Exercise sheet 1: groups and modular arithmetic

Exercise 1.

1. Compute the order of x in the group $(\mathbf{Z}/15\mathbf{Z}, +)$ for all $x \in \{1, 2, 3, 4, 5\}$.
2. Same question (when it makes sense) for their order in the multiplicative group $(\mathbf{Z}/15\mathbf{Z})^\times$.

Exercise 2. Which residue class modulo 35 corresponds to the pair $(2 \pmod 5, 3 \pmod 7)$ in the isomorphism of the Chinese Remainder Theorem?

Exercise 3. We recall that if p is a prime number, the group $(\mathbf{Z}/p\mathbf{Z})^\times$ is a cyclic group of order $p-1$.

1. Determine a generator of that group when $p \in \{5, 7, 11\}$.
2. We choose $g := 2$ as a generator of the group $(\mathbf{Z}/11\mathbf{Z})^\times$. Determine the values $\log_g(h)$ for h in $(\mathbf{Z}/11\mathbf{Z})^\times$.

Exercise 4. Let $(G, .)$ be a group. Let $x \in G$ be an element of finite order n. For $k \in \mathbf{Z}$, what is the order of x^k?

Exercise 5. Let p be a prime number and $\alpha \geqslant 1$ be an integer. Prove that $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Exercise 6. Let p be an odd prime. Denote by $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$ and by $\mathbf{F}_p^\times$ and $(\mathbf{F}_p^\times)^2$ the set of non-zero elements and the set of non-zero quadratic residues, respectively. In other words,

$$(\mathbf{F}_p^\times)^2 = \{x^2,\ x \in \mathbf{F}_p^\times\}.$$

1. Consider the group homomorphism
$$f \ :\ \begin{array}{ccc} \mathbf{F}_p^\times & \to & (\mathbf{F}_p^\times)^2 \\ x & \mapsto & x^2 \end{array}$$
determine its kernel and deduce the cardinality of $(\mathbf{F}_p^\times)^2$.
2. Consider the group homomorphism
$$g \ :\ \begin{array}{ccc} \mathbf{F}_p^\times & \to & \mathbf{F}_p^\times \\ x & \mapsto & x^{\frac{p-1}{2}} \end{array}$$
Determine its image.
3. Deduce the cardinality of the kernel of g.
4. Prove that $\mathrm{Im}(f) \subseteq \ker(g)$ and show that this inclusion is in fact an equality.

Exercise 7.

1. Let G be a finite abelian group, and let $\widehat{G}$ denote its *dual* (or *group of characters of* G). Determine, for all $\chi \in \widehat{G}$, the value of the sum
$$\frac{1}{|G|}\sum_{g \in G} \chi(g).$$
2. For all $a \in \mathbf{Z}/n\mathbf{Z}$, we denote by
$$\psi_a \ :\ \begin{array}{ccc} \mathbf{Z}/n\mathbf{Z} & \to & \mathbf{C}^\times \\ x & \mapsto & \exp\left(\frac{2i\pi a x}{n}\right) \end{array}$$
Show that $a \mapsto \psi_a$ is an isomorphism from $\mathbf{Z}/n\mathbf{Z}$ to its dual group.
3. Let $n \geqslant 1$. Using the two previous questions recover the well-know fact:
$$\forall k \in \mathbf{Z}, \quad \frac{1}{n}\sum_{a=0}^{n-1} \exp\left(\frac{2i\pi k a}{n}\right) = \begin{cases} 1 \text{ if } n \mid k \\ 0 \text{ otherwise} \end{cases}$$