Definition 7

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

Proposition 8

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

Proof

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

New goal: $m \times n$ odd

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

Definition 9

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

Proposition 10

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

Proof

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

New goal: x rational

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

Definition

$P \land (P \implies Q) \implies Q$

Theorem 11

Goal: Let P_1, P_2, P_3 be statements, $(P_1 \implies P_2 \land P_2 \implies P_3) \implies (P_1 \implies P_3)$

Proof

Assume:
1. $P_1 \implies P_2$
2. $P_2 \implies P_3$
3. P_1

New goal: P_3

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

Definition
$(P \iff Q) \iff (P \implies Q \land P \impliedby Q)$

Definition 12
$d|n \iff (\exists k \in \mathbb{Z})\ n = k \times d$

Definition 14
$(\forall m \in \mathbb{Z}^+, a, b \in \mathbb{Z})\ a = b \pmod m \iff m|(a - b)$

Proposition 16
Goal: $(n \text{ even} \iff n = 0 \pmod 2) \land (n \text{ odd} \iff n = 1 \pmod 2)$

Subgoal: n even $\iff n = 0 \pmod 2$

Assume:
1. n even

New goal: $n = 0 \pmod 2$

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

Subgoal: n odd $\iff n = 1 \pmod 2$

Assume:
1. n odd

New goal: $n = 1 \pmod 2$

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

Proposition 18
Goal: $(\forall m \in \mathbb{Z}^+, a, b \in \mathbb{Z})\ a = b \pmod m \iff ((\forall n \in \mathbb{Z}^+)\ n \times a = n \times b \pmod{n \times m})$

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

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

Assume:
3. $a = b \pmod m$
4. $n \in \mathbb{Z}^+$

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

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

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

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

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

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

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

Theorem 19

Goal: $(\forall n \in \mathbb{Z})\ 6|n \Longleftrightarrow 3|n \wedge 2|n$

Assume:
1. $n \in \mathbb{Z}$

New goal: $6|n \Longleftrightarrow 3|n \wedge 2|n$

Subgoal: $6|n \Longrightarrow 3|n \wedge 2|n$

Assume:
2. $6|n$

New goal: $3|n \wedge 2|n$

Subgoal: $3|n$

$$\begin{aligned} 6|n \Longleftrightarrow\ & (\exists i \in \mathbb{Z})\ n = 6 \times i \\ \Longrightarrow\ & (\exists j \in \mathbb{Z})\ n = 3 \times j \\ \Longleftrightarrow\ & 3|n \end{aligned}$$

Subgoal: $2|n$

$$\begin{aligned} 6|n \Longleftrightarrow\ & (\exists i \in \mathbb{Z})\ n = 6 \times i \\ \Longrightarrow\ & (\exists j \in \mathbb{Z})\ n = 2 \times j \\ \Longleftrightarrow\ & 2|n \end{aligned}$$

Subgoal: $3|n \wedge 2|n \Longrightarrow 6|n$

Assume:
2. $2|n \wedge 3|n$

New goal: $6|n$

$$
\begin{aligned}
&(\exists i \in \mathbb{Z})\ n = 2 \times i \\
&\Longrightarrow (\exists i \in \mathbb{Z})\ 3 \times n = 6 \times i \text{ as } (3) \\
&(\exists j \in \mathbb{Z})\ n = 3 \times j \\
&\Longrightarrow (\exists j \in \mathbb{Z})\ 2 \times n = 6 \times j \text{ as } (4) \\
&\Longrightarrow (\exists i,j \in \mathbb{Z})\ n = 6 \times (i - j) \text{ by } (3) \text{ and } (4) \\
&\Longrightarrow (\exists k \in \mathbb{Z})\ n = 6 \times k \\
&\Longrightarrow 6 | n
\end{aligned}
$$

Proposition 21

Goal: $(\forall k \in \mathbb{Z}^+)\ (\exists i,j \in \mathbb{N})\ 4 \times k = i^2 - j^2$

Assume:
1. $k \in \mathbb{Z}^+$

Let $i = k + 1, j = k - 1$

$$
\begin{aligned}
i^2 - j^2 &= (k+1)^2 - (k-1)^2 \\
&= 4 \times k
\end{aligned}
$$

Theorem 23

Goal: $(\forall l,m,n \in \mathbb{Z})\ l|m \land m|n \Longrightarrow l|n$

Assume:
1. $l, m, n \in \mathbb{Z}$
2. $l|m \land m|n$

New goal: $l|n$

$$
\begin{aligned}
&(\exists i \in \mathbb{Z})\ m = i \times l \\
&(\exists j \in \mathbb{Z})\ n = j \times m \\
\Longrightarrow &(\exists i,j \in \mathbb{Z})\ n = (j \times i) \times l \\
\Longrightarrow &(\exists k \in \mathbb{Z})\ n = k \times l \\
\Longrightarrow &l|n
\end{aligned}
$$

Definition

$((\exists! x)\ P(x)) \Longleftrightarrow ((\exists x)\ P(x) \land ((\forall y,z)\ P(y) \land P(z) \Longrightarrow y = z))$

Proposition 24

Goal: $(\forall n \in \mathbb{Z}, m \in \mathbb{Z}^+)\ (\exists! z)\ 0 \leq z < m \land n = z \pmod m$

Assume:
1. $m \in \mathbb{Z}^+$
2. $n \in \mathbb{Z}$