Solutions of Exercises 1 for KAP
Laura Geatti - Lea Terracini

Problem 1. *Let*

$$N = 1019, \qquad M = 1009.$$

Compute the greatest common divisor $d = \gcd(N, M)$ *and find* $a, b \in \mathbb{Z}$ *such that*

$$Na + Mb = d.$$

Solution. We have

$$1019 = 1 \cdot 1009 + 10, \quad 1009 = 100 \cdot 10 + 9, \quad 10 = 1 \cdot 9 + 1.$$

Hence $\gcd(1019, 1009) = 1$.

By the extended Euclidean algorithm we get

$1 \cdot 1019 + 0 \cdot 1009 = 1019$
$0 \cdot 1019 + 1 \cdot 1009 = 1009$
$1 \cdot 1019 + (-1) \cdot 1009 = 10$
$(-100) \cdot 1019 + (101) \cdot 1009 = 9$
$101 \cdot 1019 + (-102) \cdot 1009 = 1.$

Hence $a = 101$ and $b = -102$.

Problem 2. *a) Convert into base 8 the number* $3154_{[6]}$ *(written in base 6).*

b) Convert 45 *into base 2.*

Solution: (a) The number $3154_{[6]}$, written in base 6, corresponds to the integer

$$3 \cdot 6^3 + 1 \cdot 6^2 + 5 \cdot 6 + 4 = 718.$$

If we want to convert 718 into base 8, then we do the following divisions with remainder:

$718 = 8 \cdot 89 + 6$
$89 = 8 \cdot 11 + 1$
$11 = 8 \cdot 1 + 3$
$1 = 8 \cdot 0 + 1.$

Then

$$718 = 8^3 + 3 \cdot 8^2 + 8 + 6 = 1316_{[8]}.$$

(b) If we want to convert 45 into base 2, then we do the following divisions with remainder:

$45 = 2 \cdot 22 + 1$
$22 = 2 \cdot 11 + 0$
$11 = 2 \cdot 5 + 1$
$5 = 2 \cdot 2 + 1$
$3 = 2 \cdot 1 + 1$
$1 = 2 \cdot 0 + 1.$ Then

$$45 = 2^5 + 2^3 + 2^2 + 1 = 101101_{[2]}.$$

Problem 3. *a) Compute the additive table and the multiplicative table of* $\mathbb{Z}/5\mathbb{Z}$*:*

- *for every element* $\bar{x} \in \mathbb{Z}/5\mathbb{Z}$*, indicate its additive inverse;*
- *determine* $(\mathbb{Z}/5\mathbb{Z})^*$ *and for every element* $\bar{x} \in (\mathbb{Z}/5\mathbb{Z})^*$*, indicate its multiplicative inverse;*
- *solve the equation* $\bar{2} \cdot \bar{x} = \bar{3}$ *in* $(\mathbb{Z}/5\mathbb{Z})^*$*.*

b) Compute the additive table and the multiplicative table of $\mathbb{Z}/6\mathbb{Z}$*:*

- *for every element* $\bar{x} \in \mathbb{Z}/6\mathbb{Z}$*, indicate its additive inverse;*
- *can you solve the equation* $\bar{2} \cdot \bar{x} = \bar{3}$ *in* $\mathbb{Z}/6\mathbb{Z}$*?*
- *determine* $(\mathbb{Z}/6\mathbb{Z})^*$ *and for every element* $\bar{x} \in (\mathbb{Z}/6\mathbb{Z})^*$*, indicate its multiplicative inverse;*

c) Determine $(\mathbb{Z}/8\mathbb{Z})^*$ *and compute its multiplicative table.*

Solution. (a) Below are the additive and the multiplicative tables of $\mathbb{Z}/5\mathbb{Z}$:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Figure 1: The additive and the multiplicative tables of $\mathbb{Z}/5\mathbb{Z}$

One has $(\mathbb{Z}/5\mathbb{Z})^* = \{\bar{x} \in \mathbb{Z}/5\mathbb{Z},\ \bar{x} \neq \bar{0}\}$. From its multiplicative table one sees that

$$\bar{1}^{-1} = \bar{1}, \quad \bar{2}^{-1} = \bar{3}, \quad \bar{3}^{-1} = \bar{2}, \quad \bar{4}^{-1} = \bar{4}$$

and that $\bar{x} = \bar{4}$ solves the equation $\bar{2} \cdot \bar{x} = \bar{3}$ in $(\mathbb{Z}/5\mathbb{Z})^*$.

x	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Figure 2: The multiplicative table of $(\mathbb{Z}/5\mathbb{Z})^*$

(b) Below are the additive and the multiplicative tables of $\mathbb{Z}/6\mathbb{Z}$:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Figure 3: The additive and the multiplicative tables of $\mathbb{Z}/6\mathbb{Z}$

One has $(\mathbb{Z}/6\mathbb{Z})^* = \{\bar{x} \in \mathbb{Z}/6\mathbb{Z},\ \gcd(x,6) = 1\} = \{\bar{1}, \bar{5}\}$. From its multiplicative table one sees that

$$\bar{1}^{-1} = \bar{1}, \quad \bar{5}^{-1} = \bar{5},$$

and that the equation $\bar{2} \cdot \bar{x} = \bar{3}$ cannot be solved in $\mathbb{Z}/6\mathbb{Z}$.

x	$\bar{1}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{1}$

Figure 4: The multiplicative table of $(\mathbb{Z}/6\mathbb{Z})^*$

(c) One has $(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{x} \in \mathbb{Z}/8\mathbb{Z},\ \gcd(x,8) = 1\} = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ and its multiplicative table is given by

x	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

Figure 5: The multiplicative table of $(\mathbb{Z}/8\mathbb{Z})^*$

Problem 4. *Let φ denote the Euler φ-function. Compute $\varphi(15^3 \cdot 33 \cdot 2^4 \cdot 27)$.*

Solution: One has $15^3 \cdot 33 \cdot 2^4 \cdot 27 = 3^3 \cdot 5^3 \cdot 3 \cdot 11 \cdot 2^4 \cdot 3^3 = 2^4 \cdot 3^7 \cdot 5^3 \cdot 11$, and

$$\varphi(2^4 \cdot 3^7 \cdot 5^3 \cdot 11) = (2^4 - 2^3)(3^7 - 3^6)(5^3 - 5^2)\, 10 = 11664000.$$

Problem 5. *Compute $\overline{1009}^{-1} \pmod{1019}$.*

Solution: From the calculations in Exercise 1, $\gcd(1009, 1019) = 1$. Hence 1009 admits multiplicative inverse modulo 1019. Moreover, by the extended Euclidean algorithm one has that

$$\overline{1009}^{-1} = \overline{-102} = \overline{917}.$$

Hence $\overline{917}$ is the canonical representative of $\overline{1009}^{-1} \in (\mathbb{Z}/1019\mathbb{Z})^*$.

Problem 6. *Write explicitly the isomorphisms of multiplicative groups given by the Chinese Remainder Theorem*

$$(\mathbb{Z}/15\mathbb{Z})^* \to (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$$

and

$$(\mathbb{Z}/18\mathbb{Z})^* \to (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/9\mathbb{Z})^*.$$

Solution. One has

$$(\mathbb{Z}/15\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$$

$$(\mathbb{Z}/3\mathbb{Z})^* = \{\bar{1}, \bar{2}\}, \qquad (\mathbb{Z}/5\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

and the map 6.15 on page 78 of the Algebra notes is given by

$$\bar{1} \mapsto (\bar{1}, \bar{1}), \quad \bar{2} \mapsto (\bar{2}, \bar{2}), \quad \bar{4} \mapsto (\bar{1}, \bar{4}) \quad \bar{7} \mapsto (\bar{1}, \bar{2})$$

$$\bar{8} \mapsto (\bar{2}, \bar{3}), \quad \overline{11} \mapsto (\bar{2}, \bar{1}), \quad \overline{13} \mapsto (\bar{1}, \bar{3}) \quad \overline{14} \mapsto (\bar{2}, \bar{4}).$$

One has

$$(\mathbb{Z}/18\mathbb{Z})^* = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}, \overline{13}, \overline{17}\}$$

$$(\mathbb{Z}/2\mathbb{Z})^* = \{\bar{1}\}, \qquad (\mathbb{Z}/9\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$$

and the map 6.15 on page 78 of the Algebra notes is given by

$$\bar{1} \mapsto (\bar{1}, \bar{1}), \quad \bar{5} \mapsto (\bar{1}, \bar{5}), \quad \bar{7} \mapsto (\bar{1}, \bar{7}) \quad \overline{11} \mapsto (\bar{1}, \bar{2})$$

$$\overline{13} \mapsto (\bar{1}, \bar{4}), \quad \overline{17} \mapsto (\bar{1}, \bar{8}).$$

Problem 7. *For each of the congruences*

$$12x \equiv 16 \pmod{500}, \qquad 6x \equiv 3 \pmod{500}, \qquad 34x \equiv 6 \pmod{38}$$

state whether it admits a solution and, if so, solve it.

Solution. (a) Since $\gcd(12, 500) = 4$ divides 16, the congruence $12x \equiv 16 \pmod{500}$ admits integer solutions. It is equivalent to the congruence $3x \equiv 4 \pmod{125}$ and its solutions are all integers $x = 43 + 125k$, with $k \in \mathbb{Z}$.

(b) Since $\gcd(6, 500) = 2$ and 2 does not divide 3, the congruence $6x \equiv 3 \pmod{500}$ admits no integer solutions.

(c) Since $\gcd(34, 38) = 2$ and 2 divides 6, the congruence $34x \equiv 6 \pmod{38}$ admits integer solutions. It is equivalent to the congruence $17x \equiv 3 \pmod{19}$ and its solutions are all integers $x = 27 + 19k$, with $k \in \mathbb{Z}$.

Problem 8. *Let*

$$N = 1019, \qquad M = 5.$$

a) Find the canonical representatives of the following residue classes:

$$\overline{N-1} \pmod 5, \qquad \overline{M^{10}-7} \pmod M.$$

Solution. The canonical representative of the residue class $\overline{N-1} \pmod 5$ is just the remainder of $N-1 = 1018$ divided by 5. Hence it is 3.
Since $5 \equiv 0 \pmod 5$, one has

$$5^{10} - 7 \equiv -7 \equiv 3 \mod 5.$$

Problem 9. *a) Given that $125 = 5^3$, find three distinct pairs $(\bar{a}, \bar{b})$ of nonzero elements in $\mathbb{Z}/125\mathbb{Z}$ such that $\bar{a}\bar{b} = \bar{0}$.*

b) Show that $\overline{7}$ lies in $(\mathbb{Z}/32\mathbb{Z})^*$, determine its order and its inverse in $(\mathbb{Z}/32\mathbb{Z})^*$.

c) Determine the remainder of 7^{50} upon division by 32.

Solution. a) Since $125 = 5^3$, in $\mathbb{Z}/125\mathbb{Z}$ the product of two classes $\bar{a}$ and $\bar{b}$ is zero if and only if $5^3 \mid xy$. Three possibilities are, for example,

$$(\bar{5}, \overline{25}), \quad (\overline{25}, \bar{5}), \quad (\overline{10}, \overline{25}).$$

b) One has $\gcd(7, 32) = 1$, hence $\bar{7} \in (\mathbb{Z}/32\mathbb{Z})^*$. Its inverse is $\bar{7}^{-1} = \overline{23}$. Indeed $7 \cdot 23 = 161 \equiv 1 \pmod{23}$.

c) Since $\gcd(7, 32) = 1$, then $\bar{7} \in (\mathbb{Z}/32\mathbb{Z})^*$. One has $\phi(32) = 2^5 - 2^4 = 16$. Hence

$$7^{50} \equiv 7^{3\cdot 16+2} \equiv 7^2 \equiv 17 \mod 32.$$

Problem 10. *Prove that every integer a satisfies the congruence*

$$a^{13} \equiv a \pmod{2730}.$$

Solution. One has $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. By the Chinese Remainder Theorem

$$a^{13} \equiv a \pmod{2730} \quad \Leftrightarrow \quad a^{13} \equiv a \pmod{2} \ldots\ldots a^{13} \equiv a \pmod{13}.$$

Let p be one of the primes in $\{2, 3, 5, 7, 13\}$. If a is an integer, then either $a \equiv 0 \pmod{p}$ or $\gcd(a, p) = 1$ and $a^{13} \equiv a \pmod{p}$ is equivalent to $a^{12} \equiv 1 \pmod{p}$. Since $\varphi(p)$ divides 12 for all $p \in \{2, 3, 5, 7, 13\}$ and $a^{\varphi(p)} \equiv 1 \pmod{p}$, the initial congruence is satisfied.

Problem 11. *Show that for every element $x \in (\mathbb{Z}/7161\mathbb{Z})^*$ the order of x is a divisor of 30. Does there exist an element $x \in (\mathbb{Z}/7161\mathbb{Z})^*$ of order 30?*

Solution. One has $7161 = 3 \cdot 7 \cdot 11 \cdot 31$. By the Chinese Remainder Theorem $(\mathbb{Z}/7161\mathbb{Z})^*$ is isomorphic to the direct product

$$(\mathbb{Z}/7161\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/11\mathbb{Z})^* \times (\mathbb{Z}/31\mathbb{Z})^*,$$

of groups of order 2, 6, 10 and 30, respectively. The order of an element $x \in (\mathbb{Z}/7161\mathbb{Z})^*$ divides the lowest common multiple $\operatorname{lcm}(2, 6, 10, 30) = 30$. An element $x \in (\mathbb{Z}/7161\mathbb{Z})^*$ of order 30 exists: for example the preimage in $(\mathbb{Z}/7161\mathbb{Z})^*$ of $(1, 1, 1, a)$, where a is an element of order 30 in $(\mathbb{Z}/31\mathbb{Z})^*$ (there are $\varphi(30) = 8$ of them in $(\mathbb{Z}/31\mathbb{Z})^*$).