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. 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 $n \equiv 0 \mod p$.

- 2. (Chinese remainder theorem) Let N = nm, with gcd(n, m) = 1.
 - (a) Show that the map $F: \mathbb{Z}_N \to \mathbb{Z}_n \times \mathbb{Z}_m$, $\bar{x} \mapsto (\bar{x} \mod n, \bar{x} \mod m)$ 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 $\varphi(15^3 \cdot 33 \cdot 2^4 \cdot 27)$.

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. 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.

Sol.: One has

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

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

(b) if $p^2 \not\mid n$, 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 $L_a: G \to G$, 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.
 - (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 $11 \cdot x = 0 \mod 11$; 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 $x^{\varphi(n)} = 1 \mod n$. Since $\varphi(100) = \varphi(2^2)\varphi(5^2) = 40$, in \mathbf{Z}_{100}^* the theorem reads

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

- 6. Let G be a group and let a ∈ 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,a²,...,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 $k \mid n$, 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 $h \mid k$, 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 $k \mid h$. In particular, h = k. From gcd(m, k) = 1, there exist $\alpha, \beta \in \mathbb{Z}$ 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 $k \mid h$, 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 $x^2 \equiv 1 \mod p$ if and only if either $x \equiv 1 \mod p$ or $x \equiv -1 \mod p$. Sol.: One has $x^2 \equiv 1 \mod p$ if and only if $p \mid (x+1)(x-1)$ if and only if either $p \mid (x+1)$ or $p \mid (x-1)$ 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).

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

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

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

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

Conclusion, there are exactly $d = \gcd(s, n)$ 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 $0 < k \leq 71$ 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,
$$2^2 = 4$$
, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$.

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

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

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

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

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 $H_k = \{ \bar{x} \in \mathbb{Z}_{2^k}^* \mid \bar{x} \equiv \bar{1} \mod 4 \}$ 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

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

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

Many of the following exercises require a computer (PARI/GP or SAGEMATH).

5. Pollard ρ

1. Let n be a composite integer of 200 digits. After 10000 iterations the Pollard ρ algorithm did not find any factors. What can we conclude about the size of the prime factors?

Sol.: Recall that a random sequence $\{x_j\}_{j=1,\dots,k}$ in \mathbf{Z}_n determines a sequence in \mathbf{Z}_p , for every prime divisor p of n (cf. Exercise1, n.1). Moreover

 $gcd(x_i - x_j \mod n, n) \neq 1 \quad \Leftrightarrow \quad \text{there exists a prime } p \text{ such that } \begin{cases} p \mid n \\ x_i = x_j \mod p. \end{cases}$

In other words a coincidence occurs in \mathbf{Z}_{p} .

By the birthday paradox:

• smallest factors are found first: a coincidence is more likely to occur in \mathbf{Z}_p , where p is the smallest factor;

• it is unlikely that a coincidence occurs in \mathbf{Z}_n (equivalently that $gcd(x_i - x_j \mod n, n) = n$): hence $gcd(x_i - x_j \mod n, n) = n$):

 $x_i \mod n, n \neq 1$ is generally a non-trivial factor of n.

• a coincidence is likely to occur in \mathbf{Z}_p if k is approximately \sqrt{p} .

Conclusion: if $k = 10000 = 10^4$ iterations produced no factor p of n, probably all factors are $> k^2 = 10^8$.

2. Let n be a composite integer of 200 digits, and let B = 10000. After how many unsuccesful iterations of the Pollard ρ algorithm we can conclude that probably n has no factor $\leq B$?

Sol.: From the arguments of the previous exercise, after $k = \sqrt{B} = 10^2$ iterations we can conclude that probably n has no factor $\leq B = 10^4$.

- 3. Let $n = p \cdot q$ be an integer, product of two primes $p \ll q$.
 - (a) Estimate the variation in the amount of calculations to factor n with Pollard ρ , when the smallest factor p increases by one digit and q remains the same.
 - (b) Estimate the variation in the amount of calculations to factor n with Pollard ρ , when the smallest factor p remains the same and q increases by one digit.
 - (c) Do some experiments with PARI/GP (use pollard2(n)) and time them).
- 4. (a) (use pollard2(n)) Factor the number n = 2107971466920603317676768413248655563326842644339.
 - (b) Run the algorithm several times: observe that the initial point changes, while the number of iterates which produce a given factor remains more or less of the same size.
- 5. Using the Pollard ρ algorithm,
 - (a) factor the Mersenne numbers $M_n = 2^n 1$ per $1 \le n \le 20$; (b) factor the Fermat numbers $F_n = 2^{2^n} + 1$, per $1 \le n \le 8$.
- 6. Factor completely the integers (combine the Pollard ρ algorithm with the Miller-Rabin test):
 - $n_1 = 1077471755063687$
 - $n_2 = 1068764300000395442791$
 - $n_3 = 1000587688300000000000000000000000008574912503519308271870011$

00824221115473495059110442157250483.

007659628141113788389728281238427868281.