Smallest Counter-Example: Group Exercises

CSCI 246

February 27, 2026

Problem 1. Prove that every integer greater than 2 has a prime factor.

$$\forall n \in \mathbb{Z}.\ n \geq 2 \Rightarrow \exists p \in \mathbb{Z}.\ p \text{ is prime } \wedge p|n$$

Proof.

Assume not. Since the integers ≥ 2 are well-ordered by $\leq$, there must be a smallest counter-example, x.
Since x is a counter-example we know that $x \geq 2$ and x has no prime factor.
Since x is the smallest such counter-example, for each $2 \leq y < x$ we know y has a prime factor.
Since x has no prime factor and x is a factor of itself, x is not prime.
Since $x \geq 2$ and x is not prime, x is composite. I.e., x has some factor $1 < y < x$.
Thus, y has a prime factor. Let the prime factor be named z.
Since z is a factor of y and y is a factor of x, then z is a factor of x.
Thus, x has a prime factor: z. A contradiction.
We may then conclude that every integer greater than 2 has a prime factor. □

Problem 2. Let $a, b \in \mathbb{Z}$ be integers with $b > 0$. There exists integers $q, r \in \mathbb{Z}$, the quotent and remainder of $\frac{a}{b}$ that satisfies the properties $a = bq + r$ and $0 \leq r < b$.

$$\forall a, b \in \mathbb{Z}.\ 0 < b \Rightarrow \exists q, r \in \mathbb{Z}.\ 0 \leq r < b \wedge a = bq + r$$

Proof.

Let a and b be any integers with $b > 0$.
We must prove there is some integers q and r such that $a = bq + r$ and $0 \leq r < b$.
Note that we may rewrite $a = bq + r$ to $r = a - bq$.
Define $S = \{a - bq : q \in \mathbb{Z}.\ 0 \leq a - bq\}$ to be all values of r that satisfies $r = a - bq$ and $0 \leq r$.
Clearly, if there is any $r < b$ it must be the smallest element of S.
Assume not; i.e., let r be the smallest element of S and $r \geq b$.
Necessarily, there must have been some q such that $r = a - bq$ and $0 \geq r$.
Consider $r - b = a - bq - b = a - b(q + 1)$. Since $r \geq b$, then $r - b \geq 0$.
Clearly, $r - b \in S$ and $r - b < r$. A contradiction.
Furthermore, S must be non-empty because for any $q \leq \frac{a}{b}$ satisfies $0 \leq a - bq$.
Thus the smallest element of S exists. Let r be that element. Clearly $0 \leq r < b$ as required. □

Problem 3. Prove that every amount of change greater than 12 cents can be made using 4 cent and 5 cent coins.

$$\forall n \in \mathbb{N}.\ 12 \leq n \Rightarrow \exists a, b \in \mathbb{N}.\ n = 4a + 5b$$

Proof.

Assume not. There must be some smallest $n \geq 12$ such that there are no a and b with $n = 4a + 5b$.
Necessarily, $n \geq 16$. Since $12 = 4(3) + 5(0)$, $13 = 4(2) + 5(1)$, $14 = 4(1) + 5(2)$, and $15 = 4(0) + 5(3)$.
Since $n \geq 16$ we know that $n - 4 \geq 12$.
Since $n - 4 < n$ and $n - 4 \geq 12$, we know there is some a and b such that $n - 4 = 4a + 5b$.
Clearly, $n = 4a + 5b + 4 = 4(a + 1) + 5b$. A contradiction.
We may thus conclude that every amount of change greater than 12 cents can be made using 4 cent and 5 cent coins. □

Problem 4. Prove strong induction is sound. If a property $P(n)$ satisfies "$P(0)$ holds true" and "whenever $P(k)$ holds for all $k < n$, then $P(n)$ holds", then $P(n)$ holds for all natural numbers n.

$$\forall P.\ P(0) \Rightarrow (\forall n \in \mathbb{N}.\ (\forall k \in \mathbb{N}.\ k < n \Rightarrow P(k)) \Rightarrow P(n)) \Rightarrow \forall n \in \mathbb{N}.\ P(n)$$

Proof.

Let P be any predicate over the natural numbers such that $P(0)$ and "whenever $P(k)$ holds for all $k < N$, then $P(n)$ holds".

We must prove that $P(n)$ holds for all natural numbers.

Assume not. Let n be the smallest natural number such that $P(n)$ does not hold.

Clearly, $n \neq 0$ because by assumption $P(0)$ holds; i.e., $0 \leq n - 1 \in \mathbb{N}$.

Since n is the smallest such value that $P(n)$ does not hold, we know that for any $k < n$, $P(k)$ holds.

Thus by assumption, $P(n)$ must hold. A contradiction.

Thus $P(n)$ must hold for all n. □

Problem 5. Prove that every finite non-empty set of integers has a least element.

$$\forall n \in \mathbb{N}.\ 0 < n \Rightarrow \forall S \subseteq \mathbb{Z}.\ |S| = n \Rightarrow \exists x \in S.\ \forall y \in S.\ x \leq y$$

Proof.

Assume not. I.e., let n be the smallest cardinality in which there is a non-empty set S with cardinality n that has no smallest element.

Clearly, $|S| = n \neq 1$, since the smallest element would be the single element contained by S.

Thus $|S| = n \geq 2$. Let S' be the set obtained by removing any element from S.

Let this element be some integer a. Necessarily, $0 < |S'| < |S| = n$.

Thus S' has a smallest element. Let's call this smallest element b.

Either $a < b$ or $b > a$ (note: $a \neq b$ since a and b both appear in S)

If $a < b$, then clearly a is smaller than b the smallest element of $S' = S - \{a\}$.

Thus a is the smallest element of S, a contradiction.

In the other case, that $b < a$, then clearly b is also the smallest element of S, a contradiction.

Since both cases result in a contradiction, we may conclude that every non-empty finite subset of $\mathbb{Z}$ has a smallest element. □

Problem 6. Prove that every integer 2 or greater has a unique prime factorization.

$$\forall n \in \mathbb{Z}.\ 2 \leq n \Rightarrow \exists!(p_1, ..., p_k) \in \mathbb{Z}^*.\ \forall i \in \mathbb{N}.\ p_i \text{ is prime } \wedge p_i \leq p_{i+1} \wedge n = p_1 \times ... \times p_k$$

Proof.

Assume not. There must be a smallest $n \geq 2$ that does not have a unique prime factorization.

Either n has no prime factorization or n has at least two prime factorizations.

Case: n has no prime factorization.

Clearly, n is not prime; otherwise the prime factorization of n would be (n) itself.

Thus, n is composite and must have some factors a and b such that $n = ab$ and $1 < a, b < n$.

Since n is the smallest counter example, we know that a and b both have prime factorizations.

That is $a = p_1 \times ... \times p_k$ and $b = q_1 \times ... \times q_m$, where each p_i and q_j are prime.

Since $n = ab = p_1 \times ... \times p_k \times q_1 \times ... \times q_m$, n has a prime factorization. A contradiction.

Case: n has two distinct prime factorizations.

That is $n = p_1 \times ... \times p_k = q_1 \times ... \times q_m$ where each p_i and q_j are prime and $p \neq q$.

Clearly $p_1 | n$. Thus $p_1 | q_1 \times ... \times q_m$. Since each q_i is prime, there must be some $q_j = p_1$.

Let's re-order q such that q_j comes first. I.e., $n = q_j \times (q_1 \times ... \times q_{j-1} \times q_{j+1} \times ... \times q_m)$.

Necessarily $n' = \frac{n}{p_1} = \frac{n}{q_j}$ is an integer since p_1 is a factor of n and $1 < p_1 < n$.

Since n is the smallest counter-example, n' must have a unique factorization.

Let $n' = r_1 \times ... \times r_l = p_2 \times ... \times p_k = q_1 \times q_{j-1} \times q_{j+1} \times ... \times q_m$.

Thus, thus the factorizations of n must be equal (otherwise $r_1 \times ... \times r_l$ would not be unique).

A contradiction.

We have reached a contradiction in all cases.

Thus every integer 2 or greater has a unique prime factorization. □