Book of Proof: Part II, Conditionals

January 22, 2018

Proofs

Theorem	Something important you want to prove.
Proposition	Something not so important you want to prove.
Corollary	Something you want to prove in order to prove something else.

Definitions

Definition 4.1 An integer n is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.

Definition 4.1 An integer n is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.

Definition 4.3 Two integers have the **same parity** if they are both even or they are both odd. Otherwise they have **opposite parity**.

Definition 4.4 Suppose a and b are integers. We say that a **divides** b, written $a \mid b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a **divisor** of b, and that b is a **multiple** of a.

Definition 4.5 A natural number n is **prime** if it has exactly two positive divisors, 1 and n.

Definitions

Definition 4.6 The **greatest common divisor** of integers a and b, denoted $\gcd(a, b)$, is th largest integer that divides both a and b. The **least common multiple** of non-zero integers a and b, denoted $\operatorname{lcm}(a, b)$, is the smallest positive integer that is a multiple of both a and b.

$$\gcd(18, 24) = 6 \qquad \gcd(5, 5) = 5$$
$$\gcd(32, -8) = 8 \qquad \gcd(50, 18) = 2$$
$$\gcd(50, 9) = 1 \qquad \gcd(0, 6) = 6$$
$$\gcd(0, 0) = \text{undefined}$$
$$\operatorname{lcm}(4, 6) = 12 \qquad \operatorname{lcm}(7, 7) = 7$$

Some facts accepted without proof

If $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$, $a - b \in \mathbb{Z}$, $ab \in \mathbb{Z}$.

The Division Algorithm Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.

Every natural number greater than 1 has a unique factorization into primes.

Direct Proof

If P, then Q.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Outline for Direct Proof

Proposition If P, then Q.

Proof. Suppose P.

$\vdots$

Therefore, Q. ■

Example proof development

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.

$\vdots$

Therefore x^2 is odd, *for some reason.* $\blacksquare$

Example proof development

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.

Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.

$\vdots$

Therefore x^2 is odd, *for some reason.* ■

Example proof development

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.

Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.

$\vdots$

Thus $x^2 = 2b + 1$ for an integer b, *for some reason.*

Therefore x^2 is odd, by definition of an odd number. ■

Example proof development

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.
Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.
Thus

$$\begin{aligned} x^2 &= (2a+1)^2 && \text{by substitution} \\ &= 4a^2 + 4a + 1 && \text{by algebra} \\ &= 2(2a^2 + 2a) + 1 && \text{by algebra} \end{aligned}$$

If we let $b = 2a^2 + 2a$ then b is an integer, by math facts.
Thus $x^2 = 2b + 1$ for an integer b, by substitution.
Therefore x^2 is odd, by definition of an odd number. ∎

Example proof development

Proposition Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Example proof development

Proposition Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof.

$\vdots$

$\blacksquare$

Example proof development

Proposition Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.

$\vdots$

Therefore $a \mid c$ ∎

Example proof development

Proposition Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.
By definition, $a \mid b$ means there exists $d \in \mathbb{Z}$ with

$$b = ad$$

By definition, $b \mid c$ means there exists $e \in \mathbb{Z}$ with

$$c = be$$

$\vdots$

Thus $c = ax$ for some $x \in \mathbb{Z}$.
Therefore $a \mid c$, by definition. ∎

Example proof development

Proposition Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.
By definition, $a \mid b$ means there exists $d \in \mathbb{Z}$ with

$$b = ad$$

By definition, $b \mid c$ means there exists $e \in \mathbb{Z}$ with

$$c = be$$

By combining equations these two equations, we get

$$c = be = (ad)e = a(de)$$

Let $x = de$, then $x \in \mathbb{Z}$.
Thus $c = ax$ for some $x \in \mathbb{Z}$.
Therefore $a \mid c$, by definition. ∎

Proof by cases

Proposition If $n \in \mathbb{Z}$ then $1 + (-1)^n(2n-1)$ is a multiple of 4.
Proof. Suppose $n \in \mathbb{Z}$.
Then n is either even or odd.
Case 1. Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$ and $(-1)^n = 1$. Thus

$$1 + (-1)^n(2n-1) = 1 + (1)(2 \cdot 2k - 1) = 4k$$

which is a multiple of 4.
Case 2. Suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$ and $(-1)^n = -1$. Thus

$$1 + (-1)^n(2n-1) = 1 - (2(2k+1) - 1) = -4k$$

which is a multiple of 4.
These cases show that $1 + (-1)^n(2n-1)$ is always a multiple of 4.

Without loss of generality

Proposition If two integers have opposite parity, then their sum is odd.

Proof. Suppose m and n are integers with opposite parity.
Without loss of generality, suppose m is even and n is odd.
Thus $m = 2a$ and $n = 2b + 1$ for some $a, b \in \mathbb{Z}$.
Therefore $m + n = 2a + 2b + 1 = 2(a + b) + 1$, which is odd by definition.

Contrapositive Proof

If P, then Q.
If $\sim Q$, then $\sim P$.

P	Q	$\sim Q$	$\sim P$	$P \Rightarrow Q$	$\sim Q \Rightarrow \sim P$
T	T	F	F	T	T
T	F	T	F	F	F
F	T	F	T	T	T
F	F	T	T	T	T

$$(P \Rightarrow Q) \iff (\sim Q \Rightarrow \sim P)$$

Contrapositive Proof

Outline for Contrapositive Proof

Proposition If P, then Q.
Proof. Suppose $\sim Q$.
$\vdots$
Therefore, $\sim P$. $\blacksquare$

Example Contrapositive Proof

Proposition Suppose $x \in \mathbb{Z}$. If $7x + 9$ is even, then x is odd.
Proof. (Contrapositive)
Suppose x is not odd.
Thus x is even, and $x = 2a$ for some $a \in \mathbb{Z}$.
Then $7x + 9 = 7(2a) + 9 = 14a + 8 + 1 = 2(7a + 4) + 1$.
Thus $7x + 9 = 2b + 1$ where b is the integer $7a + 1$.
By definition, $7x + 9$ is odd.
Therefore $7x + 9$ is not even.

Congruence of Integers

Definition 5.1 Given $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, we say that a and b are **congruent modulo** n if $n \mid (a - b)$. We express this as $a \equiv b \pmod{n}$.

Example 5.1

1. $9 \equiv 1 \pmod 4$ because $4 \mid (9 - 1)$.
2. $6 \equiv 10 \pmod 4$ because $4 \mid (6 - 10)$.
3. $14 \not\equiv 8 \pmod 4$ because $4 \nmid (14 - 8)$.
4. $20 \equiv 4 \pmod 8$ because $8 \mid (20 - 4)$.
5. $17 \equiv (-4) \pmod 3$ because $3 \mid (17 - (-4))$.

They have the same remainder upon division by n.

Proof of Congruence

Proposition If $a \equiv b \pmod{n}$ then $a^2 \equiv b^2 \pmod{n}$.
Proof. Suppose $a \equiv b \pmod{n}$.
By definition, $n \mid (a - b)$.
By definition, $a - b = nc$ for some $c \in \mathbb{Z}$.

$$\begin{aligned} a - b &= nc \\ (a-b)(a+b) &= nc(a+b) \\ a^2 - b^2 &= nc(a+b) \end{aligned}$$

Since $c(a+b) \in \mathbb{Z}$, this tells us that $n \mid (a^2 - b^2)$.
By definition, $a^2 \equiv b^2 \pmod{n}$.

Proof by Contradiction

P	C	$\sim P$	$C \wedge \sim C$	$(\sim P) \Rightarrow (C \wedge \sim C)$
T	T	F	F	T
T	F	F	F	T
F	T	T	F	F
F	F	T	F	F

Outline for Proof by Contradiction

Proposition P.

Proof. Suppose $\sim P$.

$\vdots$

Therefore, $C \wedge \sim C$. ■

Example Proof by Contradiction

Proposition If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.
Proof. Suppose this is false.

Example Proof by Contradiction

Proposition If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.
Proof. Suppose this is false.
There exist $a, b \in \mathbb{Z}$ with $a^2 - 4b = 2$.

Example Proof by Contradiction

Proposition If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.
Proof. Suppose this is false.
There exist $a, b \in \mathbb{Z}$ with $a^2 - 4b = 2$.
Then $a^2 = 4b + 2 = 2(2b + 1)$, is even.

Example Proof by Contradiction

Proposition If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.
Proof. Suppose this is false.
There exist $a, b \in \mathbb{Z}$ with $a^2 - 4b = 2$.
Then $a^2 = 4b + 2 = 2(2b + 1)$, is even.
So a is even, so $a = 2c$ for some $c \in \mathbb{Z}$.

Example Proof by Contradiction

Proposition If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.
Proof. Suppose this is false.
There exist $a, b \in \mathbb{Z}$ with $a^2 - 4b = 2$.
Then $a^2 = 4b + 2 = 2(2b + 1)$, is even.
So a is even, so $a = 2c$ for some $c \in \mathbb{Z}$.

$$\begin{aligned} (2c)^2 - 4b &= 2 \\ 4c^2 - 4b &= 2 \\ 2c^2 - 2b &= 1 \\ 2(c^2 - b) &= 1 \end{aligned}$$

Example Proof by Contradiction

Proposition If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.
Proof. Suppose this is false.
There exist $a, b \in \mathbb{Z}$ with $a^2 - 4b = 2$.
Then $a^2 = 4b + 2 = 2(2b + 1)$, is even.
So a is even, so $a = 2c$ for some $c \in \mathbb{Z}$.

$$\begin{aligned}(2c)^2 - 4b &= 2 \\ 4c^2 - 4b &= 2 \\ 2c^2 - 2b &= 1 \\ 2(c^2 - b) &= 1\end{aligned}$$

But $c^2 - b \in \mathbb{Z}$.

Example Proof by Contradiction

Proposition If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.
Proof. Suppose this is false.
There exist $a, b \in \mathbb{Z}$ with $a^2 - 4b = 2$.
Then $a^2 = 4b + 2 = 2(2b + 1)$, is even.
So a is even, so $a = 2c$ for some $c \in \mathbb{Z}$.

$$\begin{aligned} (2c)^2 - 4b &= 2 \\ 4c^2 - 4b &= 2 \\ 2c^2 - 2b &= 1 \\ 2(c^2 - b) &= 1 \end{aligned}$$

But $c^2 - b \in \mathbb{Z}$.
Which implies that 1 is even, which is a contradiction. ∎

Compare Contrapositive with Contradiction

Outline for Contrapositive Proof

Proposition If P, then Q.

Proof. Suppose $\sim Q$.

$\vdots$

Therefore, $\sim P$. $\blacksquare$

Outline for Proof by Contradiction

Proposition P.

Proof. Suppose $\sim P$.

$\vdots$

Therefore, $C \wedge \sim C$. $\blacksquare$

Proving a Conditional Statement with Contradiction

Proposition If P, then Q.

Proof. Suppose P and $\sim Q$.

$\vdots$

Therefore, $C \wedge \sim C$. ■

Example

Proposition Suppose $a \in \mathbb{Z}$. If a^2 is even, then a is even.
Proof. Suppose a^2 is even and a is not even.
Then a is odd.
Then $a = 2c + 1$ for some $c \in \mathbb{Z}$.
Then

$$\begin{aligned} a^2 &= (2c+1)^2 \\ &= 4c^2 + 4c + 1 \\ &= 2(2c^2 + 2c) + 1 \end{aligned}$$

Then a^2 is odd.
Thus a^2 is even and odd, which is a contradiciton. ∎

Example

Proposition If $a, b \in \mathbb{Z}$ and $a \geq 2$, then $a \nmid b$ or $a \nmid (b+1)$.
Proof. Suppose $a, b \in \mathbb{Z}$ with $a \geq 2$ and it is not true that $a \nmid b$ or $a \nmid (b+1)$.
Then $a \mid b$ and $a \mid (b+1)$.
Then there are $c, d \in \mathbb{Z}$ with $b = ac$ and $b + 1 = ac$.
Subtracting the equations gives

$$\begin{aligned} 1 &= ad - ac \\ &= a(d - c) \end{aligned}$$

Since a is positive, $d - c$ is positive. So

$$a = 1/(d - c) < 2$$

Therefore $a \geq 2$ and $a < 2$, a contradiction. $\blacksquare$

Example

Proposition Every non-zero rational number can be expressed as a product of two irrational numbers.

Proof. Reword the proposition: If r is a non-zero rational number, then r is the product of two irrational numbers.

Suppose r is a non-zero rational number.

Then $r = a/b$ for $a, b \in \mathbb{Z}$. Also, $r = \sqrt{2}(r/\sqrt{2})$.

We know $\sqrt{2}$ is irrational, so we need to prove that $r/\sqrt{2}$ is irrational.

To show this, assume $r/\sqrt{2}$ is rational. Then $r/\sqrt{2} = c/d$ for some $c, d \in \mathbb{Z}$.

So

$$\sqrt{2} = r\frac{d}{c} = \frac{a}{b}\frac{d}{c} = \frac{ad}{bc}$$

Which means $\sqrt{2}$ is rational, which is a contradiction.

Therefore $r/\sqrt{2}$ is irrational.

Therefore $r = \sqrt{2} \cdot r/\sqrt{2}$ is a product of two irrational numbers. ∎