2.1.3 Integer Division

In integer arithmetic, if we divide a by n, we can get q and r . The relationship between these four integers can be shown as

$$a = q \times n + r$$

Integer Division is not a binary operation because it creates 2 outputs.

2.1.3 Continued

Example 2.2

Assume that $a = 255$ and $n = 11$. We can find $q = 23$ and $r = 2$ using the division algorithm.

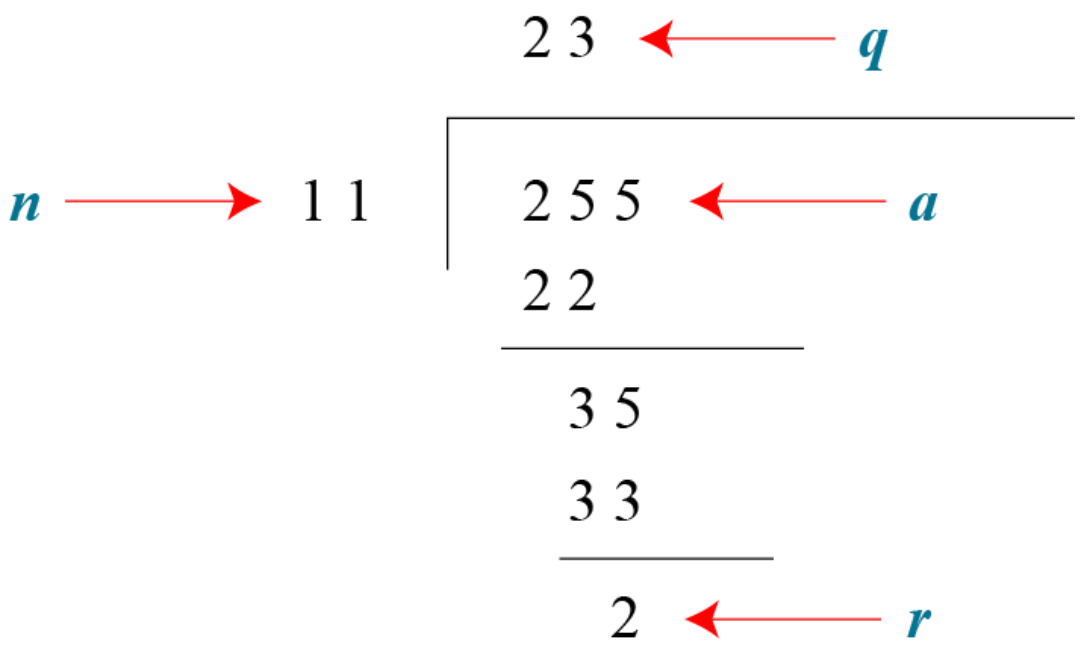


Figure 2.3 Example 2.2, finding the quotient and the remainder

2.1.4 Divisbility

If a is not zero and we let r = 0 in the division relation, we get

$$a = q \times n$$

If the remainder is zero, $n \mid a$

If the remainder is not zero, $n \nmid a$

2.1.4 Continued

Example 2.4

a. The integer 4 divides the integer 32 because $32 = 8 \times 4$. We show this as

$$4 \mid 32$$

b. The number 8 does not divide the number 42 because $42 = 5 \times 8 + 2$. There is a remainder, the number 2, in the equation. We show this as

$$8 \nmid 42$$

2.1.4 Continued

Properties

Property 1: if a|1, then a = ±1.

Property 2: if a|b and b|a, then a = ±b.

Property 3: if a|b and b|c, then a|c.

Property 4: if a|b and a|c, then a|(m × b + n × c), where m and n are arbitrary integers

2.1.4 Continued

Example 2.6

a. Since $3|15$ and $15|45$,

according to the third property, $3|45$.

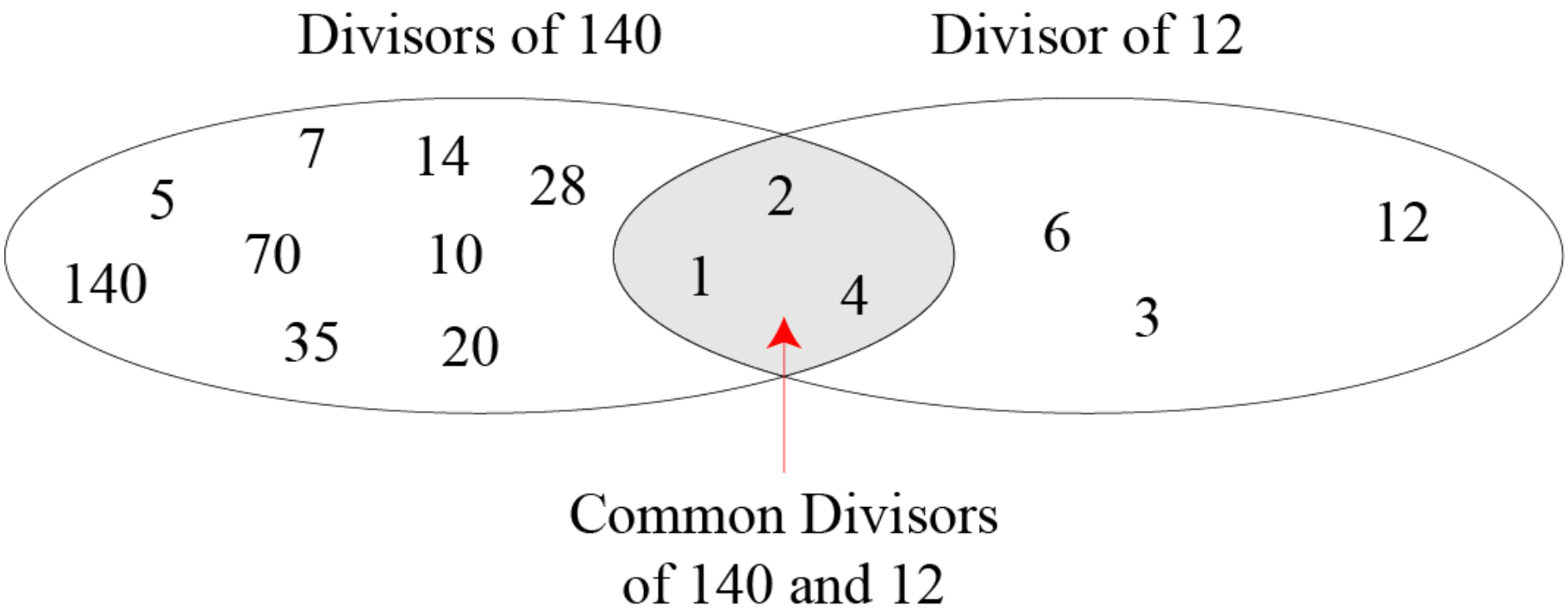
b. Since $3|15$ and $3|9$,

according to the fourth property,

$3|(15 \times 2 + 9 \times 4)$, which means $3|66$.

2.1.4 Common divisors公因數

Figure 2.6 *Common divisors of two integers*



2.1.4 Continued

Note Greatest Common Divisor

The greatest common divisor of two positive integers is the largest integer that can divide both integers.

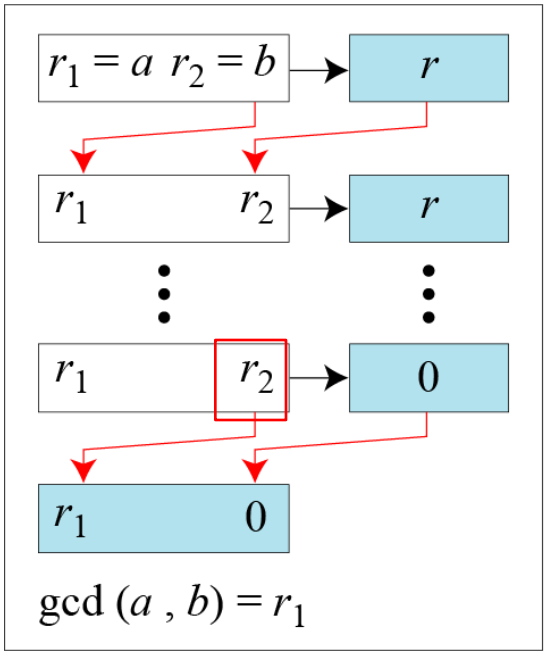
Note Euclidean Algorithm (歐幾里得算法)

Fact 1: gcd (a, 0) = a
Fact 2: gcd (a, b) = gcd (b, r), where r is the remainder of dividing a by b

$a=b*q+r$ *例子: gcd(70, 4)=gcd(4, 2)=2*

2.1.4 Continued

Figure 2.7 *Euclidean Algorithm*



a. Process

$r_1 \leftarrow a; \quad r_2 \leftarrow b;$ (Initialization)

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$

}

gcd $(a, b) \leftarrow r_1$

b. Algorithm

Note

When gcd (a, b) = 1, we say that a and b are relatively prime.

2.1.4 Continued

Example 2.7

Find the greatest common divisor of 2740 and 1760.

Solution

We have gcd (2740, 1760) = 20.

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

2.1.4 Continued

Example 2.8

Find the greatest common divisor of 25 and 60.

Solution

We have gcd (25, 60) = 5.

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

Exercise: gcd (21, 56) =

2-2 MODULAR ARITHMETIC

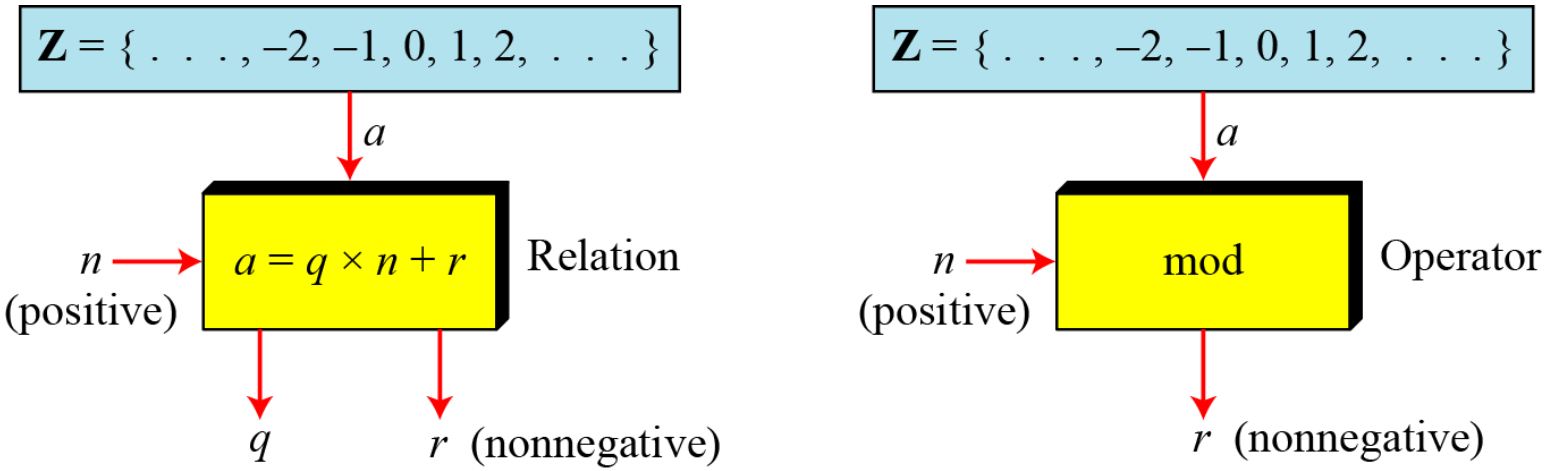
The division relationship ($a = q \times n + r$) discussed in the previous section has two inputs (a and n) and two outputs (q and r). In modular arithmetic, we are interested in only one of the outputs, the remainder r.

Topics discussed in this section:

2.2.1 Modulo Operator

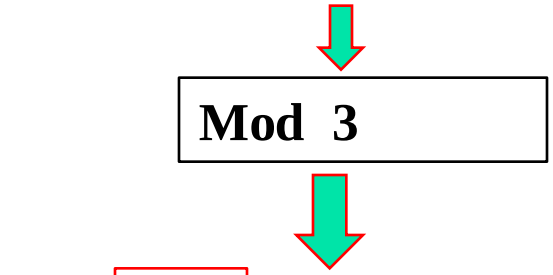
The modulo operator is shown as mod. The second input (n) is called the modulus. The output r is called the residue.

Figure 2.9 *Division algorithm and modulo operator*



2.2.1 Modulo Operator

Z= {….-10, -9, -8, -7, -6, -5, -4, -3,-2, -1, 0, 1, 2, 3, 4, 5,6 7, 8, 9, 10, …}



0	1	2
-9,	-8,	-7,
-6,	-5,	-4,
-3,	-2,	-1,
0,	1,	2,
3,	4,	5,
6	7,	8,
9,	10,	11
12	…	

同餘
寫成 -9=0=3=12 mod 3
同理:
4=1 mod 3 或 1=4 mod 3 或
4 mod 3=1 mod 3=10 mod 3
或
4 =1 =10 mod 3

Example 2.14

Find the result of the following operations:

a. 27 mod 5

b. 36 mod 12

c. −18 mod 14

d. −7 mod 10

Solution

a. Dividing 27 by 5 results in $r = 2$

b. Dividing 36 by 12 results in $r = 0$.

c. Dividing −18 by 14 results in $r = -4$. After adding the modulus $r = 10$

d. Dividing −7 by 10 results in r = −7. After adding the modulus to −7, r = 3.

2.2.2 Complete Set of Residues-完全剩餘系

- *The modulo operation creates a set, which in modular arithmetic is referred to as* ***the complete set of residues modulo n, or Z_n.***

- *將 mod n 後的餘數所形成的集合*

Figure 2.10 *Some Z_n sets*

$$\mathbf{Z}_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}$$

$$\mathbf{Z}_2 = \{ 0, 1 \}$$

$$\mathbf{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \}$$

$$\mathbf{Z}_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$$

2.2.2- Reduced Set of Residues- 縮剩餘類

- Z_n^*
- *將 mod n 後的餘數扣除掉與 n 非互質的數所形成的集合 (delete those residues that are not elative-prime to n)*

Z_{10}	A	0	1	2	3	4	5	6	7	8	9
Z_{10}^*	B	×	1	×	3	×	×	×	7	×	9

Class challenge

1) Z_{11}, Z_{11}^*

2) Z_8, Z_8^*

2.2.3 Congruence

To show that two integers are congruent, we use the congruence operator (≡). For example, we write:

"≡" ~= "同餘" ~= "mod 完後餘數相同"

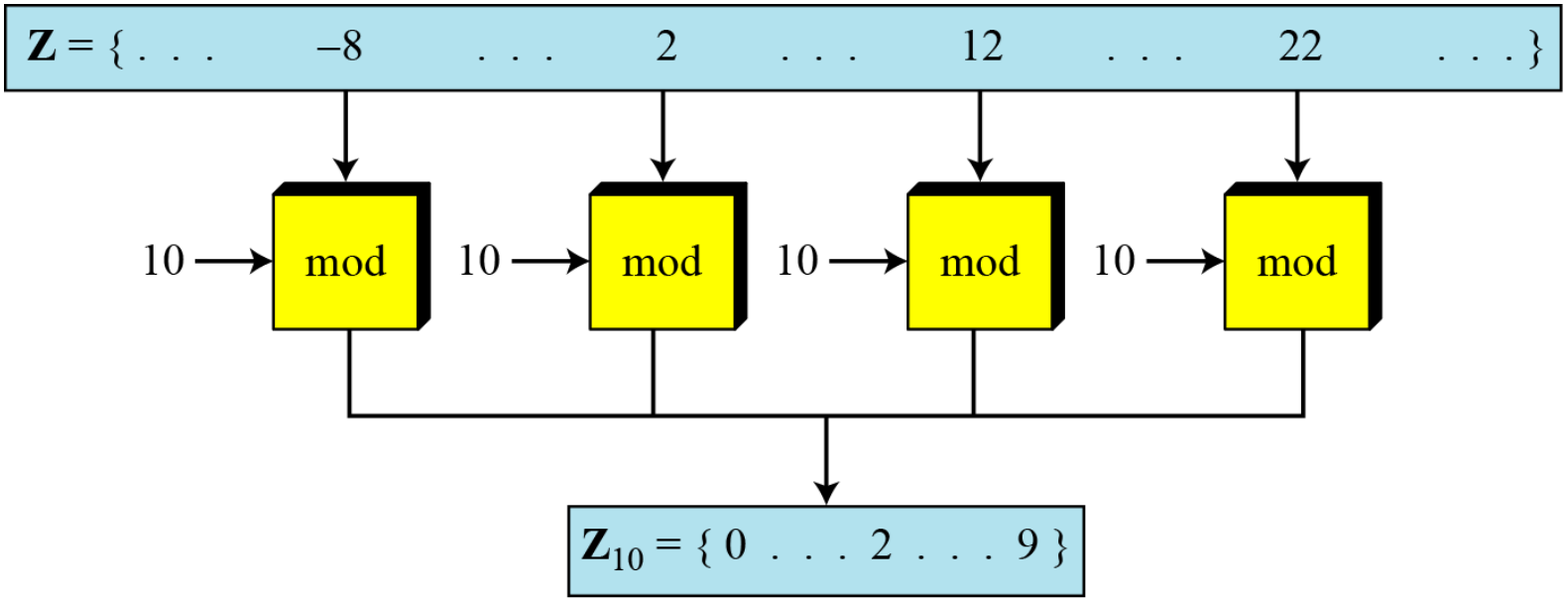
$$2 \equiv 12 \pmod{10} \qquad 13 \equiv 23 \pmod{10}$$

$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

8 ≡3 mod 5 ***13=8 mod 5***

2.2.3 Continued

Figure 2.11 *Concept of congruence*



$$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$$

Congruence Relationship

2.2.3 Continued

Residue Classes

A residue class [a] or $[a]_n$ is the set of integers congruent modulo n.

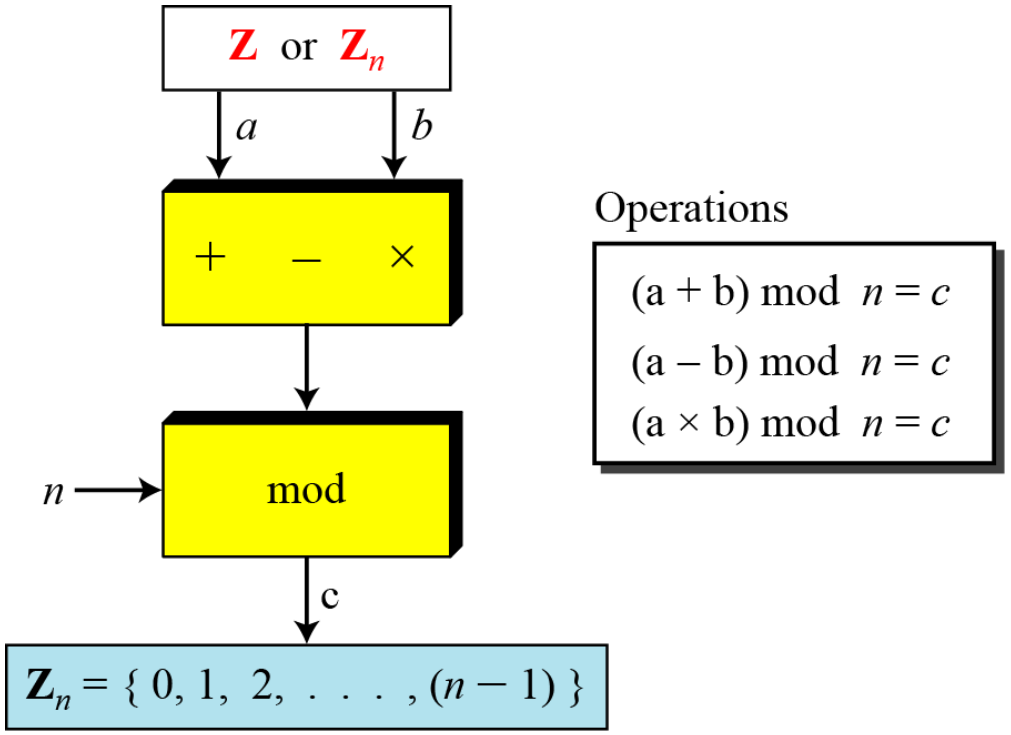
$$[0] = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$$
$$[1] = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$$
$$[2] = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$
$$[3] = \{\ldots, -12, -7, -5, 3, 8, 13, 18, \ldots\}$$
$$[4] = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$$

Class challenge: what is the n in this case?

2.2.4 Operation in Z_n

The three binary operations that we discussed for the set Z can also be defined for the set Zn. The result may need to be mapped to Zn using the mod operator.

Figure 2.13 *Binary operations in Z_n*



2.2.4 Continued

Example 2.16

Perform the following operations (the inputs come from Zn):

a. Add 7 to 14 in Z_{15}.

b. Subtract 11 from 7 in Z_{13}.

c. Multiply 11 by 7 in Z_{20}.

Solution

$$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$

$$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$

$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

2.2.4 Continued

Properties

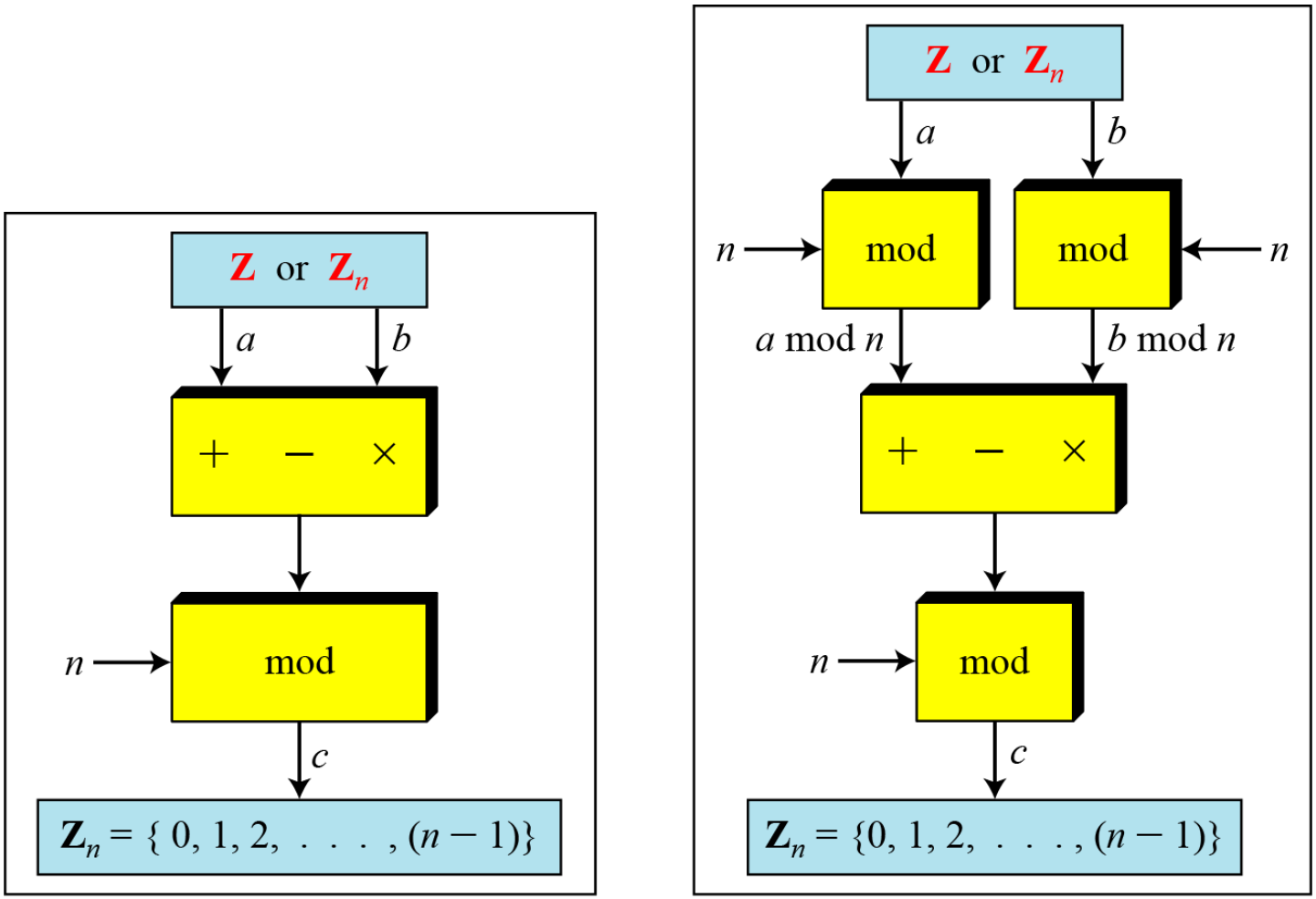
First Property: $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

Second Property: $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

Third Property: $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

2.2.4 Continued

Figure 2.14 *Properties of mode operator*



a. Original process

b. Applying properties

2.2.4 Continued

以前國高中公式: 4115161239141572 mod 3=

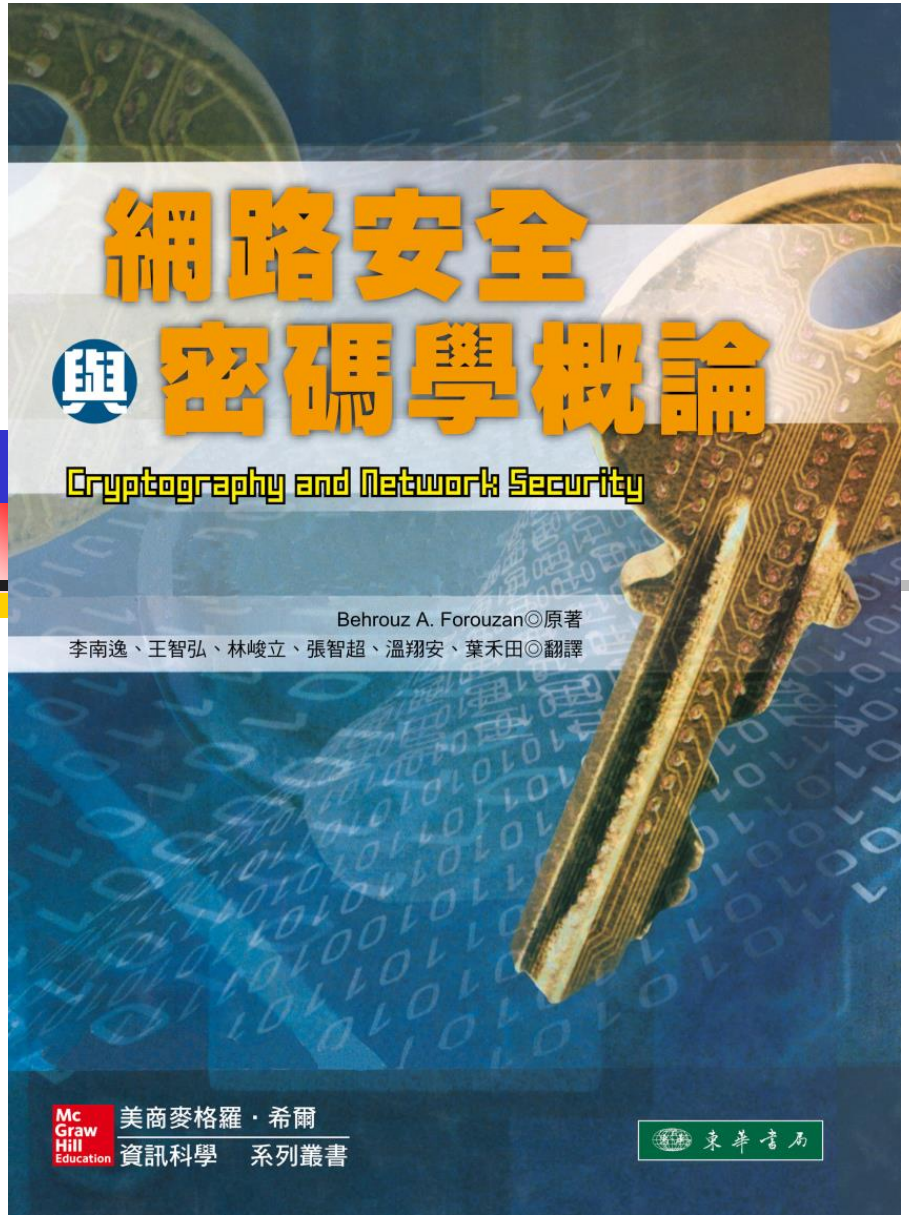
這快速計算公式 怎麼來的?

We have been told in arithmetic that the remainder of an integer divided by 3 is the same as the remainder of the sum of its decimal digits. We write an integer as the sum of its digits multiplied by the powers of 10.

$$a = a_n \times 10^n + \cdots + a_1 \times 10^1 + a_0 \times 10^0$$

For example: $6371 = 6 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 1 \times 10^0$

$$\begin{aligned} a \bmod 3 &= (a_n \times 10^n + \cdots + a_1 \times 10^1 + a_0 \times 10^0) \bmod 3 \\ &= (a_n \times 10^n) \bmod 3 + \cdots + (a_1 \times 10^1) \bmod 3 + (a_0 \times 10^0) \bmod 3 \\ &= (a_n \bmod 3) \times (10^n \bmod 3) + \cdots + (a_1 \bmod 3) \times (10^1 \bmod 3) + \\ &\quad (a_0 \bmod 3) \times (10^0 \bmod 3) \\ &= a_n \bmod 3 + \cdots + a_1 \bmod 3 + a_0 \bmod 3 \\ &= (a_n + \cdots + a_1 + a_0) \bmod 3 \end{aligned}$$



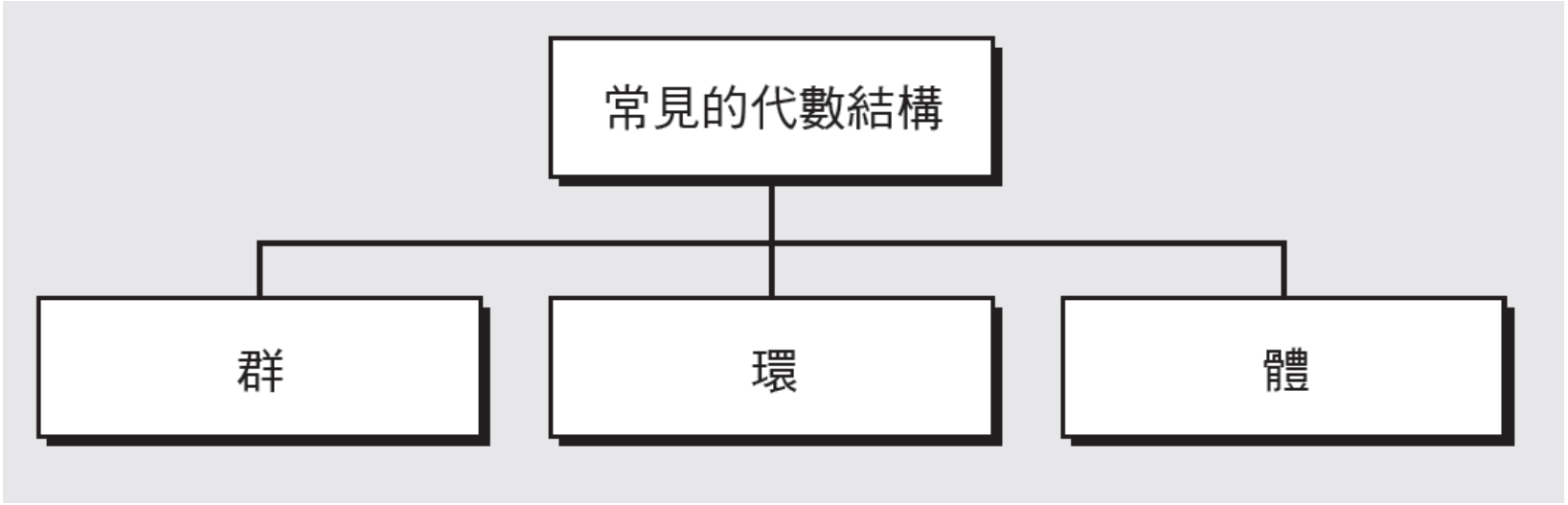
Chapter 4

密碼基礎數學 II：代數結構

學習目標

- 回顧代數結構的概念
- 定義「群」並使用範例解說
- 定義「環」並使用範例解說
- 定義「體」並使用範例解說
- 在現代區塊加密法中對 n 位元做加減乘除運算的能力來自於由GF(2^n)所構成的有限體

圖 4.1 常見的代數結構



4.1.1 群 (續)

*2.0 群 (Group): (G, *)*

*G: a set; *: an operation*

1. *Associativity: a*(b*c) = (a*b)*c*
2. *Identity: $\exists 1 \in G$, $\forall a \in G$, such that 1*a=a*1=a*
3. *Inverse: every element has inverse element. $\forall a \in G$, $\exists a^{-1} \in G$, such that a* a^{-1} =1*

Example: 1. (Z, +), I=0, *2. (R-{0}, *)*

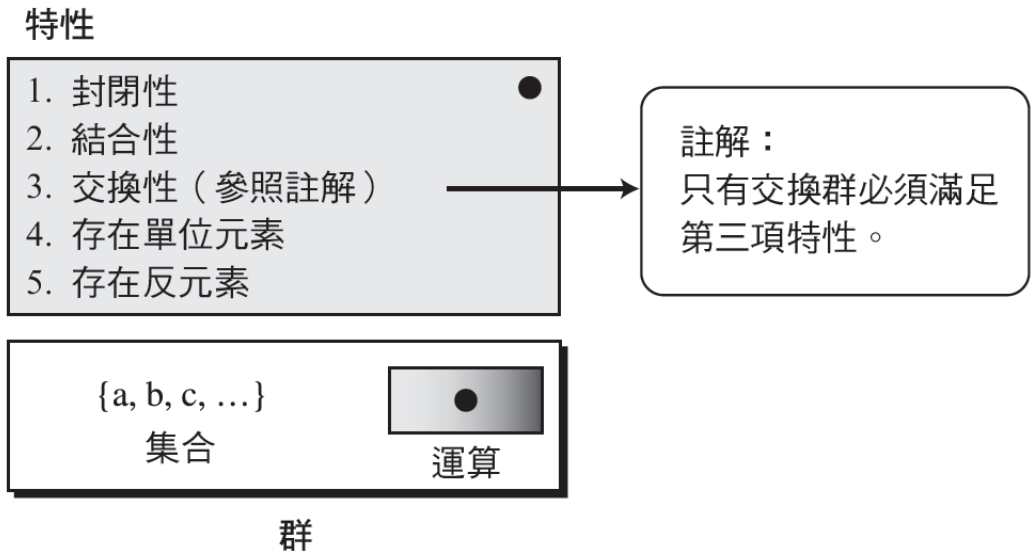
3. (Zp, *),* *4. 橢圓曲線群(進階)*

** Abelian group(Communicative group) 交換群 ➔ a*b=b*a or a+b=b+a*

4.1.1 群 (續)

- *交換群（commutative group，或稱為abelian group）*

- 交換群的特性
  1. 封閉性
  2. 結合性
  3. 存在單位元素
  4. 存在反元素
  5. 交換性



封閉性 *closed*

集合中任兩元素運算後仍然在原集合內這個性質就是所謂的封閉性.亦即 $a, b \in S$ 則 $a \bullet b \in S$.

比方說在負整數中的乘法運算就不是 closed, 而在正整數中的乘法運算就是 closed.

Why ?

結合律-1

如何讓三個元素或更多的元素運算在一起呢？

換句話說：該如何定 *a* • *b* • *c* 呢？

- http://zh.wikipedia.org/wiki/%E7%BB%93%E5%90%88%E5%BE%8B

- 在數學中，**結合律**意指在一個包含有二個以上的可結合運算元的表示式，只要運算元的位置沒有改變，其運算的順序就不會對運算出來的值有影響。亦即，重新排列表示式中的括號並不會改變其值

- Associativity: a*(b*c) = (a*b)*c

結合律-2

- 在算術中，實數的加法和乘法都是可結合的，即：

$$\left.\begin{aligned}(x+y)+z &= x+(y+z) = x+y+z \\ (x\,y)z &= x(y\,z) = x\,y\,z\end{aligned}\right\} \forall x, y, z \in \mathbb{R}.$$

- 複數和四元數的加法與乘法是可結合的。八元數的加法也是可結合的，但其乘法則是不可結合的。
- 最大公因數和最小公倍數的運算都是可結合的。

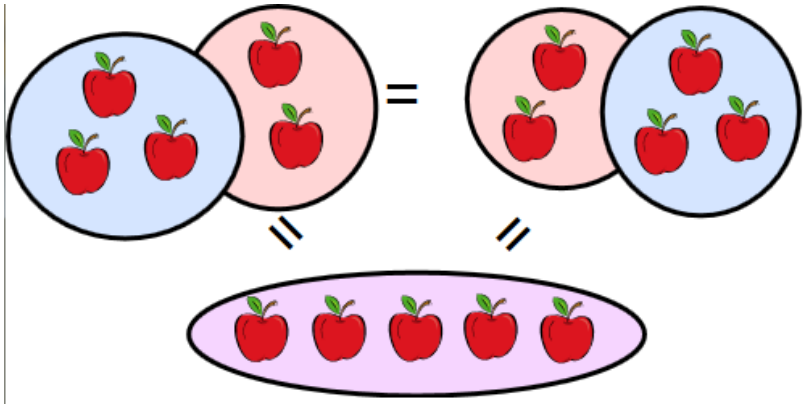
$$\left.\begin{aligned}\gcd(\gcd(x,y),z) &= \gcd(x,\gcd(y,z)) = \gcd(x,y,z) \\ \operatorname{lcm}(\operatorname{lcm}(x,y),z) &= \operatorname{lcm}(x,\operatorname{lcm}(y,z)) = \operatorname{lcm}(x,y,z)\end{aligned}\right\} \forall x, y, z \in \mathbb{Z}.$$

- 因為線性變換是個可表示成矩陣的函數，其中的函數複合則可以用矩陣乘法來表示，立即可知矩陣乘法為
- 集合的交集和聯集為可結合的：

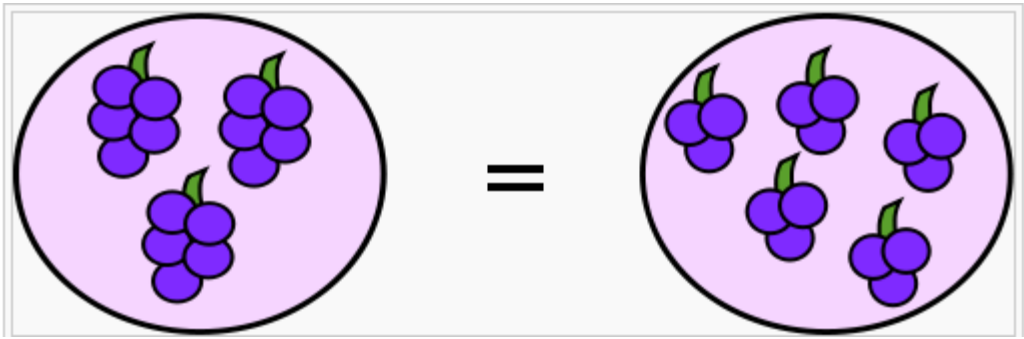
$$\left.\begin{aligned}(A \cap B) \cap C &= A \cap (B \cap C) = A \cap B \cap C \\ (A \cup B) \cup C &= A \cup (B \cup C) = A \cup B \cup C\end{aligned}\right\} \forall A, B, C.$$

交換律

- 加法的交換律3+2=2+3



- 乘法 (3 * 5 = 5* 3) 的交換律



identity

- 在一般我們有興趣的代數體系中通常都有一個很特別的元素稱為 *identity*.
- 這個元素我們通常會用 *e* 來表示, 要注意的是 *e* 是一個固定的元素它和任意的元素 *a* 運算後還是 *a*
- Example: 1. (Z, +), I=0,

  2. (R-{0}, *), I=1

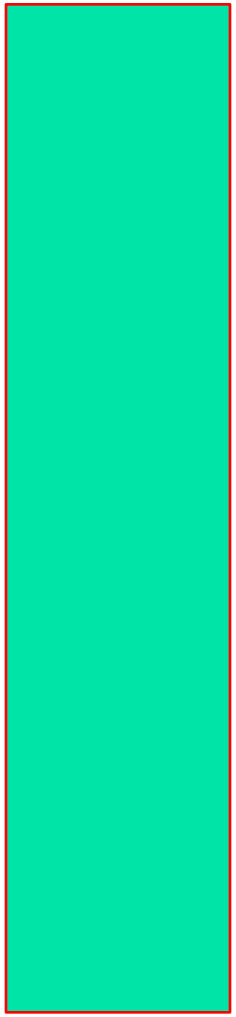
  3. (Z_{11}*, *mod 11), I=?, (Z_{11}*, + mod 11), I=?

Inverse

- 在集合中任意給定一個元素 *a*, 我們都能在集合中找到一個元素 *b* 使得 $a \bullet b = b \bullet a = e$.
- 這個元素我們稱之為 *a* 的 *inverse*而這裡的 *b* 是隨 *a* 而變的, 通常用 a^{-1} 來表示 *a* 的 inverse.
- Example:
  1. (Z, +), I=0, 3+(-3)=0
  2. (R-{0}, *), I=1, $3^{-1}=1/3=0.333\ldots$..
  3. (Z_{11}*, *mod 11), $3^{-1}=1/3=4$
  4. (Z_{11}, + mod 11), $3^{-1}=-3=8$

Exercise

- **$\langle Z^- + \{0\}, + \rangle$ is a group?** ➔
- **$\langle Z^+ + \{0\}, + \rangle$ is a group?** ➔
- **$\langle Z_{26}, +$ mod 26$\rangle$ is a group?** ➔
- **$\langle Z_{26}, *$ mod 26$\rangle$ is a group?** ➔
- **$\langle Z_5, +$ mod 5$\rangle$ is a group?** ➔
- **$\langle Z_4, +$ mod 4$\rangle$ is a group?** ➔



2.2.5 Continue

Additive Inverse

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.

Example 2.21

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).

2.2.5 Continue

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.

Example 2.22

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 2.23

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.

Example 2.24

Find all multiplicative inverse pairs in Z_{11}.

Solution

We have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), and (10, 10).

2.2.5 Continued- 如何找 乘法反元素

✓ 方法 1: 擴展歐幾里得演算法
方法二: 週期 → 稍後介紹

Note

The extended Euclidean algorithm finds the multiplicative inverses of b in Z_n when n and b are given and gcd (n, b) = 1. The multiplicative inverse of b is the value of t after being mapped to Z_n.

乘法反元素之求法-

1. 利用歐基理德演算法 $7^{-1} \bmod 23 =$

a.先用直式化簡到餘數為1, $7\overline{)\begin{matrix}23\\21\end{matrix}}^{3}$ $2\overline{)\begin{matrix}7\\6\end{matrix}}^{3}$

$\bar{2}$ $\bar{1}$

b. 再改寫成橫式 $23 = 7 * 3 + 2$

$7 = 2 * 3 + 1$

看下一頁推導

乘法反元素之求法-2

2. 利用歐基理德演算法

c. 由下而上, 依序由上一行餘數帶入下一行式子

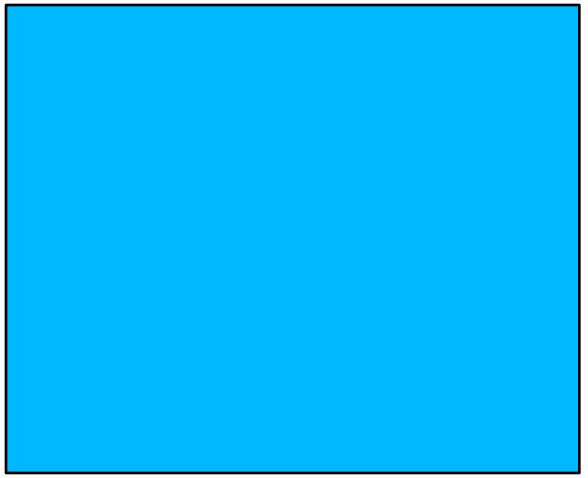
*7=(23-7*3)*3+1*

*7=23*3-7*9+1*

*10*7=23*3+1* ➔ *左右兩邊都 mod 23*

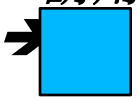
➔ *10*7 =1 mod 23* ➔ $7^{-1} \bmod 23 = 10$

One more $7^{-1} \bmod 25 = 18$



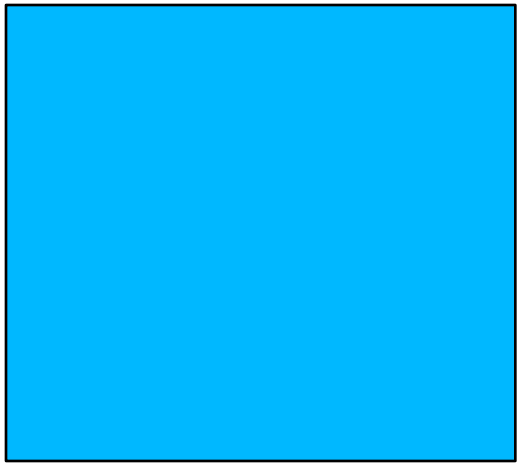
Homework-3:

1. 請用長除法求13 mod 23 的反元素 (Class Challenge)



2. 用長除法求（Individual Challenge）

$8^{-1} \bmod 25$ $(-16)^{-1} \bmod 25$



2.2.5 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).

Example: 1. (Z, +), I=0, *2. (R-{0}, *)*

3. (Zp, *mod p),* *4. 橢圓曲線群(進階)*

Class Challenge

. *(Z, +), I=0, -2+2=0*

- *(Z_{10}, +), I=0, -2+2=0, -2=?*

. *(R-{0}, *), I=?, 3^{-1}=1/3=0.3333333….*

- *(Z_{11}*, *), I=?, 3^{-1}=?*
- *(Z_{10}*, *), I=?, 3^{-1}=?*

Inverse

***Class Challenge*:**

1. (Z_{13}*, *mod 13), 3^{-1}=?, 4^{-1}=?

2. (Z_{10}*, + mod 10), 3^{-1}=-3=?

常見的Group範例

- Z 在加法的運算下是 group, 其中 0 是其 identity, 而任意的整數 n, - n 是其 inverse.

- Z在乘法的運算下它就不再是一個 group.
- 例如 2 就沒法在Z中找到一個數使得 2 乘以它以後會是 1。
- 非 0 的有理數(Q-{0})所成的集合, 在乘法的運算下它就是一個 group.

範例4.1交換群（commutative group，或稱為 abelian group）

整數餘數集合 與 加法運算子

$$G = \langle Z_n, + \rangle$$

為一交換群。

我們可以對此集合的元素　**執行加法與減法**的運算，而結果仍為此集合的元素。

範例4.2交換群

集合 Z_{n^*} 與 乘法運算子 $G = \langle Z_{n^*}, \times \rangle$

可構成一交換群

範例4.3

- 以下定義一個群 G = <{*a*, *b*, *c*, *d*}, •>，其運算如表 4.1 所示。

•	*a*	*b*	*c*	*d*
a	*a*	*b*	*c*	*d*
b	*b*	*c*	*d*	*a*
c	*c*	*d*	*a*	*b*
d	*d*	*a*	*b*	*c*

交換群的特性

- ✓*封閉性*
- ✓*結合性*
- ✓*交換性*
- ✓*存在單位元素*
- ✓*存在反元*

2.4.1 Single-Variable Linear Equations

Equations of the form $ax \equiv b \pmod{n}$ might have no solution or a limited number of solutions.

Assume that the gcd $(a, n) = d$.

If $d \nmid b$, there is no solution.

If $d \mid b$, there are d solutions.

linear congruence equations.

https://www.youtube.com/watch?v=U9Eo6Bsvm4M

2.4.1 單變數方程式

Assume that the gcd $(a, n) = d$.

If $d \nmid b$, there is no solution.

If $d \mid b$, there are d solutions.

Example 2.35

Solve the equation $10x \equiv 2 \pmod{15}$.

Solution

First we find the gcd (10 and 15) = 5. Since 5 does not divide 2, we have no solution.

Example 2.36

Solve the equation $14x \equiv 12 \pmod{18}$.

Solution gcd (14 and 18) =2，表示有2個解 x_0, x_1

$$14x \equiv 12 \pmod{18} \rightarrow \quad 7x \equiv 6 \pmod{9} \quad \rightarrow \quad x \equiv 6\,(7^{-1}) \pmod{9}$$

$$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod{9} = 6$$

$$x_1 = x_0 + 1 \times (18/2) = 15$$

有2個解是指 $x_0 \equiv 6 \bmod 18$以及 $x_1 \equiv 15 \bmod 18$之意!!

Example 2.37

Solve the equation $3x + 4 \equiv 6 \pmod{13}$.

Solution

First we change the equation to the form $ax \equiv b \pmod{n}$. We add -4 (the additive inverse of 4) to both sides, which give $3x \equiv 2 \pmod{13}$. Because gcd (3, 13) = 1, the equation has only one solution, which is $x_0 = (2 \times 3^{-1}) \bmod 13 = (2*9) = 18 \bmod 13 = 5$. We can see that the answer satisfies the original equation:

$$3 \times 5 + 4 \equiv 6 \pmod{13}.$$

Example 2.37

Solve the equation $3x + 4 \equiv 19 \pmod{13}$.

Solution

First we change the equation to the form $ax \equiv b \pmod{n}$. We add -4 (the additive inverse of 4) to both sides, which give $3x \equiv 15 \pmod{13}$. Because gcd (3, 13) = 1, the equation has only one solution, which is $x_0 = (15 \times 3^{-1}) \bmod 13 = (15 \times 9) \bmod 13 = 135 \bmod 13 = 5$. We can see that the answer satisfies the original equation:

$$3 \times 5 + 4 \equiv 19 \pmod{13}.$$

4.1.1 Continued

Example 4.8

Three cyclic subgroups *can be made from the group* $G = \langle Z_{10}^*, \times \rangle$. *G has only four elements: 1, 3, 7, and 9.*

$$1^0 \bmod 10 = 1$$

$$3^0 \bmod 10 = 1$$
$$3^1 \bmod 10 = 3$$
$$3^2 \bmod 10 = 9$$
$$3^3 \bmod 10 = 7$$

$$7^0 \bmod 10 = 1$$
$$7^1 \bmod 10 = 7$$
$$7^2 \bmod 10 = 9$$
$$7^3 \bmod 10 = 3$$

$$9^0 \bmod 10 = 1$$
$$9^1 \bmod 10 = 9$$

範例4.10(元素的級數Order)

- 在群 $G = \langle Z_6, + \rangle$ 中，個別元素的級數為：ord(0) = 1，ord(1) = 6，ord(2) = 3，ord(3) = 2，ord(4) = 3，ord(5) = 6。 *Why?*
- 在群 $G = \langle Z_{10^*}, \times \rangle$ 中，個別元素的級數為：ord(1) = 1，ord(3) = 4，ord(7) = 4，ord(9) = 2。 *Why?*

4.1.3 體(or 場) (Field)-3

<F, +, *>

1. ***<F, +> :交換群 (commutative group ，abelian group)***
2. ***<F-{0} , *> :交換群(commutative group ，abelian group):***
3. **** 對 + 分配律: (* , +) satisfies Distributed Law 。***

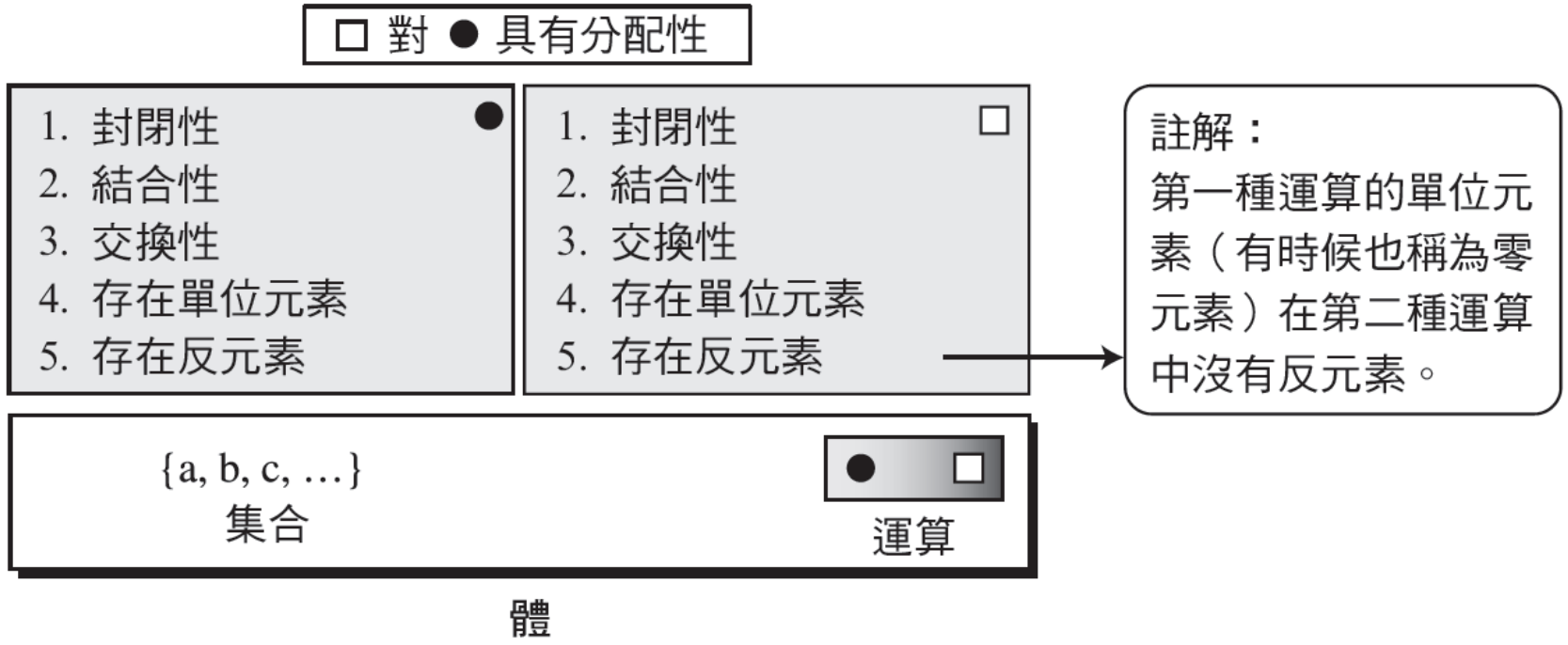
4.1.3 體(or 場) (Field)-2

＊正式的定義為，若一集合F在已定義的兩個運算“+”及“·”中，具有下列性質者，則F稱為一個場：

$F=(F, +, *)$

1. F在運算"+"中為一交換群(Abelian Group)，且具有單位元素0。
2. $F-\{0\}$➔ 非零的元素在"·"中亦為交換群。(注意，交換群有反元素存在)。
3. F中"·"對"+"運算滿足分配律(Distributed Law)。即對於所有a, b, c, F，滿足 $a \cdot (b + c) = a \cdot b + a \cdot c$。

(＊) 一個場F，若其元素個數為無限多個，F稱為無限場(Infinite Field)。反之，若F之元素為有限個，則稱為有限場(Finite Field)。



有理數、實數和複數都是體的代表。

Chapter 9

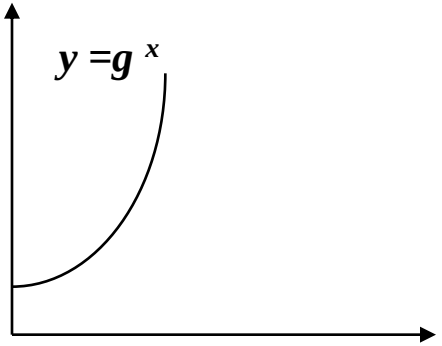
Mathematics of Cryptography

Part III: Primes and Related Congruence Equations

Objectives

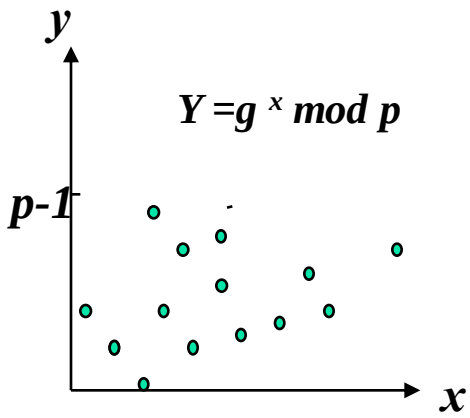
- To introduce prime numbers and their applications in cryptography.
- To discuss factorization algorithms and their applications in cryptography.
- To describe the Chinese remainder theorem and its application.

Why Number Theory?



1. *We will focus the discrete logarithm problem because ….*

2. *Given Y =g x mod p, g and p, we need to solve the x ➔ No way ; 可用在公開金鑰系統*
   / if p is a big prime */*
3. *Given Y1 =g x1 mod p, Y2 =g x2 mod p, g and p, we need to compute*
   *g x1*x2 mod p ➔ No way /* if p is a big prime */;*
   可用在連線時產生金鑰
4. *However, if we have x1 or x2, then ….*
5. *2 mod 11=2, 2^3 mod 11=8, 2^38796542 mod 11=?*



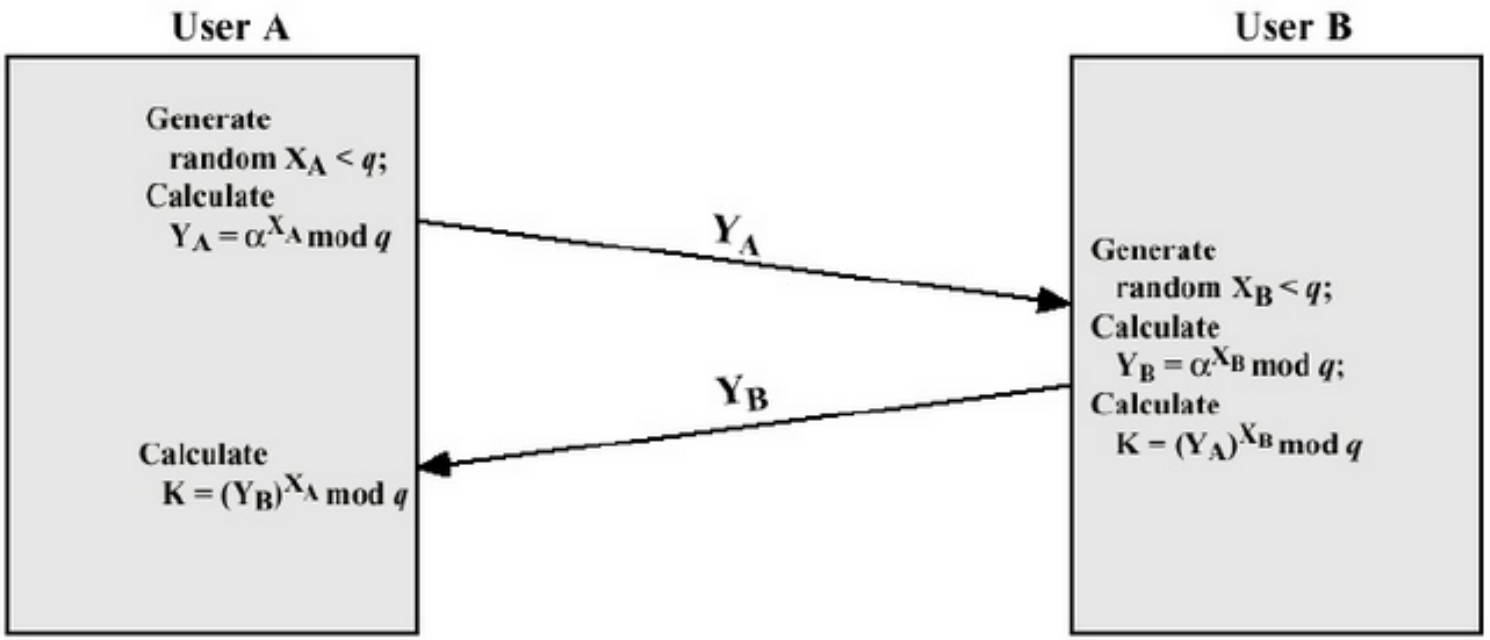
Question: why we study basic number theory?

Computational Diffie-Hellman Problem (CDHP)

- INPUT
  - The description of a finite cyclic *group* G of prime order q
  - A generator element g of G
  - $g^a, g^b \in G$, for some integers $0 < a, b < q$.
- OUTPUT
  - g^{ab}

Computational Diffie-Hellman Problem (CDHP)-- applications

用在 Network security, session keys, firewall, SSL, …



weaknesses

雅琳發現一有趣現象

$(-3)^{-1} mod 7 = -(3)^{-1} mod 7 = 2$

$(-4)^{-1} mod 7 = -(4)^{-1} mod 7 = 5$

$(-2)^{-1} mod 7 = -(2)^{-1} mod 7 = 3$

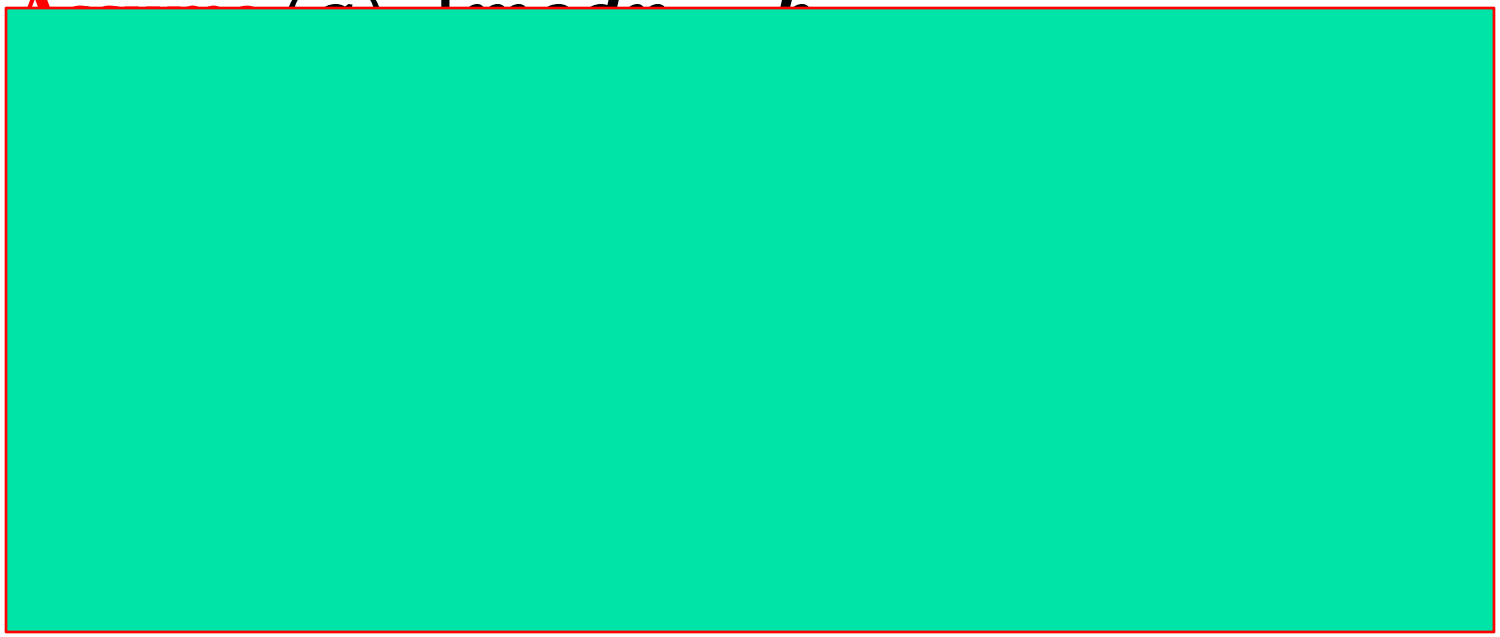
$(-5)^{-1} mod 7 = -(5)^{-1} mod 7 = 4$

$(-1)^{-1} mod 7 = -(1)^{-1} mod 7 = 6$

$(-6)^{-1} mod 7 = -(6)^{-1} mod 7 = 1$

如何證明 $(-a)^{-1} mod n = -(a)^{-1} mod n$

Assume $(a)^{-1} mod n = b$



雅琳發現一有趣現象一另一證明– inspired by 陳曉柔

$(-3) \quad mod7 = -(3)^{-1} mod7 = 2$

$$(-4)^{-1} mod7 = -(4)^{-1} mod7 = 5$$
$$(-2)^{-1} mod7 = -(2)^{-1} mod7 = 3$$
$$(-5)^{-1} mod7 = -(5)^{-1} mod7 = 4$$
$$(-1)^{-1} mod7 = -(1)^{-1} mod7 = 6$$
$$(-6)^{-1} mod7 = -(6)^{-1} mod7 = 1$$

如何證明 $(-a)^{-1} mod n = -(a)^{-1} mod n$

Class Challenge

Describe the following three questions

1. Discrete Logarithm Problem

2. Computational Diffie-Hellman problem

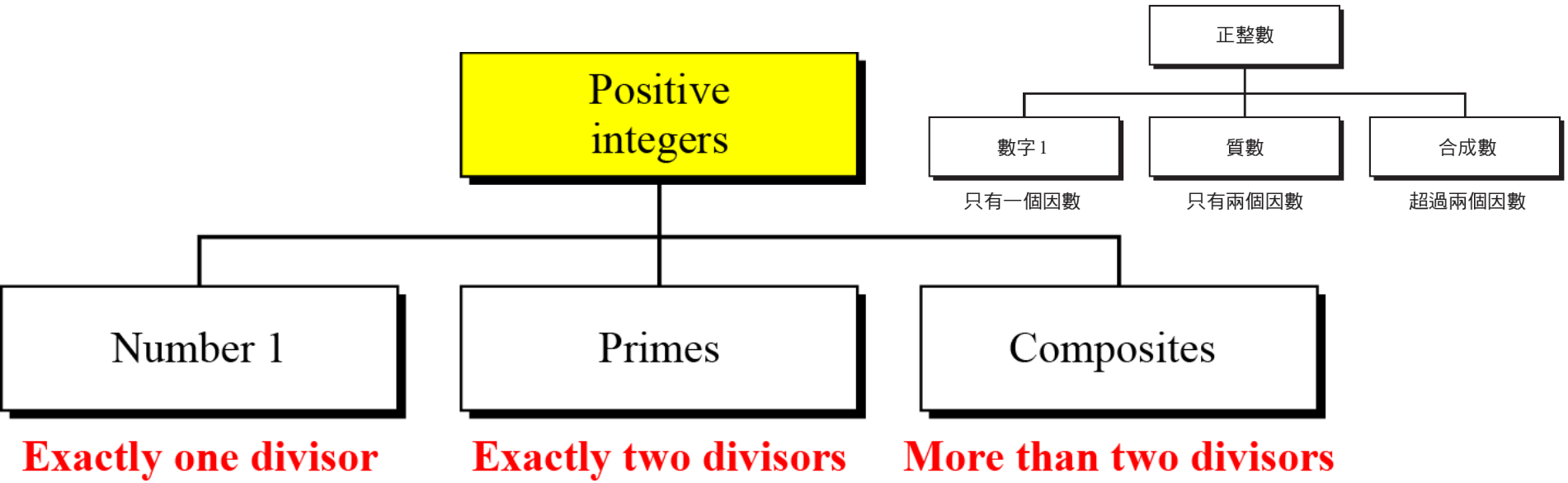
~~3. Decisional Diffie-Hellman problem~~

9-1 PRIMES

Asymmetric-key cryptography uses primes extensively. The topic of primes is a large part of any book on number theory. This section discusses only a few concepts and facts to pave the way for Chapter 10.

Topics discussed in this section:

Figure 9.1 Three groups of positive integers



Note

A prime is divisible only by itself and 1.

Example 9.1

What is the smallest prime? ***最小的質數為何？***

Solution

The smallest prime is 2, which is divisible by 2 (itself) and 1.

Euler's phi-function, $\phi(n)$, which is sometimes called the Euler's totient function plays a very important role in cryptography.

$\phi(n)$: *尤拉商數(Euler Totient Function)。表示不大於* ***n*** *，且與* ***n*** *互質之正整數的個數*

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

Class Challenge: what is the relation between $\phi(n)$ & Z_n^*

Example 9.7

What is the value of $\phi(13)$?

Solution

Because 13 is a prime, $\phi(13) = (13 - 1) = 12$.

Example 9.8

Euler's phi function $\phi(n)$
http://primes.utm.edu/glossary/xpage/eulersphi.html

What is the value of $\phi(10)$?

integer n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
phi(n)	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

Solution

We can use the third rule: $\phi(10) = \phi(2) \times \phi(5) = 1 \times 4 = 4$, because 2 and 5 are primes.

Example 9.11

What is the number of elements in Z_{14}*?

也就是要計算$\phi(14)$

Solution

The answer is $\phi(14) = \phi(7) \times \phi(2) = 6 \times 1 = 6$.

The members in Z_{14}* are 1, 3, 5, 9, 11, and 13.

Note

Interesting point: If $n > 2$, the value of $\phi(n)$ is even.

9.1.5 Fermat's Little Theorem

費瑪小定理– p is a prime

First Version

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

Second Version

$$(a, p)=1 \; a^{p} \equiv a \bmod p$$

• 定理(8)：令$\{r_1, r_2, \ldots, r_{\Phi(n)}\}$為模n之一縮剩餘系，且$(a, n) = 1$，則$\{ar_1, ar_2, \ldots, ar_{\Phi(n)}\}$亦為模n之一縮剩餘系。

証：(1) $(a, n) = 1$ 且 (r_j, n) 所以$(ar_j, n) = 1$

(2) 證明 任意兩 $ar_i \neq ar_j$。 先假設 $ar_i = ar_j \bmod n$，因為$(a, n) = 1$, 所以推論 $r_i = r_j$, 但 r_i 與 r_j 為縮剩餘系的成員應不相等 ➔ 矛盾 。

所以任一兩個 $ar_i \neq ar_j$

由 (1) & (2) ➔ 因此 $\{ar_1, ar_2, \cdots, ar_{\Phi(n)}\}$ 為模n之一縮剩餘系。

•

- ***定理(9)：尤拉定理(Euler's Theorem)***

  若(a, n) = 1，則$a^{\Phi(n)} = 1 \bmod n$。

  証：令$\{r_1, r_2, \ldots, r_{\Phi(n)}\}$為模n之一縮剩餘系，由定理(8)知若(a, n)=1，則$\{ar_1, ar_2, \ldots, ar_{\Phi(n)}\}$亦為一縮剩餘系。因此，

$$\prod_{i=1\sim\Phi(n)}(ar_i) \bmod n = a^{\Phi(n)} \prod r_i \bmod n = \prod r_i \bmod n$$

  由消去法(Cancellation)可得$a^{\Phi(n)} \bmod n = 1$。

  例一：{1,3,5,7}為模8之一縮剩餘系，{3×1,3×3,3×5,3×7}亦為模8之一縮剩餘系。因此，

  $(3 \times 1)(3 \times 3)(3 \times 5)(3 \times 7) = 1 \times 3 \times 5 \times 7 \bmod 8$

  $3^4(1 \times 3 \times 5 \times 7) = 1 \times 3 \times 5 \times 7 \bmod 8$

  $3^4 = 3^{\Phi(8)} = 1 \bmod 8$

Example 9.12

Find the result of 6^{10} mod 11.

Solution

We have 6^{10} mod 11 = 1. This is the first version of Fermat's little theorem where p = 11.

Example 9.13

Find the result of 3^{12} mod 11.

Solution

Here the exponent (12) and the modulus (11) are not the same. Use Fermat's little theorem:

$$3^{12} \bmod 11 = (3^{11} \times 3) \bmod 11 = (3^{11} \bmod 11)\ (3 \bmod 11) = (3 \times 3) \bmod 11 = 9$$

Fermat's little theorem
without using the extended Euclidean algorithm

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

Example 9.14

The answers to multiplicative inverses modulo a prime can be found without using the extended Euclidean algorithm:

a. $8^{-1} \bmod 17 = 8^{17-2} \bmod 17 = 8^{15} \bmod 17 = 15 \bmod 17$

b. $5^{-1} \bmod 23 = 5^{23-2} \bmod 23 = 5^{21} \bmod 23 = 14 \bmod 23$

c. $60^{-1} \bmod 101 = 60^{101-2} \bmod 101 = 60^{99} \bmod 101 = 32 \bmod 101$

d. $22^{-1} \bmod 211 = 22^{211-2} \bmod 211 = 22^{209} \bmod 211 = 48 \bmod 211$

定理(10)：費瑪定理(Fermat's Theorem)

令p為一質數，且(a, p) = 1 ，則$a^{p-1}=1 \bmod p$ 。

証：若p為質數，則$\Phi(p) = p-1$ ，由尤拉定理可得証。

2.3 乘法反元素之求法

已給a及n且(a, n)=1 ，如何求$a\,a^{-1}=1 \bmod n$ ？

方法一：

若$\Phi(n)$已知，則由尤拉定理可知$aa^{\Phi(n)-1}=1 \bmod n$ 。

因此，$a^{\Phi(n)-1} = a^{-1} \bmod n$ (注意：若n為質數，則$\Phi(n) = n-1$為已知。若n為合成數，則$\Phi(n)$不一定為已知)。

方法二：利用歐基里德演算法(Euclidean Algorithm)

在中學數學中，我們已熟知利用歐基里德演算法求兩整數a及n之最大公因數(Greatest Common Divisor , gcd)。我們首先介紹，利用歐基里德演算法求gcd之方法。

- *refer to textbook for detail*

First Version

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

Second Version

$$a^{k \times \phi(n) + 1} \equiv a \pmod{n}$$

Note

尤拉定理的第二種版本被應用在第10章中所介紹的RSA 密碼系統。

The second version of Euler's theorem is used in the RSA cryptosystem in Chapter 10.

Example 9.15

Find the result of $6^{24} \bmod 35$.

Solution

We have $6^{24} \bmod 35 = 6^{\phi(35)} \bmod 35 = 1$.

Example 9.16

Find the result of $20^{62} \bmod 77$.

Solution

If we let $k = 1$ on the second version, we have

$$20^{62} \bmod 77 = (20 \bmod 77)\,(20^{\phi(77)+1} \bmod 77) \bmod 77$$
$$= (20)(20) \bmod 77 = 15.$$

Multiplicative Inverses

Euler's theorem can be used to find multiplicative inverses modulo a composite.

當模數是合成數(not prime) 時，我們可以使用尤拉定理求出乘法反元素。

$$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$$

乘法反元素之求法-1

1. 利用週期

$(2^{108})^{-1} \bmod 11 = (2^{8})^{-1} = 2^{10-8} = 2^{2} = 4$

$(2^{63})^{-1} \bmod 15 = (2^{56+7})^{-1} = (2^{7})^{-1} = 2^{8-7} = 2$

乘法反元素之求法-3

2. 利用歐基理德演算法 $7^{-1} \bmod 23 =$

a.先用直式化簡到餘數為1, $7\overline{)\begin{matrix}3\\23\\21\end{matrix}}$ $2\overline{)\begin{matrix}3\\7\\6\end{matrix}}$

$\overline{2}$ $\overline{1}$

b. 再改寫成橫式 $23 = 7 * 3 + 2$

$7 = 2 * 3 + 1$

乘法反元素之求法-2

2. 利用歐基理德演算法

c. 由下而上，依序由上一行餘數帶入下一行式子

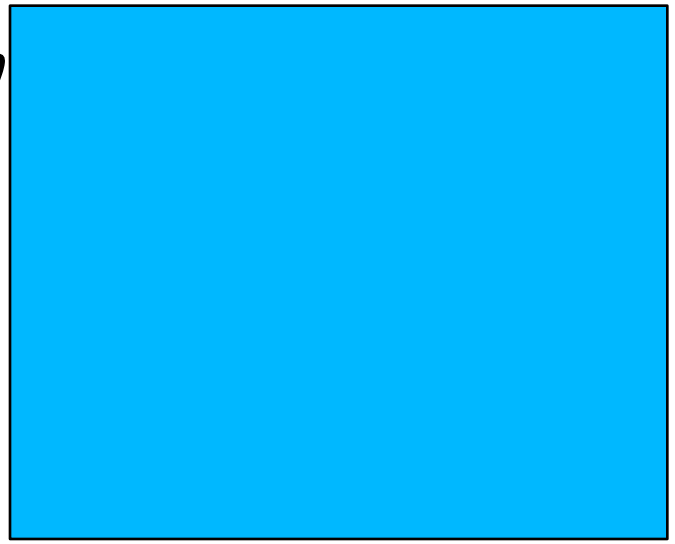
$7=(23-7*3)*3+1$

$7=23*3-7*9+1$

$10*7=23*3+1$ ➔ 左右兩邊都 mod 23

➔ $10*7 = 1 \mod 23$ ➔ $7^{-1} \mod 23 = 10$

One more $7^{-1} \mod 25 = 18$



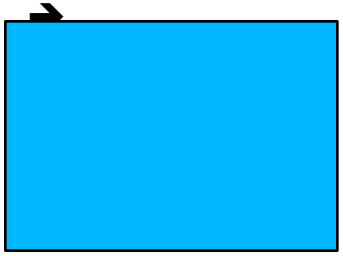
Homework-3:

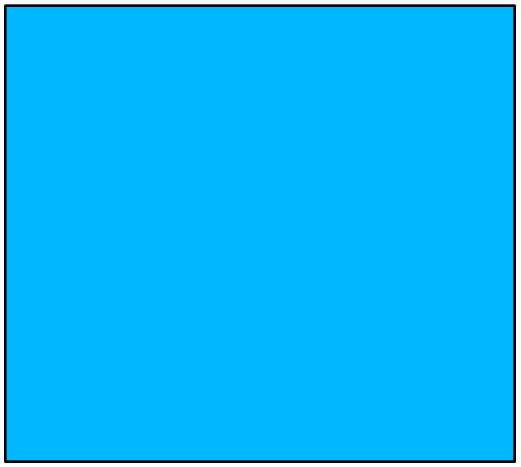
1. 請用長除法求13 mod 23 的反元素

➔16

2. $n = 3 * 5$, 求 $2^{10} \bmod n, (2^{27})^{-1} \bmod n, -(2^{27})^{-1} \bmod n$

3. 用長除法求 $8^{-1} \bmod 25$ $(-16)^{-1} \bmod 25 =$





Example 9.50

Table 9.5 shows the result of $a^i \equiv x \pmod 7$ for the group $G = \langle Z_7^*, \times \rangle$. In this group, $\phi(7) = 6$.

Table 9.5 *Example 9.50*

	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$
$a = 1$	x: 1	x: 1	x: 1	x: 1	x: 1	x: 1
$a = 2$	x: 2	x: 4	x: 1	x: 2	x: 4	x: 1
Primitive root → $a = 3$	x: 3	x: 2	x: 6	x: 4	x: 5	x: 1
$a = 4$	x: 4	x: 2	x: 1	x: 4	x: 2	x: 1
Primitive root → $a = 5$	x: 5	x: 4	x: 6	x: 2	x: 3	x: 1
$a = 6$	x: 6	x: 1	x: 6	x: 1	x: 6	x: 1

例六：令p=11，g=2，则序列<$E_x(g)$>={$2^0,2^1,2^2,2^3,\ldots,2^g$}={1,2,4,8,5,10,9,7,3,6} 如下列所示

$2^0=1 \bmod 11$，$2^6=9 \bmod 11$ ，

$2^1=2 \bmod 11$，$2^7=7 \bmod 11$ ，

$2^2=4 \bmod 11$，$2^8=3 \bmod 11$ ，

$2^3=8 \bmod 11$，$2^9=6 \bmod 11$ ，

$2^4=5 \bmod 11$，$2^{10}=1 \bmod 11$ ，

$2^5=10 \bmod 11$。

∴ T=10 。

Class challenge: find the primitive root of p=13

2) 原根(Primitive Root)

- 若 $g \in G$ 之序 $T=p-1$，則 g 稱為 模 p 之原根。
- 當 g 為 模 p 之原根時，由 g 所產生之序列 $<E_x(g)>$ 具有最大週期。
- 換句話說，具有較高的安全性。
- 理論證明，對於所有質數 p，其原根必定存在。
- 當 g 為 模 p 之原根且 a 與 $p-1$ 互質時，則 $g^a \bmod p$ 亦必為 模 p 之原根。
- 因此，模 p 之原根個數等於 $\Phi(p-1)$，其中 $\Phi(p-1)$ 稱為尤拉商數(Euler Totient Function)。表示不大於 $p-1$，且與 $p-1$ 互質之正整數的個數。

例七：在例六中 $\Phi(10)=4$ (事實上與10互質之正整數為1 ,3 ,7 ,9)，因此 $p=11$ 時共有4個原根。我們已知2為模11之原根，則 $2^1=2$,$2^3=8$, $2^7=7$, $2^9=6$ ，因此2 ,8 ,7 ,6均為模11之原根。

The idea of Discrete Logarithm

Properties of G = <Z_p^*, x> :

1. **Its elements include all integers from 1 to p − 1.**

2. **It always has primitive roots.**

3. **It is cyclic. The elements can be created using g^x where x is an integer from 1 to $\phi(n) = p - 1$.**

4. **The primitive roots can be thought as the base of logarithm.**

Homework

1. $\phi(14)$

2. $p=11, g=2$, 求 $g^8 \bmod 11$ [redacted] $g^{22} \bmod 11$ [redacted], $g^8 * g^{43} \bmod 11$ [redacted]

   求 $(g^8+g^2)^{-1} \bmod 11$ [redacted] $-(g^8+g^2) \bmod 11$ [redacted]

3. *舉出 mod 13 之所有原根:* [redacted]

4. *用* $n=3*5$, 求 $2^{10} \bmod n = 4, (2^{27})^{-1} \bmod n$ [redacted], $-(2^{27})^{-1} \bmod n =$ [redacted]

5. ***求 a. $(-7)^{-1}$ mod 11=*** ***b. (2^{-6})mod11=***

   ➔ [redacted]

6. *用快速指數運算法求* $g^{17} \bmod p$ *需幾次乘法? 幾次平方運算?*

9-4 CHINESE REMAINDER THEOREM
中國餘數定理

The Chinese remainder theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime

CRT用來求解模數兩兩相異且互質之單變數的同餘方程組

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\cdots \\
x &\equiv a_k \pmod{m_k}
\end{aligned}
$$

Example 9.35

The following is an example of a set of equations with different moduli:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

The solution to this set of equations is given in the next section; for the moment, note that the answer to this set of equations is x = 23. This value satisfies all equations: 23 ≡ 2 (mod 3), 23 ≡ 3 (mod 5), and 23 ≡ 2 (mod 7).

Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.
3. Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli (m_1, m_2, …, m_k). Call the inverses $M_1^{-1} \bmod m_1$, $M_2^{-1} \bmod m_2$, …, $M_k^{-1} \bmod m_k$.
4. The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M$$

Example 9.36

Find the solution to the simultaneous equations:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Solution

We follow the four steps.

1. $M = 3 \times 5 \times 7 = 105$

2. $M_1 = 105 / 3 = 35$, $M_2 = 105 / 5 = 21$, $M_3 = 105 / 7 = 15$

3. The inverses are $M_1^{-1} \bmod 3 = 2$, $M_2^{-1} \bmod 5 = 1$, $M_3^{-1} \bmod 7 = 1$

4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105 = 23 \bmod 105$

中國餘數定理在密碼學上有非常重要的應用。

1. *例如在 **RSA** 解密時，利用中國餘數定理，可以使解密速度加快約 **4** 倍。*
2. *藏住某一 ai 可以加密或 秘密分享*

Homework:用 CRT 求 x=2 mod 3, x=2 mod 4, and x=1mod 5 在 x 間的解

➔ 

9-6 EXPONENTIATION AND LOGARITHM

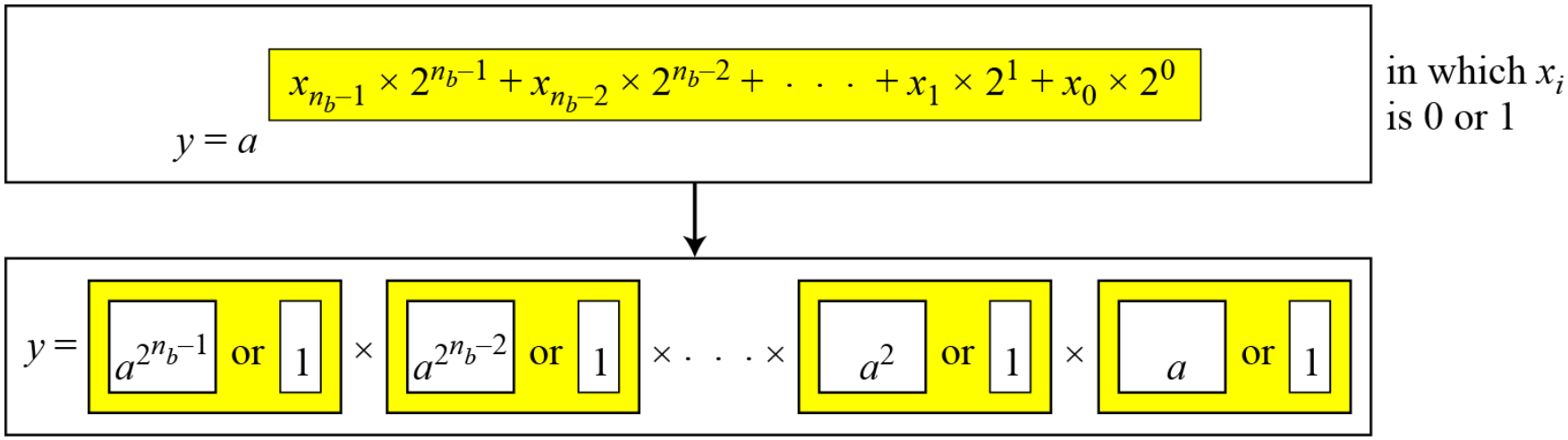
Exponentiation: $y = a^x$ $\rightarrow$ **Logarithm:** $x = \log_a y$

Topics discussed in this section:

9.6.1 Exponentiation 指數運算

9.6.2 Logarithm 對數運算

Figure 9.6 The idea behind the square-and-multiply method



Example:

$$y = a^9 = a^{1001_2} = a^8 \times 1 \times 1 \times a$$