

Exercises 1 for KAP

Laura Geatti - Lea Terracini

Problem 1. *Let*

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

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

$$Na + Mb = d.$$

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

- b) *Convert 45 into base 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 $\mathbb{Z}/6\mathbb{Z}$:*

- *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.*

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

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

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

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

and

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

Problem 7. For each of the congruences

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

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

Problem 8. Let

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

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

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

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 $\bar{7}$ 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.

Problem 10. Prove that every integer a satisfies the congruence

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

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?