of 5 mod 11.

Solution:

$\frac{(p+1)}{4} = 3$. Compute $x \equiv 5^3 (\mathrm{mod}\ 11)$ and we get $4^2 \equiv 5 (\mathrm{mod}\ 11)$.

So, the square roots of 5 mod 11 are ± 4.

Example 2.4.2

Find the square roots of 2 mod 11.

Solution:

$\frac{(p+1)}{4} = 3$. Compute $\mathrm{x} \equiv 2^3 (\mathrm{mod}\ 11)$ and we get $8^2 \equiv 9 \equiv -2 (\mathrm{mod}\ 11)$.

We found the square root of -2 mod 11, that is 8. Thus, 2 has no square root mod 11.

Square roots

Now let's consider square roots for a composite modulus.

Note that $\mathrm{x}^2 \equiv 71 (\mathrm{mod}\ 77)$ means that $\mathrm{x}^2 \equiv 71 \equiv 1 (\mathrm{mod}\ 7)$ and $\mathrm{x}^2 \equiv 71 \equiv 5 (\mathrm{mod}\ 11)$.

Note: $\frac{(p+1)}{4} = 3$, $\pm$ x $\equiv 5^3\ (mod\ 11) = 4$

Therefore, $\mathrm{x} \equiv \pm 1 (\mathrm{mod}\ 7)$ and $\mathrm{x} \equiv \pm 4 (\mathrm{mod}\ 11)$.

By CRT, we can have the solution set (4 answers):

$$\mathrm{x} \equiv \pm 15, \pm 29\ (\mathrm{mod}\ 77)$$