1. Group theory: review exercises

1. *Let $F\colon \mathbf{Z}_n \to \mathbf{Z}_p$ be the map $\bar{x} \mapsto \bar{x} \bmod p$. Show that F is well defined if and only if p divides n.*

Sol.: If $n = kp$, for $k \in \mathbf{Z}$, then $F(x + sn) = F(x + skp)$, for all $s \in \mathbf{Z}$. This shows that F is well defined on the classes of $\mathbf{Z}_n$. Conversely, F well defined on the classes of $\mathbf{Z}_n$ means in particular that $F(n) = F(0) = 0$. In particular $n \equiv 0 \bmod p$.

2. (Chinese remainder theorem) Let $N = nm$, with $\gcd(n, m) = 1$.
   (a) Show that the map $F\colon \mathbf{Z}_N \to \mathbf{Z}_n \times \mathbf{Z}_m$, $\quad \bar{x} \mapsto (\bar{x} \bmod n, \bar{x} \bmod m)$ is an isomorphism of additive groups.
   (b) Show that $F\colon \mathbf{Z}_N^* \to \mathbf{Z}_n^* \times \mathbf{Z}_m^*$ 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 $\varphi(15^3 \cdot 33 \cdot 2^4 \cdot 27)$.*

Sol.: 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

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

4. *Let n be a positive integer and let p a prime divisor of n. Verify that:*
   (a) $\varphi(p) \mid \varphi(n)$;
   (b) if $p^2 \nmid n$, 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.

Sol.: One has

$$\varphi(n) = n \cdot \prod_{d|n,\ \text{prime}} (1 - \frac{1}{d}). \qquad (*)$$

(a) Since $\varphi(p) = p((1 - \frac{1}{p})$, it is clear from (*) that $\varphi(p)$ divides $\varphi(n)$.

(b) if $p^2 \nmid n$, then $\gcd(p, n/p) = 1$. Therefore $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$.

(c) If $p \mid \frac{n}{p}$, then n and n/p have the same prime divisors. It follows from (*) that $\varphi(\frac{n}{p}) = \frac{n}{p}\prod_d(1 - \frac{1}{d})$.

5. (Lagrange's Theorem). Let G be a finite abelian group of order n.†
   (a) Show that $L_a\colon G \to G$, 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) State Lagrange's Theorem for $\mathbf{Z}_p$, with p prime.
   (d) State Lagrange's Theorem for the following groups

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

Sol.: (d) For every $x \in \mathbf{Z}_{11}$ one has $11 \cdot x = 0 \bmod 11$; similarly, for every $x \in \mathbf{Z}_{12}$ one has $12 \cdot x = 0 \bmod 12$. Since $\gcd(11, 17) = 1$, the group $\mathbf{Z}_{11} \times \mathbf{Z}_{17} \cong \mathbf{Z}_{187}$ (see Exercise 2(a)). In particular it is cyclic of order 187 and for every $(x, y) \in \mathbf{Z}_{11} \times \mathbf{Z}_{17}$ one has $187 \cdot (x, y) = (0, 0)$.
For every $a \in \mathbf{Z}_n^*$, one has $x^{\varphi(n)} = 1 \bmod n$. Since $\varphi(100) = \varphi(2^2)\varphi(5^2) = 40$, in $\mathbf{Z}_{100}^*$ the theorem reads

$$\forall a \in \mathbf{Z}_{100}^* \quad x^{40} = 1 \bmod 100.$$

† Lagrange's theorem:*Let G be a finite abelian group with n elements. Then for all $g \in G$, one has $g^n = e$.* If $G = \mathbf{Z}_p^*$, with p prime, then Lagrange's theorem is just Fermat Little Theorem. If $G = \mathbf{Z}_n^*$, for general n, then Lagrange's theorem is just Euler's theorem.

Similarly, since $\varphi(7^3) = 7^3 - 7^2 = 294$, one has

$$\forall a \in \mathbf{Z}^*_{7^3} \quad x^{294} = 1 \bmod 100.$$

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 $\gcd(m, k) = 1$.*

Sol.: (a) Suppose that $x^r = x^s$, for some $r < s \le k$. Then $x^{s-r} = e$, for $0 < s - r < k$. Contradiction.
(b) If $k \,|\, n$, then $a^n = e$. Conversely, suppose by contradiction that $a^n = e$, with k not dividing n. Then $n = mk + r$, for some $0 \le r < k$ and

$$e = a^n = a^{km}a^r = a^r.$$

Contradiction.
(c) Let h be the order of a^m. Then $h \,|\, k$, since a^m is an element of the group of order k generated by a. We are going to show that if $\gcd(m, k) = 1$, then also $k \,|\, h$. In particular, $h = k$.
From $\gcd(m, k) = 1$, there exist α, $\beta \in \mathbf{Z}$ such that $\alpha m + \beta k = 1$. Now

$$e = a^{mh} = a^{h\alpha m} = a^{h\alpha m + h\beta k} = a^h.$$

From (b) it follows that $k \,|\, h$, as desired.

7. *Prove that the order of an element $(x, y) \in \mathbf{Z}_n \times \mathbf{Z}_m$ is the least common multiple of the order of x in $\mathbf{Z}_n$ and the order of x in $\mathbf{Z}_m$.*

Sol.: If h is an integer such that $h(x, y) = (hx, hy) = (0, 0) \in \mathbf{Z}_n \times \mathbf{Z}_m$, then $ord(x) \,|\, h$ and $ord(y) \,|\, h$. Hence $lcm(ord(x), ord(y))$ divides h. The integer $k = lcm(ord(x), ord(y))$ is the smallest integer with such properties. Consequently $k = lcm(ord(x), ord(y))$ is the order of (x, y) in $\mathbf{Z}_n \times \mathbf{Z}_m$.

8. *Let $p > 2$ be a prime number. Then $x^2 \equiv 1 \bmod p$ if and only if either $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$.*

Sol.: One has $x^2 \equiv 1 \bmod p$ if and only if $p \,|\, (x+1)(x-1)$ if and only if either $p \,|\, (x+1)$ or $p \,|\, (x-1)$ if and only if either $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$.

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 $\gcd(n, s)$.*

Sol.: Let g be a generator of G. Write $x = g^j$, for some j. One has

$$x^s = g^{js} = e \quad \Rightarrow \quad n \text{ divides } js \quad \Leftrightarrow \quad \frac{n}{d} \text{ divides } j\frac{s}{d}, \quad \text{where } d = \gcd(s, n).$$

Since $\gcd(\frac{n}{d}, \frac{s}{d}) = 1$, then $\frac{n}{d}$ divides j and

$$j = k\,\frac{n}{d}, \qquad \text{for } k = 1, \dots d.$$

Conclusion, there are exacly $d = \gcd(s, n)$ solutions of the equation $x^s = e$.

10. *Determine all the generators of the cyclic group $(\mathbf{Z}_{72}, +)$.*

Sol.: The element 1 is a generator $(\mathbf{Z}_{72}, +)$. By Exercise 6(c), the element $0 < k \le 71$ is a generator if and only if $gcd(k, 72) = 1$. As $72 = 2^2 \cdot 3^2$, one has $gcd(k, 72) = 1$ if and only if k is odd and not divisible by 3.

11. *Determine all the generators of the cyclic group $(\mathbf{Z}^*_{11}, \cdot)$.*

Sol.: The element 2 is a generator of group $(\mathbf{Z}_{11}^*, \cdot)$ of order $\varphi(11) = 10$:

$$2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 5, \quad 2^5 = 10, \quad 2^6 = 9, \quad 2^7 = 7, \quad 2^8 = 3, \quad 2^9 = 6, \quad 2^{10} = 1.$$

By Exercise 6(c), there are $\varphi(10) = 4$ elements of order 10 in $\mathbf{Z}_{11}^*$, namely

$$\{2^m,\ \gcd(m, 10) = 1\} = \{2,\ 2^3 = 8,\ 2^7 = 7,\ 2^9 = 6\}.$$

12. *Determine which of the following groups is cyclic:* $\mathbf{Z}_4^*,\ \mathbf{Z}_8^*,\ \mathbf{Z}_{2^k}^*$*, for* $k > 3$.

Sol.: $\mathbf{Z}_4^* = \{1, 3\}$ is cyclic of order 2.
Since $\mathbf{Z}_8^* = \{1, 3, 5, 7\}$ and $1^2 = 3^3 = 5^2 = 8^2 = 1$, then the group $\mathbf{Z}_8^*$ is isomorphic to the product $\mathbf{Z}_2 \times \mathbf{Z}_2$. In particular, it is not cyclic.
For $k > 3$, the group $\mathbf{Z}_{2^k}^*$ is not cyclic: the map

$$\phi \colon \mathbf{Z}_{2^k}^* \to \mathbf{Z}_8^*, \quad x \mapsto x \bmod 8,$$

is a surjective homomorphism onto a group which is not cyclic. Hence it cannot be cyclic. More precisely,

$$\mathbf{Z}_{2^k}^* \cong \mathbf{Z}_4^* \times \{\bar{x} \in \mathbf{Z}_{2^k}^* \mid \bar{x} \equiv \bar{1} \mod 4\},$$

where $H_k = \{\bar{x} \in \mathbf{Z}_{2^k}^* \mid \bar{x} \equiv \bar{1} \mod 4\}$ is a cyclic group of order 2^{k-2}, generated by $\bar{1} + \bar{4} = \bar{5}$.
Conclusion: $\mathbf{Z}_{2^k}^*$ is cyclic if and only if $k = 1, 2$.

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.*

Sol.: One has $\varphi(n) = 4 \cdot 6 \cdot 10 = 240 = 2^4 \cdot 3 \cdot 5$. By the Chinese Remainder Theorem (Exercise 2(b)), there is an isomorphism

$$\mathbf{Z}_n^* \cong \mathbf{Z}_{2^4}^* \times \mathbf{Z}_3^* \times \mathbf{Z}_5^*.$$

The groups $\mathbf{Z}_3^*$ and $\mathbf{Z}_5^*$ are cyclic; the group $\mathbf{Z}_{2^4}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$ is isomorphic to the product of the cyclic groups $\mathbf{Z}_4^*$ and $H_4 := \{\bar{x} \in \mathbf{Z}_{2^4}^* \mid \bar{x} \equiv \bar{1} \mod 4\}$.
Conclusion: as a product of cyclic groups,

$$\mathbf{Z}_n^* \cong \mathbf{Z}_4^* \times H_4 \times \mathbf{Z}_3^* \times \mathbf{Z}_5^*.$$

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* $p > 2$*).*

Sol.: One has $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$. Then $\varphi(10!) = 2^{11} \cdot 3^3 \cdot 5$. Then as a product of cyclic groups

$$\mathbf{Z}_{10!}^* \cong \mathbf{Z}_4^* \times H_{11} \times \mathbf{Z}_{3^3}^* \times \mathbf{Z}_{5^2}^*,$$

where $H_{11} = \{x \in \mathbf{Z}_{2^{11}}^* \mid x \equiv 1 \bmod 4\}$.