Theorem 1.4.3

The set of primes in $\mathbb{N}$ is infinite.

Proof:

Suppose that the set of primes $W = \{p_1, p_2, \cdots, p_k\}$ is finite for some $k \in \mathbb{N}$. Let $n = p_1p_2\cdots p_k + 1 \in \mathbb{N}$. (fact) All natural number has a prime divisor $q > 1$. So, $q \mid n$, and since q is a prime, then $q \in W$ and $q \mid p_1p_2\cdots p_k$ (because $q = p_i$ for some $1 \leq i \leq k$). Also, $q \mid n$. Therefore, $q \mid (n - p_1p_2\cdots p_k)$, but $n - p_1p_2\cdots p_k = 1$. Thus $q = 1$, Contradition. Thus W is infinite.

1.4.3 Type 3: Contrapositive Proofs

Contraposition to show $\mathbf{P} \Rightarrow \mathbf{Q}$: Suppose $\sim \mathbf{Q}$, then $\cdots\cdots$. Thus $\sim \mathbf{P}$. Therefore, $\mathbf{P} \Rightarrow \mathbf{Q}$. This technique uses the tautology $(\mathbf{P} \Rightarrow \mathbf{Q}) \Leftrightarrow (\sim \mathbf{Q} \Rightarrow \sim \mathbf{P})$.

Example 1.4.5

Let $m \in \mathbb{Z}$. If m^2 is odd, then m is odd.

Solution:

Assume that m is even. Then $m = 2k$ for some $k \in \mathbb{Z}$ and $m^2 = 4k^2 = 2(2k^2)$ which is even. By contraposition, the result is proved.

Example 1.4.6

Let $x, y \in \mathbb{R}$ such that $x < 2y$. Show that if $7xy \leq 3x^2 + 2y^2$, then $3x \leq y$.

Solution:

Assume that $x < 2y$. By contraposition, assume that $3x > y$. Then, $2y - x > 0$ and $3x - y > 0$, but

$$(2y - x)(3x - y) = 7xy - 3x^2 - 2y^2 > 0 \quad \Rightarrow \quad 7xy > 3x^2 + 2y^2.$$

Therefore, if $7xy \leq 3x^2 + 2y^2$, then $3x \leq y$.

1.4.4 Type 4: Two-Directions Proofs

Two directions to show $\mathbf{P} \Leftrightarrow \mathbf{Q}$: By any method, (i) Show that $\mathbf{P} \Rightarrow \mathbf{Q}$. (ii) Show that $\mathbf{Q} \Rightarrow \mathbf{P}$. Therefore, $\mathbf{P} \Leftrightarrow \mathbf{Q}$.

Theorem 1.4.4

Let a be a prime number, and let b and c be positive integers. Prove that $a \mid bc$ if and only if $a \mid b$ or $a \mid c$.

Proof:

We show the result by two direction: „ $\Rightarrow$ " and „ $\Leftarrow$ ".

„ $\Rightarrow$ ": Assume that $a \mid bc$. By Fundamental Theorem of Arithmetic, b and c can be written uniquely as products of primes. Assume $b = p_1 p_2 \cdots p_k$ and $c = q_1 q_2 \cdots q_h$ for some $h, k \in \mathbb{N}$. But then $bc = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_h$. Since $a \mid bc$ and a is a prime, a is one of the prime factors. If $a = p_i$ for some $1 \leq i \leq k$, then $a \mid b$ or if $a = q_i$ for some $1 \leq i \leq h$, then $a \mid c$. Thus, either $a \mid b$ or $a \mid c$.

„ $\Leftarrow$ ": Assume that $a \mid b$ or $a \mid c$. Thus,

Case 1: $a \mid b$ then $b = ka$ for some $k \in \mathbb{Z}$ and hence $bc = (ka)c = (kc)a$. Thus $a \mid bc$.

Case 2: $a \mid c$ then $c = ha$ for some $h \in \mathbb{Z}$ and hence $bc = b(ha) = (bh)a$. Thus $a \mid bc$.

In either cases, $a \mid bc$.

1.4.5 Type 5: Proofs By Cases (Exhaustion)

Contradiction to show $(\mathbf{P}_1 \vee \mathbf{P}_2) \Rightarrow \mathbf{Q}$: By any method, (i) Show that $\mathbf{P}_1 \Rightarrow \mathbf{Q}$ and (ii) show that $\mathbf{P}_2 \Rightarrow \mathbf{Q}$. Using the tautology $[(\mathbf{P}_1 \vee \mathbf{P}_2) \Rightarrow \mathbf{Q}] \Leftrightarrow [(\mathbf{P}_1 \Rightarrow \mathbf{Q}) \wedge (\mathbf{P}_2 \Rightarrow \mathbf{Q})]$.

Example 1.4.7

Show that for any $x, y \in \mathbb{Z}$, if either x or y is even, then xy is even.

Solution:

We have two cases:

Case 1: Assume x-even. Then $x = 2k$ for some $k \in \mathbb{Z}$. That is $xy = 2(ky)$ which is even.

Case 2: Assume y-even. Then $y = 2h$ for some $h \in \mathbb{Z}$. That is $xy = 2(xh)$ which is even.

Thus, in both cases, xy is even.

Example 1.4.8

Let $x, y \in \mathbb{Z}$. If x and y are both odd, then xy is odd.

Solution:

a. Direct Proof: Assume x and y are odd integers. Then, there are m and n in $\mathbb{Z}$ such that $x = 2m+1$ and $y = 2n+1$. Thus, $xy = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1$. Therefore, xy is odd as well.

b1. Proof by Contradiction: Assume that xy is even. Thus $2 \mid xy$ which implies that $2 \mid x$ or $2 \mid y$ (since 2 is a prime number) which is a contradiction both ways since both of x and y are odd.

b2. Another Proof by Contradiction: Assume that xy is even. Since x and y are odd, there are m and n in $\mathbb{Z}$ such that $x = 2m+1$ and $y = 2n+1$. Thus, $xy = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1$ which is odd, contradiction. Therefore, xy is odd.

c. Proof by Contraposition: We use $\sim$ (xy is odd) $\Rightarrow \sim$ (x is odd and y is odd) which is equivalent to (xy is even) $\Rightarrow$ [(x is even) or (y is even)].

Assume that xy is even. Thus, $2 \mid xy$. Since 2 is a prime number, we have either $2 \mid x$ or $2 \mid y$. Thus, either x is even or y is even. Therefore, if x and y are odd, then xy is odd.

Exercise 1.4.1

Let $a, b \in \mathbb{Z}$. Use a contrapositive proof to show that if ab-odd, then a - odd and b-odd.

Section 1.6: Proofs Involving Quantifiers

1.6.1 Type 1: Proof of $(\exists x)\mathbf{P}(x)$

- Direct proof: Name or construct an element $x \in \mathcal{U}$ which has the property $\mathbf{P}(x)$.
- Proof by contradiction: Suppose $\sim (\exists x)\mathbf{P}(x)$. Then $(\forall x)(\sim \mathbf{P}(x))$ ... ... .Therefore, $\mathbf{Q}(x) \wedge \sim \mathbf{Q}(x)$, contradiction. Hence, $\sim (\exists x)\mathbf{P}(x)$ is false, then $(\exists x)\mathbf{P}(x)$ is true.

Example 1.6.1

Show that there is an even prime number.

Solution:

2 is a prime even number.

Example 1.6.2

Let $\mathcal{U} = \mathbb{R}$. Show that $(\exists x)[x^3 + 3x^2 + x - 1 = 0]$.

Solution:

Using direct proof: $x = -1$ is a solution. On the other hand, using a proof by contradiction:

Assume $\sim (\exists x)[x^3 + 3x^2 + x - 1 = 0] \equiv (\forall x)[x^3 + 3x^2 + x - 1 \neq 0]$. Therefore, either:

Case 1: $(\forall x)[x^3 + 3x^2 + x - 1 > 0]$ which is false for if $x = -10$, or

Case 2: $(\forall x)[x^3 + 3x^2 + x - 1 < 0]$ which is false for if $x = 10$.

Therefore, $(\exists x)[x^3 + 3x^2 + x - 1 = 0]$.

1.6.2 Type 2: Proof of $(\forall x)\mathbf{P}(x)$

- Direct proof: Let $x \in \mathcal{U}$ be arbitrary, then ... . Hence, $\mathbf{P}(x)$ is true. Since x was arbitrary chosen, $(\forall x)\mathbf{P}(x)$ is true.
- Proof by contradiction: Suppose $\sim (\forall x)\mathbf{P}(x)$. Then $(\exists x)(\sim \mathbf{P}(x))$ ... ... .Therefore, $\mathbf{Q}(x) \wedge \sim \mathbf{Q}(x)$, contradiction. Hence, $\sim (\forall x)\mathbf{P}(x)$ is false, then $(\forall x)\mathbf{P}(x)$ is true.

Example 1.6.3

Let $\mathcal{U} = \mathbb{Z}$. Show that $(\forall x)$, if x is even, then x^2 is even.

Solution:

Assume that $x \in \mathbb{Z}$ so that $x = 2k$ for some integer k. Then $x^2 = (2k)^2 = 2(2k^2)$ which is even.

Example 1.6.4

Show that for all rational numbers p and q, $\dfrac{p+q}{2}$ is rational.

Solution:

Assume that $p = \frac{x}{y}$ and $q = \frac{u}{v}$ where $x, y, u, v \in \mathbb{Z}$ with $y, v \neq 0$. Then,

$$\frac{p+q}{2} = \frac{1}{2}\left(\frac{x}{y} + \frac{u}{v}\right) = \frac{1}{2}\left(\frac{xv+yu}{yv}\right) = \frac{xv+yu}{2yv},$$

which is rational.

1.6.3 Type 3: Proof of $(\exists! x)\mathbf{P}(x)$

1. Prove that $(\exists x)\mathbf{P}(x)$ by any method.
2. Assume that $x, y \in \mathcal{U}$ such that $\mathbf{P}(x)$ and $\mathbf{P}(y)$ are true ... . Thus, $x = y$. Therefore, $(\exists! x)\mathbf{P}(x)$.

Example 1.6.5

Prove that every nonzero real number has a unique multiplicative inverse.

Solution:

Let x be any nonzero real number. We want to show that $xy = 1$ for exactly one real number y. Let $y = \frac{1}{x}$, then y is a real number. Since $x \neq 0$, then $xy = x\frac{1}{x} = 1$. Thus, x has a multiplicative inverse.

Assume that y and z are two real numbers such that $xy = xz = 1$. Since $x \neq 0$, $xy = xz$ implies that $y = z$. Therefore, every nonzero real number has a unique multiplicative inverse.

Exercise 1.6.1

Prove that every nonsingular matrix has a unique inverse.