LECTURE 8
Cyclic groups and the Euler's function

PAVEL RŮŽIČKA

Abstract. We characterize cyclic groups up to isomorphism. We prove that a subgroup and a factor group of a cyclic group is cyclic. We prove that a finite cyclic group contains a unique subgroup of order m for every divisor m of its order. We study orders of products of commuting elements of a group. We prove that a finite subgroup of a multiplicative group of all non-zero elements of a field is cyclic. Then we will study the sets of generators of cyclic groups. We will compute the Euler function and we will prove the Euler's, the (small) Fermat's, and the Wilson's theorems.

8.1. **Congruence modulo n.** Let $\mathbb{Z}$ denote the group of all integers with the operation of addition. Since the group is commutative, all subgroups of $\mathbb{Z}$ are normal. According to Exercise 7.2 all subgroups of $\mathbb{Z}$ are of the form $n \cdot \mathbb{Z}$ for a positive integer n.

Let a, b, and n be integers. We say integer a is *congruent to* b *modulo* n, and write

$$a \equiv b \pmod{n}$$

if $n \mid a - b$. Observe that $a \equiv b \pmod{n}$ if and only of $a - b \in n \cdot Z$. Therefore a is congruent to b modulo n if and only if $a \equiv_{n\cdot\mathbb{Z}} b$ (cf. Lesson 4). It follows from Lemma 4.3 that the binary relation of being congruent modulo n is an equivalence on $\mathbb{Z}$.

8.2. **Transversals.** Let $\boldsymbol{G}$ be a group and $\boldsymbol{H}$ a subgroup of the group $\boldsymbol{G}$. A *left* (respectively *right*) *transversal* for $\boldsymbol{H}$ is a set picking one element from each left (respectively right) coset of $\boldsymbol{H}$. If $\boldsymbol{H}$ is a normal subgroup of $\boldsymbol{G}$, then left and right transversals for $\boldsymbol{H}$ coincide. Clearly the size of a left (and right) transversal equals to the index of $\boldsymbol{H}$ in $\boldsymbol{G}$.

Let $\boldsymbol{G}$ be a group, $\boldsymbol{N}$ a normal subgroup of $\boldsymbol{G}$, and T a transversal for $\boldsymbol{N}$. We define a binary operation $\cdot_N$ on T so that $s \cdot_N t \equiv_N s \cdot t$, i.e, $s \cdot_N t$ is the T-representative of the coset $(s \cdot t) \cdot N$. Thus we get a group structure on the set T. The mapping $\tau_N \colon T \to G/N$ given by $t \mapsto t \cdot N$ induces an isomorphism of the groups $(T, \cdot_N)$ and $\boldsymbol{G/N}$. The existence of the isomorphism allows us to replace the factor group $\boldsymbol{G/N}$ by the group $(T, \cdot_N)$, which is usefully

---

The Lecture and the tutorial took place in Malá strana, room S11, on November 27, 2018.

especially when we have an efficient algorithm that computes $s \cdot_N t$ for all $s, t \in T$.

The set $\{0, 1, \dots, n-1\}$ forms a transversal for the subgroup $n \cdot \mathbb{Z}$ in the additive group $\mathbb{Z}$ of all integers. Let $+_n$ denote the binary operation on the transversal $\{0, 1, \dots, n-1\}$ as above, i.e., $0 \leq a +_n b \leq n-1$ and $a +_n b \equiv a + b \pmod{n}$ for all $a, b \in \{0, 1, \dots, n-1\}$. We will call the operation $+_n$ *addition modulo* n. We set

$$\mathbb{Z}_n := (\{0, 1, \dots, n-1\}, +_n).$$

For an integer z and a positive integer n let $z \bmod n$ denote the element from $\{0, 1, \dots, n-1\}$ such that $z \bmod n \equiv z \pmod{n}$. In other words $z \bmod n$ is the remainder of z when dividing by n. The map

$$\begin{aligned} \pi_n \colon \mathbb{Z} &\to \mathbb{Z}_n \\ z &\mapsto z \bmod n \end{aligned}$$

is easily seen to be a group epimorphism with kernel $n \cdot \mathbb{Z}$. Due to the Homomorphism theorem there is a unique isomorphism $\sigma \colon \mathbb{Z}/n \cdot \mathbb{Z} \to \mathbb{Z}_n$ satisfying $\pi_n = \sigma \circ \pi_{\mathbb{Z}/n \cdot \mathbb{Z}}$. Notice that σ is inverse to the isomorphism τ introduced above.

8.3. **Cyclic groups.** Let us define the *order* of a finite group $\boldsymbol{G}$ to be the number of elements of $\boldsymbol{G}$ and let us set the *order* of an infinite group to be ∞. A group $\boldsymbol{C}$ is said to be *cyclic* provided that $\boldsymbol{C}$ is generated by a single element. We will use the notation $\boldsymbol{C_g}$ for the cyclic group generated by g.

Observe that all elements of $\boldsymbol{C_g}$ are powers of g. The the map $\varepsilon_g \colon \mathbb{Z} \to \boldsymbol{C_g}$ given by $z \mapsto g^z$ is a group epimorphism. Indeed $g^{y+z} = g^y \cdot g^z$ for all $y, z \in \mathbb{Z}$. According to the First isomorphism theorem we have that $\boldsymbol{C_g} \simeq \mathbb{Z}/\ker \boldsymbol{\varepsilon_g}$. It follows from Exercise 7.2 that either $\ker \boldsymbol{\varepsilon_g} = \boldsymbol{0}$, hence $\boldsymbol{C_g} \simeq \mathbb{Z}$ or $\ker \boldsymbol{\varepsilon_g} = n \cdot \mathbb{Z}$ for some positive integer n, whence $\boldsymbol{C_g} \simeq \mathbb{Z}/n \cdot \mathbb{Z} \simeq \mathbb{Z}_n$. In the latter case, n is the order of the cyclic group $\boldsymbol{C_g}$. Therefore

Theorem 8.1. *Up to isomorphism the cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}_n$, $n \in \mathbb{N}$. The group $\mathbb{Z}$ is of an infinite order while the order of $\mathbb{Z}_n$ is n. In particular, cyclic groups are determined by their order up to isomorphism.*

Lemma 8.2. *Every factor-group and every subgroup of a cyclic group is cyclic.*

Proof. Let $\boldsymbol{C}$ is a cyclic group generated by an element g. Every factor group of $\boldsymbol{C}$ is generated by the coset of g. Therefore the factor group is cyclic. It follows from Exercise 7.2 that all non-trivial subgroups of $\mathbb{Z}$are of the form $n \cdot \mathbb{Z}$ for some positive integer n, and so isomorphic to $\mathbb{Z}$. Therefore all subgroups of the group $\mathbb{Z}$ are cyclic. Let $\boldsymbol{D}$ be a subgroup of the cyclic group $\boldsymbol{C}$. Then $\varepsilon_g^{-1}(\boldsymbol{D})$ is a subgroup $\mathbb{Z}$ due to Lemma 6.6 and $\boldsymbol{D}$ is the homomorphic image of $\varepsilon_g^{-1}(\boldsymbol{D})$. Therefore $\boldsymbol{D}$ is a homomorphic image of a cyclic group, and so the subgroup $\boldsymbol{D}$ is cyclic. □

Lemma 8.3. *Let $\boldsymbol{C}$ be a cyclic group of a finite order n. For every divisor m of n there is a unique subgroup of $\boldsymbol{C}$ of order m.*

Proof. Let g be a generator of $\boldsymbol{C}$ and $\varepsilon_g\colon \mathbb{Z} \to \boldsymbol{C}$ an epimorphism such that $\varepsilon_g(1) = g$. From $|C| = n$ we get that $\ker\varphi = n\cdot\mathbb{Z}$. According to Lemma 6.7 all subgroups of $\boldsymbol{C}$ are of the form $\varepsilon_g(k\cdot Z)$, where $n\cdot\mathbb{Z} \subseteq k\cdot\mathbb{Z}$. Note that $n\cdot\mathbb{Z} \subseteq k\cdot\mathbb{Z}$ if and only if $k \mid n$. From the First and the Third isomorphism theorem we infer that

$$\boldsymbol{C}/\varepsilon_g(k\cdot\mathbb{Z}) \simeq \mathbb{Z}/n\cdot\mathbb{Z}\Big/k\cdot\mathbb{Z}/n\cdot\mathbb{Z} \simeq \mathbb{Z}/k\cdot\mathbb{Z} \simeq \mathbb{Z}_k.$$

It follows that $[\boldsymbol{C}\colon \varepsilon_g(k\cdot\mathbb{Z})] = |\mathbb{Z}_k| = k$. We conclude that for every divisor k of n there is a unique subgroup of $\boldsymbol{C}$ of index k in $\boldsymbol{C}$. By the Lagrange theorem, the order of the subgroup is n/k. The lemma follows. □

8.4. **Orders of elements.** Let $\boldsymbol{G} = (G,\cdot)$ be a group and $g \in G$. We set

$$g^0 := u_{\boldsymbol{G}}, \quad g^n := \underbrace{g\cdots g}_{n \text{ times}} \quad \text{and} \quad g^{-n} := \underbrace{g^{-1}\cdots g^{-1}}_{n \text{ times}}, \qquad (n \in \mathbb{N}).$$

Remark 8.4. Observe that

(i) $g^{y\cdot z} = (g^y)^z$,
(ii) $g^{y+z} = g^y \cdot g^z$,

for all $g \in G$, and all $y, z \in \mathbb{Z}$.

An *order* of an element g of a group $\boldsymbol{G}$, denoted by $o(g)$, is the least $n > 0$ such that $g^n = u_{\boldsymbol{G}}$. If no such n exists, we put $o(g) := \infty$. In the first case we say that g has a *finite order*, in the latter we say that g has an *infinite order*.

Lemma 8.5. *Let $\boldsymbol{G} = (G,\cdot)$ be a group and $g \in G$. Then*

(i) *$o(g) = \infty$ if and only if $g^y \neq g^z$ for all pairs of distinct integers y, z.*
(ii) *If the element g is of a finite order, then $g^y = g^z$ if and only if $y \equiv z \pmod{o(g)}$, for all $y, z \in \mathbb{Z}$. In particular, $g^z = u_{\boldsymbol{G}}$ if and only if $o(g) \mid z$.*

Proof. Since $g^{y+z} = g^y \cdot g^z$, for all $y, z \in \mathbb{Z}$, the map $\varepsilon_g\colon \mathbb{Z} \to G$ given by $z \mapsto g^z$ is a group homomorphism. It follows from the definition that $o(g) = \infty$ if and only if $\ker\varepsilon_g = 0$ if and only if ε_g is one-to-one. This settles (i) and implies that the element g has a finite order if and only if the kernel of ε_g is non-trivial. If this is the case then $\ker\varepsilon_g = n\cdot\boldsymbol{Z}$ for some n with $0 < n = o(g)$, due to Exercise 7.2. It follows that $g^y = g^z$ if and only $y - z \in \ker\varepsilon_g$ if and only if $y \equiv z \pmod{n}$. This establishes the first part of (ii). Finally, since $u_{\boldsymbol{G}} = g^0$, we have that $g^z = u_{\boldsymbol{G}}$ if and only if $z \equiv 0 \pmod{n}$. This is exactly when $o(g) \mid z$. □

Lemma 8.6. *The order of a cyclic group equals the order of a generator of the group.*

Proof. Let $\boldsymbol{C}$ be a cyclic group and let g be a generator of $\boldsymbol{C}$ of an order n. If n is infinite, $\boldsymbol{C}$ contains infinitely many distinct powers of g due to Lemma 8.5(i), whence $\boldsymbol{C}$ is infinite as well. Suppose that $o(g) = n \in \mathbb{Z}$. It follows from Lemma 8.5(ii) that the set $C_g := \{g^0, g^1, \ldots, g^{n-1}\}$ is closed under the group operation and $g^{-i} = g^{n-i}$ for all $i \in \{0, 1, \ldots, n-1\}$. It follows that C_g is a universe of a subgroup of $\boldsymbol{C}$ containing the generator g. Therefore $C = C_g$. Finally, it follows from Lemma 8.5(ii) that all powers $g^0, g^1, \ldots, g^{n-1}$ are different. We conclude that the order of $\boldsymbol{C}$ is exactly n. □

Lemma 8.7. *The order of an element g of a finite group $\boldsymbol{G}$ divides the order of the group.*

Proof. The order, $o(g)$, of an element g equals to the order of the cyclic group $\boldsymbol{C_g}$ generated by g. The order of the subgroup $\boldsymbol{C_g}$ divides the order of $\boldsymbol{G}$, due to the Lagrange theorem. □

Let $\mathbf{gcd}(y, z)$ and $\mathbf{lcm}(y, z)$ denote that greatest common divisor and the least common multiple of integers y, z, respectively. Recall that integers y and z are said to be *relatively prime* provided that $\mathbf{gcd}(y, z) = 1$.

Lemma 8.8. *Let $\boldsymbol{G} = (G, \cdot)$ be a group and $f, g \in G$ elements of a finite order such that $f \cdot g = g \cdot f$. Then the following holds true:*

(i) $o(f \cdot g) \mid \mathbf{lcm}(o(f), o(g))$.
(ii) *if* $\mathbf{gcd}(o(f), o(g)) = 1$, *then* $o(f \cdot g) = o(f) \cdot o(g)$.

Proof. (i) Put $m = \mathbf{lcm}(o(f), o(g))$ and observe that $f^m = g^m = u_{\boldsymbol{G}}$, indeed, both $o(f) \mid m$ and $o(g) \mid m$ hold true. Since the elements f and g commute, we get that $(f \cdot g)^m = f^m \cdot g^m = u_{\boldsymbol{G}}$. It follows that $o(f \cdot g) \mid \mathbf{lcm}(o(f), o(g))$ due to Lemma 8.5.

(ii) Put $n = o(f \cdot g)$. It follows from (i) that $n \mid o(f) \cdot o(g)$. Since f and g commute we have that

$$u_{\boldsymbol{G}} = (f \cdot g)^{n \cdot o(g)} = f^{n \cdot o(g)} \cdot g^{n \cdot o(g)} = f^{n \cdot o(g)} \cdot (g^{o(g)})^n = f^{n \cdot o(g)}.$$

It follows from Lemma 8.5 that $o(f) \mid n \cdot o(g)$ and since $o(f)$ and $o(g)$ are relatively prime, we get that $o(f) \mid n$. Similarly we prove that $o(g) \mid n$ and since $\mathbf{gcd}(o(f), o(g)) = 1$, we conclude that $o(f) \cdot o(g) \mid n$. Therefore $n = o(f) \cdot o(g)$. □

Lemma 8.9. *Let $\boldsymbol{G} = (G, \cdot)$ be a group and $f, g \in G$ commuting elements of a finite order. There are non-negative integers m and k such that*

$$o(f^m \cdot g^k) = \mathbf{lcm}(o(f), o(g)).$$

Proof. Let $o(f) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and $o(g) = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$ be decompositions of the orders of the elements f, g into products of distinct primes, permitting some α_i, β_i equal 0. Note that $\mathbf{lcm}(o(f), o(g)) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_n^{\gamma_n}$,

where $\gamma_i = \max\{\alpha_i, \beta_i\}$ for all $i = 1, 2, \ldots, n$. For each $i = 1, 2, \ldots, n$ we set

$$\alpha_i' := \begin{cases} \alpha_i & \text{if } \alpha_i \leq \beta_i, \\ 0 & \text{otherwise,} \end{cases} \qquad \beta_i' := \begin{cases} \beta_i & \text{if } \beta_i < \alpha_i, \\ 0 & \text{otherwise} \end{cases}$$

and we put $m = \alpha_1' \cdot \alpha_2' \cdots \alpha_n'$ and $k = \beta_1' \cdot \beta_2' \cdots \beta_k'$. Then $\mathbf{gcd}(o(f^m), o(g^k)) = 1$ and $\mathbf{lcm}(o(f^m), o(g^k)) = \mathbf{lcm}(o(f), o(g))$. Applying Lemma 8.8(ii), we conclude that $o(f^m \cdot g^k) = \mathbf{lcm}(o(f), o(g))$. □

By induction we prove that

Corollary 8.10. *Let $g_1, g_2, \ldots, g_k$ be commuting elements of a finite order of a group $\boldsymbol{G}$.*

(i) *Then $o(g_1 \cdot g_2 \cdots g_k) \mid \mathbf{lcm}(o(g_1), o(g_1), \ldots, o(g_k))$.*

(ii) *If $o(g_1), o(g_2), \ldots, o(g_k)$ are pairwise relatively prime, then*

$$o(g_1 \cdot g_2 \cdots g_k) = o(g_1) \cdot o(g_2) \cdots o(g_k).$$

(iii) *There are $m_1, m_2, \ldots, m_k \in \mathbb{N}$ such that*

$$o(g_1^{m_1} \cdot g_2^{m_2} \cdots g_k^{m_k}) = \mathbf{lcm}(o(g_1), o(g_2), \ldots, o(g_k)).$$

Corollary 8.11. *Let $\boldsymbol{F} = (F, \cdot)$ be a finite abelian group and $g \in F$ an element of the maximum order in $\boldsymbol{A}$. Then $o(f) \mid o(g)$ for all $f \in F$.*

Proof. According to Corollary 8.10 (iii), there is $g \in F$ such that

$$o(g) = \mathbf{lcm}(\{o(f) \mid f \in F\}).$$

□

Theorem 8.12. *Every finite subgroup of the multiplicative group $\boldsymbol{F}^* = (\mathbb{F} \setminus \{0\}, \cdot)$ of a field $\boldsymbol{F}$ is cyclic.*

Proof. Let $\boldsymbol{G}$ be a finite subgroup of $\boldsymbol{F}^*$. Let n be maximum order of an element of $\boldsymbol{G}$. It follows from Corollary 8.11 that $o(g) \mid n$ for all $g \in G$, hence every element of $\boldsymbol{G}$ is a root of the polynomial $x^n - 1$. This polynomial has at most n-distinct roots, hence $|G| \leq n$. On the other hand $n \mid |G|$ as it follows from Lemma 8.7. We conclude that $n = |G|$. Therefore the group $\boldsymbol{G}$ is cyclic. □

Example 8.13. *There is no bound of $o(f \cdot g)$ by $o(f)$ and $o(g)$ in general. For example let $n \in \mathbb{N}$ and*

$$\pi := (1, 2n) \cdot (2, 2n-1) \cdot (3, 2n-2) \cdots (n, n+1),$$
$$\sigma := (2, 2n) \cdot (3, 2n-1) \cdot (4, 2n-2) \cdots (n, n+2)$$

be permutations from $\boldsymbol{S_{2n}}$. Since both π and σ are products of independent transpositions $o(\pi) = o(\sigma) = 2$. Computing that

$$\sigma \cdot \pi := (1, 2, 3, \ldots, 2n)$$

is a $2n$-cycle, we get that $o(\sigma \cdot \pi) = 2n$.

8.5. **The Euler's function.** The cyclic group $\mathbb{Z}$ of an infinite order has exactly two generators 1 and -1. A cyclic group of a finite order n is isomorphic to $\mathbb{Z}_n = (\{0, 1, \dots, n-1\}, +_n)$. The following are equivalent for an element $a \in \mathbb{Z}_n$:

(i) a is a generator of $\mathbb{Z}_n$,
(ii) $o(a) = n$,
(iii) $k \cdot a \not\equiv 0 \pmod{n}$ for all $k = 1, 2, \dots, n-1$,
(iv) $\mathbf{gcd}(a, n) = 1$.

For a positive integer n we denote by $\mathbb{Z}_n^*$ the set of all generators of the group $\mathbb{Z}_n$, i.e,

$$\mathbb{Z}_n^* := \{a \in \{1, \dots, n\} \mid \mathbf{gcd}(a, n) = 1\}. \tag{8.1}$$

The *Euler's function* is a map $\varphi\colon \mathbb{N} \to \mathbb{N}$ which assigns to a positive integer n the number of numbers from $\{1, 2, \dots, n-1\}$ that are relatively prime to n. That is, $\varphi(n) = |\mathbb{Z}_n^*|$ is the number of generators of the finite cyclic group $\mathbb{Z}_n$.

Theorem 8.14. *Let $n = p_1^{m_1} \cdots p_k^{m_k}$ be a decomposition of a positive integer n into the product of primes. Then*

$$\varphi(n) = (p_1^{m_1} - p_1^{m_1-1}) \cdots (p_k^{m_k} - p_k^{m_k-1}) = n \cdot (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}).$$

Proof. We have that $\varphi(n) = \varphi(p_1^{m_1} \dots p_k^{m_k}) = \varphi(p_1^{m_1}) \cdots \varphi(p_k^{m_k})$ due to Exercise 8.6(ii) and from Exercise 8.6(i) we infer that $\varphi(p_i^{m_i}) = p_i^{m_i} - p_i^{m_i-1}$, for all $i = 1, \dots, k$. □

Theorem 8.15. *For every positive integer n the equality*

$$n = \sum_{m|n} \varphi(m) \tag{8.2}$$

holds true.

Proof. Observe that an element g of a group $\boldsymbol{G}$ is a generator of a unique subgroup of $\boldsymbol{G}$, namely the cyclic subgroup $\boldsymbol{C_g}$ generated by g. The cyclic group $\mathbb{Z}_n$ has n elements and a unique subgroup of order m for each divisor m of n, due to Lemma 8.3. The cyclic subgroup of order m has exactly $\varphi(m)$ generators. Equality (8.2) follows. □

8.6. **The Euler's, the (small) Fermat's, and the Wilson's theorems.** The *multiplication modulo* a positive integer n is given by

$$a \cdot_n b = a \cdot b \bmod n,$$

is a binary operation on $\mathbb{Z}_n$. Note that

- The product of numbers relatively prime to n is again relatively prime to n;
- $\mathbf{gcd}(a, n) = \mathbf{gcd}(a \bmod n, n)$, for every integer a. In particular, if a is relatively prime to n, then $a \bmod n$ is relatively prime to n as well.

From this we infer that the set

$$\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n \mid \mathbf{gcd}(a, n) = 1\}$$

is closed under $\cdot_n$. Moreover, it follows from Exercise 8.2 that the multiplication $\cdot_n$ on the set $\mathbb{Z}_n^*$ is cancellative. It follows that the set $\mathbb{Z}_n^*$ together with the operation $\cdot_n$ form a group (the operation $\cdot_n$ is divisible due to Exercise 2.2).

Theorem 8.16 (The Euler's theorem)**.** *Let n be a positive integer. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \tag{8.1}$$

for every integer a co-prime to n.

Proof. Let a be an integer co-prime to n. Put $b = a \bmod n$ and observe that $b \in \mathbb{Z}_n^*$, i.e, b is co-prime to n as well. It follows from the Lagrange theorem that the order of b in $\mathbb{Z}_n^*$ divides the order of the group $\mathbb{Z}_n^*$. Since the order of $\mathbb{Z}_n^*$ is $\varphi(n)$, we infer from Lemma 8.5 that

$$1 = \underbrace{b \cdot_n \cdots \cdot_n b}_{\varphi(n) \text{ times}} = b^{\varphi(n)} \bmod n \equiv a^{\varphi(n)} \pmod{n}.$$

□

Corollary 8.17 (The (small) Fermat's theorem)**.** *Let p be a prime. Then*

$$a^{p-1} \equiv 1 \pmod{p},$$

for every integer a such that $p \nmid a$.

Proof. Since p is prime, the assumption $p \nmid a$ implies that the integer a is co-prime to p. Since $\varphi(p) = p - 1$ for every prime p, Fermat's theorem follows readily form the Euler's theorem. □

Lemma 8.18 (The Wilson's theorem)**.** *Let $1 < q$ be an integer. Then*

$$q \mid (q-1)! + 1 \text{ if and only if } q \text{ is a prime.}$$

Proof. ($\Rightarrow$) If q is not prime, then clearly $1 < \mathbf{gcd}(q, (q-1)!)$, and so $q \nmid (q-1)! + 1$. ($\Leftarrow$) Suppose that q is a prime number. Then $q \mid a^2 - 1 = (a+1)(a-1)$ if and only if $q \mid a+1$ or $q \mid a-1$, for every integer a. It follows that the only elements of the group $\mathbb{Z}_q^*$ that are equal to their inverses are 1 and $q-1$. Consequently, we can pair the remaining elements of $\mathbb{Z}_q^*$, namely the elements $2, \cdots, q-2$, so that the numbers in every pair are inverse to each other. We conclude that

$$2 \cdots (q-2) \equiv 1 \pmod{q},$$

hence

$$(q-1)! \equiv (q-1) \equiv -1 \pmod{q},$$

whence $q \mid (q-1)! + 1$. □

Exercises

Exercise 8.1. *Let n be an integer. Prove that*

(i) *if $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then*

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$$

for all $a_1, a_2, b_1, b_2 \in \mathbb{Z}$.

(ii) *if $a \equiv b \pmod{n}$, then $-a \equiv -b \pmod{n}$ for all $a, b \in \mathbb{Z}$.*

Recall that $\mathbf{gcd}(a, b)$ and $\mathbf{lcm}(a, b)$ denote the greatest common (non-negative) divisor and the least common (non-negative) multiple of integers a, b, respectively.

Exercise 8.2. *Let n be a positive integer. Prove that*

(i) *if $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then*

$$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n},$$

for all $a_1, a_2, b_1, b_2 \in \mathbb{Z}$.

(ii) *if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$, for all $a, b \in \mathbb{Z}$ and all $k \in \mathbb{N}$.*

Exercise 8.3. *Prove that*

(i) *if $a \cdot k \equiv b \cdot k \pmod{n}$ and $\mathbf{gcd}(k, n) = 1$, then $a \equiv b \pmod{n}$, for all $a, b, k \in \mathbb{Z}$ and $n \in \mathbb{N}$.*

(ii) *if $a \equiv b \pmod{n_i}$ for all $n_1, \dots, n_k$, then*

$$a \equiv b \pmod{\mathbf{lcm}(n_1, \dots, n_k)},$$

for all $a, b \in \mathbb{Z}$ and $n_1, \dots, n_k \in \mathbb{N}$.

Exercise 8.4. *Let π and σ be a as in Example 8.13. Put $\rho := (1, n+1) \cdot \sigma$ and compute that $o(\pi) = o(\rho) = 2$ while $o(\rho \cdot \pi) = n$.*

Exercise 8.5. *Let $\pi = \gamma_1 \cdots \gamma_k$ be a decomposition of a permutation $\pi \in \boldsymbol{S_n}$ into the product of independent cycles. Prove that $o(\pi) = \mathbf{lcm}(|\gamma_1|, \dots, |\gamma_k|)$.*

Exercise 8.6. (i) *Let p be a prime and m a positive integer. Prove that*

$$\varphi(p^m) = p^m - p^{m-1}.$$

(ii) *Let $n_1, n_2, \cdots, n_k$ be pairwise relatively prime integers. Prove that*

$$\varphi(n_1 \cdot n_2 \cdots n_k) = \varphi(n_1) \cdot \varphi(n_2) \cdots \varphi(n_k).$$