Assertions

- Axioms
- Proposition, Lemma, Theorem
- Corollary
- Conjecture

Types of Proofs

- Direct proofs (including Proof by cases)
- Proof by contraposition
- Proof by contradiction
- Proof by construction
- Proof by Induction
- Other techniques

Direct Proofs

- The average of any two primes greater than 2 is an integer.

- Every prime number greater than 2 can be written as the difference of two squares, i.e. $a^2 - b^2$.

Proof by cases

If n is an integer, then n(n+1)/2 is an integer

- Case 1: n is even.

  or n = 2a, for some integer a

  So n(n+1)/2 = 2a*(n+1)/2 = a*(n+1),

  which is an integer.

- Case 2: n is odd.

  n+1 is even, or n+1 = 2a, for an integer a

  So n(n+1)/2 = n*2a/2 = n*a,

  which is an integer.

Proof by contraposition

If $\sqrt{(pq)} \neq (p+q)/2$, then $p \neq q$

Direct proof left as exercise

Contrapositive:

If $p = q$, then $\sqrt{(pq)} = (p+q)/2$

Easy:

$\sqrt{(pq)} = \sqrt{(pp)} = \sqrt{(p^2)} = p = (p+p)/2 = (p+q)/2.$

Proof by Contradiction

$\sqrt{2}$ is irrational

- Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = p/q$, such that p, q have no common factors.
  Squaring and transposing,
  $p^2 = 2q^2$ (even number)
  So, p is even (previous slide)
  Or $p = 2x$ for some integer x
  So $4x^2 = 2q^2$ or $q^2 = 2x^2$
  So, q is even (previous slide)
  So, p,q are both even – they have a common factor of 2. CONTRADICTION.
  So $\sqrt{2}$ is NOT rational. Q.E.D.

Proof by Contradiction - 2

In general, start with an assumption that statement A is true. Then, using standard inference procedures infer that A is false. This is the contradiction.

Recall: for any proposition p, $p \wedge \neg p$ must be false

Existence Proofs

There exists integers x,y,z satisfying

$x^2+y^2 = z^2$

Proof: $x = 3$, $y = 4$, $z = 5$.

Existence Proofs - 2

There exists irrational b,c, such that b^c is rational (page 97)

Nonconstructive proof:

Consider $\sqrt{2}^{\sqrt{2}}$. Two cases are possible:

- Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational – DONE ($b = c = \sqrt{2}$).

- Case 2: $\sqrt{2}^{\sqrt{2}}$ is **irrational** – Let $b = \sqrt{2}^{\sqrt{2}}$, $c = \sqrt{2}$.

  Then $b^c = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}*\sqrt{2}} = (\sqrt{2})^2 = 2$

Uniqueness proofs

- E.g. the equation $ax+b=0$, a,b real, $a\neq 0$ has a unique solution.

The Use of Counterexamples

All prime numbers are odd

Every prime number can be written as the difference of two squares, i.e. $a^2 - b^2$.

Examples

- Show that if n is an odd integer, there is a unique integer k such that n is the sum of k-2 and k+3.
- Prove that there are no solutions in positive integers x and y to the equation $2x^2 + 5y^2 = 14$.
- If x^3 is irrational then x is irrational
- Prove or disprove – if x, y are irrational, x + y is irrational.

Alternative problem statements

- “show A is true if and only if B is true”
- “show that the statements A,B,C are equivalent”

Exercises

- Q8, 10, 26, 28 on page 91

What can we prove?

- The statement must be true
- We must construct a valid proof

The role of conjectures

- 3x+1 conjecture

  Game: Start from a given integer n. If n is even, replace n by n/2. If n is odd, replace n with 3n+1. Keep doing this until you hit 1.

e.g. $n=5 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1$

Q: Does this game terminate for all n?

Elegance in proofs

Q: Prove that the only pair of positive integers satisfying a+b=ab is (2,2).

- Many different proofs exist. What is the simplest one you can think of?