Congruence

Congruence (or modular arithmetic) is a useful tool and is a good playground for proving things.

Definition: Let $n \in \mathbb{N}$ and let a and b be integers. Then we say that a is congruent to b modulo N (or mod N) if $a - b$ is divisible by N. We write this

$$a \equiv b \pmod{N}.$$

Examples

- x is odd if and only if $x \equiv 1 \pmod{2}$.
- 37 is congruent to 3 mod 4.
- Every odd number is congruent to either 1 or 3 mod 4.

Proving the contrapositive

The **contrapositive** of an implication $P \implies Q$ is $\neg Q \implies \neg P$. These two statements are equivalent, so proving one is the same as proving the other.

WARNING: Don't confuse the contrapositive with the *converse* $Q \implies P$.

Problems.

1. Suppose a, b, and c are integers. If a does not divide bc, then a does not divide b.
2. Suppose $x \in \mathbb{R}$. If $x^5 - 4x^4 + 3x^3 - x^2 + 3x - 4 \geq 0$, then $x \geq 0$.
3. Suppose x is an integer. If $x^3 - 1$ is even, then x is odd.
4. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$.

Proof by contradiction

Strategy: Show $\neg P$ implies a falsehood (like $A \wedge \neg A$). Conclude P is true.

1. $\sqrt{2}$ is not a rational number.
2. There are infinitely many prime numbers.

Strategy: To show $P \implies Q$, show that $P \wedge \neg Q$ implies a falsehood.

- Show that there are no integers a and b such that $18a + 6b = 1$.