

**Definition 7**

$n \in \mathbb{N}$  is odd if  $(\exists i \in \mathbb{N}) n = 2i + 1$ .

**Proposition 8**

Goal:  $(\forall m, n \in \mathbb{N}) m \text{ and } n \text{ odd} \Rightarrow m \times n \text{ odd}$

**Proof**

Assume:

1.  $m, n \in \mathbb{N}$
2.  $m$  and  $n$  odd

New goal:  $m \times n$  odd

$$\begin{aligned}
 & (\exists i, j \in \mathbb{N}) m = 2i + 1 \wedge n = 2j + 1 \\
 \Rightarrow & (\exists i, j \in \mathbb{N}) m \times n = (2i + 1) \times (2j + 1) \\
 \Rightarrow & (\exists i, j \in \mathbb{N}) m \times n = 2(2ij + i + j) + 1 \\
 \Rightarrow & (\exists k \in \mathbb{N}) m \times n = 2k + 1 \\
 \Rightarrow & m \times n \text{ odd}
 \end{aligned}$$

**Definition 9**

$(\forall x \in \mathbb{R})$

- $(\exists m, n \in \mathbb{Z}) x = m/n \Leftrightarrow x$  rational
- $\neg(x \text{ rational}) \Leftrightarrow x$  irrational
- $x > 0 \Leftrightarrow x$  positive
- $x < 0 \Leftrightarrow x$  negative
- $\neg(x \text{ positive}) \Leftrightarrow x$  nonpositive
- $\neg(x \text{ negative}) \Leftrightarrow x$  nonnegative
- $x$  nonnegative  $\wedge x \in \mathbb{Z} \Leftrightarrow x \in \mathbb{N}$

**Proposition 10**

Goal:  $(\forall x \text{ positive}) \sqrt{x}$  rational  $\Rightarrow x$  rational

**Proof**

Assume:

1.  $x$  positive
2.  $\sqrt{x}$  rational

New goal:  $x$  rational

$$\begin{aligned}
 & (\exists p, q \in \mathbb{Z}) \sqrt{x} = p/q \\
 \Rightarrow & (\exists p, q \in \mathbb{Z}) x = (\sqrt{x})^2 = p^2/q^2 \\
 \Rightarrow & (\exists p', q' \in \mathbb{Z}) x = p'/q' \\
 \Leftrightarrow & x \text{ rational}
 \end{aligned}$$

**Definition**

$$P \wedge (P \Rightarrow Q) \Rightarrow Q$$

**Theorem 11**

Goal: Let  $P_1, P_2, P_3$  be statements,  $(P_1 \Rightarrow P_2 \wedge P_2 \Rightarrow P_3) \Rightarrow (P_1 \Rightarrow P_3)$

**Proof**

Assume:

1.  $P_1 \Rightarrow P_2$
2.  $P_2 \Rightarrow P_3$
3.  $P_1$

New goal:  $P_3$

$$\begin{aligned} &P_2 \text{ as (4) by (1) and (3)} \\ &\Rightarrow P_3 \text{ by (2) and (4)} \end{aligned}$$

**Definition**

$$(P \Leftrightarrow Q) \Leftrightarrow (P \Rightarrow Q \wedge Q \Rightarrow P)$$

**Definition 12**

$$d|n \Leftrightarrow (\exists k \in \mathbb{Z}) n = k \times d$$

**Definition 14**

$$(\forall m \in \mathbb{Z}^+, a, b \in \mathbb{Z}) a \equiv b \pmod{m} \Leftrightarrow m|(a - b)$$

**Proposition 16**

$$\text{Goal: } (n \text{ even} \Leftrightarrow n \equiv 0 \pmod{2}) \wedge (n \text{ odd} \Leftrightarrow n \equiv 1 \pmod{2})$$

Subgoal:  $n \text{ even} \Leftrightarrow n \equiv 0 \pmod{2}$

Assume:

1.  $n$  even

New goal:  $n \equiv 0 \pmod{2}$

$$\begin{aligned} n \text{ even} &\Leftrightarrow (\exists k \in \mathbb{Z}) n = 2 \times k \\ &\Leftrightarrow (\exists k \in \mathbb{Z}) (n - 0) = 2 \times k \\ &\Leftrightarrow n \equiv 0 \pmod{2} \end{aligned}$$

Subgoal:  $n \text{ odd} \Leftrightarrow n \equiv 1 \pmod{2}$

Assume:

1.  $n$  odd

New goal:  $n \equiv 1 \pmod{2}$

$$\begin{aligned} n \text{ odd} &\Leftrightarrow (\exists k \in \mathbb{Z}) n = 2 \times k + 1 \\ &\Leftrightarrow (\exists k \in \mathbb{Z}) (n - 1) = 2 \times k \\ &\Leftrightarrow n \equiv 1 \pmod{2} \end{aligned}$$

**Proposition 18**

$$\text{Goal: } (\forall m \in \mathbb{Z}^+, a, b \in \mathbb{Z}) a \equiv b \pmod{m} \Leftrightarrow ((\forall n \in \mathbb{Z}^+) n \times a \equiv n \times b \pmod{n \times m})$$

Assume:

1.  $m \in \mathbb{Z}^+$
2.  $a, b \in \mathbb{Z}$

Subgoal:  $a \equiv b \pmod{m} \implies (\forall n \in \mathbb{Z}^+) n \times a \equiv n \times b \pmod{n \times m}$

Assume:

- 3.  $a \equiv b \pmod{m}$
- 4.  $n \in \mathbb{Z}^+$

New goal:  $n \times a \equiv n \times b \pmod{n \times m}$

$$\begin{aligned}
 & (\exists i \in \mathbb{Z}) a - b = m \times i \text{ by (3)} \\
 \implies & (\exists i \in \mathbb{Z}) n \times a - n \times b = (n \times m) \times i \\
 \implies & (\exists i \in \mathbb{Z}) n \times a \equiv n \times b \pmod{n \times m} \\
 \implies & n \times a \equiv n \times b \pmod{n \times m}
 \end{aligned}$$

Subgoal:  $(\forall n \in \mathbb{Z}^+) n \times a \equiv n \times b \pmod{n \times m} \implies a \equiv b \pmod{m}$

Assume:

- 3.  $(\forall n \in \mathbb{Z}^+) n \times a \equiv n \times b \pmod{n \times m}$

New goal:  $a \equiv b \pmod{m}$

$$\begin{aligned}
 & 1 \times a \equiv 1 \times b \pmod{1 \times m} \text{ by (3)} \\
 \implies & a \equiv b \pmod{m}
 \end{aligned}$$

### Definition

- $(\forall x) x = x$
- $(\forall x,y) x = y \implies (P(x) \implies P(y))$
- $(\forall a,b,c) (a = b \wedge b = c) \implies a = c$
- $(\forall a,b,x,y) (a = b \wedge x = y) \implies (a + x = b + x = b + y)$