1. Let \( n \in \mathbb{N} \) with \( n > 1 \). Suppose \( a \equiv r \pmod{n} \) and \( b \equiv s \pmod{n} \). Show that

\[
a + b \equiv r + s \pmod{n} \quad \text{and} \quad ab \equiv rs \pmod{n}.
\]

Recall that \( \mathbb{Z}_n = \{[0], \ldots, [n-1] \} \) such that \([r] = \{nx + r : r \in \mathbb{Z}\}\). The above results show that if \([a] = [r] \) and \([b] = [s] \), then \([a + b] = [r + s] \) and \([ab] = [rs] \).

**Solution.** Suppose \( a \equiv r \pmod{n} \) and \( b \equiv s \pmod{n} \). Then \( a - r = np \), \( b - s = nq \). So, \( a + b - (r + s) = (a - r) + (b - s) = np + nq = n(p + q) \) and \( ab - rs = (np + r)(nq + s) - rs = n^2pq + np + nq = n(npq + p + q) \). Thus, \( a + b \equiv r + s \pmod{n} \) and \( ab \equiv rs \pmod{n} \).

2. Use the result in the previous problem or otherwise to show that:

\[
(a) \ 3^{2016} \equiv 1 \pmod{10} \quad (b) \ 3^{2016} + 5^{2016} \equiv 2 \pmod{28}.
\]

**Solution.** (a) In \( \mathbb{Z}_{10} \), \([3]^3 = [27] = [-3] \) so that \([3^6] = [3^3][3^3] = [1] \). Thus, \([3^{2016}] = [3^{6 \times 336}] = [1]^{336} = [1] \). Hence, \( 3^{2016} \equiv 1 \pmod{10} \).


3. Find \( \gcd(51, 288) \) and \( m, n \in \mathbb{Z} \) such that \( \gcd(51, 288) = 51n + 288m \) using the Euclidean Algorithm.

**Solution.** \( 288 = 51 \cdot 5 + 33; 51 = 33 \cdot 1 + 18; 33 = 18 \cdot 1 + 15; 18 = 15 \cdot 1 + 3 \). Thus,

\[
3 = \gcd(51, 288) = 51 \cdot 17 + 288 \cdot (-3).
\]

4. Let \( a, b, c \) be integers. Prove that if \( 3|(abc - 1) \), then \( 3|(a - 1), 3|(b - 1), \) or \( 3|(c - 1) \).

**Solution.** Assume that \( 3|(abc - 1) \), i.e., \([abc] = 1 \) in \( \mathbb{Z}_3 \). We need to show that \( 3|(a - 1), 3|(b - 1) \) or \( 3|(c - 1) \), i.e., \([a] = 1, [b] = 1 \) or \([c] = 1 \) in \( \mathbb{Z}_3 \). By contradiction, assume that \([a] \neq 1, [b] \neq 1 \) and \([c] \neq 1 \). Then each \([a], [b], [c] \) can be \([0] \) or \([2] \).

Case 1. If one of \([a], [b], [c] \) is \([0] \), then \([abc] = [0] \), contradicting the fact that \([abc] = 1 \) in \( \mathbb{Z}_3 \).

Case 2. If non of \([a], [b], [c] \) is \([0] \), then \([a] = [b] = [c] = [2] \) so that \([abc] = [8] = [2] \) in \( \mathbb{Z}_3 \), again contradicting \([abc] = [1] \).

Hence, the assumption that none of \([a], [b], [c] \) equals \([1] \) in \( \mathbb{Z}_3 \) is not true.
5. Let \( d = \gcd(a, b) \). If \( a = da' \) and \( b = db' \), show that \( \gcd(a', b') = 1 \).

**Solution 1.** Suppose \( \gcd(a', b') = m > 1 \). Then \( a' = m\hat{a} \) and \( b' = m\hat{b} \) for some integers \( \hat{a}, \hat{b} \). Then \( a = da' = dm\hat{a} \) and \( b = db' = dm\hat{b} \). Thus, \( dm > d \) and \( dm \) is a common divisor of \( a \) and \( b \), which is a contradiction.

**Solution 2.** If \( \gcd(a, b) = d \), then there are \( x, y \in \mathbb{Z} \) such that \( ax + by = d \). Hence, \( a'x + b'y = 1 \), and we have \( \gcd(a', b') = 1 \).

6. (a) Find a pair of integers \( (x, y) \) such that \( 3x + 2y = 1 \), and show that \( (x_n, y_n) = (x + 2n, y - 3n) \) also satisfies \( 3x_n + 2y_n = 1 \) for every \( n \in \mathbb{Z} \).

(b) Let \( a, b \in \mathbb{Z} \) such that \( ab \neq 0 \). Show that there are infinitely many pairs \( x, y \) of integers such that \( \gcd(a, b) = ax + by \).

**Solution.** (a) Let \( (x, y) = (1, -1) \), then \( 3x + 2y = 1 \). Thus,
\[
3(x + 2n) + 2(y - 2n) = 3x + 6n + 2y - 6n = 3x + 2y = 1.
\]
(b) Note that there is at least one pair of integers \( (x, y) \) such that \( ax + by = \gcd(a, b) \).

For every integer \( n \), let \( (x_n, y_n) = (x + bn, y - an) \). Then
\[
a(x + bn) + b(y - an) = ax + abn + by - abn = ax + by = \gcd(a, b).
\]
So, there are infinitely many pairs \( x, y \) of integers such that \( \gcd(a, b) = ax + by \).

7. Show that \( n + 1 \) and \( 3n + 2 \) are coprime.

**Solution.** Let \( (x, y) = (3, -1) \). Then \( (n + 1)x + (3n + 2)y = 3n + 3 - 3n - 2 \). So, \( \gcd(n + 1, 3n + 2) = 1 \).

8. Use the Fundamental Theorem of Arithmetic to prove that \( \sqrt[3]{3} \) and \( \log_{10} 234 \) are irrational numbers.

**Solution.** If \( \sqrt[3]{3} = p/q \) such that \( p, q \in \mathbb{N} \), then \( 3q^3 = p^3 = x \). Thus, \( 3 \) is a prime factor of \( x = p^3 \) and will appear \( 3k \) times for some positive integer. But \( x = 3p^3 \) and the prime factor will appear \( 3r + 1 \) times for some nonnegative integer. This contradicts the fundamental theorem of arithmetic that the list of prime factors in \( 3p^3 \) and \( q^3 \) are the same.

(b) Suppose \( \log_{10} 234 = p/q \) for some \( p, q \in \mathbb{N} \). Then \( 234 = 10^{p/q} \) so that \( 234^q = 10^p \). But then \( 5 \) is a prime factor of \( 10^p \), but not a prime factor of \( 234 \), and \( 234^q \), which is a contradiction. Thus, \( \log_{10} 234 \) is irrational.
9. (Extra credits) For integers \(a\) and \(b\), let \(\text{lcm}(a, b)\) be the least positive multiplier of \(a\) and \(b\).

(a) Express \(\text{gcd}(a, b)\) and \(\text{lcm}(a, b)\) in terms of prime factors of \(a\) and \(b\).

(b) Show that \(\text{lcm}(a, b) \cdot \text{gcd}(a, b) = ab\).

Solution. Let \(a = p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}\) and \(b = p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}\) with \(s_i, t_i \geq 0\). Then

\[
\text{gcd}(a, b) = p_1^{u_1}\cdots p_k^{u_k} \quad \text{and} \quad \text{lcm}(a, b) = p_1^{v_1}\cdots p_k^{v_k},
\]

where

\[
u_j = \min\{s_j, t_j\} \quad \text{and} \quad v_j = \max\{s_j, t_j\}, \quad j = 1, \ldots, k.
\]

To see this, observe that if \(d = p_1^{u_1}\cdots p_k^{u_k}\) is a common divisor of \(a\) and \(b\), then \(w_j \leq u_j\) for each \(j\), and taking \(w_j = u_j\) for each \(j\) will yield the greatest common divisor. Similarly, if \(d = p_1^{t_1}\cdots p_k^{t_k}\) is a common multiple of \(a\) and \(b\), then \(t_j \geq v_j\) for each \(j\), and and taking \(t_j = v_j\) for each \(j\) will yield the smallest common multiple.

Note that \(\max\{u_j, v_j\} + \min\{u_j, v_j\} = u_j + v_j\). Reason:

- If \(u_j \geq v_j\), then \(\max\{u_j, v_j\} + \min\{u_j, v_j\} = u_j + v_j\);
- if \(u_j \leq v_j\), then \(\max\{u_j, v_j\} + \min\{u_j, v_j\} = v_j + u_j\).

As a result,

\[
\text{gcd}(a, b) \cdot \text{lcm}(a, b) = p_1^{u_1+v_1}\cdots p_k^{u_k+v_k} = p_1^{s_1+t_1}\cdots p_k^{s_k+t_k} = ab.
\]