

# Introduction to Cryptography: Homework 1

Alvin Lin

January 2018 - May 2018

## Problem 1.5

As we learned in this chapter, modular arithmetic is the basis of many cryptosystems. As a consequence, we will address this topic with several problems in this and upcoming chapters.

1.  $15 \cdot 29 \pmod{13} = 6$
2.  $2 \cdot 29 \pmod{13} = 6$
3.  $2 \cdot 3 \pmod{13} = 6$
4.  $-11 \cdot 3 \pmod{13} = 6$

The modulo operation can be applied before the multiplication. The first factor modulo 13 comes out to 2 for all the problems and the second factor comes out to 3 for all the problems, leaving an answer of 6.

## Problem 1.6

Compute without a calculator:

1.  $1/5 \pmod{13} \equiv 1 \cdot 6 \pmod{13} \equiv 6$
2.  $1/5 \pmod{7} \equiv 1 \cdot 3 \pmod{7} \equiv 3$
3.  $3 \cdot 2/5 \pmod{7} = 3 \cdot 2 \cdot 3 \pmod{7} \equiv 4$

## Problem 1.7

We consider the ring  $\mathbb{Z}_4$ . Construct table which describes the addition of all the elements in the ring with each other.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Construct the multiplication table for  $\mathbb{Z}_4$ :

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Construct the addition and multiplication tables for  $\mathbb{Z}_6$ :

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

There are ele-

ments in  $\mathbb{Z}_4$  and  $\mathbb{Z}_6$  without a multiplicative inverse. Which elements are these? Why does a multiplicative inverse exist for nonzero elements in  $\mathbb{Z}_5$ ?

2 does not have a multiplicative inverse in  $\mathbb{Z}_4$ . 2, 3, 4 do not have multiplicative inverses in  $\mathbb{Z}_6$ . A multiplicative element exists for all nonzero elements in  $\mathbb{Z}_5$  because all nonzero elements are coprime to 5 (Because 5 is a prime number).

### Problem 1.8

What is the multiplicative inverse of 5 in  $\mathbb{Z}_{11}, \mathbb{Z}_{12}, \mathbb{Z}_{13}$ ?

$$5^{-1} \pmod{11} = 9$$

$$5^{-1} \pmod{12} = 5$$

$$5^{-1} \pmod{13} = 8$$

### Problem 1.9

Compute  $x$  as far as possible without a calculator. Where appropriate, make use of a smart decomposition of the exponent.

1.  $x = 3^2 \pmod{13} = 9$

2.  $x = 7^2 \pmod{13} = 10$

3.  $x = 3^{10} \pmod{13} = 3^4 \cdot 3^4 \cdot 3^2 \pmod{13} = 3 \cdot 3 \cdot 9 \pmod{13} = 3$

4.  $x = 7^{100} \pmod{13} = (7^2)^{50} \pmod{13} = 10^{50} \pmod{13} = 100^{25} \pmod{13} = 9^{25} \pmod{13} = (9^2)^{12} \cdot 9 \pmod{13} = 3^{12} \cdot 9 \pmod{13} = (3^4)^3 \cdot 9 \pmod{13} = 3^3 \cdot 9 \pmod{13} = 9$

5.  $7^x = 11 \pmod{13}$

$$7^2 \pmod{13} = 10$$

$$7^3 \pmod{13} = 10 \cdot 7 \pmod{13} = 5$$

$$7^4 \pmod{13} = 5 \cdot 7 \pmod{13} = 9$$

$$7^5 \pmod{13} = 9 \cdot 7 \pmod{13} = 11$$

## Problem 1.11

This problem deals with the affine cipher with the key parameters  $a = 7, b = 22$ . Decrypt the text below:

falsztyjzkywjrztjztyynaryjkyswarztyegyyj

Who write the line?

firstthesentenceandthentheevidencesaidthequeen

From *Alice In Wonderland* by Lewis Carroll

If you have any questions, comments, or concerns, please contact me at [alvin@omgimanerd.tech](mailto:alvin@omgimanerd.tech)