

# Solutions 03

- P3.1.** Define a binary relation on the set  $\mathbb{R}$  of real numbers as follows: for all  $x, y \in \mathbb{R}$ , we declare that  $x \sim y$  if there exists  $k \in \mathbb{Z}$  such that  $x - y = 2k\pi$ .
- Verify that this is an equivalence relation.
  - Describe a complete system of distinct representatives (or a transversal) for this equivalence relation.
  - Is addition well-defined on the quotient set  $\mathbb{R}/\sim$ ?
  - Is multiplication well-defined on the quotient set  $\mathbb{R}/\sim$ ?

*Solution.*

- Let  $x, y, z \in \mathbb{R}$ .

(reflexivity) For all  $x \in \mathbb{R}$ , we have  $x - x = 0 = 2(0)\pi$ , so  $x \sim x$ .

(symmetry) Suppose that  $x \sim y$ . Hence, there exists  $k \in \mathbb{Z}$  such that  $x - y = 2k\pi$ . It follows that  $y - x = 2(-k)\pi$ , so  $y \sim x$ .

(transitivity) Suppose that  $x \sim y$  and  $y \sim z$ . Hence, there exist  $j, k \in \mathbb{Z}$  such that  $x - y = 2k\pi$  and  $y - z = 2j\pi$ . It follows that

$$x - z = (x - y) + (y - z) = 2k\pi + 2j\pi = 2(k + j)\pi,$$

so  $x \sim z$ .

Since the binary relation is reflexive, symmetric, and transitive, we conclude that it is an equivalence relation.

- We claim that the real numbers  $x$  satisfying the inequalities  $0 \leq x < 2\pi$  form a complete system of distinct representatives for the equivalence relation.

We first show that every equivalence class is represented by a real number in this half-open interval  $[0, 2\pi)$ . By definition, the floor function  $x \mapsto \lfloor x \rfloor$  sends a real number  $x$  to the greatest integer less than or equal to  $x$ ;

$$\lfloor x \rfloor := \max\{m \in \mathbb{Z} \mid m \leq x\}.$$

Given a real number  $y$ , set  $k := \lfloor y/(2\pi) \rfloor$ . It follows that  $k \in \mathbb{Z}$  and

$$k \leq \frac{y}{2\pi} < k + 1 \iff 2k\pi \leq y < 2(k + 1)\pi \iff 0 \leq y - 2k\pi < 2\pi.$$

Since  $y \sim (y - 2k\pi)$ , the real number  $y - 2k\pi$  represents the equivalence class of  $y$  and belongs to the half-open interval  $[0, 2\pi)$ .

It remains to demonstrate that no two equivalence classes for real numbers in the half-open interval  $[0, 2\pi)$  coincide. Consider real numbers  $x$  and  $y$  such that  $0 \leq x < 2\pi$ ,  $0 \leq y < 2\pi$ , and  $\lfloor x \rfloor = \lfloor y \rfloor$ . The inequalities give  $0 \leq |x - y| < 2\pi$ . The equality implies that there exists a  $k \in \mathbb{Z}$  such that  $|x - y| = 2k\pi$ . It follows that  $0 \leq 2k\pi = |x - y| < 2\pi$ , so  $k = 0$ . We conclude that  $|x - y| = 0$  and  $x = y$ .

- We claim that addition does not depend on the chosen representatives in the equivalence classes. Let  $w, x, y$ , and  $z$  be real numbers such that  $w \sim x$  and  $y \sim z$ . Hence, there exists  $j, k \in \mathbb{Z}$  such that  $w - x = 2j\pi$  and  $y - z = 2k\pi$ . It follows that  $(w + y) - (x + z) = (w - x) + (y - z) = 2j\pi + 2k\pi = 2(j + k)\pi$ . Since  $w + y \sim x + z$ , addition on the quotient  $\mathbb{R}/\sim$  is well-defined.

- iv. We demonstrate that multiplication depends on the choice of representatives in the equivalence classes. For instance, we have  $0 \sim 2\pi$ , but

$$(0)\left(\frac{\pi}{8}\right) = 0 \quad \text{and} \quad 0 < (2\pi)\left(\frac{\pi}{8}\right) = \frac{\pi^2}{4} = \left(\frac{\pi}{4}\right)(\pi) < \pi$$

From part ii, we see that 0 and  $\pi^2/4$  are not equivalent. Thus, multiplication on the quotient  $\mathbb{R}/\sim$  is *not* well-defined.  $\square$

**Remark.** The quotient  $\mathbb{R}/\sim$  may be identified with the unit circle  $\{z \in \mathbb{C} \mid |z| = 1\}$ . Since the trigonometric functions are independent of the choice of representative, the equivalence class  $\theta \in \mathbb{R}/\sim$  corresponds to  $\cos(\theta) + \sqrt{-1} \sin(\theta) \in \mathbb{C}$ .

**P3.2.** The canonical order  $\leq$  on the integers  $\mathbb{Z}$  is defined as follows. For all  $m, n \in \mathbb{Z}$ , we declare that  $m \leq n$  or  $n \geq m$  if  $n - m$  is a nonnegative integer.

- i. For all  $m \in \mathbb{Z}$ , demonstrate that  $m \leq m$ .
- ii. When  $k \leq m$  and  $m \leq n$ , establish that  $k \leq n$ .
- iii. When  $m \leq n$  and  $n \leq m$ , verify that  $m = n$ .
- iv. For all  $m, n \in \mathbb{Z}$ , show that  $m \leq n$  or  $m \geq n$ .

*Solution.*

- i. For all  $m \in \mathbb{Z}$ , we have  $m - m = 0$  and  $0 \in \mathbb{N}$ , so  $m \leq m$  and the canonical order on the integers  $\mathbb{Z}$  is reflexive.
- ii. Suppose that  $k \leq m$  and  $m \leq n$ . It follows that  $m - k$  and  $n - m$  are nonnegative integers. Since  $\mathbb{N}$  is closed under addition, their sum

$$(m - k) + (n - m) = n - k$$

is also a nonnegative integer. We deduce that  $k \leq n$  and the canonical order on the integers  $\mathbb{Z}$  is transitivity.

- iii. Suppose that  $m \leq n$  and  $n \leq m$ . It follows that  $n - m$  and  $m - n$  are nonnegative integers. Setting  $d := n - m$ , we have  $d \geq 0$  and  $-d \geq 0$ . The trichotomy for nonnegative integers implies that exactly one of the following holds:  $d > 0$  or  $d = 0$ . If  $d$  were positive, then  $-d$  would be negative contradicting  $-d \geq 0$ . Thus, the only possibility is  $d = 0$  or  $m = n$ , so the canonical order on the integer  $\mathbb{Z}$  is antisymmetric.
- iv. Let  $m, n \in \mathbb{Z}$ . If  $n - m$  is a nonnegative integer, then we have  $m \leq n$ . If  $n - m$  is a negative integer (also known as not a nonnegative integer), then we have

$$-(n - m) = m - n \in \mathbb{N}$$

and  $n \leq m$ . In particular, the canonical order on the integers  $\mathbb{Z}$  is a total order.  $\square$

**P3.3.** Let  $k, m$ , and  $n$  be integers. Verify that  $\gcd(km, kn) = |k| \gcd(m, n)$ .

*Solution.* For any integer  $d$ , the following statements are equivalent:

- (a) The integer  $d$  divides the integer  $m$ .
- (b) There exists an integer  $k$  such that  $m = kd$ .
- (c) There exists an integer  $k$  such that  $-m = (-k)d$ .
- (d) The integer  $d$  divides the integer  $-m$ .

Thus, the set of divisors for an integer equals the set of divisors for its additive inverse. It follows that  $\gcd(m, n) = \gcd(-m, n) = \gcd(m, -n) = \gcd(-m, -n)$ . Hence, we may assume that  $k, m$ , and  $n$  are all nonnegative integers. When  $m = 0$ , we have

$$\gcd(km, kn) = \gcd(0, kn) = kn = k \gcd(0, n) = k \gcd(m, n).$$

Since  $\gcd(m, n) = \gcd(n, m)$ , we may assume that  $m$  and  $n$  are positive and  $m \geq n$ .

We proceed by induction on the positive integer  $m + n$ . When  $m = 1$  and  $n = 1$ , we have  $\gcd(km, kn) = \gcd(k, k) = k = k(1) = k \gcd(1, 1) = k \gcd(m, n)$ , which establishes the base case. For any positive integers  $m$  and  $n$  such that  $m \geq n$ , division with remainder shows that there exists positive integers  $q$  and  $r$  such that  $m = qn + r$  and  $0 \leq r < n$ . In particular, we have  $\gcd(m, n) = \gcd(n, r)$ . Multiplying the equation by  $k$  gives  $km = q(kn) + kr$  and  $0 \leq kr < kn$ , whence  $\gcd(km, kn) = \gcd(kn, kr)$ . Since  $n + r = n + (m - qn) = m + (1 - q)n \leq m < m + n$ , the induction hypothesis asserts that  $\gcd(kn, kr) = k \gcd(n, r)$ . We conclude that

$$\gcd(km, kn) = \gcd(kn, kr) = k \gcd(n, r) = k \gcd(m, n),$$

which completes the induction step. □

*A second solution.* As in the first solution, we may assume that  $k$  is nonnegative and both  $m$  and  $n$  are positive. When  $k = 0$ , we have

$$\gcd(km, kn) = \gcd(0, 0) = 0 = 0 \gcd(m, n) = k \gcd(m, n),$$

so we may also assume that  $k$  is positive.

As  $m$  and  $n$  are not both 0, there exist integers  $i$  and  $j$  such that  $\gcd(m, n) = im + jn$  and this is the smallest positive integer linear combination of  $m$  and  $n$ . Similarly, there exist integers  $u$  and  $v$  such that  $\gcd(km, kn) = u(km) + v(kn) = k(um + vn)$  and this is the smallest positive integer linear combination of  $km$  and  $kn$ . The positivity of  $im + jn$  and the minimality of  $k(um + vn)$  yield  $k(um + vn) \leq k(im + jn)$ . The positivity of  $um + vn$  and the minimality of  $im + jn$  implies that  $im + jn \leq um + vn$ . Combining the inequalities gives  $k(um + vn) \leq k(im + jn) \leq k(um + vn)$  so we conclude that  $\gcd(km, kn) = k(um + vn) = k(im + jn) = k \gcd(m, n)$ . □

*Outline of a third solution.* As in the first solution, we may assume that  $k, m$ , and  $n$  are all nonnegative integers. By the Fundamental Theorem of Arithmetic, there exist unique sequences  $(u_2, u_3, u_5, u_7, \dots)$ ,  $(v_2, v_3, v_5, v_7, \dots)$ , and  $(w_2, w_3, w_5, w_7, \dots)$  of nonnegative integers (where all but finitely many of the entries are 0) such that

$$k = \prod_{p \text{ prime}} p^{u_p}, \quad m = \prod_{p \text{ prime}} p^{v_p}, \quad \text{and} \quad n = \prod_{p \text{ prime}} p^{w_p}.$$

One verifies that

$$\gcd(m, n) = \prod_{p \text{ prime}} p^{\min(v_p, w_p)}.$$

It follows that

$$\begin{aligned} \gcd(km, kn) &= \prod_{p \text{ prime}} p^{\min(u_p + v_p, u_p + w_p)} = \prod_{p \text{ prime}} p^{u_p + \min(v_p, w_p)} \\ &= \left( \prod_{p \text{ prime}} p^{u_p} \right) \left( \prod_{p \text{ prime}} p^{\min(v_p, w_p)} \right) = k \gcd(m, n). \quad \square \end{aligned}$$