09/26/2022

→ STRUCTURE OF PROOFS
→ DIRECT PROOFS

STRUCTURE OF PROOFS

A proof is logical argument for the truth of a conclusion based on the truth of a set of premises.

Your goal with a proof is to convince a mathematically literate person that your conclusion follows from your premises. As we stated last week, many of your proofs will be done in the field of number theory, but these fundamental ideas apply to all mathematics and we may test your ability to make reasoned logical arguments about other fields.

In this class, every proof has three components; a preamble, a body, and conclusion.

Preamble: Here you introduce and contextualize your proof, stating information like the type of proof used (direct, contradiction, contrapositive, etc), key assumptions you're using, your want to prove statement, and/or key predicate/quantifications you'll be using.

Body: This is where you manipulate your premises to produce your conclusion. Be sure to define variables and cite theorems/laws/axioms as you rely on them.

Conclusion: Restate your conclusion and how you came upon it. This can seem unnecessary and redundant for simple direct proofs but is good form in general and legitimately useful for longer, more complex proofs.

Make a concious effort to understand and use these components. Not only is it stylistically correct, but we will explain other proof types in context of this general framework.

We now go over some miscellaneous terminology we may use which you should be aware of...

Axioms: Fundamental underlying objects that form the basis of a theory or field of knowledge.

Theorem: A statement that is proven. Much of this class is stating/proving theorems.

Lemma: A smaller theorem used in context of proving a larger theorem.

QED: Sometimes stylized as □ or ■, it stands for Quod Erat Demonstrandum, latin for "thus it is proven." Also, its cool.

WLOG: "without loss of generality". Used to take advantage of symmetries in logic to shorten proofs. Be careful not to abuse this.

example of this upcoming

DIRECT PROOF

This is the "standard proof". Again, any proof is the verification of a conclusion c based off the assumption that a number of premises $p_1, \dots, p_n$ hold. That is...

$$p_1 \land p_2 \land \dots \land p_n \Rightarrow c$$

A direct proof follows this implication exactly, as opposed to other types of proofs which instead prove a logically equivalent but symbolically different statement. An example:

Prove that the summation of an odd and even integer is odd.

We use a direct proof to show that for two integers a, b one odd, one even, $a + b = c$ is odd.

WLOG, assume a is even and b is odd. That is, by the definition of parity

$$\exists m \in \mathbb{Z},\ a = 2m \qquad \exists n \in \mathbb{Z},\ b = 2n+1$$

Then, $c = a + b = 2m + 2n + 1 = 2(m+n) + 1$

By closure $m+n$ is an integer.

Thus, $\exists m+n \in \mathbb{Z},\ c = 2(m+n) + 1 \Leftrightarrow c$ is odd.

QED

PRACTICE

Prove that the product of two odd integers is odd.

We use a direct proof to show that for two odd integers a & b, $a \cdot b = c$ is odd.

a & b are odd. That is...

$$\exists m \in \mathbb{Z},\ a = 2m+1 \qquad \exists n \in \mathbb{Z},\ b = 2n+1$$

Then, $c = a \cdot b = (2m+1)(2n+1) = 4mn + 2m + 2n + 1$

$$c = 2(2mn + m + n) + 1$$

By closure $2mn + m + n = r$ is an integer.

Thus, $\exists r \in \mathbb{Z},\ c = 2r + 1 \iff c$ is odd.

QED

Prove closure of rationals under addition.

We use a direct proof to show that $\forall x, y \in \mathbb{Q},\ x + y \in \mathbb{Q}$.

Note, the rationals are defined to be...

$$\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z} \wedge b \neq 0\}$$

$x, y \in \mathbb{Q}$. That is...

$x = \frac{a}{b} \wedge y = \frac{c}{d}$ s.t. $a, b, c, d \in \mathbb{Z} \wedge b, d \neq 0$

Then, $x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$

Note, $ad + bc \in \mathbb{Z}$ by closure, and $bd \in \mathbb{Z}$ by closure $b \neq 0 \wedge d \neq 0 \Rightarrow bd \neq 0$.

Therefore, $x + y \in \mathbb{Q}$.

QED

$a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow ac \equiv bd \pmod{n}$

We prove this via a direct proof. By definition of mod,

$$a = b + k_1 n \quad \wedge \quad c = d + k_2 n \quad \text{for} \quad k_1, k_2 \in \mathbb{Z}$$

Then,

$$ac = (b + k_1 n)(d + k_2 n) = bd + bk_2 n + dk_1 n + k_1 k_2 n^2$$

$$ac = bd + (bk_2 + dk_1 + k_1 k_2 n)\, n$$

$bk_2 + dk_1 + k_1 k_2 n \in \mathbb{Z}$ by closure of integers. Thus, by the definition of mod,

$$ac \equiv bd \pmod{n}$$

QED

The summation of any four consecutive numbers is equivalent mod 4 to 2.

We prove this via a direct proof. Note that the summation of 4 integers can be represented as

$$n + (n+1) + (n+2) + (n+3) \quad \text{for some} \quad n \in \mathbb{Z}$$

$$= 4n + 6$$

$$= 2 + 4(n+1)$$

Since $n+1 \in \mathbb{Z}$ by closure of integers, the summation is $\equiv 2 \pmod{4}$

$$\therefore \sum_{i=0}^{3} n+i \equiv 2 \pmod{4}$$

QED