Lecture 2: direct proof and proof by contradiction

September 14, 2026

1 Practice: Definitions Using Quantifiers

Definition 1.1. *An integer x is **even** iff there exists $k \in \mathbb{Z}$ such that $x = 2k$. An integer x is **odd** iff there exists $k \in \mathbb{Z}$ such that $x = 2k + 1$.*

Note:

- Only integers can be even or odd. In general, definitions should be clear what they can apply to.
- We use iff, meaning "if and only if": it's also true that an integer x is even if it's a multiple of 4, but that's not the *definition* of being even.

We can generalize evenness to arbitrary divisibility:

Definition 1.2. *For integers m and n, m **divides** n (written $m \mid n$) iff there exists an integer k such that $n = mk$.*

Now let's try to define prime numbers. A natural first attempt: "a natural number is prime iff it is only divisible by itself and 1." But this is slightly wrong — what is it missing?

Definition 1.3. *A natural number $n > 1$ is **prime** iff its only positive divisors are 1 and n. That is, $n \in \mathbb{N}$ is prime iff*

$$\forall x \in \mathbb{Z}, \quad x = 1 \text{ or } x = n \text{ or } x \nmid n.$$

Example 1.4. *How would you phrase the statement "every non-prime number (greater than 2) is divisible by a prime number"?*

Proposition 1.5. *For all $x \in \mathbb{N}$, if x is not prime and $x > 2$ then $\exists p : p$ prime and $p|x$.*

Definition 1.6. *$x \in \mathbb{R}$ is **rational** iff there exist integers m, n such that $x = m/n$.*

Example 1.7. *How would you phrase the statement "every rational number has a reduced form"? (For example, 4/8 is not reduced, but 1/2 is.)*

Proposition 1.8. *For all $x \in \mathbb{R}$, if x is rational then there exist $m, n \in \mathbb{Z}$ with $x = m/n$ and*

$$\neg\left(\exists k \in \mathbb{Z},\ k > 1 \text{ and } k \mid m \text{ and } k \mid n\right).$$

2 Proofs

Definition 2.1. *A **proof** is an argument that, given some assumptions, establishes that a statement is true.*

A proof is like an argumentative essay, but formal, precise, and as readable as possible. The assumptions of a proof may be stated explicitly in the proposition, or may be ambient (axioms, definitions, previously established results). Proving that a statement is *false* just means proving that its negation is true.

There are a few common patterns of proof, based on common patterns in propositional logic. For now, let's focus on proving statements of the form $p \implies q$: if p is true, then q is true. Note that this covers statements of the form "$\forall x \in S, P(x)$," since this is really $x \in S \implies P(x)$. (Proving $p \iff q$ requires two proofs: $p \implies q$ and $q \implies p$.)

2.1 Direct Proofs

Proposition 2.2. *If $x \in \mathbb{Z}$ is odd, then x^2 is odd.*

Proof. Since x is odd, there exists $k \in \mathbb{Z}$ such that $x = 2k+1$. Then

$$x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

So there exists $\ell \in \mathbb{Z}$ (namely $\ell = 2k^2 + 2k$) with $x^2 = 2\ell + 1$, i.e., x^2 is odd. □

Example 2.3. *For all $x \in \mathbb{Z}$, $x^2 + 3x + 2$ is even. (Try proving this both by casework on the parity of x, and by factoring — both work!)*

2.2 Proof by Contradiction

To prove that p is true, we can instead prove that $\neg p$ is false — and to prove something is false, we show that it implies nonsense. That is, if we can show $\neg p \implies$ False, then $\neg p$ cannot be true, so p must be true. The most common form of "False" is a statement of the form $q \wedge \neg q$.

Proposition 2.4. *$\sqrt{2}$ is irrational.*

Proof. Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational. Then $\sqrt{2} = m/n$ for integers m, n in reduced form (i.e., with no common factor greater than 1); in particular, m and n are not both even.

Squaring, $m^2/n^2 = 2$, so $m^2 = 2n^2$. Thus m^2 is even, so m is even; write $m = 2k$. Then $4k^2 = 2n^2$, so $n^2 = 2k^2$, meaning n^2 — and hence n — is also even.

But then m and n are both even, contradicting the fact that they are not both even. $\lightning$

So $\sqrt{2}$ is irrational. □

Proposition 2.5. *There are infinitely many primes.*

Proof. Suppose, for the sake of contradiction, that there are finitely many primes $p_1, \ldots, p_n$. Consider $x = p_1 p_2 \cdots p_n + 1$. Since x is an integer greater than 1, it must be divisible by some prime, so $p_k \mid x$ for some $k \in [n]$. Then

$$\frac{x}{p_k} = \frac{p_1 p_2 p_3 \cdots p_n}{p_k} + \frac{1}{p_k}.$$

The first term is an integer, but $\frac{1}{p_k}$ is not, so x/p_k is not an integer, contradicting $p_k \mid x$. $\lightning$

So, there are infinitely many primes. □

2.3 Negating Statements

Many of these proof techniques require negating statements, which is not always as simple as it looks (what does it mean for x to be *not* even?). Two useful rules, known as **De Morgan's Laws**, tell us how to negate *and/or* statements:

$$\neg(p \vee q) \equiv (\neg p) \wedge (\neg q), \qquad \neg(p \wedge q) \equiv (\neg p) \vee (\neg q).$$

We already used these above, when negating the reduced-form condition.

Quantifiers negate similarly:

$$\neg\big(\exists x \in S,\ P(x)\big) \equiv \forall x \in S,\ \neg P(x), \qquad \neg\big(\forall x \in S,\ P(x)\big) \equiv \exists x \in S,\ \neg P(x).$$

Example 2.6. *Negate: "there exists a real number that is greater than all other real numbers." Is the original statement true or false?*

Example 2.7. *We defined "x is odd" directly. What if instead we* defined *odd numbers as "not even"? Is it a good definition?*