20240917 MATH3301 NOTE 3[1]

Author: Be $\sqrt{-1}$maginative, and nothing will be $\frac{\mathrm{d}}{\mathrm{d}x}$ifficult!
Email: u3612704@connect.hku.hk;
Phone: +852 5693 2134; +86 19921823546;

Contents

1 Introduction

This note aims at the additive group of integers modulo b.
(1) First, we assume **Well-ordering Principle** and show its consequences.
(2) Second, we construct $\mathbb{Z}_b$ and study the order of it and its subgroups.

2 Well-ordering Principle

2.1 Writing Proofs with Well-ordering Principle

Principle 2.1. (**Well-ordering Principle**)
Let Q be a subset of $\mathbb{Z}$.
(1) If Q is *nonempty* and *bounded below*, then Q has a unique *minimum* $q_{\min}$;
(2) If Q is *nonempty* and *bounded above*, then Q has a unique *maximum* $q_{\max}$.

Proposition 2.2. If $n \in \mathbb{N}$ is not a perfect square, then $\sqrt{n} \notin \mathbb{Q}$.[2]

Proof. Assume to the contrary that $\sqrt{n} \in \mathbb{Q}$.
Step 1: Construct the following subset M of $\mathbb{Z}$.

$$M = \{m \in \mathbb{Z} : m^2 \leq n\}$$

As $1^2 = 1 \leq n \implies 1 \in M$, $M \neq \emptyset$.
As $m > n \geq 1 \implies m^2 > n^2 \geq n \implies m \notin M$, M has an upper bound n.
Hence, according to **Principle 2.1.**, M has a unique maximum m_0.
As n is not a perfect square, $m_0^2 < n < (m_0+1)^2$.
Step 2: Construct the following subset R pf $\mathbb{Z}$.

$$R = \left\{p^2 + q^2 \in \mathbb{Z} : p, q \in \mathbb{Z} \text{ and } q \neq 0 \text{ and } \sqrt{n} = \frac{p}{q}\right\}$$

As $\sqrt{n} \in \mathbb{Q} \implies \left[\exists p, q \in \mathbb{Z} \text{ with } q \neq 0, \sqrt{n} = \frac{p}{q}\right] \implies p^2 + q^2 \in R$, $R \neq \emptyset$.
As $\forall p, q \in \mathbb{Z}$ with $q \neq 0, p^2 + q^2 \geq 1$, R has a lower bound 1.
Hence, according to **Principle 2.1.**, R has a unique minimum $p_0^2 + q_0^2$.
Without loss of generality, we may assume that $p_0, q_0 > 0$, so:

$$\sqrt{n} = \frac{p_0}{q_0} > 0 \text{ and } m_0 < \sqrt{n} < m_0 + 1$$

Step 3: Construct the following $p_1, q_1 \in \mathbb{Z}$ with $q_1 \neq 0$.

$$(p_1, q_1) = ((\sqrt{n} - m_0)p_0, (\sqrt{n} - m_0)q_0) = (nq_0 - m_0p_0, p_0 - m_0q_0)$$

As $p_1^2 + q_1^2 = (\sqrt{n} - m_0)^2(p_0^2 + q_0^2) < p_0^2 + q_0^2$, $p_1^2 + q_1^2 \notin R$.
As $\sqrt{n} = \frac{p_0}{q_0} = \frac{(\sqrt{n}-m_0)p_0}{(\sqrt{n}-m_0)q_0} = \frac{p_1}{q_1}$, $p_1^2 + q_1^2 \in R$.

Hence, we arrive at a contradiction.
To conclude, our assumption is false, and we've proven $\sqrt{n} \notin \mathbb{Q}$.
Quod. Erat. Demonstrandum. $\square$

Proposition 2.3.
If $m \in \mathbb{Z}_{\geq 5}$, then no $(c_k)_{k=1}^m$ in $\mathbb{Z}[\mathrm{i}]$ generates a regular polygon.[3]

Proof. Assume to the contrary that some $(c_k)_{k=1}^m$ in $\mathbb{Z}[\mathrm{i}]$ generates a regular polygon.
Step 1: Construct the following subset R of $\mathbb{Z}$.

$$R = \{|c_2 - c_1|^2 \in \mathbb{Z} : (c_k)_{k=1}^m \text{ generates a regular polygon}\}$$

As assumed, $R \neq \emptyset$.
As $\forall (c_k)_{k=1}^m$ in $\mathbb{Z}[\mathrm{i}], |c_2 - c_1|^2 \geq 1$, R has a lower bound 1.
Hence, according to **Principle 2.1.**, R has a unique minimum $|c_{02} - c_{01}|^2$.
Without loss of generality, assume that $(c_{0k})_{k=1}^m$ is in anticlockwise orientation.
Step 2: Construct the following $(c_{1k})_{k=1}^m$ in $\mathbb{Z}[\mathrm{i}]$.

$$c_{1k} = \begin{cases} c_{01} + \mathrm{i}(c_{01} - c_{0m}) & \text{if} \quad k = 1; \\ c_{0k} + \mathrm{i}(c_{0k} - c_{0(k-1)}) & \text{if} \quad k \neq 1; \end{cases}$$

As $|c_{12} - c_{11}|^2 = \left[1 - 4\sin\frac{\pi}{m}\left(\cos\frac{\pi}{m} - \sin\frac{\pi}{m}\right)\right] |c_{02} - c_{01}|^2 < |c_{02} - c_{01}|^2$, $|c_{12} - c_{11}|^2 \notin R$.
As $(c_{1k})_{k=1}^m$ generates a regular polygon, $|c_{12} - c_{11}|^2 \in R$.
Hence, we arrive at a contradiction.
To conclude, our assumption is false, and we've proven that no $(c_k)_{k=1}^m$ in $\mathbb{Z}[\mathrm{i}]$ generates a regular polygon. Quod. Erat. Demonstrandum. $\square$

2.2 Division Algorithm

Theorem 2.4. (**Division Algorithm**)
Let a, b be two integers with $b \neq 0$.
There exists a unique pair of integers (q, r) with $0 \leq r < |b|$, such that $a = qb + r$.

Proof. Without loss of generality, assume that $b \geq 1$.
We may divide our proof into two parts.
Part 1: In this part, we prove the existence of (q, r).
Construct the following subset Q of $\mathbb{Z}$.

$$Q = \{q \in \mathbb{Z} : a - qb \geq 0\}$$

If $a \geq 0$, then $a - 0b = a \geq 0$, so $0 \in Q$, which implies $Q \neq \emptyset$;
If $a < 0$, then $a - ab = (-a)(b - 1) \geq 0$, so $a \in Q$, which implies $Q \neq \emptyset$.
As $\forall q \in \mathbb{Z}, q > a \implies a - qb < a - ab = a(1 - b) \leq 0 \implies q \notin Q$, Q has an upper

bound a. Hence, according to **Principle 2.1.**, Q has a unique maximum q_0, so:

$$q_0 \in Q \text{ and } q_0 + 1 \notin Q \implies 0 \leq a - q_0 b < b$$

To conclude, such pair of integers $(q, r) = (q_0, a - q_0 b)$ exists.
Part 2: In this part, we prove the uniqueness of (q, r).
For all such pairs of integers $(q_1, r_1), (q_2, r_2)$:

$$\begin{aligned} a = q_1 b + r_1 \text{ and } a = q_2 b + r_2 &\implies b \text{ divides } (q_1 - q_2)b = r_2 - r_1 \in (-b, b) \\ &\implies (q_1 - q_2)b = r_2 - r_1 = 0 \implies (q_1, r_1) = (q_2, r_2) \end{aligned}$$

To conclude, such pair of integers $(q, r) = (q_1, r_1) = (q_2, r_2)$ is unique.
Combine the two parts above, we've proven the theorem.
Quod. Erat. Demonstrandum. □

2.3 Greatest Common Divisor and Least Common Multiple

Definition 2.5. (**Divisibility Relation**)
Let a, b be two integers.
If there exists integer q, such that $a = qb$, then b divides a.

Definition 2.6. (**Association Relation**)
Let a_1, a_2 be two integers.
If a_1 divides a_2 and a_2 divides a_1, then a_1, a_2 are associated.

Definition 2.7. (**Common Divisor**)
Let A be a nonempty subset of $\mathbb{Z}$, and b be an integer.
If b divides all integer in A, then b is a common divisor of A.

Definition 2.8. (**Common Multiple**)
Let A be a nonempty subset of $\mathbb{Z}$, and b be an integer.
If all integer in A divides b, then b is a common multiple of A.

Definition 2.9. (**Greatest Common Divisor**)
Let A be a nonempty subset of $\mathbb{Z}$, and b be an integer. If:
1. b is a common divisor of A;
2. All common divisor b' of A divides b,
then b is a greatest common divisor of A.

Definition 2.10. (**Least Common Multiple**)
Let A be a nonempty subset of $\mathbb{Z}$, and b be an integer. If:
1. b is a common multiple of A;
2. b divides all common multiple b' of A,
then b is a least common multiple of A.

Proposition 2.11. Let $(a_k)_{k=1}^m$ be a finite list of integers.
(1) There exists a least common multiple b of $(a_k)_{k=1}^m$;
(2) For all least common multiples b_1, b_2 of $(a_k)_{k=1}^m$, b_1, b_2 are associated.

Proof. Without loss of generality, assume that each a_k is nonzero.
We may divide our proof into three parts.
Part 1: Construct the following subset B of $\mathbb{Z}$.

$$B = \{b \in \mathbb{N} : b \text{ is a common multiple of } (a_k)_{k=1}^m\}$$

As $\prod_{k=1}^m a_k$ is a common multiple of $(a_k)_{k=1}^m \implies \prod_{k=1}^m a_k \in B$, $B \neq \emptyset$.
As $\forall b \in \mathbb{N}, b \geq 1$, B has a lower bound 1.
Hence, according to **Principle 2.1.**, B has a unique minimum b_0.
Part 2: Assume to the contrary that b_0 doesn't divide some $b \in B$.
According to **Theorem 2.4.**, there exists a unique pair of integers (q, r) with $1 \leq r < b_0$, such that $b = qb_0 + r$. This implies $r = b - qb_0 \in B$, a contradiction.
Hence, our assumption is false, and we've proven that b_0 divides every $b \in B$.
Part 3: For all least common multiples b_1, b_2 of $(a_k)_{k=1}^m$:

$$\begin{aligned} b_1 \text{ is a common multiple of } (a_k)_{k=1}^m &\implies b_2 \text{ divides } b_1 \\ b_2 \text{ is a common multiple of } (a_k)_{k=1}^m &\implies b_1 \text{ divides } b_2 \end{aligned}$$

Hence, b_1, b_2 are associated.
Combine the three parts above, we've proven the proposition.
Quod. Erat. Demonstrandum. □

Proposition 2.12. Let $(a_\mu)_{\mu \in J}$ be an indexed family of integers.
(1) There exists a greatest common divisor b of $(a_\mu)_{\mu \in J}$;
(2) For all greatest common divisors b_1, b_2 of $(a_\mu)_{\mu \in J}$, b_1, b_2 are associated.

Proof. Without loss of generality, assume that each a_μ is nonzero.
We may divide our proof into three parts.
Part 1: Construct the following subset B of $\mathbb{Z}$.

$$B = \{b \in \mathbb{Z} : b \text{ is a common divisor of } (a_\mu)_{\mu \in J}\}$$

The quotient set of B under association relation is finite, so according to **Proposition**

2.11., there exists a least common multiple b_0 of B. Each $b \in B$ divides b_0.
Part 2: For all $\mu \in J$, each $b \in B$ divides a_μ, so a_μ is a common multiple of B.
According to **Definition 2.10.**, b_0 divides each a_μ.
According to **Definition 2.9.**, b_0 is indeed a common divisor of $(a_\mu)_{\mu \in J}$.
Part 3: For all greatest common divisors b_1, b_2 of $(a_\mu)_{\mu \in J}$:

$$\begin{aligned} b_1 \text{ is a common divisor of } (a_\mu)_{\mu \in J} &\implies b_1 \text{ divides } b_2 \\ b_2 \text{ is a common divisor of } (a_\mu)_{\mu \in J} &\implies b_2 \text{ divides } b_1 \end{aligned}$$

Hence, b_1, b_2 are associated.
Combine the three parts above, we've proven the proposition.
Quod. Erat. Demonstrandum. □

Remark: *Chen gives this collection of proofs, which circumvents the use of ideal.*

Proposition 2.13. Let $(a_k)_{k=1}^m$ be a finite list of nonzero integers, A be the product of each a_k, and g be a greatest common divisor of $(A/a_k)_{k=1}^m$.
A/g is a least common multiple of $(a_k)_{k=1}^m$.

Proof. We may divide our proof into two parts.
Part 1: For each a_k, as g divides A/a_k, there exists an integer λ_k, such that $A/a_k = \lambda_k g$, i.e., $A/g = \lambda_k a_k$, so a_k divides A/g. Hence, A/g is a common multiple of $(a_k)_{k=1}^m$.
Part 2: For all common divisor b of $(a_k)_{k=1}^m$, A divides all greatest common divisor of $(bA/a_k)_{k=1}^m$, and bg is one of them. Hence, A/g divides b.
Combine the two parts above, we've proven that A/g is a least common multiple of $(a_k)_{k=1}^m$. Quod. Erat. Demonstrandum. □

2.4 Principal Ideal Property

Definition 2.14. (**Ideal**)
Let I be a subset of $\mathbb{Z}$. If:
(1) $0 \in I$;
(2) $\forall r_1, r_2 \in I, r_1 + r_2 \in I$;
(3) $\forall \lambda \in \mathbb{Z}$ and $r \in I, \lambda r \in I$,
then I is an ideal of $\mathbb{Z}$.

Definition 2.15. (**Set-generated Ideal**)
Let A be a nonempty subset of $\mathbb{Z}$. Define:

$$\text{gen } A = \left\{ \sum_{k=1}^{m} \lambda_k a_k \in \mathbb{Z} : (\lambda_k)_{k=1}^m \text{ in } \mathbb{Z} \text{ and } (a_k)_{k=1}^m \ \in A \right\}$$

as the ideal generated by A.

Proposition 2.16. Let A be a nonempty subset of $\mathbb{Z}$.
The ideal generated by A is indeed an ideal of $\mathbb{Z}$.

Proof. We may divide our proof into three parts.
Part 1: $0 = \sum_{k=1}^{1} 0a$ for some $(0)_{k=1}^{1}$ in $\mathbb{Z}$ and $(a)_{k=1}^{1}$ in A, so $0 \in \text{gen } A$.
Part 2: For all $r_1, r_2 \in \text{gen } A$, without loss of generality, assume that:

$$r_1 = \sum_{k=1}^{m} \lambda_{1k} a_k, r_2 = \sum_{k=1}^{m} \lambda_{2k} a_k \text{ for some } (\lambda_{1k})_{k=1}^{m}, (\lambda_{1k})_{k=1}^{m} \text{ in } \mathbb{Z} \text{ and } (a_k)_{k=1}^{m} \text{ in } A$$

This implies $r_1 + r_2 = \sum_{k=1}^{m} (\lambda_{1k} + \lambda_{2k}) a_k \in \text{gen } A$.
Part 3: For all $\lambda \in \mathbb{Z}$ and $r \in \text{gen } A$, assume that:

$$r = \sum_{k=1}^{m} \lambda_k a_k \text{ for some } (\lambda_k)_{k=1}^{m} \text{ in } \mathbb{Z} \text{ and } (a_k)_{k=1}^{m} \text{ in } A$$

This implies $\lambda r = \sum_{k=1}^{m} (\lambda \lambda_k) a_k \in \text{gen } A$.
Combine the three parts above, we've proven that gen A is an ideal.
Quod. Erat. Demonstrandum. $\square$

Definition 2.17. (**Principal Ideal**)
Let I be an ideal of $\mathbb{Z}$.
If some (a) in $\mathbb{Z}$ generates I, then I is principal.

Proposition 2.18. Every ideal I of $\mathbb{Z}$ is principal.

Proof. Without loss of generality, assume that I contains a positive integer.
Assume to the contrary that I is not principal.
Step 1: Construct a subset $B = \mathbb{N} \cap I$ of $\mathbb{Z}$.
As assumed, $B \neq \emptyset$.
As $\forall r \in \mathbb{N}, r \geq 1$, B has a lower bound 1.
Hence, according to **Principle 2.1.**, B has a unique minimum b_0.
Step 2: As (b_0) in $\mathbb{Z}$ doesn't generate I, there exists $r \in I$, such that $r \notin \text{gen } (b_0)$.
According to **Theorem 2.4.**, there exists a unique pair of integers (q, r) with $0 \leq r < b_0$, such that $r = a + (-q)b_0 \in I$, a contradiction.
Hence, our assumption is false, and we've proven that I is principal.
Quod. Erat. Demonstrandum. $\square$

Definition 2.19. (**Sum of an Indexed Family of Ideals**)
Let $(I_\mu)_{\mu\in J}$ be an indexed family of ideals of $\mathbb{Z}$. Define:

$$\sum_{\mu\in J} I_\mu = \left\{\sum_{k=1}^{m} r_{\mu_k} : \text{Each } r_{\mu_k} \text{ in } I_{\mu_k}\right\}$$

as the sum of $(I_\mu)_{\mu\in J}$.

Proposition 2.20. Let $(I_\mu)_{\mu\in J}$ be an indexed family of ideals of $\mathbb{Z}$.
$\sum_{\mu\in J} I_\mu$ is indeed an ideal of $\mathbb{Z}$.

Proof. We may divide our proof into three parts.
Part 1: $0 = \sum_{k=1}^{1} 0 \in \sum_{\mu\in J} I_\mu$, where some I_{μ_1} contains 0.
Part 2: For all $r_1, r_2 \in \sum_{\mu\in J} I_\mu$, without loss of generality, assume that:

$$r_1 = \sum_{k=1}^{m} r_{1\mu_k}, r_2 = \sum_{k=1}^{m} r_{2\mu_k}, \text{ where each } r_{1\mu_k}, r_{2\mu_k} \in I_{\mu_k}$$

This implies $r_1 + r_2 = \sum_{k=1}^{m} (r_{1\mu_k} + r_{2\mu_k}) \in \sum_{\mu\in J} I_\mu$.
Part 3: For all $\lambda \in \mathbb{Z}$ and $r \in \sum_{\mu\in J} I_\mu$, assume that:

$$r = \sum_{k=1}^{m} r_{\mu_k}, \text{ where each } r_{\mu_k} \in I_{\mu_k}$$

This implies $\lambda r = \sum_{k=1}^{m} (\lambda r_{\mu_k}) \in \sum_{\mu\in J} I_\mu$.
Combine the three parts above, we've proven that $\sum_{\mu\in J} I_\mu$ is an ideal of $\mathbb{Z}$.
Quod. Erat. Demonstrandum. □

Proposition 2.21. Let $(a_\mu)_{\mu\in J}$ be an indexed family of integers.
For all $b \in \mathbb{Z}$, the following two statements are logically equivalent:
(1) (b) generates $\sum_{\mu\in J} \text{gen }(a_\mu)$;
(2) b is a greatest common divisor of $(a_\mu)_{\mu\in J}$.

Proof. We may divide our proof into two parts.
(1) $\implies$ (2) : Assume that (b) generates $\sum_{\mu\in J} \text{gen }(a_\mu)$.
Step 1: b divides each $a_\mu \in \text{gen }(b)$, so b is a common divisor of $(a_\mu)_{\mu\in J}$.
Step 2: For all common divisor b' of $(a_\mu)_{\mu\in J}$, b' divides $\sum_{k=1}^{m} \lambda_{\mu_k} a_{\mu_k} = b$.
The two steps above shows b is a greatest common divisor of $(a_\mu)_{\mu\in J}$.
(2) $\implies$ (1) : Assume that b is a greatest common divisor of $(a_\mu)_{\mu\in J}$.
Assume that $\sum_{\mu\in J} \text{gen }(a_\mu) = \text{gen }(b')$. We've already shown b' is a greatest common divisor of $(a_\mu)_{\mu\in J}$, so b, b' are associated, which implies (b) generates $\sum_{\mu\in J} \text{gen }(a_\mu)$.
Combine the two parts above, we've proven the logical equivalence.
Quod. Erat. Demonstrandum. □

Definition 2.22. (**Intersection of a Finite List of Ideals**)
Let $(I_k)_{k=1}^m$ be a finite list of ideals of $\mathbb{Z}$. Define:

$$\bigcap_{k=1}^{m} I_k = \{r : r \text{ in each } I_k\}$$

as the product of $(I_k)_{k=1}^m$.

Proposition 2.23. Let $(I_k)_{k=1}^m$ be a finite list of ideals of $\mathbb{Z}$.
$\cap_{k=1}^m I_k$ is indeed an ideal of $\mathbb{Z}$.

Proof. We may divide our proof into three parts.
Part 1: $0 \in \bigcap_{k=1}^m I_k$, where 0 in each I_k.
Part 2: For all $r_1, r_2 \in \bigcap_{k=1}^m I_k$, each I_k contains r_1, r_2,
so each I_k contains $r_1 + r_2$, which implies $r_1 + r_2 \in \bigcap_{k=1}^m I_k$.
Part 3: For all $\lambda \in \mathbb{Z}$ and $r \in \bigcap_{k=1}^m I_k$, each I_k contains r,
so each I_k contains λr, which implies $\lambda r = \in \bigcap_{k=1}^m I_k$.
Combine the three parts above, we've proven that $\bigcap_{k=1}^m I_k$ is an ideal of $\mathbb{Z}$.
Quod. Erat. Demonstrandum. □

Proposition 2.24. Let $(a_k)_{k=1}^m$ be a finite list of integers.
For all $b \in \mathbb{Z}$, the following two statements are logically equivalent:
(1) (b) generates $\bigcap_{k=1}^m \text{gen } (a_k)$;
(2) b is a least common multiple of $(a_k)_{k=1}^m$.

Proof. We may divide our proof into two parts.
(1) $\implies$ (2) : Assume that (b) generates $\bigcap_{k=1}^m \text{gen } (a_k)$.
Step 1: Each a_k divides $b \in \text{gen } (a_k)$, so b is a common multiple of $(a_k)_{k=1}^m$.
Step 2: For all common multiple b' of $(a_k)_{k=1}^m$, b divides $b' \in \text{gen } (b)$.
The two steps above shows b is a least common multiple of $(a_k)_{k=1}^m$.
(2) $\implies$ (1) : Assume that b is a least common multiple of $(a_k)_{k=1}^m$.
Assume that $\bigcap_{k=1}^m \text{gen } (a_\mu) = \text{gen } (b')$. We've already shown b' is a least common multiple of $(a_k)_{k=1}^m$, so b, b' are associated, which implies (b) generates $\bigcap_{k=1}^m \text{gen } (a_\mu)$.
Combine the two parts above, we've proven the logical equivalence.
Quod. Erat. Demonstrandum. □

3 The Additive Group of Integers Modulo b

3.1 Congruence Relation

Definition 3.1. (**Congruence Relation**)
Let a_1, a_2, b be three integers.
If b divides $a_1 - a_2$, then a_1 is congruent to a_2 modulo b.

Proposition 3.2. Let b be an integer.
$\equiv \pmod b$ is an equivalence relation on $\mathbb{Z}$.

Proof. We may divide our proof into three parts.
Part 1: For all $a \in \mathbb{Z}$:

$$b \text{ divides } a - a \implies a \equiv a (\text{mod } b)$$

Part 2: For all $a_1, a_2 \in \mathbb{Z}$:

$$\begin{aligned} a_1 \equiv a_2 (\text{mod } b) &\implies b \text{ divides } a_1 - a_2 \\ &\implies b \text{ divides } a_2 - a_1 \implies a_2 \equiv a_1 (\text{mod } b) \end{aligned}$$

Part 3: For all $a_1, a_2, a_3 \in \mathbb{Z}$:

$$\begin{aligned} a_1 \equiv a_2 (\text{mod } b) \text{ and } a_2 \equiv a_3 (\text{mod } b) &\implies b \text{ divides } a_1 - a_2, a_2 - a_3 \\ &\implies b \text{ divides } a_1 - a_3 \implies a_1 \equiv a_3 (\text{mod } b) \end{aligned}$$

Combine the three parts together, we've proven that $\equiv \pmod b$ is an equivalence relation on $\mathbb{Z}$. Quod. Erat. Demonstrandum. $\square$

Definition 3.3. (**Congruence Class**)
Let a, b be two integers. Define:

$$[a]_b = \{a' \in \mathbb{Z} : a' \equiv a (\text{mod } b)\}$$

as the congruence class of a modulo b

Definition 3.4. (**The Additive Group of Integers Modulo b**)
Let b be an integer.
The set $\mathbb{Z}_b$ of all congruence classes modulo b forms a group under:

$$+ : \mathbb{Z}_b \times \mathbb{Z}_b \to \mathbb{Z}_b, [a_1]_b + [a_2]_b = [a_1 + a_2]_b$$

Define this group as the additive group of integers modulo b.

Proof. We may divide our proof into four parts.
Part 1: For all inputs $([a_1]_b, [a_2]_b), ([a_1']_b, [a_2']_b) \in \mathbb{Z}_b \times \mathbb{Z}_b$:

$$\begin{aligned}([a_1]_b, [a_2]_b) = ([a_1']_b, [a_2']_b) &\implies a_1 \equiv a_1' (\text{mod } b) \text{ and } a_2 \equiv a_2' (\text{mod } b) \\ &\implies a_1 + a_2 \equiv a_1' + a_2' (\text{mod } b) \implies [a_1 + a_2]_b = [a_1' + a_2']_b\end{aligned}$$

Hence, $+$ is a well-defined binary operation on $\mathbb{Z}_b$.
Part 2: For all $[a_1]_b, [a_2]_b, [a_3]_b \in \mathbb{Z}_b$:

$$\begin{aligned}([a_1]_b + [a_2]_b) + [a_3]_b &= [a_1 + a_2]_b + [a_3]_b \\ &= [(a_1 + a_2) + a_3]_b \\ &= [a_1 + (a_2 + a_3)]_b \\ &= [a_1]_b + [a_2 + a_3]_b = [a_1]_b + ([a_2]_b + [a_3]_b)\end{aligned}$$

Hence, $+$ is associative.
Part 3: There exists $[0]_b \in \mathbb{Z}_b$, such that for all $[a]_b \in \mathbb{Z}_b$:

$$\begin{aligned}[0]_b + [a]_b = [0 + a]_b = [a]_b \\ [a]_b + [0]_b = [a + 0]_b = [a]_b\end{aligned}$$

Hence, $[0]_b$ is an identity under $+$.
Part 4: For all $[a]_b \in \mathbb{Z}_b$, there exists $[-a]_b \in \mathbb{Z}_b$, such that:

$$\begin{aligned}[-a]_b + [a]_b = [(-a) + a]_b = [0]_b \\ [a]_b + [-a]_b = [a + (-a)]_b = [0]_b\end{aligned}$$

Hence, each $[a]_b$ has an inverse $[-a]_b$ under $+$.
Combine the four parts above, we've proven that $\mathbb{Z}_b$ forms a group under $+$.
Quod. Erat. Demonstrandum. $\square$

3.2 The Order of $\mathbb{Z}_b$

Proposition 3.5. Let b be a positive integer.

$$\mathbb{Z}_b = \{[r]_b\}_{r=0}^{b-1}$$

Proof. It suffices to prove **"$\subseteq$" inclusion**.
For all $[a]_b \in \mathbb{Z}_b$, according to **Theorem 2.4.**, there exists a unique pair of integers (q, r) with $0 \le r < b$, such that $a - r = qb$, so $a \equiv r (\text{mod } b)$, which implies $[a]_b = [r]_b \in \{[r]_b\}_{r=0}^{b-1}$. Hence, $\mathbb{Z}_b \subseteq \{[r]_b\}_{r=0}^{b-1}$. Quod. Erat. Demonstrandum. $\square$

Proposition 3.6. Let b be a positive integer.

$$|\mathbb{Z}_b| = b$$

Proof. For all $[r_1]_b, [r_2]_b$ with $0 \leq r_1, r_2 < b$:

$$\begin{aligned} [r_1]_b = [r_2]_b &\implies r_1 \equiv r_2 (\text{mod } b) \\ &\implies b \text{ divides } r_1 - r_2 \in (-b, b) \implies r_1 = r_2 \end{aligned}$$

Hence, $|\mathbb{Z}_b| = |\{[r]_b\}_{r=0}^{b-1}| = b$. Quod. Erat. Demonstrandum. $\square$

3.3 The Order of a Subgroup of $\mathbb{Z}_b$

Proposition 3.7. Let b be a positive integer.
For all subgroup H of $\mathbb{Z}_b$, there exists $c \in \mathbb{N}$, such that $H = \{[qc]_b\}_{q \in \mathbb{Z}}$.

Proof. It suffices to prove **"$\subseteq$ inclusion"**.
Without loss of generality, assume that there exists $c \in \mathbb{N}$, such that $[c]_b \in H$.
Step 1: Construct the following subset C of $\mathbb{Z}$.

$$C = \{c \in \mathbb{N} : [c]_b \in H\}$$

As assumed, $C \neq \emptyset$.
As $\forall c \in \mathbb{N}, c \geq 1$, C has a lower bound 1.
Hence, according to **Principle 2.1.**, C has a unique minimum c_0.
Step 2: Assume to the contrary that some $[a]_b \in H$ is not in $\{[qc_0]_b\}_{q \in \mathbb{Z}}$.
A direct consequence is the equation $xb + yc_0 = a$ has no integral solution (x, y).
This means $a \notin \text{gen } (b, c_0) = \text{gen } (g)$, where $g \leq c_0$ is a positive greatest common divisor of (b, c_0). According to **Theorem 2.4.**, there exists a unique pair of integers (q, r) with $0 \leq r < g \leq c_0$, such that $a = qg + r$.
As $g = xb + yc_0$ for some $x, y \in \mathbb{Z} \implies [g]_b = y[c_0]_b \in H$, $[r]_b = [a]_b + (-q)[g]_b \in H$.
As $1 \leq r < c_0$, $[r]_b \notin H$, a contradiction.
Hence, our assumption is false, and we've proven that all $[a]_b \in H$ is in $\{[qc_0]_b\}_{q \in \mathbb{Z}}$.
Quod. Erat. Demonstrandum. $\square$

Proposition 3.8. Let b be a positive integer.
For all subgroup H of $\mathbb{Z}_b$, there exists $c \in \mathbb{N}$, such that $H = \{[qc]_b\}_{q=0}^{b/g-1}$, where g is a greatest common divisor of (b, c).

Proof. It suffices to prove **"$\subseteq$ inclusion"**.
According to **Proposition 4.1.**, there exists $c \in \mathbb{N}$, such that $H = \{[qc]_b\}_{q \in \mathbb{Z}}$.
For all $[qc]_b \in H$, according to **Theorem 2.4.**, there exists a unique pair of integers (q', c') with $0 \leq c' < b/g$, such that $q = \lambda b/g + q'$.

This implies $[qc]_b = [q'c + b\lambda c/g]_b = [q'c]_b \in \{[qc]_b\}_{q=0}^{b/g-1}$. Hence, $H \subseteq \{[qc]_b\}_{q=0}^{b/g-1}$. Quod. Erat. Demonstrandum. $\square$

Proposition 3.9. Let b, c be a positive integers. The order of the subgroup $\{[qc]_b\}_{q=0}^{b/g-1}$ of $\mathbb{Z}_b$ is b/g, where g is a greatest common divisor of (b, c).

Proof. For all $[q_1c]_b, [q_2c]_b$ with $0 \leq q_1, q_2 < b/g$:

$$\begin{aligned}
[q_1c]_b = [q_2c]_b &\implies q_1c \equiv q_2c (\text{mod } b) \\
&\implies q_1c - q_2c = (q_1 - q_2)c \in (-bc/g, bc/g) \text{ is a common multiple of } (b, c) \\
&\implies q_1 = q_2
\end{aligned}$$

Hence, $|\{[qc]_b\}_{q=0}^{b/g-1}| = b/g$. Quod. Erat. Demonstrandum. $\square$

References

[1] H. Ren, “Template for math notes,” 2021.

[2] 常庚哲 and 史济怀, *中科大数学分析教程第 3 版*. 中国科学技术大学出版社, 2021.

[3] 德安城, “如何证明平面内任意 $n(n \in \mathbb{Z}_{\geq 5})$ 个整点都不能组成正 n 边形？,” 2023. [Online]. Available: https://www.zhihu.com/question/25304120?sort=created