We will assume the existence of a set $\mathbb{Z}$, whose elements are called integers, along with a well-defined binary operation $+$ on $\mathbb{Z}$ (called addition), a second well-defined binary operation $\cdot$ on $\mathbb{Z}$ (called multiplication), and a relation $<$ on $\mathbb{Z}$ (called less than), and that the following fourteen statements involving $\mathbb{Z}$, $+$, $\cdot$, and $<$ are true:

A1. For all a, b, c in $\mathbb{Z}$, $(a + b) + c = a + (b + c)$.

A2. There exists a unique integer 0 in $\mathbb{Z}$ such that $a + 0 = 0 + a = a$ for every integer a.

A3. For every a in $\mathbb{Z}$, there exists a unique integer $-a$ in $\mathbb{Z}$ such that $a + (-a) = (-a) + a = 0$.

A4. For all a, b in $\mathbb{Z}$, $a + b = b + a$.

M1. For all a, b, c in $\mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

M2. There exists a unique integer 1 in $\mathbb{Z}$ such that $a \cdot 1 = 1 \cdot a = a$ for all a in $\mathbb{Z}$.

M4. For all a, b in $\mathbb{Z}$, $a \cdot b = b \cdot a$.

D1. For all a, b, c in $\mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

NT1. $1 \neq 0$.

O1. For all a in $\mathbb{Z}$, exactly one of the following statements is true: $0 < a$, $a = 0$, $0 < -a$.

O2. For all a, b in $\mathbb{Z}$, if $0 < a$ and $0 < b$, then $0 < a + b$.

O3. For all a, b in $\mathbb{Z}$, if $0 < a$ and $0 < b$, then $0 < a \cdot b$.

O4. For all a, b in $\mathbb{Z}$, $a < b$ if and only if $0 < b + (-a)$.

WOP. If S is a non-empty set of non-negative integers, then S has a least element.

Remark 1 *The above axiom is referred to as the* **Well-Ordering Principle (WOP)**. *We will assume it is true without proof.*

Proposition 2 (20 points) *(a) Let a be an integer and n a natural number. State the division algorithm for a and n.*

(b) Let a and b be integers. Define what it means for a to divide b.

(c) Let a, b be integers and let n be a natural number. Define $a \equiv b \bmod n$.

(d) Let S be a set of integers. Define what it means for $\ell \in S$ to be a least element.

Definitions. (a) The division algorithm for a and n produces unique integers q and r such that $a = qn + r$ and $0 \leq r < n$. (b) We say that a divides b if there exists an integer k such that $ak = b$. (c) We write that $a \equiv b \bmod n$ (and say that a is congruent to b modulo n) if n divides $a - b$. (d) An element $\ell \in S$ is a least element if for every $s \in S$ we have $\ell \leq s$.

Prove or disprove the following conjecture.

Conjecture 3 (10 points) *Let a, b, c be integers. If $a|bc$, then $a|b$ and $a|c$.*

Disproof. The conjecture is false. For example, let $a = 2$, $b = 2$, and $c = 1$. Then, $2|2 \cdot 1 = 2$, but 2 does not divide 1. QED.

Problem 4 (10 points) *Find the greatest common divisor of* 139 *and* 93. *Then, find integers* m *and* n *such that* $\gcd(139, 93) = 139m + 93n$.

Solution. Let us run the division algorithm a couple of times. We find that $139 = 1 \cdot 93 + 46$, that $93 = 2 \cdot 46 + 1$, and then that $46 = 46 \cdot 1 + 0$. It follows that $\gcd(139, 93) = \gcd(93, 46) = \gcd(46, 1) = 1$. Running the equations backwards, we find that $1 = 139 \cdot (-2) + 93 \cdot 3$.

Theorem 5 (10 points) *Let $P(k)$ denote a statement for every integer $k = 0, 1, 2, \ldots$. If the following are true:*

1. *$P(0)$ is true; and*
2. *The truth of $P(\ell - 1)$ implies the truth of $P(\ell)$ for every integer $\ell = 1, 2, 3, \ldots$,*

then $P(k)$ is true for all integers $k = 0, 1, 2, 3 \ldots$.

Proof. Let $F = \{n \in \mathbb{Z} : n \geq 0 \text{ and } P(n) \text{ is false}\}$. We want to show that F is empty. Suppose that it is not. In that case, F is non-empty and by definition it contains only non-negative integers. Therefore, by the well-ordering principle, F contains a least element, say ℓ. Note that $0 \notin F$ by assumption (1). Therefore, $\ell \geq 1$. This means that $\ell - 1 \geq 0$, so that $P(\ell - 1)$ is defined. Since $\ell - 1 < \ell$, the natural number $\ell - 1$ is not in F since ℓ is the least element. Therefore, $P(\ell - 1)$ is true. By assumption (2), this means that $P(\ell)$ is true, which contradicts the assumption that ℓ is in F. QED.

Proposition 6 (10 points) *Let a be an integer and n a natural number. Show that there exists an integer r such that $a \equiv r \bmod n$ and $0 \leq r < n$.* **Note:** *you do not need to prove uniqueness.*

Proof. Let $S = \{a - kn : k \in \mathbb{Z} \text{ and } a - kn \geq 0\}$. I claim that S is non-empty. If $a \geq 0$, then $a = a - 0 \cdot n$ shows that $a \in S$. If $a < 0$, then $a - a \cdot n = a(1 - n)$ is in the set because $a < 0$ and $(1 - n) \leq 0$. Therefore, S is non-empty. By construction, S contains only non-negative integers. Therefore, S has a least element, say $r = a - kn$ for some integer k. Then, $a - r = kn$ so $a \equiv r \bmod n$. Moreover, $r \geq 0$ since it is in S. So, it only remains to show that $r < n$. Suppose $r \geq n$. Then, $r - n \geq n - n = 0$. But, $r - n = a - (k + 1)n$, so it follows that $r - n \in S$. But, $r - n < r$, which contradicts the assumption that r is a least element. Hence, $r < n$. QED.

Proposition 7 (10 points) *Prove that for all $k \geq 1$,*

$$1 + 3 + \cdots + 2k - 1 = k^2.$$

Proof. We prove this by induction. The base case, when $k = 1$, is simply the statement that $1 = 1^2$, which is true. Now, suppose that for some $k \geq 1$ the equality $1 + 3 + \cdots + 2k - 1 = k^2$ holds. Adding $2(k + 1) - 1 = 2k + 1$ to both sides, we obtain $1 + 3 + \cdots + 2k - 1 + 2(k + 1) - 1 = k^2 + 2k + 1 = (k + 1)^2$, so the inductive step holds. By induction, $1 + 3 + \cdots + 1 + 2k - 1 = k^2$ for all $k \geq 1$. QED.

Proposition 8 (10 points) *Prove that $n^3 + 2n$ is divisible by 3 for all natural numbers n.*

Proof. We prove this by induction. In the base case, when $n = 1$, the formula $n^3 + 2n$ reduces to $1^3 + 2 \cdot 1 = 3$, which is divisible by 3. Now, assume that 3 divides $n^3 + 2n$ for some natural number n. We have that

$$\begin{aligned}(n+1)^3 + 2(n+1) &= n^3 + 3n^2 + 3n + 1 + 2n + 2 \\ &= (n^3 + 2n) + 3(n^2 + n + 3).\end{aligned}$$

As 3 divides $n^3 + 2n$ by hypothesis and also divides $3(n^2 + n + 3)$, it follows that 3 divides $(n+1)^3 + 2(n+1)$. Therefore, by induction, $3 | n^3 + 2n$ for all natural numbers n. QED.