Mathematical Proofs
A Transition to Advanced Mathematics

Chapter 4
More on Direct Proof and Proof by Contrapositive

Gary Chartrand Albert D. Polimeni Ping Zhang

Proofs Involving Divisibility of Integers

Divisibility of Integers

For integers a and b with $a \neq 0$, a is said to **divide** b (written $a \mid b$) if $b = ac$ for some integer c.

If a does not divide b, then we write $a \nmid b$.

$7 \mid 21$ since $21 = 7(3)$ and $6 \mid (-30)$ since $-30 = 6(-5)$.

$4 \nmid 42$ since there is no integer c such that $42 = 4c$.

If $a \mid b$, then a is a **divisor** of b and b is a **multiple** of a.

Proofs Involving Divisibility of Integers

Example 1

Result Let a, b and c be integers with $a \neq 0$ and $b \neq 0$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Assume that $a \mid b$ and $b \mid c$. Then $b = ax$ and $c = by$, where $x, y \in \mathbf{Z}$. Therefore,

$$c = by = (ax)y = a(xy).$$

Since xy is an integer, $a \mid c$. □

Example 2

Result Let $x \in \mathbf{Z}$. If $2 \mid (x^2 - 1)$, then $4 \mid (x^2 - 1)$.

Proof. Assume that $2 \mid (x^2 - 1)$. So $x^2 - 1 = 2y$ for some integer y. Thus, $x^2 = 2y + 1$ is an odd integer. It follows that x too is odd. Hence, $x = 2z + 1$ for some integer z. Then

$$\begin{aligned} x^2 - 1 &= (2z + 1)^2 - 1 = (4z^2 + 4z + 1) - 1 \\ &= 4z^2 + 4z = 4(z^2 + z). \end{aligned}$$

Since $z^2 + z$ is an integer, $4 \mid (x^2 - 1)$. □

Example 3

Result Let $n \in \mathbf{Z}$. If $5 \nmid (n^2+4)$, then $5 \nmid (n-1)$ and $5 \nmid (n+1)$.

Proof. Assume that $5 \mid (n-1)$ or $5 \mid (n+1)$. We consider these two cases.

Case 1. $5 \mid (n-1)$. Then $n-1 = 5a$ for some integer a. So, $n = 5a+1$. Hence,

$$\begin{aligned} n^2+4 &= (5a+1)^2+4 = (25a^2+10a+1)+4 \\ &= 5(5a^2+2a+1). \end{aligned}$$

Since $5a^2+2a+1 \in \mathbf{Z}$, it follows that $5 \mid (n^2+4)$.

Example 3 (continued)

Case 2. $5 \mid (n+1)$. Then $n+1 = 5b$, where $b \in \mathbf{Z}$, and so $n = 5b-1$. Hence,

$$\begin{aligned} n^2+4 &= (5b-1)^2+4 = (25b^2-10b+1)+4 \\ &= 5(5b^2-2b+1). \end{aligned}$$

Since $5b^2-2b+1 \in \mathbf{Z}$, it follows that $5 \mid (n^2+4)$. □

Even and Odd Integers

If n is an **even integer**, then $n = 2q$ for some integer q.
If n is an **odd integer**, then $n = 2q + 1$ for some integer q.

It follows that if n is divided by 2, then the only possible remainders are 0 and 1.
By the same reasoning, every integer n can be expressed as

$$n = 3q, n = 3q + 1 \text{ or } n = 3q + 2$$

or as

$$n = 4q, n = 4q + 1, n = 4q + 2 \text{ or } n = 4q + 3 \text{ for some integer } q.$$

Example 4

Result Let $x, y \in \mathbf{Z}$. Then $3 \mid xy$ if and only if $3 \mid x$ or $3 \mid y$.

Proof. First, we show that if $3 \mid x$ or $3 \mid y$, then $3 \mid xy$. Assume that $3 \mid x$ or $3 \mid y$. Without loss of generality, we may assume that 3 divides x. Then $x = 3z$ for some integer z. Hence,

$$xy = (3z)y = 3(zy).$$

Since zy is an integer, $3 \mid xy$.

Next, we use a proof by contrapositive to verify the converse. Assume that $3 \nmid x$ and $3 \nmid y$. Then either $x = 3p + 1$ or $x = 3p + 2$ for some integer p and $y = 3q + 1$ or $y = 3q + 2$ for some integer q. There are four cases.

Example 4 (continued)

Case 1. $x = 3p + 1$ *and* $y = 3q + 1$, *where* $p, q \in \mathbf{Z}$. Then

$$\begin{aligned} xy &= (3p+1)(3q+1) = 9pq + 3p + 3q + 1 \\ &= 3(3pq + p + q) + 1. \end{aligned}$$

Since $3pq + p + q$ is an integer, $3 \nmid xy$.

The proofs of the remaining cases are similar to the proof of Case 1 and are therefore omitted.

Case 2. $x = 3p + 1$ *and* $y = 3q + 2$, *where* $p, q \in \mathbf{Z}$.

Case 3. $x = 3p + 2$ *and* $y = 3q + 1$, *where* $p, q \in \mathbf{Z}$.

Case 4. $x = 3p + 2$ *and* $y = 3q + 2$, *where* $p, q \in \mathbf{Z}$. □

Proofs Involving Congruence of Integers

Congruence of Integers

For integers a, b and $n \geq 2$, a is said to be **congruent to** b **modulo** n**,** written

$$a \equiv b \pmod{n}$$

if $n \mid (a - b)$.

Examples

$17 \equiv 2 \pmod{3}$, $17 \equiv 2 \pmod{5}$ and $14 \not\equiv 4 \pmod{6}$.

Example 5

Result Let $a, b, c, d, n \in \mathbf{Z}$ where $n \geq 2$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.

Proof. Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then

$$a - b = nx \text{ and } c - d = ny$$

for some integers x and y.

Example 5 (continued)

Adding these two equations, we obtain

$$(a - b) + (c - d) = nx + ny$$

and so

$$(a + c) - (b + d) = n(x + y).$$

Since $x + y$ is an integer,

$$n \mid [(a + c) - (b + d)].$$

Hence, $a + c \equiv b + d \pmod{n}$. □

Example 6

Result Let $a, b, c, d, n \in \mathbf{Z}$ where $n \geq 2$.

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Proof. Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $a - b = nx$ and $c - d = ny$, where $x, y \in \mathbf{Z}$. Thus,

$$a = b + nx \text{ and } c = d + ny.$$

Example 6 (continued)

Multiplying these two equations, we obtain

$$\begin{aligned} ac &= (b+nx)(d+ny) = bd + dnx + bny + n^2xy \\ &= bd + n(dx + by + nxy) \end{aligned}$$

and so $ac - bd = n(dx + by + nxy)$. Since $dx + by + nxy$ is an integer, $ac \equiv bd \pmod{n}$. □

Proofs Involving Real Numbers

Some Basic Facts about Real Numbers

$a^2 \geq 0$ for $a \in \mathbf{R}$.

$a^n \geq 0$ for $a \in \mathbf{R}$ and every positive even integer n.

If $a < 0$, then $a^n < 0$ for every positive odd integer n.

Example 7

Result Let $x, y \in \mathbf{R}$. If $xy = 0$, then $x = 0$ or $y = 0$.

Proof. Assume that $xy = 0$. We consider two cases, according to whether $x = 0$ or $x \neq 0$.

Case 1. $x = 0$. Then we have the desired conclusion.

Case 2. $x \neq 0$. Multiplying $xy = 0$ by the number $1/x$, we obtain

$$\frac{1}{x}(xy) = \frac{1}{x} \cdot 0 = 0.$$

Since

$$\frac{1}{x}(xy) = \left(\frac{1}{x}x\right) y = 1 \cdot y = y,$$

it follows that $y = 0$. □

Example 8

Result Let $x \in \mathbf{R}$. If $x^3 - 7x^2 + 3x - 21 = 0$, then $x = 7$.

Proof. Observe that

$$x^3 - 7x^2 + 3x - 21 = x^2(x - 7) + 3(x - 7) = 0$$

and so $(x^2 + 3)(x - 7) = 0$. Therefore,

$$x - 7 = 0 \text{ or } x^2 + 3 = 0.$$

Since $x^2 + 3 \neq 0$, it follows that $x - 7 = 0$ and so $x = 7$. □

Set Operations

Recall: For sets A and B contained in some universal set U, the **intersection** of A and B is

$$A \cap B = \{x \ : \ x \in A \text{ and } x \in B\},$$

the **union** of A and B is

$$A \cup B = \{x \ : \ x \in A \text{ or } x \in B\},$$

the **difference** of A and B is

$$A - B = \{x \ : \ x \in A \text{ and } x \notin B\}$$

and the **complement** of A is

$$\overline{A} = U - A.$$

Example 9

Result For every two sets A and B,

$$A - B = A \cap \overline{B}.$$

Proof. First, we show that $A - B \subseteq A \cap \overline{B}$. Let $x \in A - B$. Then $x \in A$ and $x \notin B$. Since $x \notin B$, it follows that $x \in \overline{B}$. Therefore, $x \in A$ and $x \in \overline{B}$; so $x \in A \cap \overline{B}$. Hence, $A - B \subseteq A \cap \overline{B}$.
Next, we show that $A \cap \overline{B} \subseteq A - B$. Let $y \in A \cap \overline{B}$. Then $y \in A$ and $y \in \overline{B}$. Since $y \in \overline{B}$, we see that $y \notin B$. Now, because $y \in A$ and $y \notin B$, we conclude that $y \in A - B$. Thus, $A \cap \overline{B} \subseteq A - B$.

Example 10

Result Let A and B be sets. Then $A \cup B = A$ if and only if $B \subseteq A$.

Proof. First, we show that if $A \cup B = A$, then $B \subseteq A$. We use a proof by contrapositive. Assume that B is not a subset of A. Then there must be some element $x \in B$ such that $x \notin A$. Since $x \in B$, it follows that $x \in A \cup B$. However, since $x \notin A$, we have $A \cup B \neq A$.

Next, we verify the converse, namely, if $B \subseteq A$, then $A \cup B = A$. We use a direct proof here. Assume that $B \subseteq A$. To verify that $A \cup B = A$, we show that $A \subseteq A \cup B$ and $A \cup B \subseteq A$. The set inclusion $A \subseteq A \cup B$ is immediate (if $x \in A$, then $x \in A \cup B$). It remains only to show then that $A \cup B \subseteq A$. Let $y \in A \cup B$. Thus, $y \in A$ or $y \in B$. If $y \in A$, then we already have the desired result. If $y \in B$, then since $B \subseteq A$, it follows that $y \in A$. Thus, $A \cup B \subseteq A$. □

Example 11

Result For sets A, B and C,

$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

Proof. We first show that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$. Let $(x, y) \in A \times (B \cup C)$. Then $x \in A$ and $y \in B \cup C$. Thus, $y \in B$ or $y \in C$, say the former. Then $(x, y) \in A \times B$ and so $(x, y) \in (A \times B) \cup (A \times C)$. Consequently, $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.
Next, we show that $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. Let $(x, y) \in (A \times B) \cup (A \times C)$. Then $(x, y) \in A \times B$ or $(x, y) \in A \times C$, say the former. Then $x \in A$ and $y \in B \subseteq B \cup C$. Hence, $(x, y) \in A \times (B \cup C)$, implying that $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. □