Problem 1. Multiplicative Cancellation in \( \mathbb{Z} \). Many times we’ve used the fact that the integers have multiplicative cancellation, but we never proved it. Let’s prove it now.

(a) Prove that for all integers \( a, b \in \mathbb{Z} \) we have

\[
(ab = 0) \Rightarrow (a = 0 \text{ or } b = 0).
\]

[Hint: You can assume the following two facts: (1) For all \( x, y, z \in \mathbb{Z} \), \( x < y \) and \( 0 < z \) \( \Rightarrow \) \( xz < yz \). (2) For all \( x, y, z \in \mathbb{Z} \), \( x < y \) and \( z < 0 \) \( \Rightarrow \) \( yz < xz \). Now there are four cases.]

(b) Use the result of part (a) to prove that for all integers \( a, b, c \in \mathbb{Z} \) we have

\[
(ab = ac \text{ and } a \neq 0) \Rightarrow (b = c).
\]

Problem 2. Multiplicative Cancellation in \( \mathbb{Z}/n \). Fix a nonzero integer \( n \in \mathbb{Z} \) and consider the following set of abstract symbols

\[
\mathbb{Z}/n := \{[a]_n : a \in \mathbb{Z}\}.
\]

We define “equality” of symbols by \([a]_n = [b]_n \iff (n|(a - b))\) (we proved in class that this is an equivalence relation), “addition” of symbols by \([a]_n + [b]_n := [a + b]_n\) and “multiplication” of symbols by \([a]_n \cdot [b]_n := [ab]_n\).

(a) Prove that addition and multiplication of symbols is well-defined. That is, if \([a]_n = [b]_n\) and \([c]_n = [d]_n\) prove that we must have \([a]_n + [c]_n = [b]_n + [d]_n\) and \([a]_n \cdot [c]_n = [b]_n \cdot [d]_n\).

(b) One can check (but please don’t) that \( \mathbb{Z}/n \) satisfies the first eight axioms of \( \mathbb{Z} \) with additive identity element \([0]_n \in \mathbb{Z}/n\) and multiplicative identity element \([1]_n \in \mathbb{Z}/n\). Prove that the element \([a]_n \in \mathbb{Z}/n\) has a multiplicative inverse if and only if \( \gcd(a, n) = 1 \).

[Hint: Recall that \((\gcd(a, n) = 1) \iff (\exists x, y \in \mathbb{Z}, ax + ny = 1)\).]

(c) Additive cancellation in \( \mathbb{Z}/n \) works exactly as in \( \mathbb{Z} \), but multiplicative cancellation is more complicated. Prove that the following statement is true for all \([b]_n, [c]_n \in \mathbb{Z}/n\) if and only if \( \gcd(a, n) = 1 \):

\[
([a]_n \cdot [b]_n = [a]_n \cdot [c]_n) \Rightarrow ([b]_n = [c]_n).
\]

Problem 3. Induction Practice. Use induction to prove that for all integers \( n \geq 1 \) the following statement holds:

“For any \( n \) integers \( a_1, a_2, \ldots, a_n \in \mathbb{Z} \) such that \([a_i]_4 = [1]_4\) for all \( i \in \{1, 2, \ldots, n\}\), it follows that \([a_1 a_2 \cdots a_n]_4 = [1]_4\).”

[Hint: Call the statement \( P(n) \). Verify that \( P(1) \) is true. Now fix an integer \( k \geq 1 \) and assume for induction that \( P(k) \) is true. In this case, prove that \( P(k + 1) \) is also true.]


(a) Consider an integer \( n \in \mathbb{Z} \) such that \(|n| > 1\). Prove that if \([n]_4 = [3]_4\) then \( n \) has a prime factor \( p | n \) such that \([p]_4 = [3]_4\). [Hint: You can assume (from the FTA) that \( n \) is a product of primes. By the Division Theorem, every prime number \( p \) must satisfy \( p = 2, [p]_4 = [1]_4 \), or \([p]_4 = [3]_4\). Use Problem 3.]

(b) Prove that there are infinitely many positive prime numbers \( p \) such that \([p]_4 = [3]_4\).

[Hint: Assume that there are only finitely many and call them \( 3 < p_1 < p_2 < \cdots < p_n \). Now consider the number \( N := 4p_1 p_2 \cdots p_n + 3 \). Since \([N]_4 = [3]_4\), part (a) says that there exists a prime \( p | N \) such that \([p]_4 = [3]_4\). Show that this leads to a contradiction.]