ALGEBRA I (LECTURE NOTES 2017/2018) LECTURE 9 - CYCLIC GROUPS AND EULER'S FUNCTION

PAVEL RŮŽIČKA

9.1. **Congruence modulo n.** Let us have a closer look at a particular example of a congruence relation on the group $\boldsymbol{Z} = (\mathbb{Z}, +)$ of all integers with the operation of addition. Since the group $\boldsymbol{Z}$ is commutative, all subgroups of $\boldsymbol{Z}$ are normal (cf. Remark 6.2). For a positive integer n there is the subgroup $n\boldsymbol{Z}$ with the universe

$$n\mathbb{Z} := \{na \mid a \in \mathbb{Z}\} = \{b \in \mathbb{Z} \mid n \mid b\}$$

of the group $\boldsymbol{Z}$. In fact, these are the only subgroups of $\boldsymbol{Z}$:

Lemma 9.1. *Let $\boldsymbol{A}$ be a non-trivial subgroup of $\boldsymbol{Z}$. Then $\boldsymbol{A} = n\boldsymbol{Z}$ where n is the smallest positive integer from $\boldsymbol{A}$.*

Proof. Let $\boldsymbol{A} = (A, \cdot)$ be a non-trivial subgroup of $\boldsymbol{Z}$. Since $\boldsymbol{A}$ is non-trivial, it contains a positive integer, indeed, if $s < 0$ belongs to $\boldsymbol{A}$, then $0 < -s \in A$ as well. Let n be the smallest positive integer in $\boldsymbol{A}$. Since $n\boldsymbol{Z}$ is clearly the least subgroup of $\boldsymbol{Z}$ containing n, we have that $n\boldsymbol{Z} \subseteq \boldsymbol{A}$. Let $s \in A$. Dividing s by n with remainder, we find integers t, r such that $s = n \cdot t = r$ and $0 \leq r < n$. From $r = s - n \cdot t \in A$ we infer that $r = 0$, since otherwise it will violate the choice of n. Therefore $n \mid s$, and so $s \in n\mathbb{Z}$. We conclude that $\boldsymbol{A} \subseteq n\boldsymbol{Z}$, and so the two subgroups are equal. □

Adding the trivial subgroup to the picture we get that

Corollary 9.2. *All subgroups of the group $\boldsymbol{Z}$ are of the form $n\boldsymbol{Z}$ for some non-negative integer n.*

We say integer s is *congruent with* an integer t *modulo* n, and write

$$s \equiv t \pmod{n},$$

if s is congruent with t modulo $n\boldsymbol{Z}$, that is, if $s \equiv_{n\mathbb{Z}} t$. By the definition of the congruence relation modulo a normal subgroup in Subsection 7.5 (and the commutativity of the group $\boldsymbol{Z}$), we have that

$$s \equiv t \pmod{n} \text{ if and only if } n \mid t - s. \tag{9.1}$$

Date: December 4, 2017.

It follows from Lemma 7.23 that

Corollary 9.3. *Let n be an integer. The following properties hold true.*

(i) *If* $s_1 \equiv t_1 \pmod{n}$ *and* $s_2 \equiv t_2 \pmod{n}$*, then*

$$s_1 + s_2 \equiv t_1 + t_2 \pmod{n},$$

for all $s_1, s_2, t_1, t_2 \in \mathbb{Z}$.

(ii) *If* $s \equiv t \pmod{n}$*, then* $-s \equiv -t \pmod{n}$*, for all* $s, t \in \mathbb{Z}$.

Exercise 9.1. *Prove Corollary 9.3 readily from the definition of the congruence modulo n.*

Let us denote by $\mathbf{gcd}(s,t)$ and $\mathbf{lcm}(s,t)$ respectively the greatest common (non-negative) divisor and the least common (non-negative) multiple of integers s, t. The next exercises cover some additional properties of congruences modulo positive integers.

Exercise 9.2. *Let n be a positive integer. Prove that*

(i) *if* $s_1 \equiv t_1 \pmod{n}$ *and* $s_2 \equiv t_2 \pmod{n}$*, then*

$$s_1 s_2 \equiv t_1 t_2 \pmod{n},$$

for all $s_1, s_2, t_1, t_2 \in \mathbb{Z}$.

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

Exercise 9.3. *Prove that*

(i) *if* $su \equiv tu \pmod{n}$ *and* $\mathbf{gcd}(u,n) = 1$*, then* $s \equiv t \pmod{n}$*, for all* $s, t, u \in \mathbb{Z}$ *and* $n \in \mathbb{N}$.

(ii) *if* $s \equiv t \pmod{m_i}$ *for all* $m_1, \dots, m_k$*, then*

$$s \equiv t \pmod{\mathbf{lcm}(m_1, \dots, m_k)},$$

for all $s, t \in \mathbb{Z}$ *and* $m_1, \dots, m_k \in \mathbb{N}$.

9.2. **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 $\boldsymbol{H}$.

Clearly, the size of a left (respectively right) transversal, say L (respectively R), equals to the size of the set of all left (respectively right) cosets of $\boldsymbol{H}$. That is

$$|L| = |R| = [\boldsymbol{G} : \boldsymbol{H}].$$

If $\boldsymbol{N}$ is a normal subgroup of the group $\boldsymbol{G}$, then left and right transversals for $\boldsymbol{N}$ coincide. In this case we will talk about *transversals* for $\boldsymbol{N}$.

Assume that we have a group $\boldsymbol{G}$, a normal subgroup $\boldsymbol{N}$ of $\boldsymbol{G}$, and a transversal T for $\boldsymbol{N}$, often containing the unit of $\boldsymbol{G}$. If we have a *nice* algorithm that for a given $a, b \in T$ computes $c \in T$ such that $a \cdot b \cdot N = c \cdot N$, we can view the elements of the factor group $\boldsymbol{G/N}$ as elements of the transversal T. The group operation of $\boldsymbol{G/N}$ will then be determined by our algorithm.

The set $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$ is a transversal for the subgroup $n\boldsymbol{Z}$ in the additive group $\boldsymbol{Z}$ of all integers. Given an integer s, we divide s by n with reminder. We denote the reminder by $s \bmod n$. This allows us to define a binary operation on the set $\mathbb{Z}_n$,denoted by $+_n$, as follows:

$$s +_n t := (s + t) \bmod n \in \mathbb{Z}_n \text{ for all } s, t \in \mathbb{Z}_n.$$

We will call the operation $+_n$ the *addition modulo* n. As discussed above $\boldsymbol{Z_n} = (\mathbb{Z}_n, +_n)$ is a group. The homomorphism $\pi_n\colon \boldsymbol{Z} \to \boldsymbol{Z}_n$, given by $s \mapsto s \bmod n$, maps $\boldsymbol{Z}$ onto $\boldsymbol{Z_n}$. It is straightforward that $\ker \pi_n = n\boldsymbol{Z}$, and so there is a (unique) isomorphism $\mu_n\colon \boldsymbol{Z}/n\boldsymbol{Z} \to \boldsymbol{Z_n}$ such that $\pi_n = \mu_n \circ \pi_{\boldsymbol{Z}/n\boldsymbol{Z}}$ due to The homomorphism theorem. The isomorphism μ_n is given by the correspondence $s \cdot n\boldsymbol{Z} \mapsto s \bmod n$.

9.3. **Cyclic groups.** The *order* of a finite group is the number of its elements while the *order* of an infinite group is set to be ∞. A group $\boldsymbol{C}$ is *cyclic* if it is generated by a single element, say g. We will use the notation $\langle g \rangle$ for the cyclic group generated by g.

Observe that all elements of $\langle g \rangle$ are powers of g, and the map $\varepsilon_g\colon \boldsymbol{Z} \to \langle g \rangle$ given by $s \mapsto g^s$ is a group homomorphism onto $\langle g \rangle$. According to The first isomorphism theorem $\langle g \rangle \simeq \boldsymbol{Z}/\ker \varepsilon_g$. Applying Lemma 9.1 it follows that either $\ker \varepsilon_g = \boldsymbol{0}$ and $\langle g \rangle \simeq \boldsymbol{Z}$ or $\ker \varepsilon_g = n\boldsymbol{Z}$ for some positive integer n and $\langle g \rangle \simeq \boldsymbol{Z}/n\boldsymbol{Z} \simeq \boldsymbol{Z_n}$. In the latter case, n is the order of $\langle g \rangle$ as well as the order of g. We showed that

Theorem 9.4. *Up to isomorphism the cyclic groups are* $\boldsymbol{Z}$ *and* $\boldsymbol{Z_n}$, $n \in \mathbb{N}$. *The group* $\boldsymbol{Z}$ *is of an infinite order while the order of* $\boldsymbol{Z_n}$ *is* n. *In particular, a cyclic group is determined by its order up to isomorphism.*

Lemma 9.5. *Let* $\varphi\colon \boldsymbol{G} \to \boldsymbol{H}$ *be a group homomorphism and* $\boldsymbol{K}$ *a subgroup of the group* $\boldsymbol{H}$. *Then*

$$\varphi^{-1}(\boldsymbol{K}) := \{g \in G \mid \varphi(g) \in K\}$$

is a subgroup of $\boldsymbol{G}$.

Proof. Since $\varphi(u_{\boldsymbol{G}}) = u_{\boldsymbol{H}} \in K$, we have that $u_{\boldsymbol{G}} \in \varphi^{-1}(K)$. In particular, $\varphi^{-1}(K)$ is non-empty. If $g, h \in \varphi^{-1}(K)$, then $\varphi(g \cdot h^{-1}) = \varphi(g) \cdot \varphi(h)^{-1} \in K$, hence $g \cdot h^{-1} \in \varphi^{-1}(K)$. $\square$

Lemma 9.6. *Every factor-group and every subgroup of a cyclic group is cyclic.*

Proof. Let $\boldsymbol{C}$ is a cyclic group generated by g. Then a factor group of $\boldsymbol{C}$ is generated by the coset of g, in particular it is cyclic. According to Lemma 9.1 non-trivial subgroups of $\boldsymbol{Z}$ are isomorphic to $\boldsymbol{Z}$. In particular, every subgroup of $\boldsymbol{Z}$ is cyclic. If $\boldsymbol{D}$ is a subgroup of $\boldsymbol{C}$, then $\varepsilon_g^{-1}(\boldsymbol{D})$ is a subgroup $\boldsymbol{Z}$ and $\boldsymbol{D}$ is its homomorphic image. We conclude that $\boldsymbol{D}$ is cyclic. □

Let m, n be positive integers such that $m \mid n$. Then $n\mathbb{Z} \subseteq m\mathbb{Z}$ and the group $m\boldsymbol{Z}/n\boldsymbol{Z}$ is cyclic due to Lemma 9.6. Observe that $\ker \varepsilon_{1+_m n\boldsymbol{Z}} = (n/m)\boldsymbol{Z}$, hence

$$m\boldsymbol{Z}/n\boldsymbol{Z} \simeq \boldsymbol{Z_{n/m}}. \tag{9.2}$$

Lemma 9.7. *If m divides n, there is a unique subgroup of $\boldsymbol{Z_n}$ of order m.*

Proof. It follows from (9.2) that $\varepsilon_1((n/m)\boldsymbol{Z})$ is a subgroup of $\boldsymbol{Z_n}$ of order m. On the other hand, if $\boldsymbol{D}$ is a subgroup of $\boldsymbol{Z_n}$ of order m, then $\varepsilon_1^{-1}(\boldsymbol{D}) = (n/m)\boldsymbol{Z}$, again due to (9.2). It follows that the subgroup of $\boldsymbol{Z_n}$ of order m is unique. □

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

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

Remark 9.8. Observe that

(i) $g^{s \cdot t} = (g^s)^t$,
(ii) $g^{s+t} = g^s \cdot g^t$,

for all $g \in G$, and all $s, t \in \mathbb{Z}$.

An *order* of an element g of a group $\boldsymbol{G}$, denote 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 9.9. *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 $\langle g \rangle$ generated by g. The order of the subgroup $\langle g \rangle$ divides the order of G, due to the Lagrange theorem. □

Lemma 9.10. *Let $\boldsymbol{G} = (G, \cdot)$ be a group and $g \in G$. Then*

(i) *$o(g) = \infty$ if and only if $g^s \neq g^t$ for all pairs of distinct integers s, t.*

(ii) *If the element g is of a finite order, then $g^s = g^t$ if and only if $s \equiv t \pmod{o(g)}$, for all $s, t \in \mathbb{Z}$. In particular, $g^s = u_{\boldsymbol{G}}$ if and only if $o(g) \mid s$.*

Proof. Since $g^{s+t} = g^s \cdot g^t$, for all $s, t \in \mathbb{Z}$, the map $\varepsilon \colon \mathbb{Z} \to G$ given by $s \mapsto g^s$ is a group homomorphism. It follows from the definition and Corollary 7.11 that $o(g) = \infty$ if and only if $\ker \varepsilon = 0$ if and only if φ 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 is non-trivial. If this is the case then $\ker \varepsilon = n\boldsymbol{Z}$ wher $0 < n = o(g)$, due to Lemma 9.1. It follows that $g^s = g^t$ if and only $t - s \in \ker \varepsilon$ if and only if $t \equiv s \pmod{n}$. Since $u_{\boldsymbol{G}} = g^0$ we conclude that $g^s = u_{\boldsymbol{G}}$ if and only if $s \equiv 0 \pmod{n}$. This is exactly when $o(g) \mid s$, and so we have proved (ii). □

Recall that integers s and t are said to be *relatively prime* provided that $\mathbf{gcd}(s, t) = 1$.

Lemma 9.11. *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 9.10.

(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 9.10 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 $n = o(f) \cdot o(g)$. □

Corollary 9.12. *Let $\boldsymbol{G} = (G, \cdot)$ be a group and $f, g \in G$ commuting elements of a finite order. Putting $m = \mathbf{gcd}(o(f), o(g))$, we get that*

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

By induction we prove that

Corollary 9.13. *Let $g_1, \dots, g_k$ be commuting elements of a finite order of a group $\boldsymbol{G}$.*

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

(ii) *If* $o(g_1), \dots, o(g_n)$ *are pairwise relatively prime, then*

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

(iii) *There are* $m_1, \dots, m_{k-1} \in \mathbb{N}$ *such that*

$$o(g_1^{m_1} \cdots g_{k-1}^{m_{k-1}} \cdot g_k) = \mathbf{lcm}(o(g_1), \dots, o(g_k)).$$

Exercise 9.4. *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* $o(\pi) = \mathbf{lcm}(|\gamma_1|, \dots, |\gamma_k|)$.

Corollary 9.14. *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 9.13 (iii), there is $g \in F$ such that

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

□

Theorem 9.15. *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 9.14 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 9.9. We conclude that $n = |G|$. Therefore the group $\boldsymbol{G}$ is cyclic. □

Example 9.16. *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*

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

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

Exercise 9.5. *Can you guess the product* $\pi \cdot \sigma$ *without computing it?*

Exercise 9.6. *Let* π *and* σ *be a as in Example 9.16. Put* $\rho := (1, n+1) \cdot \sigma$ *and compute that* $o(\pi) = o(\rho) = 2$ *while* $o(\rho \cdot \pi) = n$.

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

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

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

$$\mathbb{Z}_n^* := \{s \in \{1, \dots, n\} \mid \mathbf{gcd}(s, n) = 1\}. \tag{9.3}$$

The *Euler's function* is a map $\varphi \colon \mathbb{N} \to \mathbb{N}$ which assigns to a positive integer n the number of generators of $\boldsymbol{Z_n}$, i.e, $\varphi(n) = |\mathbb{Z}_n^*|$, for all $n \in \mathbb{N}$.

Lemma 9.17. *Let p be a prime and $m \in \mathbb{N}$. Then $\varphi(p^m) = p^m - p^{m-1}$.*

Proof. Since p is a prime, we have that

$$\{s \in \{1, 2, \dots, p^m\} \mid p \text{ divides } s\} = \{pt \mid t \in \{1, \dots, p^{m-1}\}\}.$$

Therefore the set $\{1, 2, \dots, p^m\}$ contains exactly p^{m-1} numbers divisible by p. The rest are elements relatively prime to p, thus $\varphi(p^m) = p^m - p^{m-1}$. □

The *cartesian product* $\boldsymbol{G}_1 \times \cdots \times \boldsymbol{G}_n$ of groups $\boldsymbol{G}_1, \dots, \boldsymbol{G}_n$ consists of all tuples $\langle g_1, \dots, g_n \rangle$ such that $g_i \in G_i$ for all $i \in \{1, 2, \dots, n\}$. Elements of $\boldsymbol{G}_1 \times \cdots \times \boldsymbol{G}_n$ are multiplied coordinate-wise.

Lemma 9.18. *Let $n_1, \dots, n_k$ be positive integers. If they are pairwise relatively prime, then*

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

Proof. Let $\langle s_1, \dots, s_k \rangle$ be an element $\boldsymbol{Z_{n_1}} \times \cdots \times \boldsymbol{Z_{n_k}}$. Since $o(s_i) \mid n_i$, for all $i = 1, \dots, k$, the orders $o(s_1), \dots, o(s_k)$ are relatively prime. We get that

$$o(\langle s_1, \dots, s_k \rangle) = o(s_1) \cdots o(s_k),$$

due to Lemma 9.13 (i). It follows that $\langle s_1, \dots, s_k \rangle$ is a generator of $\boldsymbol{Z_{n_1}} \times \cdots \times \boldsymbol{Z_{n_k}}$ if and only if s_i generates $\boldsymbol{Z}_{n_i}$ for all $i \in \{1, 2, \dots, k\}$. We conclude that the cartesian product $\boldsymbol{Z_{n_1}} \times \cdots \times \boldsymbol{Z_{n_k}}$ is cyclic of order $n_1 \cdots n_k$ and $\varphi(n_1 \cdots n_k) = \varphi(n_1) \cdots \varphi(n_k)$. □

Exercise 9.7. *Prove that $\boldsymbol{Z_{n_1}} \times \cdots \times \boldsymbol{Z_{n_k}}$ is cyclic if and only if $n_1, \cdots, n_k$ are pairwise relatively prime.*

Theorem 9.19. *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*

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

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 Lemma 9.18 and $\varphi(p_i^{m_i}) = p_i^{m_i} - p_i^{m_i-1}$, for all $i = 1, \dots, k$, due to Lemma 9.17. □

Theorem 9.20. *For every positive integer n the equality*

$$n = \sum_{m|n} \varphi(m) \tag{9.4}$$

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 $\langle g \rangle$ consisting of all powers of g. The cyclic group $\boldsymbol{Z_n}$ has n elements, a unique subgroup of order m for each $m \mid n$, due to Lemma 9.7, and the subgroup of order m has exactly $\varphi(m)$ generators. Equality (9.4) follows. □

The *multiplication modulo* a positive integer n is given by

$$s \cdot_n t = s \cdot t \bmod n,$$

is a binary operation on $\mathbb{Z}_n$. It follows from Exercise 9.2 that the set

$$\mathbb{Z}_n^* := \{s \in \mathbb{Z}_n \mid s \equiv 1 \pmod{n}\}$$

together with the operation $\cdot_n$ form a group. We will denote the group by $\boldsymbol{Z_n^*}$.

Theorem 9.21 (Euler's theorem)**.** *Let n be a positive integer. Then*

$$s^{\varphi(n)} \equiv 1 \pmod{n}, \tag{9.5}$$

for all integers s co-prime to n.

Proof. Let s be an integer co-prime to n. Then $s \equiv t \pmod{n}$ for some $t \in \mathbb{Z}_n^*$. The order of t in $\boldsymbol{Z_n^*}$ divides $\varphi(n) =$ the order of $\boldsymbol{Z_n^*}$, due to Lemma 9.9. It follows from Lemma 9.10 that

$$\underbrace{t \cdot_n \cdots \cdot_n t}_{\varphi(n) \text{ times}} = 1,$$

hence $t^{\varphi(n)} \equiv 1 \pmod{n}$. Since $s^{\varphi(n)} \equiv t^{\varphi(n)} \pmod{n}$, due to Exercise 9.2, we conclude that (9.5) holds true. □

Corollary 9.22 (Fermat's theorem)**.** *Let p be a prime. If $p \nmid s$, then*

$$s^{p-1} \equiv 1 \pmod{p}.$$

Proof. Since p is prime, an integer s is co-prime to p if and only if $p \nmid s$. Since $\varphi(p) = p - 1$ for every prime p, Fermat's theorem follows readily form Euler's theorem. □

Lemma 9.23 (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. (⇒) If q is not prime, then clearly $1 < \mathbf{gcd}(q, (q-1)!)$, and so $q \nmid (q-1)! + 1$. (⇐) Suppose that q is a prime number. Then $q \mid s^2 - 1 = (s+1)(s-1)$ if and only if $q \mid s+1$ or $q \mid s+1$. It follows that the only elements of the group $\boldsymbol{Z}_{\boldsymbol{q}}^{*}$ that are equal to their inverses are 1 and $q-1$. Consequently, we can pair the remaining elements of $\boldsymbol{Z}_{\boldsymbol{q}}^{*}$, namely $2, \cdots, q-2$, so that the members of 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 $q \mid (q-1)! + 1$. □