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.

2 Highest common factor

Exercise 2.1 *Find*

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

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. $\mathrm{hcf}(963, 312)$

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. $52 \mod 121$.

Exercise 3.2 *Prove that if* $d = \mathrm{hcf}(a, n)$, *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 $0 \leq x < 8$.

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

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

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