Number Theory and Cryptography

Dit-Yan Yeung

Department of Computer Science and Engineering
Hong Kong University of Science and Technology

COMP 2711: Discrete Mathematical Tools for Computer Science

Contents

Cryptography

Cryptography is the study of methods for secure communication between **senders** and **receivers** in the presence of **adversaries**.

The original message is called the **plaintext** and the encrypted message is called the **ciphertext**.

The **security strength** of a cryptosystem is tied to the amount of computing power needed to break it.

Mod

One of the oldest private-key cryptosystems is the **Caesar cipher**, which can be implemented using a scheme known as **arithmetic mod** n.

Definition

For an integer m and a positive integer n,

$$m \bmod n$$

is the smallest nonnegative integer r such that $m = nq + r$ for some integer q.

Euclid's Division Theorem

Theorem 1.1 (Euclid's division theorem)

Let n be a positive integer. Then for every integer m, there exist unique integers q and r such that $m = nq + r$ and $0 \leq r < n$.

Definition

In the equality given in Euclid's division theorem, m is called the **dividend**, n is called the **divisor**, q is called the **quotient**, and r is called the **remainder**.

Examples

Example 1

To compute 10 mod 7, we note that $10 = 7 \cdot 1 + 3$ and hence $10 \bmod 7 = 3$.

Example 2

To compute -10 mod 7, we note that $-10 = 7 \cdot (-2) + 4$ and hence $-10 \bmod 7 = 4$.

Remark

In general $(-m) \bmod n \neq -(m \bmod n)$.

Example

Example 3

Using 0 for A, 1 for B, and so on, let the numbers from 0 to 25 stand for the 26 letters of the English alphabet. In this way, a message can be represented as a sequence of strings of numbers. For example, the word SEA is represented as the string 18 4 0. What does the numerical representation of this word become if every letter is shifted 10 places to the right? What character string does it represent?

Remarks

Remark

To implement a Caesar cipher with shift s, each number n corresponding to a letter in the plaintext generates the number $(n + s) \bmod 26$ for the ciphertext.

Every private-key cryptosystem requires the sender and receiver to share a **codebook** in advance.

Public Key and Secret Key

Public-key cryptography overcomes the limitations of private-key cryptography by eliminating the need for agreeing on a secret code in advance between the sender and receiver.

Two parties (Alice and Bob) each have a pair of keys, a **public key** and a **secret key**:

Alice's public key:	KP_A
Alice's secret key:	KS_A
Bob's public key:	KP_B
Bob's secret key:	KS_B

Encryption and Decryption Functions

Let P_A, S_A, P_B, and S_B denote the (encryption or decryption) functions associated with the keys KP_A, KS_A, KP_B, and KS_B, respectively.

We require that each key pair be chosen such that, for any message M,

$$S_A(P_A(M)) = P_A(S_A(M)) = M$$
$$S_B(P_B(M)) = P_B(S_B(M)) = M.$$

In other words, the two functions corresponding to each key pair are **inverse functions** of each other.

Encryption and Decryption Functions (cont'd)

1. Alice sends Bob a message M: Alice uses Bob's public key KP_B to encrypt M to create the ciphertext $C = P_B(M)$.
2. Bob decrypts the encrypted message C: Bob uses his secret key KS_B to decrypt C to restore the original message $M = S_B(C) = S_B(P_B(M))$.

Modular Arithmetic

Definition

Let i and j be integers and n be a positive integer. Then i is **congruent** to j modulo n, denoted by $i \equiv j \pmod{n}$, if n divides $i - j$. If i and j are not congruent modulo n, we write $i \not\equiv j \pmod{n}$.

Theorem 1.2

Let i and j be integers and n be a positive integer. Then $i \equiv j \pmod{n}$ if and only if $i \bmod n = j \bmod n$.

Proof

Proof.

By Euclid's division theorem, there exist unique integers q, q', r, and r', with $0 \le r < n$ and $0 \le r' < n$, such that

$$\begin{aligned} i &= nq + r \\ j &= nq' + r'. \end{aligned}$$

By subtracting, we get

$$\begin{aligned} i - j &= n(q - q') + (r - r') \\ \frac{i-j}{n} &= q - q' + \frac{r - r'}{n}, \end{aligned}$$

where $r - r'$ is an integer such that $-(n-1) \le r - r' \le n - 1$.

Proof (cont'd)

Proof (cont'd).

Since $n \mid (i - j)$ by definition, the left-hand side of the above equation is an integer. We note that the only way for the right-hand side to be an integer is when $r - r' = 0$, or $r = r'$. Because $r = i \bmod n$ and $r' = j \bmod n$, we can conclude that $i \bmod n = j \bmod n$. □

Lemma

Lemma 1.3

$i \bmod n = (i + kn) \bmod n$ for any integer k.

Proof.

By Euclid's division theorem, there exist unique integers q and r, with $0 \le r < n$, such that

$$i = nq + r$$

and hence $i \bmod n = r$.

Adding kn to both sides of the equation above, we get

$$i + kn = n(q + k) + r$$

and hence $(i + kn) \bmod n = r$.

Consequently, $i \bmod n = (i + kn) \bmod n$. □

Lemma

Lemma 1.4

$$\begin{aligned} (i + j) \bmod n &= \big(i + (j \bmod n)\big) \bmod n \\ &= \big((i \bmod n) + j\big) \bmod n \\ &= \big((i \bmod n) + (j \bmod n)\big) \bmod n. \end{aligned}$$

Proof

Proof.

Here we prove that the first and last terms are equal. The other equalities can be proved similarly.

By Euclid's division theorem, there exist unique integers q and q' such that

$$\begin{aligned} i &= nq + (i \bmod n) \\ j &= nq' + (j \bmod n). \end{aligned}$$

Adding these two equations together mod n and applying Lemma 1.3, we obtain

$$\begin{aligned} (i + j) \bmod n &= \big(nq + (i \bmod n) + nq' + (j \bmod n)\big) \bmod n \\ &= \big(n(q + q') + (i \bmod n) + (j \bmod n)\big) \bmod n \\ &= \big((i \bmod n) + (j \bmod n)\big) \bmod n. \end{aligned}$$

□

Lemma

Lemma 1.5

$$\begin{aligned} (i \cdot j) \bmod n &= \big(i \cdot (j \bmod n)\big) \bmod n \\ &= \big((i \bmod n) \cdot j\big) \bmod n \\ &= \big((i \bmod n) \cdot (j \bmod n)\big) \bmod n. \end{aligned}$$

Remark

Lemmas 1.4 and 1.5 are very useful when computing sums or products mod n in which the numbers are large.

Definitions

Definition

The set of integers $\{0, 1, 2, \ldots, n-1\}$ is denoted by Z_n.

Definition

The addition and multiplication mod n operations are denoted by $+_n$ and $\cdot_n$, respectively:

$$\begin{aligned} i +_n j &\stackrel{\text{def}}{=} (i + j) \bmod n \\ i \cdot_n j &\stackrel{\text{def}}{=} (i \cdot j) \bmod n. \end{aligned}$$

Commutativity

Theorem 1.6

$$\begin{aligned} a +_n b &= b +_n a \\ a \cdot_n b &= b \cdot_n a. \end{aligned}$$

Proof.

This follows from the commutativity of ordinary addition and multiplication.

$$\begin{aligned} a +_n b &= (a + b) \bmod n \\ &= (b + a) \bmod n \\ &= b +_n a. \end{aligned}$$

The proof for $\cdot_n$ is similar. □

Associativity

Theorem 1.7

$$a +_n (b +_n c) = (a +_n b) +_n c$$
$$a \cdot_n (b \cdot_n c) = (a \cdot_n b) \cdot_n c.$$

Proof

Proof.
This follows from Lemma 1.4 and the associativity of ordinary addition and multiplication.

$$\begin{aligned} a +_n (b +_n c) &= \big(a + (b +_n c)\big) \bmod n \\ &= \big(a + ((b + c) \bmod n)\big) \bmod n \\ &= \big(a + (b + c)\big) \bmod n \\ &= \big((a + b) + c\big) \bmod n \\ &= \big(((a + b) \bmod n) + c\big) \bmod n \\ &= \big((a +_n b) + c\big) \bmod n \\ &= (a +_n b) +_n c. \end{aligned}$$

The proof for $\cdot_n$ is similar. □

Distributive Law

Theorem 1.8

$$a \cdot_n (b +_n c) = a \cdot_n b +_n a \cdot_n c.$$

Proof.
This follows from Lemmas 1.4 and 1.5 and the distributive law of ordinary addition and multiplication.

$$\begin{aligned} a \cdot_n (b +_n c) &= \big(a \cdot (b +_n c)\big) \bmod n \\ &= \big(a \cdot ((b + c) \bmod n)\big) \bmod n \\ &= \big(a \cdot (b + c)\big) \bmod n \\ &= (a \cdot b + a \cdot c) \bmod n \\ &= \big((a \cdot b) \bmod n + (a \cdot c) \bmod n\big) \bmod n \\ &= a \cdot_n b +_n a \cdot_n c. \end{aligned}$$

Additive Identity and Multiplicative Identity

Definition
Because

$$0 +_n i = i$$
$$1 \cdot_n i = i$$

for all $i \in Z_n$, 0 is the **additive identity** and 1 is the **multiplicative identity**.

Cryptography using Addition mod n

Encryption:
$C = P(M) = M +_n a$

Decryption:
$M = S(C) = C +_n (-a)$, where $-a$ is the **additive inverse** of a.

The Caesar cipher is a special case of this scheme.

Cryptography using Multiplication mod n

Encryption:
$C = P(M) = M \cdot_n a$

Decryption:
$M = S(C) = C \cdot_n a^{-1}$, where a^{-1} is the **multiplicative inverse** of a in Z_n (if it exists).

Example

Example 4

For each of the following three cases, determine if the above cryptosystem is feasible: (a) $n = 12, a = 4, M = 5$; (b) $n = 12, a = 3, M = 6$; and (c) $n = 12, a = 5, M = 7$.

Remark

We will find later that the problem of deciding whether the cryptosystem is feasible is equivalent to deciding whether the (unique) multiplicative inverse of a in Z_n exists.

Linear Congruence

The problem of using multiplication mod n for cryptography involves deciding whether the modular equation

$$a \cdot_n x = b$$

has a unique solution in Z_n.

Remark

The modular equation $a \cdot_n x = b$ may also be written as the following congruence

$$ax \equiv b \pmod{n},$$

which is called a **linear congruence**.

Multiplicative Inverse

Definition

For any $a \in Z_n$, an element $a' \in Z_n$ is said to be the **multiplicative inverse** of a in Z_n if and only if

$$a' \cdot_n a = a \cdot_n a' = 1.$$

The multiplicative inverse of a is often denoted by a^{-1} like the case for real numbers.

Lemma

Lemma 2.1

Suppose a has a multiplicative inverse a^{-1} in Z_n. Then for any $b \in Z_n$, the equation

$$a \cdot_n x = b$$

has the unique solution

$$x = a^{-1} \cdot_n b.$$

Proof

Proof.

We multiple both sides of the equation by a^{-1} to obtain

$$a^{-1} \cdot_n (a \cdot_n x) = a^{-1} \cdot_n b.$$

By the associative law, we get

$$(a^{-1} \cdot_n a) \cdot_n x = a^{-1} \cdot_n b.$$

Since $a^{-1} \cdot_n a = 1$ by definition, we obtain

$$x = a^{-1} \cdot_n b.$$

Proof (cont'd)

Proof (cont'd).

This shows that $x = a^{-1} \cdot_n b$ is a solution to the equation. To show that this solution is unique, we use a proof by contradiction. Assume that there exists another solution $c \neq a^{-1} \cdot_n b$ such that

$$a \cdot_n c = b.$$

Multiplying both sides of this equation by a^{-1}, we get $c = a^{-1} \cdot b$ which contradicts the assumption. Therefore, the solution $x = a^{-1} \cdot_n b$ is unique. □

Remark

Multiplying b by a^{-1} mod n may be seen as "dividing" b by a in Z_n.

Example

Example 5

Show that $a^{-1} = 5$ is the multiplicative inverse of $a = 5$ in Z_{12}. Hence find the solution to the following equation:

$$5 \cdot_{12} x = 11.$$

Corollary

Corollary 2.2

Suppose there exists a $b \in Z_n$ such that the equation

$$a \cdot_n x = b$$

has no solution. Then a does not have a multiplicative inverse in Z_n.

Proof.

This is a proof by contradiction. Suppose $a \cdot_n x = b$ has no solution. Suppose further that a does have a multiplicative inverse a^{-1} in Z_n. By Lemma 2.1, $x = a^{-1} \cdot_n b$ is the solution to the equation. This contradicts the hypothesis given in the corollary that the equation has no solution. Thus, the supposition that a has a multiplicative inverse in Z_n must be incorrect. Therefore, it must be the case that a does not have a multiplicative inverse in Z_n. □

Theorem

Theorem 2.3

If an element of Z_n has a multiplicative inverse, then the inverse must be unique.

Proof.

Suppose an element a of Z_n has a multiplicative inverse a' and another multiplicative inverse a''. Then, by definition, both a' and a'' are solutions to the equation $a \cdot_n x = 1$. However, by Lemma 2.1, the solution to the equation $a \cdot_n x = 1$ is unique. Therefore, it must be that $a' = a''$. □

Converting Modular Equations to Normal Equations

Lemma 2.4

The equation

$$a \cdot_n x = 1$$

has a solution in Z_n if and only if there exist integers x and y such that

$$ax + ny = 1.$$

Proof

Proof.
The equation
$$a \cdot_n x = 1$$
can be expressed as
$$ax \bmod n = 1,$$
or, by Euclid's division theorem,
$$ax = qn + 1$$
for some integer q. Rearranging the equation and taking $y = -q$, we have
$$ax + (-q)n = ax + ny = 1.$$
□

Remark

Remark
We will show later that this lemma can help us to prove that a has an inverse mod n if and only if a and n are relatively prime.

Theorem

Theorem 2.5
An integer a has a multiplicative inverse in Z_n if and only if there exist integers x and y such that $ax + ny = 1$.

Proof.
This follows directly from Lemma 2.4 and the definition of multiplicative inverse. □

Corollary

Corollary 2.6
If $a \in Z_n$ and x and y are integers such that $ax + ny = 1$, then the multiplicative inverse of a in Z_n is $x \bmod n$.

Proof.
Because $ax = 1 + (-y)n$, by Lemma 1.3,
$$a \cdot_n x = \big(1 + (-y)n\big) \bmod n = 1 \bmod n = 1.$$
From Lemma 1.5,
$$a \cdot_n x = a \cdot_n (x \bmod n).$$
Therefore the multiplicative inverse of a in Z_n is $x \bmod n$. □

Greatest Common Divisor

Definition

For two integers j and k, the largest integer d that is a factor of both j and k is called their **greatest common divisor** (GCD) which is denoted by $\gcd(j, k)$.

Definition

Two integers j and k are said to be **relatively prime** if $\gcd(j, k) = 1$.

Lemma

Lemma 2.7

If $a \in Z_n$ and x and y are integers such that $ax + ny = 1$, then a and n are relatively prime, i.e., $\gcd(a, n) = 1$.

Proof.

For any common divisor k of a and n, there must exist integers s and q such that

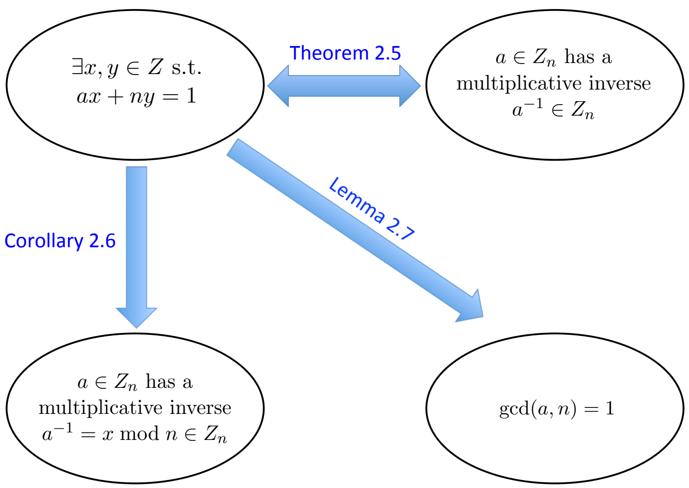
$$a = sk, \qquad n = qk.$$

Substituting these into the equation $ax + ny = 1$ gives

$$1 = ax + ny = skx + qky = k(sx + qy),$$

implying that k must be a divisor of 1. Because the only integer divisors of 1 are ± 1, we must have $k = \pm 1$. Therefore, $\gcd(a, n) = 1$. □

Summary of Key Results



Lemma

Lemma 2.8

If an integer a has a multiplicative inverse in Z_n, then $\gcd(a, n) = 1$.

Proof.

This follows directly from Theorem 2.5 and Lemma 2.7. □

Remark

Remark

It is natural to ask whether the converse of Lemma 2.8 is also true, i.e., whether the statement "if $\gcd(a, n) = 1$, then a has a multiplicative inverse in Z_n" is true, because such a result could be used to test whether a has a multiplicative inverse in Z_n.

Euclid's Division Theorem

Theorem 2.9 (Euclid's division theorem, restricted version)

Let n be a positive integer. Then for every nonnegative integer m, there exist unique integers q and r such that $m = nq + r$ and $0 \leq r < n$.

Remark

The only difference between this restricted version and the general version (Theorem 1.1) is that m must be nonnegative here.

Proof

Proof.

Our proof goes through two steps. The first step, on existence, shows that there exists at least one pair of integers q and r such that $m = nq + r$ and $0 \leq r < n$. The second step, on uniqueness, shows that the pair is unique. To construct a proof by contradiction, we first assume that there is a nonnegative integer m for which no such q and r exist. We choose the smallest such nonnegative integer m if there are multiple ones. If $m < n$, then we can write $m = n \cdot 0 + m$ with $0 \leq m < n$, i.e., there exist $q = 0$ and $r = m$. If $m \geq n$, then $0 \leq m - n < m$. Since m is the smallest nonnegative integer for which no such q and r exist and the nonnegative integer $m - n$ is smaller than m, there must exist integers q' and r' such that $m - n = nq' + r'$ and $0 \leq r' < n$. But then $m = n(q' + 1) + r'$, implying that there exist $q = q' + 1$ and $r = r'$ such that $m = nq + r$ and $0 \leq r < n$. Thus, both cases lead to contradiction. By the principle of proof by contradiction, at least one pair of integers q and r must exist.

Proof (cont'd)

Proof (cont'd).

To prove uniqueness of the pair, we assume that there exist two pairs (q, r) and (q^*, r^*) such that $m = nq + r$ and $m = nq^* + r^*$ with $0 \leq r < n$ and $0 \leq r^* < n$. By subtraction, we get $0 = n(q - q^*) + (r - r^*)$ or $n(q - q^*) = r^* - r$. Because $0 \leq r, r^* \leq n - 1$, $0 \leq |r^* - r| \leq n - 1 < n$ and so

$$0 \leq n\,|q - q^*| = \left|n(q - q^*)\right| = |r^* - r| < n$$

$$0 \leq |q - q^*| = \frac{|r^* - r|}{n} < 1.$$

The only way for the above to hold is when $|q - q^*| = |r^* - r| = 0$, which implies that $q = q^*$ and $r = r^*$. Thus the pair is unique. □

Remark

Remark

We can generalize this restricted version of Euclid's division theorem to the general version. If m is a negative integer, then $-m$ is positive and hence there exist unique integers q' and r' such that $-m = nq' + r'$ and $0 \leq r' < n$. Rewriting it, we get $m = n(-q') + (-r')$. Let us consider two cases. If $r' = 0$, then there exist unique integers $q = -q'$ and $r = 0$ such that $m = nq + r$. If $0 < r' < n$, we note that $m = n(-q' - 1) + (n - r')$ and hence there exist unique integers $q = -(q' + 1)$ and $r = n - r'$ such that $m = nq + r$.

Lemma

Lemma 2.10

If j, k, q, and r are positive integers such that $k = jq + r$, then $\gcd(j, k) = \gcd(r, j)$.

Proof.

It suffices to show that j and k have exactly the same set of common factors as r and j. To do this, we first show that if d is a common factor of j and k, then it is also a common factor of r and j. Second, we show that if d is a common factor of r and j, then it is also a common factor of j and k.

Proof (cont'd)

Proof (cont'd).

If d be a common factor of j and k, then there must exist integers i_1 and i_2 such that $j = i_1 d$ and $k = i_2 d$. Substituting these into the equation $k = jq + r$ gives

$$\begin{aligned} i_2 d &= i_1 dq + r \\ r &= d(i_2 - i_1 q), \end{aligned}$$

showing that d is a factor of r and hence a common factor of r and j. Similarly, if d is a common factor of r and j, then there must exist integers i_3 and i_4 such that $r = i_3 d$ and $j = i_4 d$. Substituting these into the equation $k = jq + r$ gives

$$k = i_4 dq + i_3 d = d(i_4 q + i_3),$$

showing that d is a factor of k and hence a common factor of j and k. □

Remark

Remark

Although we do not need to assume $r < j$ to prove this lemma, Euclid's division theorem tells us that we may assume $r < j$. Moreover, because we assume in the lemma that j, q, and r are positive, we have $j < k$. Thus, this important lemma reduces the problem of finding $\gcd(j, k)$ to the simpler one of finding $\gcd(r, j)$.

Corollary 2.11

If j, k, and q are positive integers such that $k = jq$, then $\gcd(j, k) = j$.

Proof.

From Lemma 2.10, we know that $\gcd(j, k) = \gcd(0, j)$. Because any integer is a divisor of 0, $\gcd(0, j) = j$ and hence $\gcd(j, k) = j$. □

Example

Example 6

Using Lemma 2.10 and Corollary 2.11, find the GCD of 32 and 152 using a recursive procedure.

Euclid's GCD Algorithm

Remark

The above procedure illustrates a recursive algorithm, called **Euclid's GCD algorithm**, for finding the greatest common divisor of two positive integers.

Algorithm (Euclid's GCD algorithm)

The algorithm is expressed in pseudocode below:

function gcd(j, k) // $0 < j < k$
if k mod $j = 0$
  return j
else
  return gcd(r, j)
end if

Euclid's Extended GCD Algorithm

Theorem 2.12

If j and k are positive integers, then there exist integers x and y such that $\gcd(j, k) = jx + ky$.

Remark

Instead of giving a formal proof of this theorem, we provide an example here to illustrate the procedure of finding a linear combination of x and y.

Example

Example 7

Find the GCD of 198 and 252, and two integers x and y such that $\gcd(198, 252) = 198x + 252y$.

Solution. We first use Euclid's GCD algorithm to find $\gcd(198, 252)$ as illustrated below:

$$\begin{aligned} 252 &= 198 \cdot 1 + 54 \\ 198 &= 54 \cdot 3 + 36 \\ 54 &= 36 \cdot 1 + 18 \\ 36 &= 18 \cdot 2. \end{aligned}$$

Thus $\gcd(198, 252) = 18$.

Example (cont'd)

We now work backward to express $\gcd(198, 252)$ as a linear combination of 198 and 252:

From third equation:	$18 = 54 - 36 \cdot 1$	$\gcd(198, 252) = 36 \cdot (-1) + 54 \cdot 1$
From second equation:	$36 = 198 - 54 \cdot 3$	$\gcd(198, 252) = 198 \cdot (-1) + 54 \cdot 4$
From first equation:	$54 = 252 - 198 \cdot 1$	$\gcd(198, 252) = 198 \cdot (-5) + 252 \cdot 4$

Therefore, $x = -5$ and $y = 4$.

This procedure can be tabulated systematically as follows:

i	$j[i]$	$k[i]$	$q[i]$	$r[i]$	$x[i]$	$y[i]$
0	198	252	1	54		
1	54	198	3	36		
2	36	54	1	18		
3	18	36	2	0	1	0
2			1		-1	1
1			3		4	-1
0			1		-5	4

Remark

Remark

The above example illustrates a recursive algorithm, called **Euclid's extended GCD algorithm**, for finding the greatest common divisor of two positive integers and expressing it as a linear combination of the two integers.

Theorem

Theorem 2.13

Let j and k be positive integers. There exist integers x and y such that $jx + ky = 1$ if and only if $\gcd(j, k) = 1$.

Proof.

The 'only if' part has been proved in Lemma 2.7. For the 'if' part, it follows from Theorem 2.12 that $\gcd(j, k) = jx + ky = 1$. This completes the proof. □

Corollaries

Corollary 2.14

An integer $a \in Z_n$ has a multiplicative inverse in Z_n if and only if $\gcd(a, n) = 1$.

Proof.

This follows from Lemma 2.4 and Theorem 2.13. □

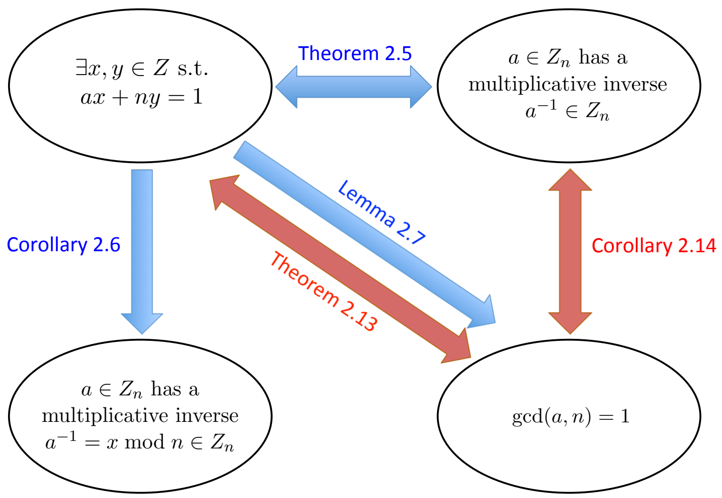
Corollary 2.15

Let p be a prime. Then every positive integer $a \in Z_p$ has a multiplicative inverse in Z_p.

Proof.

If p is prime, then $\gcd(a, p) = 1$ for every positive $a \in Z_p$. From Corollary 2.14, a must have a multiplicative inverse in Z_p. □

Summary of Key Results



Corollary

Corollary 2.6 for computing the multiplicative inverse can now be elaborated as in the following corollary.

Corollary 2.16

If $a \in Z_n$ has a multiplicative inverse in Z_n, then we can compute it by running Euclid's extended GCD algorithm to determine the integers x and y such that $ax + ny = 1$. The multiplicative inverse of a in Z_n is $x \bmod n$.

Remark

Although Euclid's extended GCD algorithm always gives unique integers x and y to satisfy the equation $ax + ny = 1$ for given n and $a \in Z_n$, it should be noted that x and y are in fact not unique in general. However, the multiplicative inverse in Z_n, if exists, is unique according to Theorem 2.3.

Definition

Definition

If a and b are integers with $a \neq 0$, we say that a **divides** b if there is an integer c such that $b = ac$. When a divides b, we say that a is a **factor** of b and b is a **multiple** of a. The notation $a \mid b$ denotes that a divides b and $a \nmid b$ denotes that a does not divide b.

Theorem

Theorem 2.17

Let a, b, and c be integers. Then

(i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

(ii) if $a \mid b$, then $a \mid bc$ for all integers c;

(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof

Proof.

(i) Because $a \mid b$ and $a \mid c$, there exist integers s and t such that $as = b$ and $at = c$. Hence, $b + c = as + at = a(s + t)$. Therefore, $a \mid (b + c)$.
(ii) Because $a \mid b$, there exists an integer s such that $as = b$. For any integer c, multiplying both sides of the equation $as = b$ by c gives $acs = bc$. Therefore, $a \mid bc$.
(iii) Because $a \mid b$ and $b \mid c$, there exist integers s and t such that $as = b$ and $bt = c$. Combining the two equations gives $ast = c$. Therefore, $a \mid c$. □

Lemma

Lemma 2.18

If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof.

Because $\gcd(a, b) = 1$, by Theorem 2.12 there are integers x and y such that $ax + by = 1$. Multiplying both sides of this equation by c, we obtain

$$acx + bcy = c.$$

Because $a \mid bc$, by part (ii) of Theorem 2.17, we have $a \mid bcy$. Because $a \mid acx$ and $a \mid bcy$, by part (i) of Theorem 2.17, we can conclude that $a \mid (acx + bcy)$ or $a \mid c$. □

Lemma

A variant and generalization of the lemma above is given in the following lemma, which can be used to prove the uniqueness of the prime factorization of a positive integer.

Lemma 2.19

If p is a prime and $p \mid a_1 a_2 \cdots a_n$ where each a_i is an integer, then $p \mid a_j$ for some j.

Proof

Proof.

Because $p \mid a_1 a_2 \cdots a_n$, there exists an integer q such that $pq = a_1 a_2 \cdots a_n$. Dividing both sides of the equation by p, we get

$$q = \frac{a_1 a_2 \cdots a_n}{p}.$$

Because p is a prime, it has no factors other than 1 and itself. So there must exist an integer a_j such that when the above equation is expressed as follows

$$q = a_1 \cdot a_2 \cdots \frac{a_j}{p} \cdots a_n,$$

each of the n factors on the right-hand side is an integer to make the product (equal to q) also an integer. Therefore, $p \mid a_j$. □

Fundamental Theorem of Arithmetic

Theorem 2.20 (Fundamental theorem of arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in nondecreasing order.

Proof

Proof.

The proof involves two parts: existence and uniqueness.
For the existence part, we let $P(n)$ be the proposition that the integer n can be written as a prime or as the product of two or more primes. The base case $P(2)$ is true, because 2 is itself a prime. For the inductive step, we take the inductive hypothesis that $P(k-1)$ is true for any $k \geq 3$. Under this assumption, we want to show that $P(k)$ is also true. There are two cases to consider, namely, when k is prime and when k is composite. If k is prime, we immediately see that $P(k)$ is true. Otherwise, k is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b < k$. By the inductive hypothesis, both $P(a)$ and $P(b)$ are true and hence both a and b can be written as the product of primes. Thus, if k is composite, it can be written as the product of primes, namely, those primes in the factorization of a and those in the factorization of b.

Proof (cont'd)

Proof (cont'd).

For the uniqueness part, we use a proof by contradiction. Suppose a positive integer n can be written as the product of primes in two different ways, say, $n = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots q_t$, where p_i and q_j are primes such that $p_1 \leq p_2 \leq \cdots \leq p_s$ and $q_1 \leq q_2 \leq \cdots \leq q_t$ and s and t are positive integers. We remove all common primes from the two factorizations to give $p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$, where no prime occurs on both sides of this equation and u and v are positive integers. By Lemma 2.19, it follows that $p_{i_1} \mid q_{j_k}$ for some k. Because no prime divides another prime, this is impossible. Consequently, there can be at most one factorization of n into primes in nondecreasing order. □

Exponentiation mod n

Cryptography using exponentiation mod n can provide a much greater level of security than that using modular addition and multiplication.

From Lemma 1.5, we have

$$a^j \bmod n = \underbrace{a \cdot_n a \cdot_n \cdots \cdot_n a}_{j \text{ factors}}.$$

Lemma 3.1

For any $a \in Z_n$ and any nonnegative integers i and j,

$$(a^i \bmod n) \cdot_n (a^j \bmod n) = a^{i+j} \bmod n$$
$$(a^i \bmod n)^j \bmod n = a^{ij} \bmod n.$$

Lemma

Lemma 3.2

Let p be a prime number. For any fixed positive integer a in Z_p, the numbers

$$1 \cdot_p a,\ 2 \cdot_p a,\ \ldots,\ (p-1) \cdot_p a$$

are a permutation of the set $\{1, 2, \ldots, p-1\}$.

Proof

Proof.

From Corollary 2.15, every positive integer a in Z_p has a multiplicative inverse a^{-1} in Z_p. Let i and j be two positive integers in Z_p such that $i \cdot_p a = j \cdot_p a$. Thus we have

$$\begin{aligned}(i \cdot_p a) \cdot_p a^{-1} &= (j \cdot_p a) \cdot_p a^{-1} \\ i \cdot_p (a \cdot_p a^{-1}) &= j \cdot_p (a \cdot_p a^{-1}) \\ i &= j.\end{aligned}$$

This shows that multiplication mod p defines a bijection from the set $\{1, 2, \ldots, p-1\}$ to itself and hence a permutation of the set. □

Fermat's Little Theorem

Theorem 3.3 (Fermat's little theorem – version 1)

Let p be a prime number. For every positive integer a in Z_p, we have

$$a^{p-1} \bmod p = 1.$$

Proof

Proof.

Because p is a prime, Lemma 3.2 tells us that the numbers $1 \cdot_p a, 2 \cdot_p a, \ldots, (p-1) \cdot_p a$ are a permutation of the set $\{1, 2, \ldots, p-1\}$. Thus

$$\begin{aligned}1 \cdot_p 2 \cdot_p \cdots \cdot_p (p-1) &= (1 \cdot_p a) \cdot_p (2 \cdot_p a) \cdot_p \cdots \cdot_p ((p-1) \cdot_p a) \\ &= 1 \cdot_p 2 \cdot_p \cdots \cdot_p (p-1) \cdot_p (a^{p-1} \bmod p).\end{aligned}$$

Multiplying both sides of the above equation by the multiplicative inverses in Z_p of $2, 3, \ldots, p-1$, we get

$$1 = a^{p-1} \bmod p.$$

This proves the theorem. □

Fermat's Little Theorem

Corollary 3.4 (Fermat's little theorem – version 2)

Let p be a prime number. For every positive integer a that is not a multiple of p, we have

$$a^{p-1} \bmod p = 1.$$

Proof.

Because a is not a multiple of p, a mod p is a positive integer. Thus, by Theorem 3.3 and Lemma 1.5,

$$1 = (a \bmod p)^{p-1} \bmod p = a^{p-1} \bmod p.$$

□

Example 8

What is the remainder after dividing 3^{50} by 7?

Corollary

Corollary 3.5

Let p be a prime number and m be a nonnegative integer. For every positive integer a that is not a multiple of p, we have

$$a^m \bmod p = a^{m \bmod (p-1)} \bmod p.$$

Proof

Proof.

By Euclid's division theorem, we can express m as

$$m = k(p-1) + m \bmod (p-1),$$

for some integer k. This allows us to express a^m mod p as

$$\begin{aligned} a^m \bmod p &= a^{k(p-1)+m \bmod (p-1)} \bmod p \\ &= \left((a^{k(p-1)} \bmod p) \cdot a^{m \bmod (p-1)}\right) \bmod p \\ &= \left((a^{p-1} \bmod p)^k \cdot a^{m \bmod (p-1)}\right) \bmod p. \end{aligned}$$

By Fermat's little theorem, $a^{p-1} \bmod p = 1$. Therefore,

$$a^m \bmod p = a^{m \bmod (p-1)} \bmod p.$$

□

RSA Key Pair Generation

Bob's key pair (public key and secret key) is generated according to the following procedure:

1. Choose two large prime numbers p and q each with at least 150 digits.
2. Compute $n = pq$.
3. Choose a number $e \neq 1$ such that $\gcd\big(e, (p-1)(q-1)\big) = 1$.
4. Compute d as the multiplicative inverse e^{-1} of e in $Z_{(p-1)(q-1)}$, i.e., $ed \bmod (p-1)(q-1) = 1$.
5. Publish (e, n) as the public key.
6. Keep d as the secret key.

RSA Encryption and Decryption

Alice encrypts a message $x \in Z_n$ and sends the ciphertext to Bob according to the following procedure:

1. Get the public key (e, n) of Bob from some public directory.
2. Compute $y = x^e \bmod n$ as the ciphertext using the public key.
3. Send the ciphertext y to Bob.

Bob receives the ciphertext from Alice and decrypts it according to the following procedure:

1. Receive y from Alice.
2. Compute $z = y^d \bmod n$ as the decrypted message using the secret key.
3. Read the decrypted message z.

Example

Example 9

$$
\begin{aligned}
p &= 61,\ \ q = 53 \\
n &= pq = 3233 \\
e &= 17 \\
d &= 2753 \\
ed \bmod (p-1)(q-1) &= (17 \cdot 2753) \bmod 3120 = 1 \\
\text{Public key} &: (e, n) = (17, 3233) \\
\text{Secret key} &: d = 2753 \\
\text{Encryption} &: y = x^e \bmod n = x^{17} \bmod 3233 \\
\text{Decryption} &: z = y^d \bmod n = y^{2753} \bmod 3233
\end{aligned}
$$

Theoretical Guarantee

Remark

To show that the RSA cryptosystem works, we need to show that $z = x$, i.e., $x^{ed} \bmod n = x$.

Lemma 3.6

$$
\begin{aligned}
y^d \bmod p &= x \bmod p \\
y^d \bmod q &= x \bmod q.
\end{aligned}
$$

Proof

Proof.

We only need to give the proof for the first result because that for the second one is very similar. Because $y = x^e \bmod n$,

$$y^d \bmod p = (x^e \bmod pq)^d \bmod p = (x^e \bmod p)^d \bmod p = x^{ed} \bmod p.$$

Recall that $ed \bmod (p-1)(q-1) = 1$. Thus we can write

$$ed = k(p-1)(q-1) + 1,$$

for some integer k. Consequently,

$$
\begin{aligned}
y^d \bmod p &= x^{k(p-1)(q-1)+1} \bmod p \\
&= x^{k(p-1)(q-1)} x \bmod p \\
&= (x^{k(p-1)(q-1)} \bmod p) \cdot_p (x \bmod p) = (x^{k(p-1)(q-1)} \bmod p) \cdot_p x.
\end{aligned}
$$

Proof (cont'd)

Proof (cont'd).

We consider two cases:

- Case 1 ($x^{k(q-1)}$ is not a multiple of p):
  By Fermat's little theorem, $\left(x^{k(q-1)}\right)^{p-1} \bmod p = x^{k(p-1)(q-1)} \bmod p = 1$. It thus follows that
  $$y^d \bmod p = 1 \cdot_p x = x \bmod p.$$
- Case 2 ($x^{k(q-1)}$ is a multiple of p):
  Because p is prime, the fact that $x^{k(q-1)}$ is a multiple of p implies that x is also a multiple of p and hence $x \bmod p = 0$. Thus,
  $$\begin{aligned} y^d \bmod p &= (x^{k(p-1)(q-1)} \bmod p) \cdot_p (x \bmod p) \\ &= (x^{k(p-1)(q-1)} \bmod p) \cdot_p 0 = 0 = x \bmod p. \end{aligned}$$

□

Remark

Remark

Lemma 3.6 can be rewritten as

$$\begin{aligned} (y^d - x) \bmod p &= 0 \\ (y^d - x) \bmod q &= 0, \end{aligned}$$

which tells us that $y^d - x$ is a multiple of the prime number p and a multiple of the prime number q.

RSA

Theorem 3.7 (Rivest, Shamir, and Adleman)

The RSA procedure for encoding and decoding messages works correctly, i.e., $x^{ed} \bmod n = x^{ed} \bmod pq = x$.

Proof

Proof.

Lemma 3.6 tells us that $y^d - x$ is a multiple of the prime number p and a multiple of the prime number q. It thus follows that $y^d - x$ is a multiple of $n = pq$. Applying Lemma 1.4, we get

$$(y^d - x) \bmod n = \left((y^d \bmod n) - x\right) \bmod n = 0.$$

Because both x and $y^d \bmod n$ are in Z_n, i.e., $0 \le x \le n-1$ and $0 \le y^d \bmod n \le n-1$, we have

$$-(n-1) \le (y^d \bmod n) - x \le n-1.$$

The only integer in the range for $(y^d \bmod n) - x$ that makes $\left((y^d \bmod n) - x\right) \bmod n = 0$ is 0. Also, $x = x \bmod n$ because $x \in Z_n$. So,

$$y^d \bmod n = x^{ed} \bmod n = x = x \bmod n.$$

□

Breaking RSA

Remark

Some possible ways of breaking RSA include:

- From the public key (e, n), factorize n to get its two prime factors p and q and then find the secret key d by computing the multiplicative inverse of e in $Z_{(p-1)(q-1)}$.
- From the public key (e, n), find the original message x directly by computing the eth root mod n of the ciphertext $y = x^e \bmod n$.

Fortunately, as of now, these number theory problems are computationally hard or intractable (but not impossible). However, advances in the computing power may make it possible in the future.

Implementation Issues

In RSA encryption, we need to compute

$$y = x^e \bmod n,$$

where

$$\begin{aligned} x &\approx 150 \text{ digits} \\ e &\approx 120 \text{ digits} \\ n\,(= pq) &\approx 300 \text{ digits.} \end{aligned}$$

How can we do this efficiently?

Naive Approaches

Two (im)possible approaches:

1. Compute x^e and then take mod n:
   Time requirement: $e - 1 \approx 10^{120}$ multiplications, 1 mod operation
   Memory requirement: x^e has about $150 \cdot 10^{120}$ digits
2. Take advantage of Lemma 1.5 to compute the following iteratively:

$$x^{i+1} \bmod n = (x^i \bmod n)x \bmod n, \qquad i = 1, 2, \ldots, e-1.$$

   Time requirement: $e - 1 \approx 10^{120}$ multiplications, $e - 1 \approx 10^{120}$ mod operations
   Memory requirement: each number $(x^i \bmod n)x$ has about 450 digits

Modular Exponentiation by Squaring

A significantly more efficient method is called **modular exponentiation by squaring**. We illustrate it using a small example.

Example 10

Compute $x^e \bmod n = 5^{23} \bmod 55$ using modular exponentiation by squaring.

Solution. We first express $e = 23$ as a sum of powers of 2:

$$23 = 16 + 4 + 2 + 1 = 2^4 + 2^2 + 2^1 + 2^0.$$

We then express $x^e = 5^{23}$ as

$$5^{23} = 5^{2^4} \cdot 5^{2^2} \cdot 5^{2^1} \cdot 5^{2^0}.$$

Example (cont'd)

The following terms are then computed via repeated squaring:

$$\begin{aligned}
l_0 &= x & &= x^{2^0} \bmod n & &= 5^{2^0} \bmod n \\
l_1 &= (l_0 \cdot l_0) \bmod n & &= x^{2^1} \bmod n & &= 5^{2^1} \bmod n \\
l_2 &= (l_1 \cdot l_1) \bmod n & &= x^{2^2} \bmod n & &= 5^{2^2} \bmod n \\
l_3 &= (l_2 \cdot l_2) \bmod n & &= x^{2^3} \bmod n & &= 5^{2^3} \bmod n \\
l_4 &= (l_3 \cdot l_3) \bmod n & &= x^{2^4} \bmod n & &= 5^{2^4} \bmod n.
\end{aligned}$$

Thus we can compute $x^e \bmod n = 5^{23} \bmod 55$ as

$$\begin{aligned}
5^{23} \bmod 55 &= (5^{2^4} \cdot 5^{2^2} \cdot 5^{2^1} \cdot 5^{2^0}) \bmod 55 \\
&= \big(l_4 \cdot (l_2 \cdot (l_1 \cdot l_0) \bmod 55) \bmod 55\big) \bmod 55.
\end{aligned}$$

Modular Exponentiation by Squaring

Modular exponentiation by squaring is much more efficient.

- Compute the l_i terms:
  Time requirement: $\approx \log_2 e$ multiplications, $\approx \log_2 e$ mod operations
- Compute $x^e \bmod n$ using the precomputed l_i terms:
  Time requirement: $\leq \log_2 e$ multiplications, $\leq \log_2 e$ mod operations

Some "ballpark" numbers to illustrate the efficiency of this scheme:

$$\begin{aligned}
e &= 10^{120} \\
2\log_2 e &= 240 \log_2 10 \approx 797 \ll e - 1.
\end{aligned}$$

Chinese Remainder Theorem

Theorem 4.1 (Chinese remainder theorem – restricted version)

Let m_1 and m_2 be two positive integers that are relatively prime and a_1 and a_2 be arbitrary integers in Z_{m_1} and Z_{m_2}, respectively. Then the equations

$$\begin{aligned}
x \bmod m_1 &= a_1 \\
x \bmod m_2 &= a_2
\end{aligned}$$

have a unique solution $x \in Z_{m_1 m_2}$.

Proof

Proof.

It suffices to show that the function $f : Z_{m_1 m_2} \to Z_{m_1} \times Z_{m_2}$ with $f(x) = (x \bmod m_1, x \bmod m_2)$ is a bijection, or, equivalently, f is a one-to-one function from a set to another set of the same cardinality.

It is easy to see that

$$|Z_{m_1 m_2}| = m_1 m_2 = |Z_{m_1}| \cdot |Z_{m_2}| = |Z_{m_1} \times Z_{m_2}|.$$

To show that f is one-to-one, let us consider any two elements x and y in $Z_{m_1 m_2}$ such that $f(x) = f(y)$. This implies

$$\begin{aligned}
x \bmod m_1 &= y \bmod m_1 \\
x \bmod m_2 &= y \bmod m_2,
\end{aligned}$$

Proof (cont'd)

Proof (cont'd).

or equivalently

$$(x-y) \bmod m_1 = 0 \qquad (x-y) \bmod m_2 = 0,$$

showing that $x-y$ is a multiple of m_1 and a multiple of m_2. Because $\gcd(m_1, m_2) = 1$, it follows that $x-y$ is a multiple of $m_1 m_2$, i.e.,

$$(x-y) \bmod m_1 m_2 = 0.$$

Because both x and y are in $Z_{m_1 m_2}$, we have

$$-(m_1 m_2 - 1) \leq x - y \leq m_1 m_2 - 1.$$

The only integer in the range for $x-y$ that makes $(x-y) \bmod m_1 m_2 = 0$ is 0, i.e., $x = y$. Therefore f is one-to-one.

This completes the proof. □

Constructing the Solution

Remark

The proof above is only an existence proof without telling us what the solution is. Here we give the procedure for constructing the solution which also serves the purpose of a constructive proof.

Suppose we have two numbers α and β such that

$$\begin{array}{ll} \alpha \bmod m_1 = 1 & \beta \bmod m_2 = 1 \\ \alpha \bmod m_2 = 0 & \beta \bmod m_1 = 0. \end{array}$$

We note that

$$x = (a_1\alpha + a_2\beta) \bmod m_1 m_2$$

is the solution because

$$x \bmod m_1 = \big((a_1\alpha + a_2\beta) \bmod m_1 m_2\big) \bmod m_1 = (a_1\alpha + a_2\beta) \bmod m_1 = a_1 + 0 = a_1$$
$$x \bmod m_2 = \big((a_1\alpha + a_2\beta) \bmod m_1 m_2\big) \bmod m_2 = (a_1\alpha + a_2\beta) \bmod m_2 = 0 + a_2 = a_2.$$

Constructing the Solution (cont'd)

Remark (cont'd)

Note that α is a multiple of m_2 and $\alpha \bmod m_1 = 1$. Thus

$$\alpha = m_2 m_2^{-1},$$

where m_2^{-1} is the multiplicative inverse of m_2 in Z_{m_1}, satisfies the requirement. Similarly,

$$\beta = m_1 m_1^{-1},$$

where m_1^{-1} is the multiplicative inverse of m_1 in Z_{m_2}, also satisfies the requirement. Therefore,

$$x = \left(a_1 m_2 m_2^{-1} + a_2 m_1 m_1^{-1}\right) \bmod m_1 m_2$$

is the solution.

Chinese Remainder Theorem (General Version)

Theorem 4.2 (Chinese remainder theorem – general version)

Let $m_1, m_2, \ldots, m_n$ be n positive integers that are pairwise relatively prime and $a_1, a_2, \ldots, a_n$ be n arbitrary integers in $Z_{m_1}, Z_{m_2}, \ldots, Z_{m_n}$, respectively. Then the system of equations

$$\begin{aligned} x \bmod m_1 &= a_1 \\ x \bmod m_2 &= a_2 \\ &\vdots \\ x \bmod m_n &= a_n \end{aligned}$$

has a unique solution $x \in Z_{m_1 m_2 \cdots m_n}$.

Example

Example 11

There are $n \leq 100$ people in a party. When groups of 15 are formed, one group only has 8 people. Then the n people have dinner together with 8 sitting at each table, but three tables end up with 9 people. How many people are in the party?