1 Statements

1.1 Class Handout, Chapter 1.3, Implications.

`Let` a, b, `and` c `be integers, with` a `and` b `non-zero. If` $(ab) \mid (ac)$, `then` $b \mid c$.

Proof 1.

Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$.

Suppose $(ab) \mid (ac)$. Then $\exists k \in \mathbb{Z}$ *s.t.* $ac = (ab)k$.

Divide both sides of the equation by a:

$$c = bk.$$

Since $k \in \mathbb{Z}$, by definition of divides, $b \mid c$.

■

1.2 Class Handout, Chapter 1.4, Contrapositive and Converse

`Prove that for all real numbers` a `and` b, `if` $a \in \mathbb{Q}$ `and` $ab \notin \mathbb{Q}$, `then` $n \notin Q$.

Proof 2.

Let $a, b \in \mathbb{Q}$.

Assume for the sake of contradiction that if $a \in \mathbb{Q}$ and $ab \notin \mathbb{Q}$, we have $b \in \mathbb{Q}$.

Then, $\exists p, q, m, n \in \mathbb{Z}$ *s.t.* $a = \frac{m}{n}$ and $b = \frac{p}{q}$.

Hence,

$$ab = \frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq}$$

As $mp, nq \in \mathbb{Z}$, $ab \in \mathbb{Q}$.

⋇ This contradicts with the fact that $ab \notin \mathbb{Q}$.

So, b must not be rational.

■

1.3 Chapter 1.1 # 7(c)

`Prove the square of an even integer is divisible by 4.`

Proof 3.

Suppose $x \in \mathbb{Z}$ is even. Then $\exists k \in \mathbb{Z}$ *s.t.* $x = 2k$.

Then, $x^2 = (2k)^2 = 4k^2$.

Since $k^2 \in \mathbb{Z}$, we have $4 \mid 4k^2$.

■

Theorem 1.1 (Archimedean Principle). *For every real number x, there is an integer n, such that $n > x$.*

1.4 Chapter 1.1 # 11

`For every positive real number` ε`, there exists a positive integer` N `such that` $\frac{1}{n} < \varepsilon$ `for all` $n \geq N$.

Proof 4.

Suppose $\varepsilon \in \mathbb{R}$ and $\varepsilon > 0$.

Since $\varepsilon \in \mathbb{R}$, we have $\frac{1}{n} \in \mathbb{R}$.

Then, by Archimedean Principle, $\exists n \in \mathbb{Z}$ *s.t.* $n > \frac{1}{\varepsilon}$.

Hence, $n\varepsilon > 1$ or $\varepsilon > \frac{1}{n}$.

Suppose $N \in \mathbb{Z}$ *s.t.* $N = \left\lceil \frac{1}{\varepsilon} \right\rceil$

$\left\lceil \frac{1}{\varepsilon} \right\rceil$ *means the integer greater to* $\frac{1}{\varepsilon}$ *if* $\frac{1}{\varepsilon} \notin \mathbb{Z}$*, and the integer equals to* $\frac{1}{\varepsilon}$ *if* $\frac{1}{\varepsilon} \in \mathbb{Z}$.

Hence, $N \geq \frac{1}{\varepsilon}$.

As $n > \frac{1}{\varepsilon}$, we have $n \geq N$

■

1.5 Chapter 1.1 # 12

`Use the Archimedean Principle (Theorem 1.1) to prove if` x `is a real number, then there exists a positive integer` n `such that` $-n < x < n$.

Proof 5.

Suppose $x \in \mathbb{R}$.

$\boxed{\text{Case 1}}$ If $x > 0$, then $-x < 0$ (i.e., $-x < 0 < x$).

By the Archimedean Principle, $\exists n \in \mathbb{Z}$ *s.t.* $n > x$.

Multiply (-1) on both sides of the inequality:

$$-n < -x$$

As $-x < 0 < x$,

$$-n < -x < 0 < x < n,$$

which means $-n < x < n$, and n is positive.

$\boxed{\text{Case 2}}$ If $x < 0$, then $-x > 0$ (i.e., $-x > 0 > x$)

Since $x \in \mathbb{R}$, we have $-x \in \mathbb{R}$.

By the Archimedean Principle, $\exists n \in \mathbb{Z}$ *s.t.* $n > -x$.

Multiply (-1) on both sides of the inequality:

$$-n < x$$

As $x < 0 < -x$,

$$-n < x < 0 < -x < n,$$

which means $-n < x < n$, and n is positive.

In all cases, we have proven that $x \in \mathbb{R} \implies \exists n \in \mathbb{Z},\ n > 0\ s.t.\ -n < x < n$.

■

1.6 Chapter 1.1 # 13

`Prove that if` x `is a positive real number, then there exists a positive integer` n `such that` $\frac{1}{n} < x < n$.

Proof 6.

Suppose $x \in \mathbb{R},\ x > 0$

$\boxed{\text{Case 1}}$ If $0 < x \leq 1$, then $\frac{1}{x} \geq 1$.

Hence, $x \leq 1 \leq \frac{1}{x}$.

As $x \in \mathbb{R}$, $\frac{1}{x} \in \mathbb{R}$, then by the Archimedean Principle (Theorem 1.1):

$$\exists n \in \mathbb{Z}\ s.t.\ n > \frac{1}{x}.$$

Hence, $nx > 1$ or $x > \frac{1}{n}$.

As $x \leq \frac{1}{x}$, $n > \frac{1}{x}$, and $x > \frac{1}{n}$, we have

$$\frac{1}{n} < x < n.$$

$\boxed{\text{Case 2}}$ If $x > 1$, then $0 < \dfrac{1}{x} < 1$.

Hence, $\dfrac{1}{x} < 1 < x$.

As $x \in \mathbb{R}$, by the Archimedean Principle:

$$\exists n \in \mathbb{Z} \ s.t. \ n > x > 0$$

Hence, $\dfrac{1}{n} < \dfrac{1}{x}$

As $\dfrac{1}{x} < x$, $\dfrac{1}{n} < \dfrac{1}{x}$, and $n > x$, we have

$$\frac{1}{n} < x < n$$

In all cases, we proven that $x \in \mathbb{R}, \ x > 0 \implies \exists n \in \mathbb{Z}, n > 0 \ s.t. \ \dfrac{1}{n} < x < n$.

■

1.7 Handout Chapter 1.4-2 More Contradictions and Equivelance

`There are no positive integer solutions to the equation` $x^2 - y^2 = 10$.

Proof 7.

Assume for the sake of contradiction that there are positive integer solutions to the equation $x^2 - y^2 = 10$.

Suppose $\exists x, y \in \mathbb{Z}$ and $x > 0, \ y > 0 \ s.t. \ x^2 - y^2 = 10$.

Then, we have $x^2 = 10 + y^2$.

Since $x > 0, \ x^2 > 0$, we have $10 + y^2 > 0$.

Then, $y^2 > -10$.

⋇ This contradicts with the fact that $y^2 \geq 0$ if $y \in \mathbb{Z}$.

So, our assumption is wrong. There must be no positive integer solutions to the equation $x^2 - y^2 = 10$.

■

1.8 Handout Chapter 1.4-2 More Contradictions and Equivelance

`Show that if` $a \in \mathbb{Q}$ `and` $b \in \mathbb{Q}'$, `then` $a + b \in \mathbb{Q}'$

Remark. *The notation $\mathbb{Q}$ means the set for rational numbers, and $\mathbb{Q}'$ means the set for irrational numbers.*

Proof 8.

Suppose $a \in \mathbb{Q}$ and $b \in \mathbb{Q}'$

Assume for the sake of contradiction that $a + b \in \mathbb{Q}$.

Then, $\exists m, n, p, q \in \mathbb{Z}$ such that $a = \dfrac{m}{n}$ and $a + b = \dfrac{p}{q}$.

Then,

$$b = \frac{p}{q} - a = \frac{p}{q} - \frac{m}{n} = \frac{pn - mq}{qn} \in \mathbb{Q}$$

Since $pn - mq \in \mathbb{Q}$ and $qn \in \mathbb{Z}$, we have $b = \dfrac{pn - mq}{qn} \in \mathbb{Q}$.

$\divideontimes$ This contradicts with the fact that $b \in \mathbb{Q}'$.

So, $a + b$ must be irrational.

$\blacksquare$

> *1.9 Handout Chapter 1.4-2 More Contradictions and Equivelance*
>
> `If` $n \in \mathbb{N}$ `and` $2^n - 1$ `is prime, then` n `is prime.`

Proof 9.

We will prove the contrapositive: if n is not prime, then $2^n - 1$ is not prime.

Suppose n is not prime. Then, $\exists a, b \in \mathbb{Z}$ with $1 < a, b < n$ *s.t.* $n = ab$.

Then, $2^n - 1 = 2^{ab} = (2^a)^b - 1$.

Notice that for $x^w - 1$, by polynomial long division, have

$$x^w - 1 = (x - 1)\left(x^{w-1} + x^{w-2} + \cdots + 1\right),$$

Substitute $x = 2^a$ and $w = b$, we have

$$2^n - 1 = (2^a - 1)\left[(2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1\right].$$

Since $(2^a - 1) \in \mathbb{Z}$ and $\left[(2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1\right] \in \mathbb{Z}$, we see that $2^n - 1$ is not prime.

$\blacksquare$