Part II: Proving Conditional Statements

Ch. 4: Direct Proof

§4.1 Theorems

Def: **Theorem** is mathematical statement that can be & has been verified as true.
Proof is written verification/argument showing that theorem is unquestionably true.
Definition is exact, unambiguous explanation of meaning of word or phrase.

$$\begin{array}{ccccc} & & \text{Theorem} & & \\ & \nearrow & & \searrow & \\ \text{Lemma} & & \text{Proposition} & & \text{Corollary} \end{array} \left.\vphantom{\begin{array}{c}a\\a\\a\end{array}}\right\} \text{All theorems}$$

§4.2 Definitions

Q: How do you know 12 is even?

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

12, -52, 0

Definition 4.2 An integer n is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.

7, -13

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

Note: Definitions are biconditional ($\Longleftrightarrow$) even when phrased otherwise.

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.

$6 \mid 18$, $3 \nmid 10$

e.g. Divisors of 42: $\{a \in \mathbb{Z} : a \mid 42\} = \{1, 2, 3, 6, 7, 14, 21, 42, -1, -2, -3, -6, -7, -14, -21, -42\}$

ex. What are the divisors of 0? $\mathbb{Z}$.

Definition 4.5 A number $n \in \mathbb{N}$ is **prime** if it has exactly two positive divisors, 1 and n. If n has more than two positive divisors, it is called **composite**. (Thus n is composite if and only if $n = ab$ for $1 < a, b < n$.)

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

Definition 4.6 The **greatest common divisor** of integers a and b, denoted $\gcd(a,b)$, is the 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 integer in $\mathbb{N}$ that is a multiple of both a and b.

ASSUME a, b NOT BOTH 0

$\gcd(0,5) = 5$

Fact 4.1 If a and b are integers, then so are their sum, product and difference. That is, if $a, b \in \mathbb{Z}$, then $a+b \in \mathbb{Z}$, $a-b \in \mathbb{Z}$ and $ab \in \mathbb{Z}$.

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

e.g. GIVEN 5, 17 : $17 = 3 \cdot 5 + 2 \quad (0 \le 2 < 5)$

$5 = 0 \cdot 17 + 5 \quad (0 \le 5 < 17)$

§4.3 DIRECT PROOF

HOW TO PROVE $P \Rightarrow Q$

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

IF P IS TRUE, Q MUST BE TRUE.

IF P IS FALSE, NOTHING TO PROVE.

Outline for Direct Proof

Proposition If P, then Q.

BEGINNING *Proof.* Suppose P.

⋮ ← LOGIC, DEFINITIONS, STANDARD MATH, ETC.

Therefore Q. ■ END

ex. THEOREM. THE PRODUCT OF TWO ODD INTEGERS IS ODD.

PROOF.

START ASSUME $x, y \in \mathbb{Z}$ ARE ODD.

DEF BY DEF, $x = 2a+1$, $y = 2b+1$ FOR SOME $a, b \in \mathbb{Z}$.

DIRECT PROOF

THEN $xy = (2a+1)(2b+1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1$.

SET $c = 2ab + a + b$.

DEF THEN $xy = 2c + 1$.

END THEREFORE, xy IS ODD. ■

ex. **COROLLARY.** IF x IS AN ODD INTEGER THEN x^2 IS ODD.

PROOF. SINCE $x^2 = x \cdot x$ IS THE PRODUCT OF TWO ODD INTEGERS, THIS FOLLOWS IMMEDIATELY FROM THE PREVIOUS THEOREM. ■

ex.

Proposition Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.
By Definition 4.4, we know $a \mid b$ means $b = ad$ for some $d \in \mathbb{Z}$.
Likewise, $b \mid c$ means $c = be$ for some $e \in \mathbb{Z}$.
Thus $c = be = (ad)e = a(de)$, so $c = ax$ for the integer $x = de$.
Therefore $a \mid c$. ■

STRATEGY: TO SHOW $m = n$, SHOW (1) $m \le n$ (2) $n \le m$

ex.

Proposition If $a, b, c \in \mathbb{N}$, then $\text{lcm}(ca, cb) = c \cdot \text{lcm}(a, b)$.

PROOF: ASSUME $a, b, c \in \mathbb{N}$.
LET $m = \underbrace{\text{LCM}(ca, cb)}$ & $n = c \cdot \underbrace{\text{LCM}(a, b)}$

$m = cau = cbv$, $u, v \in \mathbb{N}$ $\qquad$ $\underbrace{= ax = by}$, $x, y \in \mathbb{N}$

$\frac{1}{c} m = au = bv$ $\qquad$ $n = (ca)x = (cb)y$

$\therefore \frac{1}{c} m$ IS A MULTIPLE OF a & b. $\qquad$ $\therefore n$ IS POS. MULT. OF ca & cb.

BY DEF, $\text{LCM}(a, b) \le \frac{1}{c} m$ $\qquad$ BY DEF, $m \le n$

$c \cdot \text{LCM}(a, b) \le m$

$n \le m$

$\therefore (m \le n) \wedge (n \le m) \Rightarrow (m = n)$ ■

P

Proof. Assume $a, b, c \in \mathbb{N}$. Let $m = \text{lcm}(ca, cb)$ and $n = c \cdot \text{lcm}(a, b)$. We will show $m = n$. By definition, $\text{lcm}(a, b)$ is a positive multiple of both a and b, so $\text{lcm}(a, b) = ax = by$ for some $x, y \in \mathbb{N}$. From this we see that $n = c \cdot \text{lcm}(a, b) = cax = cby$ is a positive multiple of both ca and cb. But $m = \text{lcm}(ca, cb)$ is the *smallest* positive multiple of both ca and cb. Thus $m \le n$.

On the other hand, as $m = \text{lcm}(ca, cb)$ is a multiple of both ca and cb, we have $m = cax = cby$ for some $x, y \in \mathbb{Z}$. Then $\frac{1}{c} m = ax = by$ is a multiple of both a and b. Therefore $\text{lcm}(a, b) \le \frac{1}{c} m$, so $c \cdot \text{lcm}(a, b) \le m$, that is, $n \le m$.

We've shown $m \le n$ and $n \le m$, so $m = n$. The proof is complete. ■

ex. **Proposition** Let x and y be positive numbers. If $x \le y$, then $\sqrt{x} \le \sqrt{y}$.

PROOF: ASSUME $x \le y$

THEN $x - y \le 0$

$\underbrace{(\sqrt{x} + \sqrt{y})}_{\text{POS. BY DEF}}(\sqrt{x} - \sqrt{y}) \le 0$

P

$\therefore \sqrt{x} - \sqrt{y} \le 0$

THUS $\sqrt{x} \le \sqrt{y}$ ■

STRATEGY: REWRITE EQ'S / INEQUALITIES TO DEVELOP IDEA FOR PROOF.

Proof. Suppose $x \le y$. Subtracting y from both sides gives $x - y \le 0$.
This can be written as $\sqrt{x}^2 - \sqrt{y}^2 \le 0$.
Factor this as a difference of two squares to get $(\sqrt{x} - \sqrt{y})(\sqrt{x} + \sqrt{y}) \le 0$.
Dividing both sides by the positive number $\sqrt{x} + \sqrt{y}$ produces $\sqrt{x} - \sqrt{y} \le 0$.
Adding $\sqrt{y}$ to both sides gives $\sqrt{x} \le \sqrt{y}$. ■

ex. **9.** Suppose a is an integer. If $7 \mid 4a$, then $7 \mid a$.

Proof. Suppose $7 \mid 4a$.
By definition of divisibility, this means $4a = 7c$ for some integer c.
Since $4a = 2(2a)$ it follows that $4a$ is even, and since $4a = 7c$, we know $7c$ is even.
But then c can't be odd, because that would make $7c$ odd, not even.
Thus c is even, so $c = 2d$ for some integer d.
Now go back to the equation $4a = 7c$ and plug in $c = 2d$. We get $4a = 14d$.
Dividing both sides by 2 gives $2a = 7d$.
Now, since $2a = 7d$, it follows that $7d$ is even, and thus d cannot be odd.
Then d is even, so $d = 2e$ for some integer e.
Plugging $d = 2e$ back into $2a = 7d$ gives $2a = 14e$.
Dividing both sides of $2a = 14e$ by 2 produces $a = 7e$.
Finally, the equation $a = 7e$ means that $7 \mid a$, by definition of divisibility. ■

ex. **26.** Every odd integer is a difference of two squares. (Example $7 = 4^2 - 3^2$, etc.)

PROOF: ASSUME n IS AN ODD INTEGER.
BY DEFINITION, $n = 2k+1$ FOR SOME $k \in \mathbb{Z}$.
SINCE $2k+1 = k^2 + 2k + 1 - k^2 = (k+1)^2 - k^2$
THEREFORE $n = a^2 - b^2$, WITH $b = k \in \mathbb{Z}$, $a = k+1 \in \mathbb{Z}$. ■

§ 4.4 Using Cases

ex. **16.** If two integers have the same parity, then their sum is even. (Try cases.)

Proof: Assume $x, y \in \mathbb{Z}$ have same parity.

Case 1: x, y both even. Then $x = 2a$, $y = 2b$, $a, b \in \mathbb{Z}$.
Then $x + y = 2a + 2b = 2(a+b) = 2c$, with $c \in \mathbb{Z}$.
$\therefore$ $x+y$ is even.

Case 2: x, y both odd. Then $x = 2a+1$, $y = 2b+1$, $a, b \in \mathbb{Z}$.
Then $x+y = 2a+1+2b+1 = 2(a+b+1) = 2c$, $c = a+b+1 \in \mathbb{Z}$.
$\therefore$ $x+y$ is even.

Thus, in either case, $x+y$ is even. ∎

Typical Cases:

- Pos / Neg / 0
- Empty set / Non-empty set
- Even / Odd
- Abs value < 1, $= 1$, > 1

§ 4.5 Similar Cases

ex. **17.** If two integers have opposite parity, then their product is even.

Proof: Assume $x, y \in \mathbb{Z}$ have opposite parity.

(W.L.O.G.) Without loss of generality, let $x = 2a$, $y = 2b+1$, $a, b \in \mathbb{Z}$.

Then $xy = (2a)(2b+1) = 2[a(2b+1)] = 2c$ with $c = a(2b+1) \in \mathbb{Z}$.
Therefore, xy is even. ∎