Exercises 2 for KAP
Laura Geatti - Lea Terracini

Problem 1. *For each of the following groups*

$$\mathbb{Z}/12\mathbb{Z}, \quad (\mathbb{Z}/100\mathbb{Z})^*, \quad \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}, \quad \mathbb{Z}/11\mathbb{Z} \times (\mathbb{Z}/17\mathbb{Z})^*, \quad (\mathbb{Z}/7^3\mathbb{Z})^*$$

(a) determine the order;

(b) list the possible orders of its elements;

(c) choose an element in the group ($\neq 1$) and verify that (2.) of Corollary 4.9 in the Algebra notes holds true.

Problem 2. *Let $n \in \mathbb{N}$. Show that*

(a) Verify that $\varphi(n)$ is even, for every integer $n > 2$;

(b) if a prime p divides n, then $\varphi(p)$ divides $\varphi(n)$;

(c) if p^2 does not divide n, then $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$;

(d) if p divides $\frac{n}{p}$, then $\varphi(\frac{n}{p}) = \frac{n}{p}\prod_{d|n}(1 - \frac{1}{d})$, where d varies in the set of distinct prime divisors of n.

Problem 3. *Let $\bar{x} = \overline{222487}$ and $\bar{y} = \overline{46375}$.*
Determine the orders of $\bar{x}$ and $\bar{y}$ in the groups

$$\mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/35\mathbb{Z}, \quad \mathbb{Z}/7\mathbb{Z}, \quad \mathbb{Z}/11\mathbb{Z}.$$

Problem 4. *Let $n = 1517$.*

(a) Prove that for all $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$, the order of $\bar{x}$ is equal to $\frac{n}{\gcd(x,n)}$.

(b) Determine the order of $\bar{x} = \overline{185}$ in $\mathbb{Z}/n\mathbb{Z}$.

Problem 5. *Verify that $p = 347$ is prime. State Fermat Little Theorem for $p = 347$ and check it for some classes $\bar{x} \in \mathbb{Z}_p^*$.*

Problem 6. *A Carmichael number is a composite integer n such that*

$$a^{n-1} \equiv 1, \quad \forall a \in \mathbb{Z}, \quad \textit{with } \gcd(a, n) = 1.$$

Let n be a square free composite integer. Prove that n is a Charmichael number if and only if it has the following property

$$\textit{if } p \textit{ divides } n, \textit{ then } p - 1 \textit{ divides } n - 1.$$

Problem 7. *Construct your own RSA set of keys N, E, D.*
(N the modulus, E the encrypting key, D the decrypting key).

Problem 8. *(mini RSA) Mr. White wants to receive encrypted messages and has the RSA set of keys*

$$N = 779, \quad E = 31, \quad D = 511.$$

(a) Check that N, E, D are a good set of keys.
(b) Send the message $m = 11$ to Mr. White after having encrypted it.

Problem 9. *Let $N \in \mathbb{Z}_{>0}$ and let E_1, $E_2 \in \mathbb{Z}_{>0}$ be coprime.*

(a) Show that you can determine m, knowing

$$m^{E_1} \pmod{N} \qquad \text{and} \qquad m^{E_2} \pmod{N}.$$

(b) Let $E_1 = 47$, $E_2 = 53$ and $N = 101$. Find m knowing that

$$m^{E_1} \equiv 28 \pmod{101}, \qquad m^{E_2} \equiv 83 \pmod{101}.$$

Problem 10. *Determine all the solutions of the equation $\bar{x}^2 = \bar{1}$ in $\mathbb{Z}/11\mathbb{Z}$ and in $\mathbb{Z}/15\mathbb{Z}$.*

Problem 11. *Let p be a prime. Prove that*

$$(p-1)! \equiv -1 \pmod{p}.$$

Problem 12. *Let p be a prime.*

(a) Show that if g is a primitive root modulo p, then g^k is a primitive root modulo p if and only if $\gcd(k, p-1) = 1$.

(b) Let $\bar{a}$ and $\bar{b}$ be primitive roots modulo p. Show that $\log_{\bar{a}} \bar{b}$ is invertible modulo $p-1$.

Problem 13. *Find a primitive root modulo $p = 47$.*

Problem 14. *Compute the orders of $\overline{2}$ in $\mathbb{Z}/35\mathbb{Z}$ and in $(\mathbb{Z}/35\mathbb{Z})^*$.*

Problem 15. *a) Prove that 2 is a primitive root modulo $11, 13, 19$, but not modulo 17.*

b) Prove that $\log_{\bar{2}} \bar{3}$ does not exist in $(\mathbb{Z}/17\mathbb{Z})^*$.

c) Compute $\log_{\bar{2}} \bar{3}$ in $(\mathbb{Z}/11\mathbb{Z})^*$, $(\mathbb{Z}/13\mathbb{Z})^*$, and $(\mathbb{Z}/19\mathbb{Z})^*$.

Problem 16. *Suppose we know that $p = 2^{16} + 1 = 65537$ is a prime and that 3 is a primitive root modulo p.*

a) How many primitive roots mod p are there?

b) What is the order of $\bar{2}$ in $(\mathbb{Z}/p\mathbb{Z})^*$? is 2 a primitive root modulo p?

c) What is the order of $\bar{9}$ in $(\mathbb{Z}/p\mathbb{Z})^*$? is 9 a primitive root modulo p?

d) Without any calculations, write down at least five different primitive roots modulo p.

e) Show that $\log_{\bar{3}} \bar{2}$ in $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiple of 2^{11}.

f) Show that a is a primitive root modulo p if and only if the equation $x^2 - a = 0$ has no solutions in $\mathbb{Z}/p\mathbb{Z}$.

Problem 17. *Mr. White and Mr. Red agree on the prime $p = 151$ and on the primitive root $g = 6$ modulo p. The secret key of Mr. White is $W = 111$, the secret key of Mr. Red is $R = 76$. After performing a Diffie-Hellman protocol, what is the secret key that they will share?*