1 Modular Congruence, Concluded

So to wrap up proofs involving modular congruence, here's a variant on a proof appearing in the book.

Proposition 1. *For integers k and n, if $k^2 \not\equiv k \pmod{n}$, then $k \not\equiv 1 \pmod{n}$ and $k \not\equiv 0 \pmod{n}$.*

Proof. Our most effective approach to this proof is by way of its contrapositive; we shall instead prove the statement: "if $k \equiv 1 \pmod{n}$ or $k \equiv 0 \pmod{n}$, then $k^2 \equiv k \pmod{n}$". This statement lends itself naturally to a casewise analysis, since our premise now asserts that either $k \equiv 1 \pmod{n}$ or $k \equiv 0 \pmod{n}$.

Case 1: $k \equiv 1 \pmod{n}$**.** By multiplicativity of congruence, since $k \equiv 1 \pmod{n}$, $k \cdot k \equiv 1 \cdot 1 \pmod{n}$; thus $k^2 \equiv 1 \pmod{n}$, so by transitivity, $k^2 \equiv k \pmod{n}$.

Case 2: $k \equiv 0 \pmod{n}$**.** By multiplicativity of congruence, since $k \equiv 0 \pmod{n}$, $k \cdot k \equiv 0 \cdot 0 \pmod{n}$; thus $k^2 \equiv 0 \pmod{n}$, so by transitivity, $k^2 \equiv k \pmod{n}$. □

2 Proof of set properties

We often wish to prove proplerties of sets: that two sets are equal, or that one is the subset of another. Since we are now doing formal proof, specific definitions of these are necessary.

Definition 1. A set A is a subset of a set B (written $A \subseteq B$) if and only if for all $a \in A$, it follows that $a \in B$.

Proving that $A \subseteq B$ for specific A and B is thus rephrasable as an implication: "if $a \in A$, then $a \in B$", which we can then prove by normal proof methods. For instance, a result from problem set 1:

Proposition 2. *For any sets A and B, $A \subseteq A \cup B$.*

Proof. We shall consider as our premise the assignment of x as a name for some element of A, and proceed to the conclusion that $x \in A \cup B$. This transpires obviously from the definition of $A \cup B$: an object is an element of $A \cup B$ is it is either an element of A or and element of B. Since $x \in A$, it follows that $x \in A \cup B$. □

Equality can be phrased in a way amenable to this approach as well:

Definition 2. Two sets A and B are equal if $A \subseteq B$ and $B \subseteq A$.

And then asserting equality requires demonstrating two separate inclusions, as in this example:

Proposition 3. *For any sets A, B, and C, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.*

Proof. We shall start by demonstrating $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Consider some $x \in A \cup (B \cap C)$. Thus, x is either in A or in $B \cap C$. We may proceed casewise:

Case I: $x \in A$**.** Then, by definition of union, $x \in A \cup B$, and likewise, $x \in A \cup C$; thus, x is an element of their intersection, $(A \cup B) \cap (A \cup C)$.

Case I: $x \in B \cap C$**.** Then, by interpretation of this intersection, x must be an element of both B and C. Since $x \in B$, it follows that $x \in A \cup B$, and likewise from $x \in C$ it follows that $x \in A \cup C$; thus, x is an element of their intersection, $(A \cup B) \cap (A \cup C)$.

Now we must demonstrate that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. Let $x \in (A \cup B) \cap (A \cup C)$. Then, it is the case that x is an element of both $A \cup B$ and $A \cup C$, so there are two possibilities:

Case I: $x \in A$**.** Then, by definition of union, $x \in A \cup (B \cap C)$.

Case II: $x \notin A$**.** Then, sicne $x \in A \cup B$, x *must* be an element of B; likewise, sicne $x \in A \cup C$, x must be an element of.

□