1. Group theory: review exercises

- 1. Let $F: \mathbf{Z}_n \to \mathbf{Z}_p$ be the map $\bar{x} \mapsto \bar{x} \mod p$. Show that F is well defined if and only if p divides n.
- 2. Let N = nm, with gcd(n, m) = 1.
 - (a) Show that the map $F: \mathbf{Z}_N \to \mathbf{Z}_n \times \mathbf{Z}_m$, $\bar{x} \mapsto (\bar{x} \mod n, \bar{x} \mod m)$ is an isomorphism of additive groups.
 - (b) Show that $F: \mathbf{Z}_N^* \to \mathbf{Z}_n^* \times \mathbf{Z}_m^*$ is an isomorphism of multiplicative groups.
 - (c) Check (a) and (b) for N = 15 and for N = 18.
- 3. Let φ denote the Euler φ -function. Compute $\varphi(15^3 \cdot 33 \cdot 2^4 \cdot 27)$.
- 4. Sia n be a positive integer and let p a prime divisor of n. Verify that: (a) $\varphi(p) \mid \varphi(n);$

 - (b) if $p^2 \not\mid n$, then $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$; (c) if $p \mid \frac{n}{p}$, then $\varphi(\frac{n}{p}) = \frac{n}{p} \prod_d (1 \frac{1}{d})$, where d varies among the prime divisors of n.
- 5. (Lagrange's Theorem). Let G be a finite abelian group of order n.
 - (a) Show that $L_a: G \to G$, defined by $L_a(g) := ag$, for $a, g \in G$, is a bijective map.
 - (b) Show that for all $g \in G$ one has $g^n = e$ (here e denotes the identity element).
 - (c) (Fermat Little Theorem) State Lagrange's Theorem for \mathbf{Z}_p , with p prime.
 - (c) State Lagrange's Theorem for the following groups

$$\mathbf{Z}_{11}, \quad \mathbf{Z}_{12}, \quad \mathbf{Z}_{100}^*, \quad \mathbf{Z}_{11} \times \mathbf{Z}_{17}, \quad \mathbf{Z}_{7^3}^*.$$

- 6. Let G be a group and let $a \in G$ be an element of order k (by definition k is the smallest positive integer for which $a^k = 1$). Prove the following statements:
 - (a) the powers $\{a, a^2, \dots, a^k = e\}$ of a are all distinct;
 - (b) $a^n = e$ if and only if k divides n;
 - (c) the order of a^m is equal to k if and only if gcd(m, k) = 1.
- 7. Prove that the order of an element $(\bar{x}, \bar{y}) \in \mathbf{Z}_n \times \mathbf{Z}_m$ is the *least common multiple* of the order of \bar{x} in \mathbf{Z}_n and the order of \bar{x} in \mathbf{Z}_m .
- 8. Let p > 2 be a prime number. Then $x^2 \equiv 1 \mod p$ if and only if either $x \equiv 1 \mod p$ or $x \equiv -1 \mod p$.
- 9. Let G be a cyclic group of order n and let $s \in \mathbf{N}$. Then the number of solutions of the equation $x^s = e$ is equal to gcd(n, s).
- 10. Determine all the generators of the cyclic group $(\mathbf{Z}_{72}, +)$.
- 11. Determine all the generators of the cyclic group $(\mathbf{Z}_{11}^*, \cdot)$.
- 12. Determine which of the following groups is cyclic: \mathbf{Z}_{4}^{*} , \mathbf{Z}_{8}^{*} , $\mathbf{Z}_{2^{k}}^{*}$, for k > 3.
- 13. Let $n = 616 = 2^3 \cdot 7 \cdot 11$.
 - (a) Compute $\varphi(n)$;
 - (b) Write \mathbf{Z}_n^* as a product of cyclic groups.
- 14. Write $\mathbf{Z}_{10!}^*$ as a product of cyclic groups. (recall that \mathbf{Z}_p^* is cyclic, for all p prime, and $\mathbf{Z}_{p^k}^*$ is cyclic, for all primes p > 2).