Revision Exercises Week 4
Public Key Cryptography

Hans Georg Schaathun

12th November 2015

1 Equations

Problem 1.1 *How many solutions $x \in \mathbb{Z}_{12}$ exist for each of the following congruences:*

$$4 \cdot x \equiv 1 \pmod{12}, \tag{1}$$
$$4 \cdot x \equiv 2 \pmod{12}, \tag{2}$$
$$4 \cdot x \equiv 4 \pmod{12}. \tag{3}$$

Give reasons for your answers, either by listing the complete set of solutions, or otherwise.

Solution: The first equation has no solution. This is seen because a solution would be an inverse of 4 modulo 12, but 4 and 12 have a common factor 2 (or 4) so 4 has no inverse.

The second equation also has no solution. We try[a] different possible values of x, see table below, and find that the LHS cycles through the values 0, 4, and 8 modulo 12. We can never get 2.

x	0	1	2	3	4	5	6	...
LHS	0	4	8	12	16	20	24	...
LHS mod 12	0	4	8	0	4	8	0	...

The third has four solutions where $0 \le x < 12$. This can also be seen in the table above. The left hand side cycles through three different values, every third value is 4, solving the equation. When x runs from 0 to 12, we get four solutions.

[a]It is possible to make more abstract arguments. It is however, a general fact about rings that the product ax will cycle repeatedly through a subset of the ring as x varies. Tabulating will

tell you exactly what this cycle is, and thus the simple approach is safe.

2 Highest common factor

Exercise 2.1 *Find*

1. $\mathrm{hcf}(18, 12)$
2. $\mathrm{hcf}(19, 8)$

Solution:

1. $\mathrm{hcf}(18, 12) = 6$
2. $\mathrm{hcf}(19, 8) = 1$

Exercise 2.2 *Prove that Euclid's Division Theorem is also valid for negative numbers m.*

Hint. *Note that if $m < 0$, then $-m > 0$ and the restricted version can be applied to $m' = -m$ to get numbers q' and r' to solve $m' = nq' + r'$. Note that q may be negative, while r cannot, so $q = -q'$ and $r = -r'$ is not quite the sol. Can you add/subtract a little bit to these numbers to get $0 \leq r < n$ and satisfy Euclid's theorem?*

Exercise 2.3 *Using Euclid's Algorithm, find*

1. $\mathrm{hcf}(121, 77)$
2. $\mathrm{hcf}(963, 312)$

Solution:

1. $\mathrm{hcf}(121, 77) = 11$
2. $\mathrm{hcf}(963, 312) = 3$

Exercise 2.4 *Prove that Euclid's Division Theorem is also valid for negative numbers m.*

Hint. *Note that if $m < 0$, then $-m > 0$ and the restricted version can be applied to $m' = -m$ to get numbers q' and r' to solve $m' = nq' + r'$. Note that q may be negative, while r cannot, so $q = -q'$ and $r = -r'$ is not quite the solution. Can you add/subtract a little bit to these numbers to get $0 \leq r < n$ and satisfy Euclid's theorem?*

3 Multiplicative inverses

Exercise 3.1 *Find the multiplicative inverses of*

1. $7 \mod 26$.
2. $28 \mod 81$.
3. $52 \mod 121$.

SOLUTION:

1. $7 \mod 26 = 15$.
2. $28 \mod 81 = 55$.
3. $52 \mod 121 = 7$.

Exercise 3.2 *Prove that if $d = \text{hcf}(a, n)$, then it is possible to find $x, y \in \mathbb{Z}$ so that*

$$d = a \cdot x + n \cdot y.$$

Exercise 3.3 *Consider the affine cipher*

$$e_{k_1,k_2}(x) = k_1 \cdot x + k_2 \mod n.$$

The decryption function can be written on the same form

$$d_{k_1',k_2'}(y) = k_1' \cdot y + k_2' \mod n,$$

for suitable choices of (k_1', k_2'). Find the decryption key (k_1', k_2') for each of the following encryption keys:

1. $(8, 3) \mod 26$.
2. $(7, 17) \mod 256$.

Problem 3.1 *Solve the following equation*

$$3 \cdot x \equiv 1 \pmod 8,$$

where $0 \leq x < 8$.

SOLUTION: It can be seen that $3^{-1} \mod 8 = 3^a$. Multiplying the equation by 3 we get

$$x \equiv 3 \cdot 1 = 3 \pmod 8.$$

We conclude that $x = 3$.

[a] Use the Extended Euclidean Algorithm if you do not see the inverse instantly

Problem 3.2 *Consider* $n = 59$ *and* $a = 6$.

1. *Show how you use Euclid's algorithm to find* $\text{hcf}(6, 59)$.
2. *Use the Extended Euclidean Algorithm to find the multiplicative inverses of* $6 \pmod{59}$.

Solution: We tabulate the values for q and r according to Euclid's division theorem. Subsequently, we fill in the values for x and y according to the Extended Euclidean Algorithm, as follows:

a	n	q	r	x	y
6	59	0	6	$1 - (-1) \cdot 9 = 10$	-1
59	6	9	5	$0 - 1 \cdot 1 = -1$	1
6	5	1	1	1	0

We see that $\text{hcf}(6, 59) = 1$ and $6^{-1} \mod 59 = 10$.

4 Some more simple exercises

Exercise 4.1 *Write down all the powers of* 5 *in* $\mathbb{Z}_7$. *What do you observe?*

Exercise 4.2 *Write down the product* $3 \cdot x$ *for every* $x \in \mathbb{Z}_8$. *What do you observe?*

Exercise 4.3 *Consider the following elements* x *in their respective rings. Find* x^{-1} *for each value of* x.

1. $x = 7 \in \mathbb{Z}_{29}$

Exercise 4.4 *Consider the following elements* x *in their respective rings. Find* $-x$ *for each value of* x.

1. $x = 7 \in \mathbb{Z}_{29}$