02/28/2022

→ GENERAL PROOF INFO
→ PROOF BY CONTRAPOSITIVE/CONTRADICTION

At this point you're familiar with the structure of proofs and have seen examples of direct proofs. Here's a recap of some of the proofs we went through last discussion:

The summation of an odd and even integer is odd.

$$\forall x \in \mathbb{Z}^{EVEN}, \forall y \in \mathbb{Z}^{ODD}, \; x+y \in \mathbb{Z}^{ODD}$$

The product of two odd integers is odd.

$$\forall x,y \in \mathbb{Z}^{ODD}, \; xy \in \mathbb{Z}^{ODD}$$

Closure of rationals under addition.

$$\forall x,y \in \mathbb{Q}, \; x+y \in \mathbb{Q}$$

Note when these theorems are represented via predicates and quantifiers, they all use universal quantifiers, and our approach was to define arbitrary elements in-keeping with the quantification which we then manipulated to reach our conclusion. For lack of a better descriptor, lets call this approach a standard proof for this discussion only.

Generally speaking, standard proofs are the approach to use when proving universall-quantified statements, although for small finite sets a proof by exhaustion may be feasible. However, we may instead wish to disprove a statement, and said statement may instead be existentially-quantified. In these instances it may be appropriate to use a proof by example. We summarize this below:

QUANTIFIER \ GOAL	PROVE	DISPROVE
$\forall$	standard	example
$\exists$	example	standard

We should note, it is not actually neccessary to find the element that satisfies the statement when using a proof by example, simply show that it must exist.

PROOF BY CONTRAPOSITIVE

Recall that any proof is the verification of a conclusion c based off the assumption that a number of premises $p_1, \dots, p_n := P$ hold. That is...

$$P \Rightarrow c$$

However, you may run into instances where proving this directly is difficult. In these instances, we can take advantage of laws of equivalence to prove a logically equivalent but symbolically different statement that is easier to prove. As the name suggests, in a **proof by contrapositive** we use the fact that an implication is equivalent to its contrapositive:

$$P \Rightarrow c \equiv \neg c \Rightarrow \neg P \equiv \neg c \Rightarrow (\neg p_1 \vee \neg p_2 \vee \dots \vee \neg p_n)$$

That is if c does not hold then at least one of the premises did not hold.

PROOF BY CONTRADICTION

Proofs by Contradiction are similar to proofs by contrapositive in that you prove a logically equivalent but symbolically different statement. In this instance, it is more intuitive to think of the conclusion c as a stand-alone statement we wish to prove:

$$c \equiv 1 \Rightarrow c \equiv \neg c \Rightarrow 0$$

In other words, if we show that the statement c not holding implies a contradiction 0, then we have proven that c must be true.

We now go to an example proof that utilizes contradiction / contrapositive.

Prove that $\sqrt{2}$ is irrational.

We prove this via a proof by contradiction. That is, we assume that $\sqrt{2} \in \mathbb{Q}$ and show this implies a contradiction.

By the definition of a rational number:

$$\sqrt{2} = p/q \quad \text{s.t} \quad p, q \in \mathbb{Z} \wedge q \neq 0$$

Additionally, we assert that p/q is in simplest form i.e they share no common factors.

Note that any rational can be put into simplest form by cancelling out common factors until none remain, so this is a totally valid condition for us to assert.

Then,

$$\sqrt{2} = p/q \Rightarrow 2 = p^2/q^2 \Rightarrow p^2 = 2q^2$$

Note that $q^2 \in \mathbb{Z}$ by closure, so $p^2 \in \mathbb{Z}^{EVEN}$

LEMMA: If n^2 is even for some integer n, then n is even.

We prove this via a proof by contrapositive, that is we show that $n \in \mathbb{Z}^{ODD} \Rightarrow n^2 \in \mathbb{Z}^{ODD}$

$$n \in \mathbb{Z}^{ODD} \iff \exists k \in \mathbb{Z}, \; n = 2k+1$$

Then, $n^2 = (2k+1)^2 = 4k^2 + 2k + 2k + 1 = 2(2k^2 + 2k) + 1$

Because $2k^2 + 2k \in \mathbb{Z}$ by closure, $n^2 \in \mathbb{Z}^{ODD}$ by definition of parity.

Again, $p^2 \in \mathbb{Z}^{EVEN} \Rightarrow p \in \mathbb{Z}^{EVEN}$ by the lemma.

Note, $p \in \mathbb{Z}^{EVEN} \iff \exists m \in \mathbb{Z}, \; p = 2m$

so, $p^2 = 2q^2 \Rightarrow (2m)^2 = 2q^2 \Rightarrow 4m^2 = 2q^2 \Rightarrow 2m^2 = q^2$

$m^2 \in \mathbb{Z}$ by closure $\Rightarrow q^2 \in \mathbb{Z}^{EVEN}$ by definition of parity

$\Rightarrow q \in \mathbb{Z}^{EVEN}$ by the lemma

Thus $p, q \in \mathbb{Z}^{EVEN}$. However, this means they share 2 as a common factor and we asserted that p/q was in simplest form. $\therefore$ this is a contradiction.

$\sqrt{2} \in \mathbb{Q} \Rightarrow \Leftarrow$, thus we have shown by contradiction that $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$.

QED.

Some key takeaways from this proof:

- → note the appropriate usage of a lemma
- → note how we stated we were using a proof by contradiction / contrapositive in our preambles
- → note how we were sure to point out that these indirect proofs did indeed prove our statement in the conclusions

PRACTICE

Prove that if $x^3 - x > 0$, then $x > -1$

We prove this via a proof by contrapositive, that is, we show that

$$x \leq -1 \Rightarrow x^3 - x \leq 0$$

CASE 1: $x = -1$

Then, $x^3 - x = 0 \leq 0$

CASE 2: $x < -1$

Then, $x^3 - x = x(x^2 - 1)$ i.e the product of a negative and positive which is negative.

Thus we have shown that $x^3 - x > 0 \Rightarrow x > 0$ by proving its contrapositive.

QED

Prove $\forall a \in \mathbb{Z}$, $a \not\equiv 0 \pmod 4 \Rightarrow a \not\equiv 0 \pmod 8$

We prove this via a proof by contrapositive. That is, we show that

$$\forall a \in \mathbb{Z}, \quad a \equiv 0 \pmod 8 \Rightarrow a \equiv 0 \pmod 4$$

By the definition of mod,

$$a \equiv 0 \pmod 8 \Leftrightarrow \exists k \in \mathbb{Z}, \ a = 0 + 8k$$

$$a = 0 + 8k \Rightarrow a = 0 + 4(2k)$$

$2k \in \mathbb{Z}$ by closure, so by the definition of mod,

$$a \equiv 0 \pmod 4$$

Thus we have shown that $a \equiv 0 \pmod 8 \Rightarrow a \equiv 0 \pmod 4$ by proving its contrapositive.

QED

You are given that $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ are all irrational. Prove that $\sqrt{2}+\sqrt{3}$ is also irrational.

We prove this via a proof by contradiction, that is we show that $\sqrt{2}+\sqrt{3} \in \mathbb{Q}$ implies a contradiction.

By the definition of the rationals,

$$\sqrt{2}+\sqrt{3} = a/b \quad \text{s.t} \quad a, b \in \mathbb{Z} \wedge b \neq 0$$

We square both sides to attain...

$$(\sqrt{2}+\sqrt{3})^2 = 2 + 2\sqrt{6} + 3 = a^2/b^2 \Rightarrow \sqrt{6} = 1/2(a^2/b^2 - 5)$$

Note that $1/2(a^2/b^2 - 5) \in \mathbb{Q}$ by closure. So, $\sqrt{6} \in \mathbb{Q}$. But we now that $\sqrt{6} \in \mathbb{R} \setminus \mathbb{Q}$. This is a contradiction.

Thus we have shown that $\sqrt{2}+\sqrt{3} \in \mathbb{R} \setminus \mathbb{Q}$ because $\sqrt{2}+\sqrt{3} \in \mathbb{Q} \Rightarrow \Omega$.

QED

Prove that any composite number has at least one factor less than or equal to its square root.

We prove this via a proof by contradiction, that is we show that if an integer n had factors $f_1, \ldots, f_k$ all greater than $\sqrt{n}$, this would imply a contradiction.

$$n = \prod_{i=1}^{k} f_i \wedge \forall i \in \{1, \ldots k\}, f_i > \sqrt{n} \Rightarrow n > \sqrt{n}^k$$

Because n is composite, $k \geq 2$ so $\sqrt{n}^k \geq n$. Thus, $n > n$ which is clearly a contradiction.

$\therefore$, we have proved that any composite number has at least one factor less than its square root.

QED