



中山大學
SUN YAT-SEN UNIVERSITY

Module I. Fundamentals of Information Security

Chapter 2

Cryptographic Techniques

Web Security: *Principles & Applications*

School of Data & Computer Science, Sun Yat-sen University

2.3 Mathematical Foundations

□ Mathematical Foundations of Public-Key Cryptography

- ✧ Prime factorizations of integers
- ✧ The *Euclidean* Algorithm
- ✧ *Bézout's* Theorem
- ✧ Linear Congruence
- ✧ The Extended_*Euclidean* Algorithm
- ✧ The Chinese Remainder Theorem
- ✧ *Euler's* φ function
- ✧ *Euler's* Theorem and the Corollary
- ✧ *Fermat's* Little Theorem
- ✧ Primitive Root and Discrete Logarithm

2.3.1 Prime Factorizations of Integers

2.3.1 Prime Factorizations of Integers

❑ *Fundamental Theorem of Arithmetic* (算术基本定理)

- ✧ Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes when the prime factors are written in order of non-decreasing size. (*Euclid*, 300 BC)

❑ *Greatest Common Divisor* (最大公因数)

- ✧ Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the ***greatest common divisor*** (GCD) of a and b , often denoted as $\gcd(a, b)$.

2.3.2 The *Euclidean Algorithm*

2.3.2 The *Euclidean Algorithm* (欧几里德辗转相除法)

— Book VII. Fundamentals of number theory 几何原本·第VII卷

□ *Lemma 0.*

✧ Let $a = bq + r$, where a , b , q , and r are integers. Then
 $\gcd(a, b) = \gcd(b, r)$.

✧ *Proof.*

- ◆ Suppose d divides both a and b . Recall that if $d|a$ and $d|b$, then $d|a-bk$ for any integer k . It follows that d also divides $a-bq = r$. Hence, any common division of a and b is also a common division of b and r .
- ◆ Suppose that d' divides both b and r , then d' also divides $bq+r = a$. Hence, any common divisor of b and r is also common divisor of a and b .
- ◆ Consequently, $\gcd(a, b) = \gcd(b, r)$.
- ◆ Note: $a = bq + r$, $0 \leq r < b$, aka $r = a \bmod b$ if the quotient q ignored. r is the (*least positive*) remainder of the division.

2.3.2 The *Euclidean Algorithm*

□ *Lemma 0.*

✧ Let $a = bq + r$, where a, b, q , and r are integers. Then
 $\gcd(a, b) = \gcd(b, r)$.

□ *Remark.*

✧ Suppose a and b are positive integers, $a \geq b$. Let $r_0 = a$ and $r_1 = b$, we successively apply the division algorithm and the gcd is the last nonzero remainder

$$\begin{aligned}r_0 &= r_1 q_1 + r_2, & 0 < r_2 < r_1 \\r_1 &= r_2 q_2 + r_3, & 0 < r_3 < r_2 \\&\dots \\r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\r_{n-1} &= r_n q_n \\ \gcd(a, b) &= \gcd(r_0, r_1) \\&= \gcd(r_1, r_2) \\&= \dots \\&= \gcd(r_{n-2}, r_{n-1}) \\&= \gcd(r_{n-1}, r_n) \\&= \gcd(r_n, 0) = r_n.\end{aligned}$$

2.3.2 The *Euclidean Algorithm*

□ *Lemma 0.*

✧ Let $a = bq + r$, where a, b, q , and r are integers. Then
 $\gcd(a, b) = \gcd(b, r)$.

□ *Remark.*

✧ Suppose a and b are positive integers, $a \geq b$. Let $r_0 = a$ and $r_1 = b$, we successively apply the division algorithm and the gcd is *the last nonzero remainder*.

$$r_0 = r_1 q_1 + r_2, \quad 0 < r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3, \quad 0 < r_3 < r_2$$

...

$$r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n$$

$$\gcd(a, b) = \gcd(r_0, r_1)$$

$$= \gcd(r_1, r_2)$$

$$= \dots$$

$$= \gcd(r_{n-2}, r_{n-1})$$

$$= \gcd(r_{n-1}, r_n)$$

$$= \gcd(r_n, 0) = r_n$$

The last nonzero remainder

2.3.2 The *Euclidean Algorithm*

□ *Lemma 0.*

- ✧ Let $a = bq + r$, where a , b , q , and r are integers. Then
 $\gcd(a, b) = \gcd(b, r)$.

□ *Example.*

- ✧ Find the GCD of 662 and 414.
✧ Compute as

$$662 = 414 \cdot 1 + 248$$

$$414 = 248 \cdot 1 + 166$$

$$248 = 166 \cdot 1 + 82$$

$$166 = 82 \cdot 2 + 2$$

$$82 = 2 \cdot 41$$

2.3.2 The *Euclidean Algorithm*

□ *Lemma 0.*

- ✧ Let $a = bq + r$, where a , b , q , and r are integers. Then
 $\gcd(a, b) = \gcd(b, r)$.

□ *Example.*

- ✧ Find the GCD of 662 and 414.
✧ Compute as

$$662 = 414 \cdot 1 + 248$$

$$414 = 248 \cdot 1 + 166$$

$$248 = 166 \cdot 1 + 82$$

$$166 = 82 \cdot 2 + 2$$

$$82 = 2 \cdot 41$$

So, $\gcd(662, 414) = 2$

2.3.2 The *Euclidean* Algorithm

□ *The Euclidean Algorithm*

```
procedure gcd(a, b: positive integers)
begin
  x := a;
  y := b;
  while (y ≠ 0)
  begin
    r := x mod y;
    x := y;
    y := r;
  end; {gcd(a, b)=x}
end;
```

✧ The time complexity (for **mod** operation) is $O(\log b)$, where $a \geq b$.

2.3.2 The *Euclidean* Algorithm

❑ *The Euclidean Algorithm*

```
function Euclid( $a, b$ : positive integers): positive integer
begin
  if  $b=0$ 
  then
    return ( $a$ )
  else
    return (Euclid( $b, a \bmod b$ );
end;
```

- ✧ Another recursive form of *Euclidean* Algorithm.
- ✧ Think about it.

2.3.3 Bézout's Theorem

2.3.3 Bézout's Theorem (Étienne Bézout, 1779)

□ *Theorem 1.*

- ✧ If a and b are *positive* integers, then there exists integers s and t such that $\gcd(a, b) = sa + tb$.

□ *Remark.*

- ✧ a and b are positive. s and t can be any integers.
- ✧ The equation $\gcd(a, b) = sa + tb$ is called **Bézout's identity** (贝祖恒等式). The integers s and t are called **Bézout coefficients** of a and b (贝祖系数).
- ✧ Proof omitted.

□ *Example.*

- ✧ $\gcd(252, 198) = 18$.
- ✧ By working backward through the divisions of *The Euclidean Algorithm*, we get $s = 4$, $t = -5$ such that
$$18 = 4 \cdot 252 + (-5) \cdot 198.$$
- ✧ Ref. to Section 2.3.5: *The Extended Euclidean Algorithm*

2.3.3 Bézout's Theorem

□ Lemma 1.

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

✧ *Proof.*

◆ By *Theorem.1*, there exists integers s and t such that $sa + tb = 1$, or $sa + tbc = c$.

◆ Since $a \mid sa$ and $a \mid tbc$.

◆ Therefore $a \mid c$.

2.3.3 Bézout's Theorem

□ Lemma 1.

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

□ Lemma 2.

- ✧ If p is a prime and $p \mid a_1 a_2 \dots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i .

- ✧ *Proof.*

- ♦ If $\gcd(p, a_1) = 1$ then by *Lemma.1* it should be $p \mid a_2 a_3 \dots a_n$.
and if $\gcd(p, a_2) = 1$, by *Lemma.1* again, it should be $p \mid a_3 \dots a_n$.

... ..

until an i ($i \leq n$) found such that $\gcd(p, a_i) \neq 1$.

- ♦ In this case $p \mid a_i$ for p is a prime.
- ♦ The existence of such an i is assured, or $\gcd(p, a_1 a_2 \dots a_n) = 1$, a contradiction.

2.3.3 Bézout's Theorem

□ *Lemma 1.*

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

□ *Lemma 2.*

✧ If p is a prime and $p \mid a_1 a_2 \dots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i .

□ *Lemma 3.*

✧ The uniqueness of the prime factorization of a positive integer.

✧ *Proof.*

2.3.3 Bézout's Theorem

□ Lemma 1.

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

□ Theorem 2.

✧ Let m be a positive integer, a, b and c be integers, $c \neq 0$. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

✧ *Proof.*

♦ $ac \equiv bc \pmod{m}$ means $m \mid (ac - bc)$. That is $m \mid (a - b)c$.

♦ Now $\gcd(c, m) = 1$. By *Lemma 1*, we have

$m \mid (a - b)$. That is $a \equiv b \pmod{m}$.

2.3.3 Bézout's Theorem

□ *Remark.*

✧ Let m be a positive integer, and a, b be integers. The following descriptions are equivalent:

- ◆ $a \equiv b \pmod{m}$.
- ◆ $a - b = km$ for some integer k .
- ◆ $m \mid (a - b)$.
- ◆ $a \bmod m = b \bmod m$.

2.3.4 Linear Congruence

2.3.4 Linear Congruence (线性同余式/线性同余方程/模线性方程)

□ *Definition 1.*

✧ A congruence of the form

$$ax \equiv b \pmod{m}.$$

where m is a positive integer as the moduli, a and b are integers, and x is a variable, is called a **linear congruence**. (线性同余式)

□ *Question.*

✧ How to find all integers x that satisfy the congruence?

□ *Definition 2.*

✧ For integer a and moduli m , if there is an integer y such that the linear congruence

$$ya \equiv 1 \pmod{m},$$

holds, then y is said to be an **inverse** of a modulo m . (a 的模 m 逆元)

□ *Remark.*

✧ Acquiescently, m is a positive integer as the moduli of the congruence.

✧ $ya \equiv 1 \pmod{m}$ means $(ya - 1) = km$ for some integer k .

2.3.4 Linear Congruence

□ *Theorem 3.*

- ✧ If a and m are relatively prime integers, $a > 0$ and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m . (模 m 逆元存在与唯一性定理)

□ *Remark.*

- ✧ If the condition $\gcd(a, m) = 1$, $m > 1$ holds, then
 - ◆ there is a unique positive integer, less than m , denoted by a^{-1} , that is an inverse of a modulo m , and any other inverse of a modulo m is congruence to a^{-1} modulo m .
- ✧ *Theorem.3* is proved by the method of existence proof, applying the *Extended_Euclidean Algorithm*, finding such an inverse of a modulo m .

2.3.4 Linear Congruence

□ Theorem 3.

- ✧ If a and m are relatively prime integers, $a > 0$ and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m .

□ Example.

- ✧ Find an inverse of 3 modulo 7.
- ✧ *Solution.*
- ✧ $\gcd(3, 7) = 1$. Then by *Theorem.3*, the inverse of 3 modulo 7 exists.
- ✧ We use the *Euclidean Algorithm* (or *Extended_Euclidean Algorithm*) to find $\gcd(3, 7)$. It ends at $7 = 2 \cdot 3 + 1$.
- ✧ As the example following *Theorem.1*, by *working backward* through the divisions of the *Euclidean Algorithm*, we get $-2 \cdot 3 + 1 \cdot 7 = 1$.
 - ◆ Now $a = 3$, $m = 7$ and $\gcd(a, m) = 1$.
 - ◆ By *Theorem.1*, there exists integer s and t such that $sa + tm = \gcd(a, m) = 1$ or $(sa - 1) = -tm$.
 - ◆ By *Definition.2*, s is an inverse of a modulo m .
- ✧ So -2 is an inverse of 3 modulo 7.
- ✧ Every integers congruent to -2 modulo 7 is an inverse of 3 modulo 7, such as 5, -9 , 12, and so on.

2.3.4 Linear Congruence

□ Theorem 3.

- ✧ If a and m are relatively prime integers, $a > 0$ and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m .

□ Example.

- ✧ Find the solutions of $3x \equiv 4 \pmod{7}$.
- ✧ *Solution.*
- ✧ We already know -2 is an inverse of 3 modulo 7: $-2 \cdot 3 \equiv 1 \pmod{7}$.
- ✧ The congruence $3x \equiv 4 \pmod{7}$ means $3x \bmod 7 = 4 \bmod 7$.
- ✧ Multiplying both sides of the equation by -2 shows that
$$-2 \cdot 3x \bmod 7 = -2 \cdot 4 \bmod 7.$$
- ✧ But
$$\begin{aligned} -2 \cdot 3x \bmod 7 &= [(-2 \cdot 3 \bmod 7) \cdot (x \bmod 7)] \bmod 7 \\ &= [1 \cdot (x \bmod 7)] \bmod 7 = x \bmod 7. \end{aligned}$$
- ✧ Therefore
$$x \bmod 7 = -2 \cdot 4 \bmod 7 = -8 \bmod 7 = 6 \bmod 7 = \dots$$
- ✧ That is $x \equiv 6 \pmod{7}$.
- ✧ The solution are all the x such that $x \equiv 6 \pmod{7}$: 6, 13, 20, . . . , and -1, -8, -15, . . .

2.3.4 Linear Congruence

□ *Remark.*

- ✧ How to **working backward** through the divisions of the *Euclidean Algorithm*? By the Algorithm we have the sequence of

$$a_0 = b_0q_1 + b_1$$

$$b_0 = b_1q_2 + b_2$$

$$b_1 = b_2q_3 + b_3$$

...

$$b_{k-1} = b_kq_{k+1} + b_{k+1}$$

$$b_k = b_{k+1}q_{k+2} + \text{gcd}(a_0, b_0)$$

$$b_{k+1} = b_{k+2}q_{k+3} \cdot$$

- ✧ $\text{gcd}(a_0, b_0)$ is the last non-zero remainder.
- ✧ Then $\text{gcd}(a_0, b_0) = f(b_k, b_{k+1}, q_{k+2}) = f^{(1)}(b_{k-1}, b_k, q_{k+1}, q_{k+2})$
 $= f^{(2)}(b_{k-2}, b_{k-1}, q_k, q_{k+1}, q_{k+2}) = \dots$
 $= f^{(k+1)}(a_0, b_0, q_1, q_2, q_3, \dots, q_{k+2})$

2.3.4 Linear Congruence

□ Example.

✧ To find $\gcd(287, 91)$, by *Euclidean Algorithm* we have the sequence of

$$287 = 91 \cdot 3 + 14$$

$$91 = 14 \cdot 6 + 7$$

$$14 = 7 \cdot 2 + 0$$

✧ Or let

$$a_0 = 287, b_0 = 91,$$

$$a_0 = b_0 q_1 + b_1$$

$$b_0 = b_1 q_2 + b_2$$

$$b_1 = b_2 q_3, \text{ here } \gcd(a_0, b_0) = b_2 (= 7)$$

✧ Then

$$\begin{aligned} \gcd(a_0, b_0) &= b_2 = b_0 - b_1 q_2 = b_0 - (a_0 - b_0 q_1) q_2 \\ &= -a_0 q_2 + b_0 (1 + q_1 q_2) \\ &= -6a_0 + 19b_0 \end{aligned}$$

2.3.4 Linear Congruence

□ Example.

✧ Find an inverse of 101 modulo 4620.

✧ *Solution.*

✧ To find $\gcd(101, 4620)$, by *Euclidean Algorithm* we have the sequence of

$$4620 = 45 \cdot 101 + 75$$

$$101 = 1 \cdot 75 + 26$$

$$75 = 2 \cdot 26 + 23$$

$$26 = 1 \cdot 23 + 3$$

$$23 = 7 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1.$$

remainders

$\gcd(101, 4620)=1$

quotients

2.3.4 Linear Congruence

□ Example.

✧ Find an inverse of 101 modulo 4620.

✧ *Solution.*

✧ Now $\gcd(101, 4620) = 1$. We can find the *Bézout coefficients* for 101 and 4620 by working backwards through these steps, expressing $\gcd(101, 4620) = 1$ in terms of each successive pair of remainders.

$$\begin{aligned}1 &= 3 - 1 \cdot 2 \\&= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\&= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \\&= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26 \\&= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75 \\&= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) \\&= -35 \cdot 4620 + 1601 \cdot 101.\end{aligned}$$

✧ Now -35 and 1601 are *Bézout coefficients* of 4620 and 101, and 1601 is an inverse of 101 modulo 4620.

2.3.4 Linear Congruence

□ Example.

✧ Find an inverse of 101 modulo 4620.

✧ *Solution.*

✧ Now $\gcd(101, 4620) = 1$. We can find the *Bézout coefficients* for 101 and 4620 by working backwards through these steps, expressing $\gcd(101, 4620) = 1$ in terms of each successive pair of remainders.

$$\begin{aligned}1 &= 3 - 1 \cdot 2 \\&= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\&= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \\&= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26 \\&= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75 \\&= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) \\&= -35 \cdot 4620 + 1601 \cdot 101.\end{aligned}$$

reserving

✧ Now -35 and 1601 are *Bézout coefficients* of 4620 and 101, and 1601 is an inverse of 101 modulo 4620.

2.3.4 Linear Congruence

□ Example.

✧ Find an inverse of 101 modulo 4620.

✧ *Solution.*

✧ Now $\gcd(101, 4620) = 1$. We can find the *Bézout coefficients* for 101 and 4620 by working backwards through these steps, expressing $\gcd(101, 4620) = 1$ in terms of each successive pair of remainders.

$$\begin{aligned}1 &= 3 - 1 \cdot 2 \\&= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\&= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \\&= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26 \\&= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75 \\&= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) \\&= -35 \cdot 4620 + 1601 \cdot 101.\end{aligned}$$

expanding

✧ Now -35 and 1601 are *Bézout coefficients* of 4620 and 101, and 1601 is an inverse of 101 modulo 4620.

2.3.4 Linear Congruence

□ Example.

✧ Find an inverse of 101 modulo 4620.

✧ *Solution.*

✧ Now $\gcd(101, 4620) = 1$. We can find the *Bézout coefficients* for 101 and 4620 by working backwards through these steps, expressing $\gcd(101, 4620) = 1$ in terms of each successive pair of remainders.

$$1 = 3 - 1 \cdot 2$$

$$= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$$

$$= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$$

$$= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26$$

$$= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75$$

$$= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$$

$$= -35 \cdot 4620 + 1601 \cdot 101.$$

coefficients

✧ Now -35 and 1601 are *Bézout coefficients* of 4620 and 101, and 1601 is an inverse of 101 modulo 4620.

2.3.5 The Extended *Euclidean* Algorithm

2.3.5 The Extended *Euclidean* Algorithm (扩展欧几里德算法)

□ Remark.

- ✧ Let $ax + by = \gcd(a, b)$, $a \geq b > 0$. (Theorem.1)
 - ✧ How to find x , y , and $\gcd(a, b)$? (Diophantus equation)
 - ✧ Let $a' = b$, $b' = a \bmod b$. By *Bézout's Theorem* we have
$$\gcd(a', b') = a'x' + b'y' \quad \text{or}$$
$$\gcd(b, a \bmod b) = bx' + (a \bmod b)y'.$$
 - ✧ By *Lemma 0*, we know that
$$\gcd(a, b) = \gcd(b, a \bmod b) = \gcd(a', b').$$
 - ✧ Then
$$\begin{aligned}\gcd(a, b) &= \gcd(a', b') \\ &= a'x' + b'y' \\ &= bx' + (a \bmod b)y' \\ &= bx' + (a - (a \operatorname{div} b)b)y' \\ &= ay' + b(x' - (a \operatorname{div} b)y')\end{aligned}$$
- So $x = y'$, and $y = x' - (a \operatorname{div} b)y'$ is a solution to the equation $ax + by = \gcd(a', b') = \gcd(a, b)$.

2.3.5 The Extended_Euclidean Algorithm

□ Remark.

✧ Let $a'' = b'$, $b'' = a' \bmod b'$ we also have

$$\gcd(a'', b'') = a'y'' + b'(x'' - (a' \operatorname{div} b')y'').$$

So $x' = y''$, and $y' = x'' - (a' \operatorname{div} b')y''$ is a solution to the equation

$$a'x' + b'y' = \gcd(a'', b'') = \gcd(a', b') = \gcd(a, b).$$

✧ Let $a^{(3)} = b''$, $b^{(3)} = a'' \bmod b''$ we also have

$$\gcd(a^{(3)}, b^{(3)}) = a''y^{(3)} + b''(x^{(3)} - (a'' \operatorname{div} b'')y^{(3)}).$$

So $x'' = y^{(3)}$, and $y'' = x^{(3)} - (a'' \operatorname{div} b'')y^{(3)}$.

.....

✧ Let $a^{(k+1)} = b^{(k)}$, $b^{(k+1)} = a^{(k)} \bmod b^{(k)}$ we have

$$\gcd(a^{(k+1)}, b^{(k+1)}) = a^{(k)}y^{(k+1)} + b^{(k)}(x^{(k+1)} - (a^{(k)} \operatorname{div} b^{(k)})y^{(k+1)}).$$

So $x^{(k)} = y^{(k+1)}$, and $y^{(k)} = x^{(k+1)} - (a^{(k)} \operatorname{div} b^{(k)})y^{(k+1)}$.

✧ Continue this process until $b^{(k+1)} = a^{(k)} \bmod b^{(k)} = 0$ obtained.

✧ Then $\gcd(a, b) = \gcd(a', b') = \gcd(a'', b'')$

$$= \dots$$

$$= \gcd(a^{(k+1)}, b^{(k+1)})$$

$$= \gcd(a^{(k+1)}, 0)$$

$$= a^{(k+1)} (=b^{(k)}).$$

2.3.5 The Extended_*Euclidean* Algorithm

□ *Remark.*

✧ Since we have

$$\gcd(a, b) = a^{(k+1)}.$$

✧ Then The equation

$$a^{(k+1)}x^{(k+1)} + b^{(k+1)}y^{(k+1)} = \gcd(a, b).$$

has a solution

$$x^{(k+1)} = 1, y^{(k+1)} = 0.$$

◆ in fact, $y^{(k+1)}$ can take any positive integer because $b^{(k+1)}=0$.

2.3.5 The Extended_Euclidean Algorithm

□ *Remark.*

✧ Since we have

$$\gcd(a, b) = a^{(k+1)}.$$

✧ Then The equation

$$a^{(k+1)}x^{(k+1)} + b^{(k+1)}y^{(k+1)} = \gcd(a, b).$$

has a solution

$$x^{(k+1)} = 1, y^{(k+1)} = 0.$$

◆ in fact, $y^{(k+1)}$ can take any positive integer because $b^{(k+1)}=0$.

✧ If we have put every $a^{(i)}$ and $b^{(i)}$ in the process on record, by working backward,

$$x^{(k)} = y^{(k+1)}, \text{ and } y^{(k)} = x^{(k+1)} - (a^{(k)} \text{ div } b^{(k)})y^{(k+1)}.$$

we can finally find x and y .

2.3.5 The Extended_*Euclidean* Algorithm

❑ *The Extended_Euclidean Algorithm.*

```
ADT triple {  
    x, y, d: longint;  
} ee;  
triple function Extended_Euclid(a, b: positive integers)  
begin  
    if b=0 then  
        return(1, 0, a);  
    ee := Extended_Euclid (b, a mod b);  
    x := ee.y;  
    y := ee.x - (a div b)*ee.y;  
    return (x, y, ee.d);  
end;
```


2.3.5 The Extended_Euclidean Algorithm

□ Example.

✧ Find $\gcd(662, 414)$.

✧ *Solution.*

✧ Construct a forward procedure


$$a^{(k+1)} = b^{(k)},$$

$$b^{(k+1)} = a^{(k)} \bmod b^{(k)}.$$

until $k = 5$, $b^{(5)} = 0$.

✧ We get

$$\gcd(a, b) = a^{(5)} = b^{(4)} = 2.$$



k	a	b
0	662	414
1	414	248
2	248	166
3	166	82
4	82	2
5	2	0

2.3.5 The Extended_Euclidean Algorithm

□ Example.

✧ Find gcd(662, 414).

✧ *Solution.*

✧ Construct a forward procedure

$$a^{(k+1)} = b^{(k)},$$

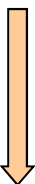
$$b^{(k+1)} = a^{(k)} \bmod b^{(k)}.$$

until $k = 5$, $b^{(5)} = 0$.

✧ We get

$$\gcd(a, b) = a^{(5)} = b^{(4)} = 2.$$

✧ Take $x^{(5)}=1$, $y^{(5)}=0$.



k	a	b	x	y
0	662	414		
1	414	248		
2	248	166		
3	166	82		
4	82	2		
5	2	0	1	0

2.3.5 The Extended_Euclidean Algorithm

□ Example.

✧ Find $\gcd(662, 414)$.

✧ *Solution.*

✧ Construct a forward procedure

$$a^{(k+1)} = b^{(k)},$$

$$b^{(k+1)} = a^{(k)} \bmod b^{(k)}.$$

until $k = 5$, $b^{(5)} = 0$.

✧ We get

$$\gcd(a, b) = a^{(5)} = b^{(4)} = 2.$$

✧ Take $x^{(5)}=1$, $y^{(5)}=0$.

✧ Construct a backward process

$$x^{(k)} = y^{(k+1)},$$

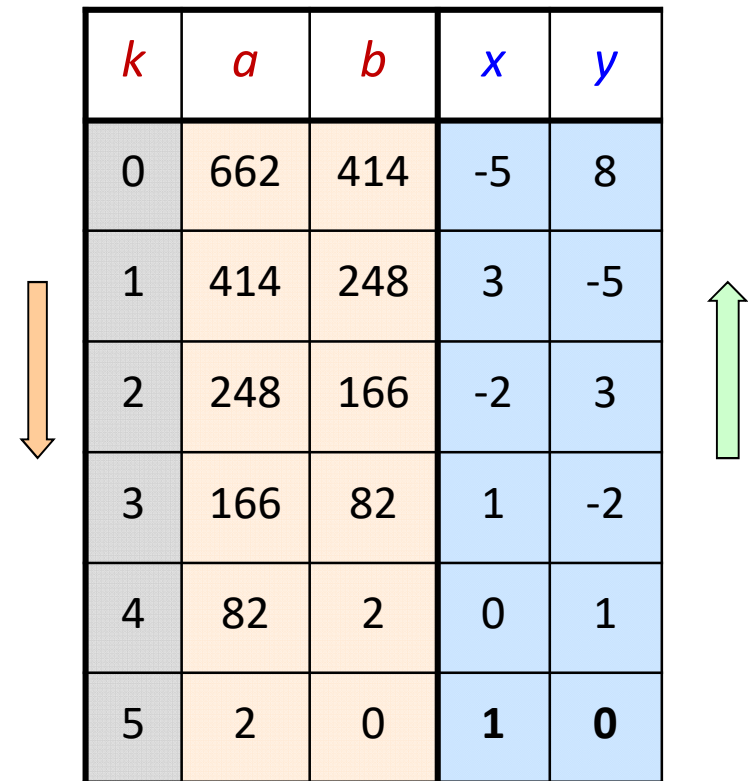
$$y^{(k)} = x^{(k+1)} - (a^{(k)} \text{ div } b^{(k)})y^{(k+1)}.$$

✧ Now the *Diophantus* equation

$$662x + 414y = \gcd(662, 414)$$

has a solution of

$$x = -5, y = 8.$$



k	a	b	x	y
0	662	414	-5	8
1	414	248	3	-5
2	248	166	-2	3
3	166	82	1	-2
4	82	2	0	1
5	2	0	1	0

2.3.6 The Chinese Remainder Theorem

2.3.6 The Chinese Remainder Theorem (中国剩余定理)

□ Remark.

✧ In 4ST century, the Chinese mathematician *Sun-Tsu* ask: There are certain things whose number is unknown. When divided by 3 , the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?

- ◆ 《孙子算经》[魏晋南北朝]: 有物不知其数, 三分之余二, 五分之余三, 七分之余二, 此物几何?
- ◆ 《数书九章》大衍求一术
 - 求解一次同余式组, [南宋]秦九韶 1247。
- ◆ The notion of congruence was first introduced and used by *Carolus Fridericus Gauss* in his *Disquisitiones Arithmeticae* (算术探究) of 1801. This puzzle can be: What are the solutions of the systems of congruence

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

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}.$$

2.3.6 The Chinese Remainder Theorem

□ Theorem 4.

- ✧ Let m_1, m_2, \dots, m_n be pairwise relatively prime positive integers and a_1, a_2, \dots, a_n arbitrary integers. Then the congruence system

$$\left. \begin{array}{l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n} \end{array} \right\} \text{system } S.$$

has a unique solution modulo m , $m = m_1 m_2 \dots m_n$.

- ✧ That is, there is a solution x with $0 \leq x < m$ to the system, and all other solutions to the system are congruent modulo m to this solution.

2.3.6 The Chinese Remainder Theorem

□ Theorem 4.

✧ Proof.

- ◆ Let $M_k = m/m_k$ for $k=1, 2, \dots, n$. That is, M_k is the product of the moduli except for m_k , and
$$(M_s \bmod m_k) = 0 \text{ for } s \neq k.$$
- ◆ Now we have
$$\gcd(M_k, m_k) = 1 \text{ for } k=1, 2, \dots, n$$
because m_1, m_2, \dots, m_n are pairwise relatively prime integers.
- ◆ From Theorem.3, there is an integer y_k , an inverse of M_k modulo m_k , such that

$$M_k y_k \equiv 1 \pmod{m_k}, k = 1, 2, \dots, n.$$

- ◆ Now form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n.$$

- ◆ Then x is a simultaneous solution by showing

$$\begin{aligned} x \bmod m_k &= (a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n) \bmod m_k \\ &= a_k M_k y_k \bmod m_k = a_k \bmod m_k, k = 1, 2, \dots, n. \end{aligned}$$

- ◆ That is

$$x \equiv a_k \pmod{m_k}, k = 1, 2, \dots, n.$$

2.3.6 The Chinese Remainder Theorem

□ Theorem 4.

✧ Proof.

- ◆ Let x_1 and x_2 , $x_1 > x_2$, be two different solutions of the congruence system:

$$x \equiv a_k \pmod{m_k}, k = 1, 2, \dots, n.$$

- ◆ Then

$$x_1 - a_i = s_i m_i, \text{ for some integer } s_i, i = 1, 2, \dots, n, \text{ and}$$

$$x_2 - a_i = t_i m_i, \text{ for some integer } t_i, i = 1, 2, \dots, n.$$

- ◆ Thus $x_1 - x_2 = (s_i - t_i) m_i, i = 1, 2, \dots, n.$

○ In another word, $x_1 - x_2 \equiv 0 \pmod{m_i}, i = 1, 2, \dots, n.$

and m_i is a factor of $x_1 - x_2, i = 1, 2, \dots, n.$

- ◆ In another hand, m_1, m_2, \dots, m_n are pairwise relatively prime integers. Hence $m = m_1 m_2 \dots m_n$ is also a factor of $x_1 - x_2.$
- ◆ This means $x_1 - x_2 \geq m.$
- ◆ Therefore, there is only one solution modulo $m.$

2.3.6 The Chinese Remainder Theorem

□ Example.

✧ Find the solutions of the systems of congruence system

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

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}.$$

✧ Solution.

✧ Let $m = 3 \cdot 5 \cdot 7 = 105$, then

$$M_1 = 5 \cdot 7 = 35, y_1 = 2 \text{ (an inverse of } M_1 \text{ modulo 3).}$$

$$M_2 = 3 \cdot 7 = 21, y_2 = 1 \text{ (an inverse of } M_2 \text{ modulo 5).}$$

$$M_3 = 3 \cdot 5 = 15, y_3 = 1 \text{ (an inverse of } M_3 \text{ modulo 7).}$$

✧ A solution is

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 233 \equiv 23 \pmod{105}.$$

✧ The numbers of things to Sun-Tsu's example is $23 + k \cdot 105$, $k = 0, 1, 2, \dots$

2.3.6 The Chinese Remainder Theorem

□ Remark.

✧ Let m_1, m_2, \dots, m_n ($m_i \geq 2, i=1, 2, \dots, n$) be pairwise relatively prime positive integers and $m = m_1 m_2 \dots m_n$.

✧ Applying the *Chinese Remainder Theorem* we construct the relation

$$R: (a_1, a_2, \dots, a_n) \rightarrow x,$$

from Cartesian product $A_1 \times A_2 \times \dots \times A_n$ to M .

Here $A_i = \{0, 1, \dots, m_i - 1\}$, $M = \{0, 1, \dots, m - 1\}$, and $x \in M$ is a solution to the system: $x \equiv a_i \pmod{m_i}, i=1, 2, \dots, n$.

✧ We show that R is a bijection.

(1) By the *Chinese Remainder Theorem*, x is determined uniquely from any given (a_1, a_2, \dots, a_n) , thus R has its functionality.

(2) If x is the image of two n -tuple (a_1, a_2, \dots, a_n) and (b_1, b_2, \dots, b_n) in R .

Think that x is a solution to the system $x \equiv a_i \pmod{m_i}$ and also a solution to $x \equiv b_i \pmod{m_i}, i=1, 2, \dots, n$. Then

$$a_i \pmod{m_i} = b_i \pmod{m_i}, i=1, 2, \dots, n.$$

Considering $a_i < m_i$ and $b_i < m_i$ for any i , it has to be

$$a_i = b_i, i=1, 2, \dots, n$$

This means R is one-to-one.

2.3.6 The Chinese Remainder Theorem

□ Remark.

✧ Let m_1, m_2, \dots, m_n ($m_i \geq 2, i=1, 2, \dots, n$) be pairwise relatively prime positive integers and $m = m_1 m_2 \dots m_n$.

✧ Applying the *Chinese Remainder Theorem* we construct the relation

$$R: (a_1, a_2, \dots, a_n) \rightarrow x,$$

from Cartesian product $A_1 \times A_2 \times \dots \times A_n$ to M .

Here $A_i = \{0, 1, \dots, m_i - 1\}$, $M = \{0, 1, \dots, m - 1\}$, and $x \in M$ is a solution to the system: $x \equiv a_i \pmod{m_i}, i=1, 2, \dots, n$.

✧ We show that R is a bijection.

(3) Any integer $x \in M$ can be uniquely represented by the n-tuple in the Cartesian product $A_1 \times A_2 \times \dots \times A_n$

$$(a_1, a_2, \dots, a_n), a_i = x \bmod m_i, i=1, 2, \dots, n.$$

✧ It is easy to find that x is a solution of the system

$$x \equiv a_i \pmod{m_i}, i=1, 2, \dots, n.$$

✧ This means the constructed n-tuple (a_1, a_2, \dots, a_n) is the preimage of x in relation R and R is onto.

2.3.6 The Chinese Remainder Theorem

□ Example.

- ✧ Let m_1, m_2, \dots, m_n ($m_i \geq 2, i=1, 2, \dots, n$) be pairwise relatively prime positive integers and $m = m_1 m_2 \dots m_n$.
- ✧ Any integer $x \in M = \{0, 1, \dots, m-1\}$ can be uniquely represented by the n-tuple:

$$(a_1, a_2, \dots, a_n), a_i = x \bmod m_i, i=1, 2, \dots, n.$$

- ✧ Keeping (m_1, m_2, \dots, m_n) in secret, it is very difficult to decrypt x from (a_1, a_2, \dots, a_n) .
- ✧ As in Sun-Tsu's example, $(m_1, m_2, m_3) = (3, 5, 7)$ is the secret key. The number $x=23$ is represented by $(a_1, a_2, a_3) = (2, 3, 2)$:

$$a_1 = x \bmod m_1 = 23 \bmod 3 = 2$$

$$a_2 = x \bmod m_2 = 23 \bmod 5 = 3$$

$$a_3 = x \bmod m_3 = 23 \bmod 7 = 2$$

2.3.7 Euler's φ function

2.3.7 Euler's φ function (Euler's Totient function, 欧拉 φ 函数)

□ *Definition.*

- ✧ For a positive integer m , consider the ring $Z_m = \{0, \dots, m-1\}$. Euler's φ function $\varphi(m)$ is the number of integers in Z_m which are coprime to m .
 - ◆ Denoting the collection of all the integers coprime to m in Z_m as Z'_m , then $\varphi(m) = |Z'_m|$.
 - ◆ Z'_m is called the reduced residue system of m (m 的既约剩余系).
 - ◆ $\varphi(m)$ is the number of positive integers less than and prime to m .

□ *Example.*

- ✧ $\varphi(8) = 4$.
 - ◆ 1, 3, 5, 7 are coprime to 8. Then $Z'_8 = \{1, 3, 5, 7\}$.
- ✧ Conventionally, $\varphi(1) = 1$.

2.3.7 Euler's ϕ function

□ Lemma 4.

✧ Let $m = p^k$, p is prime and k is positive. Then $\phi(m) = \phi(p^k) = p^k - p^{k-1}$.

✧ *Proof.*

- ◆ An integer n is coprime to $m = p^k$ (p is prime) if and only if it contains no p as its factor. Integers in Z_m containing p as factor are $1p, 2p, 3p, \dots, p^{(k-1)}p$.
- ◆ Remove them from Z_m , $m - p^{k-1} = p^k - p^{k-1}$ number of integers are left which are coprime to m .

□ Example.

✧ $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 4$.

□ Remark

✧ When $k=1$, The equation becomes $\phi(p) = p - 1$.

✧ The equation can be the form of

$$\phi(p^k) = p^k - p^{k-1} = p^k (1 - 1/p).$$

2.3.7 Euler's ϕ function

□ Lemma 5.

✧ $\phi(p) = p-1$ if p is prime. ($p \neq 1$ because 1 is not prime)

✧ *Proof.*

◆ For prime p is coprime to any positive integer less than p , that is
 $Z'_p = \{1, 2, \dots, p-1\}$.

□ Example.

✧ $Z'_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. $\phi(11) = 10$.

□ Lemma 6.

✧ Let $m = pq$, p and q are positive integers and are *relatively prime*. Then

$$\phi(m) = \phi(pq) = \phi(p)\phi(q).$$

✧ *Proof.*

◆ See next slide.

□ Example.

✧ $\phi(56) = \phi(8 \times 7) = \phi(8) \times \phi(7) = 4 \times 6 = 24$.

✧ A misunderstanding:

$$\phi(56) = \phi(8 \times 7) = \phi(8) \times \phi(7) = (8-1) \times (7-1) = 42.$$

2.3.7 Euler's φ function

□ Lemma 6.

✧ Let $m = pq$, p and q are positive integers and are *relatively prime*. Then

$$\varphi(m) = \varphi(pq) = \varphi(p)\varphi(q).$$

✧ *Proof.*

(1) Let $a \in Z_p$, $b \in Z_q$, $x \in Z_{pq}$. Applying the *Chinese Remainder Theorem*, the relation $R: (a, b) \rightarrow x$ from $Z_p \times Z_q$ to Z_{pq} is a bijection. Here x is the unique solution of the congruence system (modulo pq):

$$x \equiv a \pmod{p}, x \equiv b \pmod{q}.$$

○ See *slide 41: Remark*.

(2) We prove that “ $\gcd(p, a) = 1$ and $\gcd(q, b) = 1$ ” \Leftrightarrow “ $\gcd(pq, x) = 1$ ”.

\Leftarrow Let $\gcd(pq, x) = 1$.

- ◆ From $x \equiv a \pmod{p}$ we have $x = k'p + a$ for some integer k' .
- ◆ By *Lemma 0* we get $\gcd(x, p) = \gcd(p, a)$.
- ◆ Suppose that $\gcd(p, a) = k$, then $a = a'k$, $p = p'k$ for some a' and p' . Then $x = k'p + a = k'p'k + a'k = k(k'p' + a')$.

2.3.7 Euler's φ function

□ Lemma 6.

✧ Let $m = pq$, p and q are positive integers and are *relatively prime*. Then

$$\varphi(m) = \varphi(pq) = \varphi(p)\varphi(q).$$

✧ *Proof.*

(1) Let $a \in Z_p$, $b \in Z_q$, $x \in Z_{pq}$. Applying the *Chinese Remainder Theorem*, the relation $R: (a, b) \rightarrow x$ from $Z_p \times Z_q$ to Z_{pq} is a bijection. Here x is the unique solution of the congruence system (modulo pq):

$$x \equiv a \pmod{p}, x \equiv b \pmod{q}.$$

○ See *slide 41: Remark*.

(2) We prove that “ $\gcd(p, a) = 1$ and $\gcd(q, b) = 1$ ” \Leftrightarrow “ $\gcd(pq, x) = 1$ ”.

\Leftarrow Let $\gcd(pq, x) = 1$.

- ◆ From $x \equiv a \pmod{p}$ we have $x = k'p + a$ for some integer k' .
- ◆ By *Lemma 0* we get $\gcd(x, p) = \gcd(p, a)$.
- ◆ Suppose that $\gcd(p, a) = k$, then $a = a'k$, $p = p'k$ for some a' and p' .
Then $x = k'p + a = k'p'k + a'k = k(k'p' + a')$.

2.3.7 Euler's ϕ function

□ Lemma 6.

✧ Let $m = pq$, p and q are positive integers and are *relatively prime*. Then

$$\phi(m) = \phi(pq) = \phi(p)\phi(q).$$

✧ *Proof.*

(1) Let $a \in Z_p$, $b \in Z_q$, $x \in Z_{pq}$. Applying the *Chinese Remainder Theorem*, the relation $R: (a, b) \rightarrow x$ from $Z_p \times Z_q$ to Z_{pq} is a bijection. Here x is the unique solution of the congruence system (modulo pq):

$$x \equiv a \pmod{p}, x \equiv b \pmod{q}.$$

○ See *slide 41: Remark*.

(2) We prove that “ $\gcd(p, a) = 1$ and $\gcd(q, b) = 1$ ” \Leftrightarrow “ $\gcd(pq, x) = 1$ ”.

\Leftarrow Let $\gcd(pq, x) = 1$.

- ◆ From $x \equiv a \pmod{p}$ we have $x = k'p + a$ for some integer k' .
- ◆ By *Lemma 0* we get $\gcd(x, p) = \gcd(p, a)$.
- ◆ Suppose that $\gcd(p, a) = k$, then $a = a'k$, $p = p'k$ for some a' and p' . Then $x = k'p + a = k'p'k + a'k = k(k'p' + a')$.
- ◆ That is, k is a common divisor of p and x . But $\gcd(pq, x) = 1$. So it has to be $k = 1$, and hence $\gcd(p, a) = 1$.
- ◆ In the same way, we can prove that $\gcd(p, b) = 1$.

2.3.7 Euler's φ function

□ Lemma 6.

✧ Let $m = pq$, p and q are positive integers and are *relatively prime*. Then

$$\varphi(m) = \varphi(pq) = \varphi(p)\varphi(q).$$

✧ *Proof.*

(1) Let $a \in Z_p$, $b \in Z_q$, $x \in Z_{pq}$. Applying the *Chinese Remainder Theorem*, the relation $R: (a, b) \rightarrow x$ from $Z_p \times Z_q$ to Z_{pq} is a bijection. Here x is the unique solution of the congruence system (modulo pq):

$$x \equiv a \pmod{p}, x \equiv b \pmod{q}.$$

(2) We prove that “ $\gcd(p, a) = 1$ and $\gcd(q, b) = 1$ ” \Leftrightarrow “ $\gcd(pq, x) = 1$ ”.

\Rightarrow Let $\gcd(p, a) = 1$ and $\gcd(q, b) = 1$.

- ◆ From $x = k'p + a$, we get $\gcd(x, p) = \gcd(p, a) = 1$.
- ◆ From $x = k''q + b$, we get $\gcd(x, q) = \gcd(q, b) = 1$.
- ◆ Suppose that $\gcd(pq, x) = k$, then $k \mid pq$ and $k \mid x$.
- ◆ In another hand, p and q are *relatively prime*. It has to be either $k \mid p$ or $k \mid q$.
- ◆ From $k \mid x$, $k \mid p$ and $\gcd(x, p) = 1$ we have $k = 1$.
- ◆ From $k \mid x$, $k \mid q$ and $\gcd(x, q) = 1$ we also have $k = 1$.
- ◆ Thus $\gcd(pq, x) = k = 1$.

2.3.7 Euler's ϕ function

□ Lemma 6.

✧ Let $m = pq$, p and q are positive integers and are *relatively prime*. Then

$$\phi(m) = \phi(pq) = \phi(p)\phi(q).$$

✧ *Proof.*

(1) Let $a \in Z_p$, $b \in Z_q$, $x \in Z_{pq}$. Applying the *Chinese Remainder Theorem*, the relation $R: (a, b) \rightarrow x$ from $Z_p \times Z_q$ to Z_{pq} is a bijection. Here x is the unique solution of the congruence system (modulo pq):

$$x \equiv a \pmod{p}, x \equiv b \pmod{q}.$$

(2) We prove that $\gcd(p, a) = 1$ and $\gcd(q, b) = 1 \Leftrightarrow \gcd(pq, x) = 1$.

(3) From (1) and (2), let $a \in Z'_p$, $b \in Z'_q$, then any $c \in Z'_{pq}$ can be uniquely represent as an ordered pair (a, b) . The relation

$$R' : (a, b) \rightarrow c$$

from $Z'_p \times Z'_q$ to Z'_{pq} is also a bijection. The number of c , say $|Z'_{pq}|$, is the same as $|Z'_p| \times |Z'_q|$. That is $\phi(pq) = \phi(p)\phi(q)$.

2.3.7 Euler's φ function

□ Lemma 7.

✧ Let $m = pq$, p and q are primes, $p \neq q$. Then
$$\varphi(m) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

□ Lemma 8.

✧ Let $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ where p_i are primes and $k_i > 0$ for $i=1..r$, $p_s \neq p_t$ for $1 \leq s < t \leq r$. Then

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \dots \varphi(p_r^{k_r}) \\ &= p_1^{k_1} [1 - (1/p_1)] p_2^{k_2} [1 - (1/p_2)] \dots p_r^{k_r} [1 - (1/p_r)] \\ &= m [1 - (1/p_1)] [1 - (1/p_2)] \dots [1 - (1/p_r)].\end{aligned}$$

□ Example.

✧ $\varphi(1323) = \varphi(3^3 \times 7^2) = 1323 \times (1 - 1/3) \times (1 - 1/7) = 756.$

2.3.8 Euler's Theorem

2.3.8 Euler's Theorem (欧拉定理)

□ Theorem 5.

- ✧ Let a and m be integers, $m > 0$ such that $\gcd(a, m) = 1$. Then
$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

□ Remark.

- ✧ The existence of *inverse* of a modulo m .
- ◆ As defined in *Definition.2*, for a moduli m , if there is an integer y such that
$$ya \equiv 1 \pmod{m},$$
 y is said to be an *inverse* of a modulo m .
 - ◆ Now $a^{\phi(m)} = a^{\phi(m)-1} \times a \equiv 1 \pmod{m}$. Thus $a^{\phi(m)-1}$ is an inverse of a modulo m .
- ✧ *Euler's Theorem* is a generalization (arbitrary modulus) of *Fermat's Little Theorem*.

2.3.8 Euler's Theorem

□ Theorem 5.

✧ Let a and m be integers, $m > 0$ such that $\gcd(a, m) = 1$. Then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

✧ Proof.

(1) Let $Z'_m = \{x_1, x_2, \dots, x_{\phi(m)}\}$ be the reduced residue system of m , and let $S = \{ax_1 \bmod m, ax_2 \bmod m, \dots, ax_{\phi(m)} \bmod m\}$, we prove that $Z'_m = S$.

○ For any i , $1 \leq i \leq \phi(m)$, a and x_i are all coprime to m , and then ax_i are also coprime to m . Therefore

$$ax_i \bmod m \in Z'_m.$$

○ For any $x_i, x_j \in Z'_m$, $x_i \neq x_j$ we get $ax_i \bmod m \neq ax_j \bmod m$.

Otherwise $ax_i \equiv ax_j \pmod{m}$. Now $\gcd(a, m) = 1$. By *Bézout's Theorem.2*,

$$x_i \equiv x_j \pmod{m}$$

and hence $x_i = x_j$, because $x_i, x_j < m$, a contradiction.

○ It is not depending on the necessity that $ax_i \bmod m = x_i$.

2.3.8 Euler's Theorem

□ Theorem 5.

✧ Let a and m be integers, $m > 0$ such that $\gcd(a, m) = 1$. Then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

✧ Proof.

(2) Construct

$$\begin{aligned} & (a^{\phi(m)} x_1 x_2 \dots x_{\phi(m)}) \pmod{m} \\ &= [(ax_1) (ax_2) \dots (ax_{\phi(m)})] \pmod{m} \\ &= [(ax_1 \pmod{m}) (ax_2 \pmod{m}) \dots (ax_{\phi(m)} \pmod{m})] \pmod{m} \\ &= (x_1 x_2 \dots x_{\phi(m)}) \pmod{m}. \end{aligned}$$

○ But x_i ($i = 1.. \phi(m)$) are coprime to m , and so is $x_1 x_2 \dots x_{\phi(m)}$.

○ By *Bézout's Theorem.2*, from

$$(a^{\phi(m)} x_1 x_2 \dots x_{\phi(m)}) \pmod{m} = (x_1 x_2 \dots x_{\phi(m)}) \pmod{m},$$

we have $a^{\phi(m)} \pmod{m} = 1 \pmod{m}$.

○ That is, $a^{\phi(m)} \equiv 1 \pmod{m}$.

◆ Remark.

○ *Bézout's Theorem.2* aka the Cancellation Law

• If $\gcd(c, p) = 1$, then

$$ac \equiv bc \pmod{p} \Rightarrow a \equiv b \pmod{p}.$$

2.3.8 Euler's Theorem

□ Corollary.

✧ Let p and q be primes satisfied $N=pq$. n is any integer with $0 < n < N$, k is a positive integer. Then

$$n^{k\phi(N)+1} \equiv n \pmod{N}.$$

✧ Proof.

- ◆ If $\gcd(n, N)=1$, the proof is ended by virtue of *Euler's Theorem*.
- ◆ Otherwise, without loss of generality, let $\gcd(n, N)=p$. Then $n=cp$ with some positive integer c , $0 < c < q$. It must be $\gcd(c, q)=1$ because q is prime and thus $\gcd(cp, q)=1$.
- ◆ That is $\gcd(n, q)=1$.
- ◆ By *Euler's Theorem*, $n^{\phi(q)} \equiv 1 \pmod{q}$.
- ◆ By the rules of Modular Arithmetic, $[n^{\phi(q)}]^{k\phi(p)} \equiv 1 \pmod{q}$. That is $n^{k\phi(N)} \equiv 1 \pmod{q}$,
for $\phi(N) = \phi(pq) = \phi(p)\phi(q)$.
- ◆ Therefore, there is some integer s such that $n^{k\phi(N)} - 1 = sq$.
- ◆ Multiplying each side by $n=cp$, $n^{k\phi(N)+1} - n = sqn = sqcp = scN$.
- ◆ That is, $n^{k\phi(N)+1} \equiv n \pmod{N}$.

2.3.9 Fermat's Little Theorem

2.3.9 Fermat's Little Theorem (1640, 费马小定理)

□ Theorem 6.

- ✧ If p is a *prime* number and a is an integer not divisible by p , then
$$a^{p-1} \equiv 1 \pmod{p}.$$
- ✧ Further more, if a is positive, *Fermat's Little Theorem* is equivalent to
$$a^p \equiv a \pmod{p}.$$
- ✧ *Theorem 6* can be proved directly from *Theorem 5*.

□ Example.

- ✧ $a = 13, p = 7, a^p = 13^7 = 62748517, a^{p-1} = 13^6 = 4826809$
$$a^p - a = 62748517 - 13 = 62748504 = 8964072 \times 7$$
$$a^{p-1} = 4826809 = 689544 \times 7 + 1 = qp + 1$$
- ✧ $a = 14, p = 7, a^p = 14^7 = 105413504, a^{p-1} = 14^6 = 7529536$
$$a^p - a = 105413504 - 14 = 105413490 = 15059070 \times 7$$
$$a^{p-1} = 7529536 = 1075648 \times 7 = qp, \text{Theorem.6 failed.}$$

2.3.10 Primitive Root and Discrete Logarithm

10.1 Primitive Root (原根/素根)

□ *Definition.*

- ✧ Let a and n be positive integers, $a < n$, $\gcd(a, n) = 1$. Consider the sequence

$$a, a^2, a^3, \dots$$

If m is the least positive integer such that

$$a^m \equiv 1 \pmod{n}.$$

then m is said to be the order of a modulo n (a 关于模 n 的阶/指数/生成周期), noted $m = \text{ord}_n a$, or $m = \text{ord } a$.

- ✧ By *Euler's Theorem*,

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

that is, $m = \text{ord}_n a$ exists and $m \leq \phi(n)$.

2.3.10 Primitive Root and Discrete Logarithm

10.1 Primitive Root

□ *Property 1.*

✧ If $m = \text{ord}_n a$, $k > 0$ such that

$$a^k \equiv 1 \pmod{n}.$$

then $m \mid k$.

✧ **证明:** 假设结论不成立, 即有 $k = qm + r$, $0 < r < m$. 则

$$\begin{aligned} 1 &\equiv a^k \\ &= a^{qm+r} \\ &= (a^m)^q a^r \\ &\equiv a^r \pmod{n}. \end{aligned}$$

这里 $0 < r < m$, 与 $m = \text{ord}_n a$ 矛盾。

✧ *Property 1* 表明, 如果 k 是素数, 则只能 $m = k$, 即 $\text{ord}_n a = k$; 如果 k 不是素数, 则 $\text{ord}_n a$ 存在于 k 的因子中。

2.3.10 Primitive Root and Discrete Logarithm

10.1 Primitive Root

□ *Property 2.*

✧ 若 $m = \text{ord}_n a$, 则 $\{1, a, a^2, \dots, a^{m-1}\}$ 中的各个元素模 n 两两不同余。

✧ **证明:** 假设结论不成立, 不妨设有 $j, k, 0 \leq j < k \leq m-1$, 使得

$$a^j \equiv a^k \pmod{n}.$$

由 $\gcd(a, n)=1$ 得 $\gcd(a^j, n)=1$ 。上式两边消去 a^j , 得

$$1 \equiv a^{k-j} \pmod{n}.$$

这里 $0 < k-j < m$, 与 $m = \text{ord}_n a$ 矛盾。

✧ 注意到: $a^{m+j} \bmod n = a^m a^j \bmod n$

$$= [(a^m \bmod n) (a^j \bmod n)] \bmod n$$

$$= a^j \bmod n.$$

故 a 关于模 m 的幂序列

$$a, a^2, a^3, \dots, a^{m-1}, a^m, a^{m+1}, a^{m+2}, \dots$$

的周期是 m , 即 $a, a^2, a^3, \dots, a^{m-1}, a^m, a, a^2, a^3, \dots$

2.3.10 Primitive Root and Discrete Logarithm

10.1 Primitive Root

□ Definition.

✧ Let a and n be positive integers, $a < n$, $\gcd(a, n) = 1$. If $m = \text{ord}_n a$ and $m = \phi(n)$, then a is said to be a primitive root of n . (a 称为 n 的一个原根或素根)

- ◆ **Euler's Theorem** : Let a and n be integers, $n > 0$ such that $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.
- ◆ 给定模底 n ，对于任何 $a \in \mathbb{Z}_n'$ 都有 $\gcd(a, n) = 1$ ，于是由 **Euler's Theorem** 有 $a^{\phi(n)} \equiv 1 \pmod{n}$ 。若 $\phi(n)$ 是素数，由 **Property 1** 有 $\text{ord}_n a = \phi(n)$ ， a 是 n 的素根。否则如果对 $\phi(n)$ 的任一个因子 q ， $a^q \equiv 1 \pmod{n}$ 都不成立，则 $\text{ord}_n a = \phi(n)$ ， a 是 n 的素根。
- ◆ 如果取 n 为素数 p ， a 是 p 的一个素根，则 $\phi(p) = p-1$ 是 a 关于模 p 的阶， $a^{p-1} \equiv 1 \pmod{p}$ 。类似 **Property 2** 可以证明： $\{a, a^2, \dots, a^{p-1}\}$ 中的各个元素模 p 两两不同余，从而构成了 p 的非0剩余类，即与 $\{1, 2, \dots, p-1\}$ 模 p 等价。

2.3.10 Primitive Root and Discrete Logarithm

10.1 Primitive Root

□ 例:

✧ 设模底为素数 $p = 23$ ，求其最小素根。

✧ 解:

- ◆ 目前没有求素根的一般方法，只能参照性质测试可能性，寻找满足条件 $a^{\varphi(p)} = a^{p-1} = a^{22} \equiv 1 \pmod{23}$ 的最小的 a 。
- ◆ 素分解 $\varphi(p)=22 = 2*11$ ，这是两个可能的模 p 的阶。
- ◆ 对 $a = 2, 3, \dots, 22 (=p-1)$ 逐一测试：
 - 对于某一个 a ，如果有 $a^2 \equiv 1 \pmod{23}$ 或者 $a^{11} \equiv 1 \pmod{23}$ 的情况出现，则有 $\text{ord}_p a \leq 2$ 或者 $\text{ord}_p a \leq 11$ ，因而 $\text{ord}_p a \neq \varphi(p)$ ，此时可以排除 a 是23的素根的可能性，转向测试下一个 a 。
 - 否则再测试此 a 是否能够满足 $a^{\varphi(p)} \equiv 1 \pmod{23}$ 。
- ◆ 本例最后得到的最小素根是5。

2.3.10 Primitive Root and Discrete Logarithm

10.2 Discrete Logarithm (离散对数)

□ *Definition.*

✧ 设有正整数 a 和 n , $a < n$, $\gcd(a, n) = 1$ 。若 a 是模 n 的一个素根, 则对任意整数 b , $\gcd(b, n) = 1$, 存在唯一的整数 i , $1 \leq i \leq n-1$, 使得

$$b \equiv a^i \pmod{n}.$$

i 称为 b 以 a 为基底的模 n 的指数 (离散对数), 记作 $\text{ind}_{a,n}(b)$ 。

◆ 模 n 经常被取为素数 p 。

□ 离散对数的性质:

$$(1) \text{ind}_{a,p}(1) = 0, \text{ind}_{a,p}(a) = 1.$$

$$(2) \text{ind}_{a,p}(xy) \equiv [\text{ind}_{a,p}(x) + \text{ind}_{a,p}(y)] \pmod{\varphi(p)}.$$

$$(3) \text{ind}_{a,p}(x^r) \equiv [r \times \text{ind}_{a,p}(x)] \pmod{\varphi(p)}.$$

✧ 性质 (1) 直接由定义得到; 性质 (3) 可以由性质 (2) 直接证明。

✧ 下面给出性质 (2) 的详细证明。

2.3.10 Primitive Root and Discrete Logarithm

10.2 Discrete Logarithm

□ 离散对数的性质:

$$(2) \text{ind}_{a,p}(xy) \equiv [\text{ind}_{a,p}(x) + \text{ind}_{a,p}(y)] \pmod{\phi(p)}.$$

✧ 证明

◆ 设 $i = \text{ind}_{a,p}(x)$, $j = \text{ind}_{a,p}(y)$, $k = \text{ind}_{a,p}(xy)$. 由定义得:

$$x \equiv a^i \pmod{p}, y \equiv a^j \pmod{p}, xy \equiv a^k \pmod{p}.$$

◆ 由模算术运算规则:

$$\begin{aligned} xy \bmod p &= [(x \bmod p) (y \bmod p)] \bmod p \\ &= [(a^i \bmod p) (a^j \bmod p)] \bmod p \\ &= a^{i+j} \bmod p \end{aligned}$$

◆ 因此: $a^{i+j} \bmod p = a^k \pmod{p}$, 或 $a^{i+j} \equiv a^k \pmod{p}$.

◆ 考察模 p 的周期序列

$$1, a, a^2, a^3, \dots, a^{p-1}, a^p, a^{p+1}, a^{p+2}, \dots$$

2.3.10 Primitive Root and Discrete Logarithm

10.2 Discrete Logarithm

□ 离散对数的性质:

$$(2) \text{ind}_{a,p}(xy) \equiv [\text{ind}_{a,p}(x) + \text{ind}_{a,p}(y)] \pmod{\phi(p)}.$$

✧ 证明. (continued)

- ◆ 由定义, a 是模 p 的一个素根。因此周期序列

$$1, a, a^2, a^3, \dots, a^{p-1}, a^p, a^{p+1}, a^{p+2}, \dots$$

的周期是 $\phi(p)$, 且同一周期内的各个元素模 p 两两不同余 (参见 a 关于模 n 的阶的定义部分的性质2)。

- ◆ 由于 $a^{i+j} \equiv a^k \pmod{p}$, a^{i+j} 和 a^k 在上述周期序列中的间隔必须是周期 $\phi(p)$ 的整数倍, 即存在整数 d , 使得

$$(i+j) - k = d\phi(p).$$

- ◆ 即: $k \equiv (i+j) \pmod{\phi(p)}.$
- ◆ 亦即: $\text{ind}_{a,p}(xy) \equiv [\text{ind}_{a,p}(x) + \text{ind}_{a,p}(y)] \pmod{\phi(p)}.$
- ◆ 性质 (2) 得证。

2.3.10 Primitive Root and Discrete Logarithm

10.2 Discrete Logarithm

□ 离散对数的计算:

- ✧ 对于 $C^d \equiv M \pmod{p}$, or $M \equiv C^d \pmod{p}$.
- ✧ 已知 C, p 。由 d 求 M 是容易的, 只需要进行一次求幂运算。由 M 求 d 则需要指数级计算。如果 p 取得足够大, 就能实现足够的安全强度。

□ 例:

- ✧ 求解离散对数 $\text{ind}_{3, 17}(15)$.
- ✧ 解: 问题即为求解同余式 $3^x \equiv 15 \pmod{17}$.
 - (1) 验证3是模17的一个素根;
 - (2) 逐一测试 $x = 1, 2, 3, \dots, 16$, 得到 $x=6$ 时,
$$3^6 \equiv 15 \pmod{17}.$$
成立。