# Basic Properties of the Integers

(Lesson 1)

**1.** For each of the following pairs of integers $a$ and $b$, determine their greatest common divisor, their least common multiple, and write their greatest common divisor in the form $ax + by$ for some integers $x$ and $y$.

(a) $a = 792, b = 275$

(b) $a = 507885, b = 60808$

**2.** Prove that if $n$ is composite then there are integers $a$ and $b$ such that $n$ divides $ab$ but $n$ does not divide either $a$ or $b$.

**3.** If $p$ is a prime, prove that there do not exist nonzero integers $a$ and $b$ such that $a^2 = pb^2$. (Why this proves $\sqrt{p}$ is not a rational number.)

**4.** Write down explicitly all the elements in the residue classes of $\mathbb{Z}/18\mathbb{Z}$.

**5.** Suppose $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0$ is any positive integer. Show that $a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9$. (Note that this is the usual arithmetic rule that the remainder after division by 9 is the same as the sum of the decimal digits mod 9. In particular, an integer is divisible by 9 if and only if the sum of its digits is divisible by 9).

**6.** Compute the remainder when $37^{100}$ is divided by 29.

**7.** Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\overline{0}$ and $\overline{1}$.

**8.** Let $a, b \in \mathbb{Z}$. Prove that $a^2 + b^2$ never leaves a remainder of 3 when divided by 4. (Hint: use the previous exercise.)

**9.** Prove that the equation $x^2 + y^2 = 3z^2$ has no solutions for $x, y, z \in \mathbb{Z}$.

**10.** Prove that if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

**11.** Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if $a$ and $n$ are not relatively prime, there exists an integer $b$ with $1 \leq b < n$ such that $ab \equiv 0 \pmod n$ and deduce that there cannot be an integer $c$ such that $ac \equiv 1 \pmod n$.

**12.** Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove that if $a$ and $n$ are relatively prime then there is an integer $c$ such that $ac \equiv 1 \pmod n$. (Use the fact that the g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers.)

**13.** Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$is the set of elements $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition 4 . Verify this directly in the case $n = 12$.

**14.** (a) Prove that if $n$ is squarefree (i.e., $n > 1$ and $n$ is not divisible by the square of any prime), then $\sqrt{n}$ is irrational.

(b) Prove that $\sqrt[3]{2}$ is irrational.

**15.** Let $a$ and $b$ be nonzero integers and let $d = (a, b)$. Prove that $a/d$ and $b/d$ are relatively prime.

**16.** Let $m, r, r' \in \mathbb{Z}$. Prove that if $(r, m) = 1 = (r', m)$, then $(rr', m) = 1$.

**17.** Assume that $d = sa + tb$ is a $\mathbb{Z}$-linear combination of integers $a$ and $b$. Find infinitely many pairs of integers $(s_k, t_k)$ with $d = s_k a + t_k b$.

**18.** If $a$ and $b$ are relatively prime and if each divides an integer $n$, then their product $ab$ also divides $n$.

**19.** Let $a, b, c \in \mathbb{Z}$ with $a > 0$. Prove that $a(b, c) = (ab, ac)$. (One must assume that $a > 0$ lest $a(b, c)$ be negative.)

**20.** A Pythagorean triple is a 3-tuple $(a, b, c)$ of positive integers for which

$$a^2 + b^2 = c^2.$$

A Pythagorean triple is called primitive if $\gcd(a, b, c) = 1$. (*Definition.* A common divisor of nonzero integers $a_1, a_2, \ldots, a_n$ is an integer $c$ such that $c \mid a_i$ for all $i \in \{1, \ldots, n\}$. The largest of the common divisors is called its greatest common divisor.)

(a) Consider a complex number $z = q + ip$, where $q > p$ are positive integers. Prove that

$$(q^2 - p^2, 2qp, q^2 + p^2)$$

is a Pythagorean triple by showing that $|z^2| = |z|^2$. (One can prove that every primitive Pythagorean triple $(a, b, c)$ is of this type.)

(b) Show that the Pythagorean triple $(9, 12, 15)$ (which is not primitive) is not of the type given in part (a).

**21.** Let $X$ and $Y$ be finite sets. Show that there is a bijection $f\colon X \to Y$ if and only if $|X| = |Y|$. (By definition, a set is finite if it is empty or if it can be put in a one-to-one correspondence with $[k] = \{1, 2, \ldots, k\}$, for some integer $k \geq 1$.)

**22.** (Pigeonhole Principle) If $X$ and $Y$ are finite sets with the same number of elements, show that the following conditions are equivalent for a function $f\colon X \to Y$.

(a) $f$ is bijective

(b) $f$ is injective

(c) $f$ is surjective

**23.** (a) Let $f : X \to Y$ be a function, and let $(S_i)_{i \in I}$ be a family of subsets of $X$. Prove that

$$f\left(\bigcup_{i \in I} S_i\right) = \bigcup_{i \in I} f(S_i)$$

(b) If $S_1$ and $S_2$ are subsets of a set $X$, and if $f\colon X \to Y$ is any function, prove that $f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$. Give an example in which $f(S_1 \cap S_2) \neq f(S_1) \cap f(S_2)$.

(c) If $S_1$ and $S_2$ are subsets of a set $X$, and if $f\colon X \to Y$ is an injection, prove that $f(S_1 \cap S_2) = f(S_1) \cap f(S_2)$.

**24.** Let $f : X \to Y$ be a function.

(a) If $(B_\lambda)_{\lambda\in\Lambda}$ is a family of subsets of $Y$, prove that

$$f^{-1}\left(\bigcup_{\lambda\in\Lambda} B_\lambda\right) = \bigcup_{\lambda\in\Lambda} f^{-1}(B_\lambda) \quad \text{and} \quad f^{-1}\left(\bigcap_{\lambda\in\Lambda} B_\lambda\right) = \bigcap_{\lambda\in\Lambda} f^{-1}(B_\lambda).$$

(b) If $B \subseteq Y$, prove that $f^{-1}\left(B^{\complement}\right) = f^{-1}(B)^{\complement}$, where $B^{\complement}$ denotes the complement of $B$ respect to $Y$.

**25.** Let $f : X \to Y$ be a function. Define a relation on $X$ by $x \equiv x'$ if $f(x) = f(x')$. Prove that $\equiv$ is an equivalence relation. (If $x \in X$ and $f(x) = y$, the equivalence class $[x]$ is usually denoted by $f^{-1}(y)$, the inverse image of $\{y\}$.)