

# **An Introduction to Mathematical Cryptography**

## *Solutions*

Solutions for *An Introduction to Mathematical Cryptography (2014)* - Hoffstein,  
Pipher, Silverman

**Le Quoc Dung**

Moscow

# Chapter 2

**Exercise (2.3).** Let  $g$  be a primitive root of  $\mathbb{F}_p$

- (a) Suppose that  $x = a$  and  $x = b$  are both integer solutions to the congruence  $g^x \equiv h \pmod{p}$ . Prove that  $a \equiv b \pmod{p-1}$ . Explain why this implies that the map (2.1) on page 64 is well-defined
- (b) Prove that  $\log_g(h_1 h_2) = \log_g(h_1) + \log_g(h_2)$  for all  $h_1, h_2 \in \mathbb{F}_p^*$
- (c) Prove that  $\log_g(h^n) = n \log_g(h)$  for all  $h \in \mathbb{F}_p^*$  and  $n \in \mathbb{Z}$

*Proof.* (a) Because  $a$  and  $b$  are both solutions to the congruence  $g^x \equiv h \pmod{p}$ ,

$$\begin{cases} g^a \equiv h \pmod{p} \\ g^b \equiv h \pmod{p} \end{cases}$$

$$\begin{aligned} &\Rightarrow g^{-b} \equiv h^{-1} \pmod{p} \\ &\Rightarrow g^a g^{-b} \equiv h h^{-1} \equiv 1 \pmod{p} \\ &\Rightarrow g^{a-b} \equiv 1 \pmod{p}, \text{ but } g \text{ is primitive root of } \mathbb{F}_p \\ &\Rightarrow \phi(p)|(a-b) \Leftrightarrow (p-1)|(a-b) \\ &\Rightarrow a-b \equiv 0 \pmod{p-1} \\ &\Rightarrow a \equiv b \pmod{p-1} \end{aligned}$$

(b) Suppose that

$$\begin{cases} h_1 \equiv g^{x_1} \pmod{p} \\ h_2 \equiv g^{x_2} \pmod{p} \end{cases}$$

$$\begin{aligned} &\Rightarrow x_1 = \log_g h_1 \text{ and } x_2 = \log_g h_2 \quad (1) \\ &\text{And } h_1 h_2 \equiv g^{x_1+x_2} \pmod{p} \\ &\Rightarrow x_1 + x_2 = \log_g(h_1 h_2) \quad (2) \\ &\text{From (1) and (2), } \log_g h_1 + \log_g h_2 = \log_g(h_1 h_2) \end{aligned}$$

(c) Same as (b).

□

**Exercise (2.5).** Let  $p$  be an odd prime and let  $g$  be a primitive root modulo  $p$ . Prove that  $a$  has a square root modulo  $p$  if and only if its discrete logarithm  $\log_g(a)$  modulo  $p-1$  is even.

We have  $g^{p-1} \equiv 1 \pmod{p}$ .

(1) If  $a$  has square root modulo  $p$ , then there is  $b$ :  $b \equiv a^2 \pmod{p}$

$$\Rightarrow \log_g a = \log_g(b^2) = 2\log_g b \pmod{p-1}$$

$\Rightarrow \log_g a$  is even.

(2) If  $\log_g a$  modulo  $p-1$  is even

$$\Rightarrow \log_g a = 2\log_g b \pmod{p-1} \text{ with some } b \in \mathbb{F}_p$$

$$\Rightarrow \log_g a = \log_g(b^2) \pmod{p-1}$$

$$\Rightarrow a \equiv b^2 \pmod{p-1}$$

$\Rightarrow a$  has square root modulo  $p-1$

**Exercise (2.10).** The exercise describes a public key cryptosystem that requires Bob and Alice to exchange several messages. We illustrate the system with an example.

Bob and Alice fix a publicly known prime  $p = 32611$ , and all of other numbers used are private. Alice takes her message  $m = 11111$ , chooses a random exponent  $a = 3589$ , and sends the number  $u = m^a \pmod{p} = 15950$  to Bob. Bob chooses a random exponent  $b = 4037$  and sends  $v = u^b \pmod{p} = 15422$  back to Alice. Alice then computes  $w = v^{15619} \equiv 27257 \pmod{32611}$  and sends  $w = 27257$  to Bob. Finally, Bob computes  $w^{31883} \pmod{32611}$  and recovers the value 11111 of Alice's message.

- Explain why this algorithm works. In particular, Alice uses the numbers  $a = 3589$  and 15619 as exponents. How are they related? Similarly, how are Bob's exponents  $b = 4037$  and 31883 related?
- Formulate a general version of this cryptosystem, i.e., using variables, and show how it works in general.
- What is the disadvantage of this cryptosystem over Elgamal? (*Hint.* How many times must Alice and Bob exchange data?)
- Are there any advantages of this cryptosystem over Elgamal? In particular, can Eve break it if she can solve the discrete logarithm problem? Can Eve break it if she can solve the Diffie-Hellman problem?

*Proof.* (a) We have  $3589 \times 15619 \equiv 4037 \times 31883 \equiv 1 \pmod{p-1}$

(b) Alice chooses  $a$  and  $a'$  satisfy that  $aa' \equiv 1 \pmod{p-1}$

Bob chooses  $b$  and  $b'$  satisfy that  $bb' \equiv 1 \pmod{p-1}$

From this, we have  $aa' = k(p-1) + 1$  and  $bb' = l(p-1) + 1$

$$\Rightarrow v \equiv u^b \equiv (m^a)^b \equiv m^{ab} \pmod{p}$$

$$\Rightarrow w \equiv v^{a'} \equiv (m^{ab})^{a'} \equiv m^{aa'b} \pmod{p}$$

$$\Rightarrow w^{b'} \equiv m^{aa'bb'} \equiv m^{[k(p-1)+1]x[l(p-1)+1]} \equiv m^{D(p-1)+1} \equiv m \pmod{p}$$

□

**Exercise (2.11).** The group  $S_3$  consists of the following six distinct elements

$$e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$$

where  $e$  is the identity element and multiplication is performed using the rules

$$\sigma^3 = e, \quad \tau^2 = e, \quad \tau\sigma = \sigma^2\tau$$

Compute the following values in the group  $S_3$ :

$$(a) \tau\sigma^2 \quad (b) \tau(\sigma\tau) \quad (c) (\sigma\tau)(\sigma\tau) \quad (d) (\sigma\tau)(\sigma^2\tau)$$

Is  $S_3$  a commutative group?

*Proof.* (a)  $\tau\sigma^2 = \tau\sigma\sigma = \sigma^2\tau\sigma = \sigma\sigma^2\tau = \sigma^3\tau = e\tau = \tau$

(b)  $\tau(\sigma\tau) = (\tau\sigma)\tau = \sigma^2\tau\tau = \sigma^2\tau^2 = \sigma^2e = \sigma^2$

(c)  $(\sigma\tau)(\sigma\tau) = \sigma(\tau\sigma)\tau = \sigma(\sigma^2\tau)\tau = \sigma^3\tau^2 = ee = e$

(d)  $(\sigma\tau)(\sigma^2\tau) = (\sigma\tau)(\tau\sigma) = \sigma\tau^2\sigma = \sigma e\sigma = \sigma^2$

$S_3$  is not a commutative group because:

$\sigma\tau = \sigma\tau$  but  $\tau\sigma = \sigma^2\tau$  (2 distinct elements in  $S_3$ ) □

**Exercise (2.12).** Let  $G$  be a group, let  $d \geq 1$  be an integer, and define a subset of  $G$  by

$$G[d] = \{g \in G : g^d = e\}$$

(a) Prove that if  $g$  is in  $G[d]$ , then  $g^{-1}$  is in  $G[d]$

(b) Suppose that  $G$  is commutative. Prove that if  $g_1$  and  $g_2$  are in  $G[d]$ , then their product  $g_1 \star g_2$  is in  $G[d]$

(c) Deduce that if  $G$  is commutative, then  $G[d]$  is a group.

(d) Show by an example that if  $G$  is not a commutative group, then  $G[d]$  need not be a group.  
(Hint. Use Exercise 2.11.)

*Proof.* (a) Because  $g \star g^{-1} = e \Rightarrow g \star e \star g^{-1} = e$

$\Rightarrow g \star g \star g^{-1} \star g^{-1} = e \Rightarrow g^2 \star (g^{-1})^2 = e$

Do more  $d-2$  times and we get  $g^d \star (g^{-1})^d = e$

$\Rightarrow e \star (g^{-1})^d = e \Rightarrow (g^{-1})^d = e \Rightarrow g^{-1} \in G[d]$

(b) We have  $g_1^d = e$  and  $g_2^d = e$

Because  $G$  is commutative,  $g_1^d \star g_2^d = (g_1 \star g_2)^d$

$\Rightarrow (g_1 \star g_2)^d = e \star e = e \Rightarrow g_1 \star g_2 \in G[d]$

(c) From (b), we have  $\forall g_1, g_2 \in G[d]$ , then  $g_1 \star g_2 \in G[d]$

We easily see that  $e \in G[d]$ , so it is identity element of  $G[d] \Rightarrow$  identity law.

From (a) we have inverse law.

With  $a, b, c \in G[d]$ , which means  $a^d = b^d = c^d = e$ , then

$a^d \star (b^d \star c^d) = a^d \star (bc)^d$  (because  $G$  is commutative)  $= (a \star b \star c)^d = (a \star b)^d \star c^d = (a^d \star b^d) \star c^d$

$\Rightarrow$  associative law.

So,  $G[d]$  is a group.

(d) Using exercise 2.11,  $S_3[2] = \{\tau, \sigma\tau, \sigma^2, \tau, e\}$ . Because  $(\sigma\tau)\tau = \sigma\tau^2 = \sigma \notin S_3[2]$ ,  $S_3[2]$  is not a group. □

**Exercise (2.13).** Let  $G$  and  $H$  be groups. A function  $\phi : G \rightarrow H$  is called a (group) *homomorphism* if it satisfies

$$\phi(g_1 \star g_2) = \phi(g_1) \star \phi(g_2) \text{ for all } g_1, g_2 \in G$$

(Note that the product  $g_1 \star g_2$  uses the group law in the group  $G$ , while the product  $\phi(g_1) \star \phi(g_2)$  uses the group law in the group  $H$ .)

(a) Let  $e_G$  be the identity element of  $G$ , let  $e_H$  be identity element of  $H$ , and let  $g \in G$ . Prove that

$$\phi(e_G) = e_H \quad \text{and} \quad \phi(g^{-1}) = \phi(g)^{-1}$$

(b) Let  $G$  be a commutative group. Prove that the map  $\phi : G \rightarrow G$  defined by  $\phi(g) = g^2$  is a homomorphism. Give an example of a noncommutative group for which this map is not a homomorphism.

(c) Same question as (b) for the map  $\phi(g) = g^{-1}$

*Proof.* (a)  $\forall g \in G: g = g \star e = e \star g$

$$\Rightarrow \phi(g) = \phi(g \star e_G) = \phi(e_G \star g)$$

$$\Rightarrow \phi(g) = \phi(g) \star \phi(e_G) = \phi(e_G) \star \phi(g)$$

Because  $\phi(g) \in H$ ,  $\phi(e_G)$  is identity element of  $H \Leftrightarrow \phi(e_G) = e_H$

In group  $G$ ,  $g \star g^{-1} = e_G$

$$\Rightarrow \phi(g \star g^{-1}) = \phi(e_G)$$

$$\Rightarrow \phi(g) \star \phi(g^{-1}) = \phi(e_G)$$

$$\Rightarrow \phi(g) \star \phi(g^{-1}) = e_H$$

$$\Rightarrow \phi(g^{-1}) = \phi(g)^{-1}$$

(b)  $\phi: G \rightarrow G, \phi(g) = g^2$

$\forall g_1, g_2 \in G, \phi(g_1 \star g_2) = (g_1 \star g_2)^2 = g_1^2 \star g_2^2$  (because  $G$  is commutative).

And we have  $g_1^2 \star g_2^2 = \phi(g_1) \star \phi(g_2)$ , which means  $\phi(g_1 \star g_2) = \phi(g_1) \star \phi(g_2)$

$\Rightarrow G$  is homomorphism.

Now we consider group in Exercise 2.11 and the map  $\phi: G \rightarrow G, \phi(g) = g^2$

$$\Rightarrow \phi(e) = e^2 = e, \phi(\sigma) = \sigma^2, \phi(\tau) = \tau^2 = e, \phi(\sigma\tau) = (\sigma\tau)^2 = e$$

We have:  $\phi(\sigma\tau) = e \neq \sigma^2 = \phi(\sigma)\phi(\tau)$

$\Rightarrow$  Therefore,  $G$  is not homomorphism.

(c)  $\phi: G \rightarrow G, \phi(g) = g^{-1}$

$\forall g_1, g_2 \in G, g_1 g_1^{-1} = e, g_2 g_2^{-1} = e$

$$\Rightarrow g_1 g_1^{-1} g_2 g_2^{-1} = e, \text{ but } G \text{ is commutative}$$

$$\Rightarrow (g_1 g_2)(g_1^{-1} g_2^{-1}) = e$$

$$\Rightarrow g_1^{-1} g_2^{-1} = (g_1 g_2)^{-1}$$

$$\Rightarrow \phi(g_1 g_2) = (g_1 g_2)^{-1} = g_1^{-1} g_2^{-1} = \phi(g_1) \phi(g_2)$$

$\Rightarrow G$  is homomorphism.

Now we consider group in Exercise 2.11 and the map  $\phi: G \rightarrow G, \phi(g) = g^{-1}$ . We have

$$\sigma\sigma^2 = e = \sigma^2\sigma = e, \quad \tau^2 = e, \quad (\sigma\tau)^2 = e, \quad (\sigma^2\tau)^2 = e$$

$$\Rightarrow \phi(\sigma\tau) = \sigma\tau \quad \text{and} \quad \phi(\sigma) = \sigma^2, \phi(\tau) = \tau$$

$$\Rightarrow \phi(\sigma\tau) = \sigma\tau \neq \sigma^2\tau = \phi(\sigma)\phi(\tau)$$

$\Rightarrow G$  is not homomorphism. □

**Exercise (2.14).** Prove that each of the following maps is a group homomorphism.

(a) The map  $\phi: \mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$  that sends  $a \in \mathbb{Z}$  to  $a \bmod N$  in  $\mathbb{Z}/N\mathbb{Z}$ .

$$\forall a, b \in \mathbb{Z},$$

$$\begin{aligned} \phi(ab) &= (ab) \pmod{N} \\ &= (a \bmod N)(b \bmod N) \pmod{N} \\ &= \phi(a)\phi(b) \end{aligned}$$

$\Rightarrow$  homomorphism.

(b) The map  $\phi: \mathbb{R}^* \rightarrow \text{GL}_2(\mathbb{R})$  defined by  $\phi(a) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$

$$\forall a, b \in \mathbb{R}^*, \phi(ab) = \begin{pmatrix} ab & 0 \\ 0 & (ab)^{-1} \end{pmatrix}$$

$$\text{And we have } \phi(a)\phi(b) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & a^{-1}b^{-1} \end{pmatrix}$$

It is clear that  $(ab)^{-1} = a^{-1}b^{-1}$ , so  $\phi(ab) = \phi(a)\phi(b) \Rightarrow$  homomorphism.

(c) The discrete logarithm map  $\log_g : \mathbb{F}_p^* \rightarrow \mathbb{Z}/(p-1)\mathbb{Z}$ , where  $g$  is a primitive root modulo  $p$

$\phi(a) = x$  satisfying  $g^x \equiv a \pmod{p}$

$\forall a, b \in \mathbb{F}_p^*, \phi(a) = x: g^x \equiv a \pmod{p}$  and  $\phi(b) = y: g^y \equiv b \pmod{p}$

$\Rightarrow \phi(a)\phi(b) = x + y$  (Because  $x, y \in \mathbb{Z}/(p-1)\mathbb{Z}$ , rule of group is addition modulo  $p-1$ )

And we have  $g^{x+y} \equiv ab \pmod{p} \Rightarrow \phi(ab) = x + y$

$\Rightarrow \phi(a)\phi(b) = \phi(ab)$

$\Rightarrow$  homomorphisms.

**Exercise (2.15).** (a) Prove that  $\text{GL}_2(\mathbb{F}_p)$  is a group. If  $A$  and  $B$  is 2 matrices in  $\text{GL}_2(\mathbb{F}_p)$ , then  $AB$  also in  $\text{GL}_2(\mathbb{F}_p)$  (because result will be modulo 2)

Identity element is  $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  because  $AE = EA = A \quad \forall A \in \text{GL}_2(\mathbb{F}_p)$

$\forall A \in \text{GL}_2(\mathbb{F}_p)$ , because  $\det A \neq 0 \Rightarrow A$  has inverse in  $\text{GL}_2(\mathbb{F}_p)$

$\forall A, B, C \in \text{GL}_2(\mathbb{F}_p) : (AB)C = A(BC)$

Therefore,  $\text{GL}_2(\mathbb{F}_p)$  is a group.

(b) Show that  $\text{GL}_2(\mathbb{F}_p)$  is a noncommutative group for every prime  $p$ . Suppose we have  $A =$

$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \text{GL}_2(\mathbb{F}_p)$  and  $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in \text{GL}_2(\mathbb{F}_p)$

Top left element of product  $AB$  is  $(a_{11}b_{11} + a_{12}b_{21}) \pmod{p}$

Top left element of product  $BA$  is  $(b_{11}a_{11} + b_{12}a_{21}) \pmod{p}$

If we choose  $a_{12} \neq b_{21}^{-1}a_{21}b_{21} \pmod{p}$ , then  $AB \neq BA$ , which means noncommutative.

(c) Describe  $\text{GL}_2(\mathbb{F}_p)$  completely. That is, list its elements and describe the multiplication table.

$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_4 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, A_5 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, A_6 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

Multiplication table:

	$A_1$	$A_2$	$A_3$	$A_4$	$A_5$	$A_6$
$A_1$	$A_3$	$A_5$	$A_1$	$A_6$	$A_2$	$A_4$
$A_2$	$A_4$	$A_6$	$A_2$	$A_5$	$A_1$	$A_3$
$A_3$	$A_1$	$A_2$	$A_3$	$A_4$	$A_5$	$A_6$
$A_4$	$A_2$	$A_1$	$A_4$	$A_3$	$A_6$	$A_5$
$A_5$	$A_6$	$A_4$	$A_5$	$A_2$	$A_3$	$A_1$
$A_6$	$A_5$	$A_3$	$A_6$	$A_1$	$A_4$	$A_2$

(d) How many elements are there in the group  $\text{GL}_2(\mathbb{F}_p)$ ?

First row  $u_1$  is any vector but  $(0,0)$ . We have  $p^2 - 1$  ways.

Second row  $u_2$  is any vector but multiple of first vector. We have  $p^2 - p$  ways (remove  $0u_1$  to  $(p-1)u_1$ ).

$\Rightarrow$  There are  $(p^2 - 1)(p^2 - p)$  elements.

(d) How many elements are there in the group  $\text{GL}_n(\mathbb{F}_p)$ ?

Similar to (d), we need first row  $u_1$  is any vector but  $(0,0)$ . We have  $p^n - 1$  ways.

Second vector  $u_2$  is any vector but a multiple of first row. We have  $p^n - p$  ways.

Third vector  $u_3$  is any vector but a linear combination of  $u_1$  and  $u_2$ . The number of  $a_1u_1 + a_2u_2$  is the number of pair  $(a_1, a_2)$  and there is  $p^2$  possibilities  $(a_1, a_2 \in \mathbb{F}_p)$ . So third vector has  $p^n - p^2$  ways.

In general,  $n$ -th vector is any vector but a linear combination of  $u_1, u_2, \dots, u_{n-1}$ , so there is  $p^n - p^{n-1}$  ways.

$\Rightarrow$  There are  $(p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$  elements.

**Exercise (2.17). shank\_bsgs.py**

**Exercise (2.18).** Solve each of the following simultaneous systems of congruences (or explain why no solutions exists).

- (a)  $x \equiv 3 \pmod{7}$  and  $x \equiv 4 \pmod{9}$

$$N = 7 \times 9 = 63$$

$$T_1 = 63/7 = 9, T_1^{-1} \pmod{7} = 4$$

$$T_2 = 63/9 = 7, T_2^{-1} \pmod{9} = 4$$

$$\Rightarrow x \equiv 3 \times 9 \times 4 + 4 \times 7 \times 4 \equiv 220 \equiv 31 \pmod{63}$$

- (b)  $x \equiv 137 \pmod{423}$  and  $x \equiv 87 \pmod{191}$

$$N = 423 \times 191 = 90793$$

$$T_1 = N/423 = 191, T_1^{-1} \pmod{423} = 392$$

$$T_2 = N/191 = 423, T_2^{-1} \pmod{191} = 14$$

$$\Rightarrow x \equiv 137 \times 191 \times 392 + 87 \times 423 \times 14 \equiv 27209 \pmod{N}$$

- (c) Cannot calculate because  $\gcd(451, 697) = 41 \neq 1$

- (d)  $x \equiv 5 \pmod{9}$ ,  $x \equiv 6 \pmod{10}$  and  $x \equiv 7 \pmod{11}$

$$N = 9 \times 10 \times 11 = 990$$

$$T_1 = N/9 = 110, T_1^{-1} \pmod{9} = 5$$

$$T_2 = N/10 = 99, T_2^{-1} \pmod{10} = 9$$

$$T_3 = N/11 = 90, T_3^{-1} \pmod{11} = 6$$

$$\Rightarrow x \equiv 5 \times 110 \times 5 + 6 \times 99 \times 9 + 7 \times 90 \times 6 \equiv 986 \pmod{N}$$

- (e)  $x \equiv 37 \pmod{43}$ ,  $x \equiv 22 \pmod{49}$  and  $x \equiv 18 \pmod{71}$

$$N = 43 \times 49 \times 71 = 149597$$

$$T_1 = N/43 = 3479, T_1^{-1} \pmod{43} = 32$$

$$T_2 = N/49 = 3053, T_2^{-1} \pmod{49} = 36$$

$$T_3 = N/71 = 2107, T_3^{-1} \pmod{71} = 37$$

$$\Rightarrow x \equiv 37 \times 3479 \times 32 + 22 \times 3053 \times 36 + 18 \times 2107 \times 37 \equiv 11733 \pmod{N}$$

Code in: **modular.py**

**Exercise (2.19).** Solve the 1700-year-old Chinese remainder problem from the *Sun Tzu Suan Ching* stated on page 84.

$$x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5} \text{ and } x \equiv 2 \pmod{7} \Rightarrow x \equiv 23 \pmod{105}$$

**Exercise (2.20).** Let  $a, b, m, n$  be integers with  $\gcd(m, n) = 1$ . Let

$$c \equiv (b - a) \cdot m^{-1} \pmod{n}$$

.

Prove that  $x = a + cm$  is a solution to

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n} \tag{1}$$

and that every solution to (1) has the form  $x = a + cm + ymn$  for some  $y \in \mathbb{Z}$

**Exercise (2.21).** (a) Let  $a, b, c$  be positive integers and suppose that

$$a \mid c, \quad b \mid c, \quad \text{and} \quad \gcd(a, b) = 1$$

Prove that  $ab \mid c$

Because  $a \mid c \Leftrightarrow c = ka, (k \in \mathbb{Z})$  and  $b \mid c \Leftrightarrow c = lb (l \in \mathbb{Z})$

$\Rightarrow ka = lb$ . But  $\gcd(a, b) = 1 \Rightarrow a \mid l \Leftrightarrow l = ma, (m \in \mathbb{Z})$

$\Rightarrow c = lb = lma \Rightarrow ab \mid c$

(b) Let  $x = c$  and  $x = c'$  be two solutions to the system of simultaneous congruences in the Chinese remainder theorem. Prove that

$$c \equiv c' \pmod{m_1 m_2 \dots m_k}$$

If  $c \equiv c' \pmod{m_i}$ , then  $c \equiv c' \pmod{m_1 m_2 \dots m_k}$

**Exercise (2.23).** Find square roots modulo the following composite moduli

- (a) 215
- (b) 2654
- (c) 1712, 2477, 3187, 1002
- (d)  $(\pm 1 \cdot 317 \cdot 1 \pm 1 \cdot 124 \cdot 3 \pm 10 \cdot 28 \cdot 10) \pmod{868}$

**Exercise (2.24).** Let  $p$  be an odd prime, let  $a$  be an integer that is not divisible by  $p$ , and let  $b$  is a square root of  $a$  modulo  $p$ . This exercise investigates the square root of  $a$  modulo powers of  $p$

- (a) Prove that for some choice of  $k$ , the number  $b + kp$  is a square root of  $a$  modulo  $p^2$ , i.e.,  $(b + kp)^2 \equiv a \pmod{p^2}$
- (b) The number  $b = 537$  is a square root of  $a = 476$  modulo the prime  $p = 1291$ . Use the idea in (a) to compute a square root of 476 modulo  $p^2$
- (c) Suppose that  $b$  is a square root of  $a$  modulo  $p^n$ . Prove that for some choice of  $j$ , the number  $b + jp^n$  is a square root of  $a$  modulo  $p^{n+1}$
- (d) Explain why (c) implies the following statements: If  $p$  is an odd prime and if  $a$  has a square root modulo  $p$ , then  $a$  has a square root modulo  $p^n$  for every power of  $p$ . Is this true if  $p = 2$ ?
- (e) Use the method in (c) to compute the square root of 3 modulo  $13^3$ , given that  $9^2 \equiv 3 \pmod{13}$

*Proof.* (a) Let  $f(b_n) = b_n^2 - a \pmod{p^n}$ , with  $b_1 = b \Rightarrow f(b_1) = b^2 - a \equiv 0 \pmod{p}$

We need to find  $b_2$ ,  $f(b_2) = b_2^2 - a \equiv 0 \pmod{p^2}$

Which means,  $f(b_1 + kp) = (b_1 + kp)^2 - a = b_1^2 + 2b_1kp + (kp)^2 - a \equiv 0 \pmod{p^2}$

$\Leftrightarrow 2b_1k \equiv -(b_1^2 - a)/p \pmod{p^2}$  (because  $b_1^2 - a \equiv 0 \pmod{p}$ )

And because  $2b_1 \not\equiv 0 \pmod{p^2}$ , then exist  $k$  satisfying the equation

$$(b) \quad k = [-(b^2 - a)/p \times \text{INVERSE}(2b, p^2)] \pmod{p^2}$$

(c) We prove by induction that for each  $n \geq 1$ , there is a  $b_n \in \mathbb{Z}$  such that

- $f(b_n) = b_n^2 - a \equiv 0 \pmod{p^n}$
- $b_n \equiv b \pmod{p^n}$



The case  $n = 1$  is trivial, using  $b_1 = b$ . If the inductive hypothesis holds for  $n$ , which means:

$$\begin{cases} f(b_n) = b_n^2 - a \pmod{p^n} \\ b_n = b \pmod{p^n} \end{cases} \quad (2)$$

With  $b_{n+1}$ ,  $f(b_{n+1}) = b_{n+1}^2 - a \equiv 0 \pmod{p^{n+1}}$ . We write  $b_{n+1} = b_n + p^n t_n$

$$\Rightarrow f(b_{n+1}) = b_n^2 + 2b_n p^n t_n + p^{2n} t_n^2 - a \equiv 0 \pmod{p^{n+1}}$$

$$\Rightarrow b_n^2 + 2b_n p^n t_n - a \equiv 0 \pmod{p^{n+1}} \text{ (because } 2n \geq n+1 \text{)}$$

$$\Rightarrow 2b_n t_n \equiv -(b_n^2 - a)/p^n \pmod{p^{n+1}} \text{ (from (2))}$$

Therefore, exists solution for  $t_n$  because we assumed that  $2b_n \equiv 0 \pmod{p^n}$

$$\Rightarrow f(b_{n+1}) \equiv 0 \pmod{p^{n+1}}, \text{ and } b_{n+1} \equiv b_n \pmod{p^n}$$

This proof is used for  $b + j p^n$  modulo  $p^n$ , not for  $p^{n+1}$

(d) Using induction we get that. If  $p = 2$ , then any integers is right

□

**Exercise (2.31).** Let  $R$  and  $S$  be rings. A functions  $\phi : R \rightarrow S$  is called a (*ring*) *homomorphism* if it satisfies

$$\phi(a + b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(a \star b) = \phi(a) \star \phi(b) \quad \text{for all } a, b \in R$$

(a) Let  $0_R, 0_S, 1_R$  and  $1_S$  denote the additive and multiplicative identities of  $R$  and  $S$ , respectively. Prove that

$$\phi(0_R) = 0_S, \quad \phi(1_R) = 1_S, \quad \phi(-a) = -\phi(a), \quad \phi(a^{-1}) = \phi(a)^{-1},$$

where the last equality holds for those  $a \in R$  that have a multiplicative inverse.

(b) Let  $p$  be a prime, and let  $R$  be a ring with the property that  $pa = 0$  for every  $a \in R$ . (Here  $pa$  means to add  $a$  to itself  $p$  times.) Prove that the map

$$\phi : R \rightarrow R, \quad \phi(a) = a^p$$

is a ring homomorphism. It is called the *Frobenius homomorphism*.

*Proof.* With  $\phi(a + b) = \phi(a) + \phi(b)$  and  $\phi(a \star b) = \phi(a) \star \phi(b)$  for all  $a, b \in R$

(a) In  $R, \forall a \in R : a + 0_R = 0_R + a = a$

$$\Rightarrow \phi(a) = \phi(a + 0_R) = \phi(0_R + a)$$

$$\Rightarrow \phi(a) = \phi(a) + \phi(0_R) = \phi(0_R) + \phi(a)$$

$$\text{Let } \phi(a) = b \in S. \text{ Hence } b = b + \phi(0_R) = \phi(0_R) + b$$

$$\Rightarrow \phi(0_R) = 0_S$$

$$\text{In } R, \forall a \in R : a \star 1_R = 1_R \star a = a$$

$$\Rightarrow \phi(a \star 1_R) = \phi(1_R \star a) = \phi(a)$$

$$\Rightarrow \phi(a) \star \phi(1_R) = \phi(1_R) \star \phi(a) = \phi(a)$$

$$\Rightarrow \phi(1_R) = 1_S$$

$$\text{With } \phi(-a) = -\phi(a), \text{ we have in } R, a + (-a) = (-a) + a = 0_R$$

$$\Rightarrow \phi(a + (-a)) = \phi((-a) + a) = \phi(0_R)$$

$$\Rightarrow \phi(a) + \phi(-a) = \phi(-a) + \phi(a) = \phi(0_R) = 0_S$$

$$\Rightarrow \phi(-a) = -\phi(a)$$

$$\text{With } \phi(a^{-1}) = \phi(a)^{-1}, \text{ we have in } R, a \star a^{-1} = a^{-1} \star a = 1_R$$

$$\phi(a \star a^{-1}) = \phi(a^{-1} \star a) = \phi(1_R)$$

$$\Rightarrow \phi(a) \star \phi(a^{-1}) = \phi(a^{-1}) \star \phi(a) = \phi(1_R) = 1_S$$

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

(b)  $\phi: R \rightarrow R, \phi(a) = a^p$   
 $\Rightarrow \phi(a+b) = (a+b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i}$   
 And we have  $p \mid \binom{p}{i} = \frac{p!}{(p-i)!i!}$  (because  $p$  is prime)  
 $\Rightarrow 1 \leq i \leq p-1: \binom{p}{i} = 0$  (because  $pa = 0$ )  
 $\Rightarrow \phi(a+b) = a^p + b^p = \phi(a) + \phi(b)$  (1)  
 $\Rightarrow \phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$  (2)  
 From (1) and (2)  $\Rightarrow$  ring homomorphism

□

**Exercise (2.32).** Prove Proposition 2.41

We have  $a_1 \equiv a_2 \pmod{m} \Rightarrow m \mid (a_1 - a_2)$   
 $\Rightarrow \exists k \in R: a_1 - a_2 = k \star m$   
 Similarly,  $\exists l \in R: b_1 - b_2 = l \star m$   
 $\Rightarrow a_1 - a_2 + b_1 - b_2 = (k + l) \star m$   
 $\Leftrightarrow m \mid (a_1 + b_1 - (a_2 + b_2))$   
 $\Leftrightarrow a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$   
 Similarly for  $a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$

$$\begin{cases} a_1 = a_2 + k \star m \\ b_1 = b_2 + l \star m \end{cases}$$

$\Rightarrow a_1 \star b_1 = (a_2 + k \star m)(b_2 + l \star m) = a_2 \star b_2 + a_2 \star l \star m + k \star b_2 \star m + k \star l \star m^2$   
 $\Rightarrow m \mid (a_1 \star b_1 - a_2 \star b_2)$   
 $\Rightarrow a_1 \star b_1 \equiv a_2 \star b_2 \pmod{m}$

**Exercise (2.33).** Prove Proposition 2.43

According to Exercise 2.32, if we have

$$\begin{cases} a' \in \bar{a} \Leftrightarrow a' \equiv a \pmod{m} \\ b' \in \bar{b} \Leftrightarrow b' \equiv b \pmod{m} \end{cases}$$

$$\Rightarrow \begin{cases} a' + b' \equiv a + b \pmod{m} \\ a' \star b' \equiv a \star b \pmod{m} \end{cases}$$

$\Rightarrow a' + b' \in \overline{a+b}$  and  $a' \star b' \in \overline{a \star b}$ . Hence the set is **closed**

We have  $m \equiv 0 \pmod{m} \Rightarrow \forall a \in R, \bar{a} + \bar{m} = \overline{a+m} = \bar{a} = \overline{m+a} = \bar{m} + \bar{a}$

$\Rightarrow$  **identity element** is  $\bar{m}$

Also, because  $R$  is ring,  $m + (-x) \in R, x \in R$

$\forall a \in R, \bar{a} + \overline{m-a} = \overline{a+m-a} = \bar{m} = \overline{m-a+a}$

$\Rightarrow \overline{m-a}$  is additive inverse of  $a$

Easily see that  $\overline{a+b} = \overline{a+b+c} = \overline{a+b+c} = \overline{a+b} + \bar{c} = (\bar{a} + \bar{b}) + \bar{c}$

**associative**

$\forall a, b \in R, \bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a} \Rightarrow$  **commutative**

We have  $a \star 1 \equiv a \pmod{m} \forall a \in R$

$\Rightarrow \bar{a} \star \bar{1} = \overline{a \star 1} = \bar{a} = \overline{1 \star a} = \bar{1} \star \bar{a}$

$\Rightarrow$  **multiplicative identity** is  $\bar{1}$

$\forall a, b, c \in R, a(bc) = (ab)c \pmod{m}$

$\Rightarrow \bar{a} \star (\bar{b} \star \bar{c}) = \overline{a \star (b \star c)} = \overline{a \star bc} = \overline{abc} = \overline{ab \star c} = (\bar{a} \star \bar{b}) \star \bar{c} \Rightarrow$  **associative**

And  $\bar{a} \star \bar{b} = \overline{a \star b} = \overline{b \star a} = \bar{b} \star \bar{a} \Rightarrow$  **commutative**

With  $\bar{a} \star (\bar{b} + \bar{c}) = \overline{a \star (b+c)} = \overline{a \star (b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = \bar{a} \star \bar{b} + \bar{a} \star \bar{c} \Rightarrow$  **distribute**

Hence,  $R/(m)$  is a ring

**Exercise (2.34).** Let  $\mathbb{F}$  be a field and let  $\mathbf{a}$  and  $\mathbf{b}$  be nonzero polynomials in  $\mathbb{F}[x]$

(a) Prove that  $\deg(\mathbf{a} \cdot \mathbf{b}) = \deg(\mathbf{a}) + \deg(\mathbf{b})$

Let  $a = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ , with  $a_i \in \mathbb{F}[x] \Rightarrow \deg(\mathbf{a}) = n$

Let  $b = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$ , with  $a_i \in \mathbb{F}[x] \Rightarrow \deg(b) = m$

$\Rightarrow \deg(a \cdot b) = m + n = \deg(a) + \deg(b)$

(b) Prove that  $\mathbf{a}$  has a multiplicative inverse in  $\mathbb{F}[x]$  if and only if  $\mathbf{a}$  is in  $\mathbb{F}$ , i.e., if and only if  $\mathbf{a}$  is a constant polynomial

With  $\mathbf{a} = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

Suppose that  $\mathbf{a}$  has multiplicative inverse in  $\mathbb{F}[x]$   $\mathbf{b} = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$

$$\Rightarrow \mathbf{ab} = \sum_{i=0}^n a_i x^i \sum_{j=0}^m b_j x^j = 1$$

$$\Rightarrow \sum_{i=0}^n \sum_{j=0}^m a_i b_j x^{i+j} = 1$$

Which means  $a_0 b_0 = 1$ , other coefficients is 0, so  $\mathbf{a}$  is constant polynomial

(c) Prove that every nonzero element of  $\mathbb{F}[x]$  can be factored into a product of irreducible polynomials. (*Hint.* Use (a), (b) and induction on the degree of the polynomial.)

(d) Let  $R$  be ring  $\mathbb{Z}/6\mathbb{Z}$ . Give an example to show that (a) is false for some polynomials  $\mathbf{a}$  and  $\mathbf{b}$  in  $R[x]$

$$a = 2x^2 + 3x + 1, b = 3x + 2$$

$$\Rightarrow ab = x^2 + 3x + 2$$

$$\deg(ab) = 2 < 3 = \deg(a) + \deg(b)$$

**Exercise (2.35, 2.36).** Programming on Sagemath

**Exercise (2.37).** Prove that the polynomial  $x^3 + x + 1$  is irreducible in  $\mathbb{F}_2[x]$

If  $f(x) = x^3 + x + 1$  has any factor rather than 1 and itself, it must have degree less than 3. So we have  $0, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1, x$  but  $f(x)$  is not divided by any of them. Hence irreducible

**Exercise (2.38).** Programming on Sagemath

**Exercise (2.39).** The field  $\mathbb{F}_7[x]/(x^2 + 1)$  is a field with 49 elements, which for the moment we denote by  $\mathbb{F}_{49}$

Using example 2.58, every element in  $\mathbb{F}_7[x]/(x^2 + 1)$  has form  $f(x) = a + bx$ , so in  $\mathbb{F}_{49}$  it has form  $a + bi$  (here  $i^2 = -1$ )

(a) Is  $2 + 5x$  is a primitive root in  $\mathbb{F}_{49}$ ? No because  $(2 + 5x)^8 = 1$

(b) Is  $2 + x$  is a primitive root in  $\mathbb{F}_{49}$ ? Yes

(c) Is  $1 + x$  is a primitive root in  $\mathbb{F}_{49}$ ? No because  $(1 + x)^{24} = 1$

**Exercise (2.41).** Let  $\mathbb{F}$  is a finite field.

(a) Prove that there is an integer  $m \geq 1$  such that if we add 1 to itself  $m$  times,

$$\underbrace{1 + 1 + \cdots + 1}_{m \text{ ones}}$$

then we get 0. Note that here 1 and 0 are the multiplicative and additive identity elements of the field  $\mathbb{F}$ .

Because 1 is element of  $\mathbb{F}$ , then  $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$  always is an element of  $\mathbb{F}$ . And  $\mathbb{F}$  is finite field, so

there is  $m \geq 1$  such that  $\underbrace{1 + 1 + \cdots + 1}_{m \text{ times}}$  equals to 0 (1, 1+1, 1+1+1, ... cannot all be different)

- (b) Let  $m$  be the smallest positive integer with the property described in (a). Prove that  $m$  is prime. This prime is called the *characteristic of the field*  $\mathbb{F}$

Suppose that  $m$  can be factor, so  $m = pq$  ( $1 < p, q < m$ )  $\Rightarrow \underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} = 0$

$$\overbrace{\underbrace{(1 + 1 + \cdots + 1)}_{p \text{ times}} + \underbrace{(1 + 1 + \cdots + 1)}_{p \text{ times}} + \cdots + \underbrace{(1 + 1 + \cdots + 1)}_{p \text{ times}}}_{q \text{ times}}$$

Because  $\mathbb{F}$  is a finite field,  $\underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} = a \in \mathbb{F}$

$\Rightarrow q \cdot a = 0$  ( $q > 1$  and  $a$  cannot be 0 because  $m$  is the smallest number that satisfies  $1 + 1 + \cdots + 1 = 0$ )

$\Rightarrow$  contraction  $\Rightarrow \mathbb{F}$  cannot be a field.

So  $m$  is a prime