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

Proposition 8: product of odd integers is odd

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

Proposition 10: rational square root

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: modus ponens
$P \land (P \implies Q) \implies Q$

Theorem 11: implication transitivity

$(\forall P_1, P_2, P_3 \text{ statement})\ (P_1 \implies P_2 \land P_2 \implies P_3) \implies (P_1 \implies P_3)$

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: bi-implication
$(P \iff Q) \iff (P \implies Q \land P \impliedby Q)$

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

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

Proposition 16: parity as congruence

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

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

Assume:
1. n even

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

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

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

Assume:
1. n odd

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

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

Proposition 18: linearity of congruence

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

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

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

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

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

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

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

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

Theorem 19: divisibility of prime products

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

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

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

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

Assume:
2. $6|n$

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

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: $3|n \land 2|n \Longrightarrow 6|n$

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

New goal: $6|n$

$$\begin{aligned} &(\exists i \in \mathbb{Z})\ n = 2 \times i \\ \implies &(\exists i \in \mathbb{Z})\ 3 \times n = 6 \times i \text{ as } (3) \\ &(\exists j \in \mathbb{Z})\ n = 3 \times j \\ \implies &(\exists j \in \mathbb{Z})\ 2 \times n = 6 \times j \text{ as } (4) \end{aligned}$$

$\implies (\exists i,j \in \mathbb{Z})\ n = 6 \times (i - j)$ by (3) and (4)

$\implies (\exists k \in \mathbb{Z})\ n = 6 \times k$

$\implies 6|n$

Proposition 21: difference of squares

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: divisibility transitivity

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

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

New goal: $l|n$

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

Definition

$((\exists! x)\ P(x)) \iff ((\exists x)\ P(x) \land ((\forall y,z)\ P(y) \land P(z) \implies y = z))$

Proposition 24: unique existence of proper congruence

Lemma 24.1: congruence transitivity

Goal: $n \equiv x \pmod m \land n \equiv y \pmod m \implies x \equiv y \pmod m$

Assume:
1. $n \equiv x \pmod m : (\exists i \in \mathbb{Z})\ (x - n) = i \times m$
2. $n \equiv y \pmod m : (\exists j \in \mathbb{Z})\ (y - n) = j \times m$

New goal: $x \equiv y \pmod m$

$$\begin{aligned} & (\exists i,j \in \mathbb{Z})\ x - y = (i - j) \times m \text{ by } (1) \text{ and } (2) \\ \Longrightarrow\ & (\exists k \in \mathbb{Z})\ x - y = k \times m \\ \Longleftrightarrow\ & x \equiv y \pmod m \end{aligned}$$

Let $P(z) : 0 \leq z < m \land n \equiv z \pmod m$

Goal: $(\forall m \in \mathbb{Z}^+, n \in \mathbb{Z})\ (\exists! z)\ P(z)$

New goal: $(\forall m \in \mathbb{Z}^+, n \in \mathbb{Z})\ ((\exists z)\ P(z)) \land ((\forall x,y)\ P(x) \land P(y) \Longrightarrow x = y)$

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

New goal: $((\exists z)\ P(z)) \land ((\forall x,y)\ P(x) \land P(y) \Longrightarrow x = y)$

Subgoal: $(\exists z)\ P(z)$

Missing
This goal is not proved

Subgoal: $(\forall x,y)\ P(x) \land P(y) \Longrightarrow x = y$

Assume:
3. x, y exists
4. $0 \leq x < m \land n \equiv x \pmod m$
5. $0 \leq y < m \land n \equiv y \pmod m$

New goal: $x = y$

Missing
$-1 < i < 1 \Longrightarrow i = 0$

$$\begin{aligned} & -m < -y \leq 0 \text{ by } (4) \text{ as } (6) \\ & -m < x - y < m \text{ by } (4) \text{ and } (6) \text{ as } (7) \\ & x \equiv y \pmod m \text{ by } (4), (5) \text{ and } (\text{L24.1}) \\ \Longleftrightarrow\ & (\exists i \in \mathbb{Z})\ x - y = i \times m \\ \Longleftrightarrow\ & (\exists i \in \mathbb{Z})\ -m < i \times m < m \text{ by } (7) \\ \Longleftrightarrow\ & (\exists i \in \mathbb{Z})\ -1 < i < 1 \text{ by cancellation} \\ \Longleftrightarrow\ & i = 0 \text{ by magic} \\ \Longrightarrow\ & x - y = 0 \\ \Longleftrightarrow\ & x = y \end{aligned}$$

Proposition 25: parity of square

Goal: $(\forall n \in \mathbb{Z})\ n^2 \equiv 0 \pmod 4 \lor n^2 \equiv 1 \pmod 4$

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

New goal: $n^2 \equiv 0 \pmod 4 \lor n^2 \equiv 1 \pmod 4$

$$(\exists! z \in \mathbb{Z})\ 0 \leq z < 2 \land n \equiv z \pmod 2 \text{ by } (\text{P24})$$

Missing
$0 \le z < 2 \implies z = 0 \lor z = 1$

Assume:
2. $z = 0 \lor z = 1$

Case $z = 0$

Subgoal: $n \equiv 0 \pmod 2 \implies$
$n^2 \equiv 0 \pmod 4 \lor n^2 \equiv 1 \pmod 4$

Assume:
3. $n \equiv 0 \pmod 2$

New goal:
$n^2 \equiv 0 \pmod 4 \lor n^2 \equiv 1 \pmod 4$

$$\begin{aligned} & (\exists i \in \mathbb{Z})\ n = i \times 2 \\ \implies & (\exists i \in \mathbb{Z})\ n^2 = i^2 \times 4 \\ \implies & (\exists j \in \mathbb{Z})\ n^2 = j \times 4 \\ \implies & n^2 \equiv 0 \pmod 4 \\ \implies & n^2 \equiv 0 \pmod 4 \lor n^2 \equiv 1 \pmod 4 \end{aligned}$$

Case $z = 1$

Subgoal: $n \equiv 1 \pmod 2 \implies$
$n^2 \equiv 0 \pmod 4 \lor n^2 \equiv 1 \pmod 4$

Assume:
3. $n \equiv 1 \pmod 2$

New goal:
$n^2 \equiv 0 \pmod 4 \lor n^2 \equiv 1 \pmod 4$

$$\begin{aligned} & (\exists i \in \mathbb{Z})\ n = i \times 2 + 1 \\ \implies & (\exists i \in \mathbb{Z})\ n^2 = 4 \times (i^2 + i) + 1 \\ \implies & (\exists j \in \mathbb{Z})\ n^2 = 4 \times j + 1 \\ \implies & n^2 \equiv 1 \pmod 4 \\ \implies & n^2 \equiv 0 \pmod 4 \lor n^2 \equiv 1 \pmod 4 \end{aligned}$$

Lemma 27: congruence at ends of combinations

Definition: combinations

$$\binom{p}{m} = \frac{p!}{(p-m)!m!}$$

Goal: $(\forall p \in \mathbb{Z}^+, m \in \mathbb{N})\ p > 1 \land (m = 0 \lor m = p) \implies \binom{p}{m} \equiv 1 \pmod p$

Note
Added condition $p > 1$ for the statement to be correct.

Assume:
1. $p \in \mathbb{Z}^+, m \in \mathbb{N}$
2. $p > 1$

New goal: $m = 0 \lor m = p \implies \binom{p}{m} \equiv 1 \pmod p$

Assume:
3. $m = 0 \lor m = p$

Case $m = 0$

Subgoal: $m = 0 \implies \binom{p}{m} \equiv 1 \pmod p$

Assume:
4. $m = 0$

Case $m = p$

Subgoal: $m = p \implies \binom{p}{m} \equiv 1 \pmod p$

Assume:
4. $m = p$

New goal: $\binom{p}{m} \equiv 1 \pmod{p}$

$$\binom{p}{0} = \frac{p!}{p! \times 1} = 1$$

$$\implies \binom{p}{m} \equiv 1 \pmod{p}$$

New goal: $\binom{p}{m} \equiv 1 \pmod{p}$

$$\binom{p}{p} = \frac{p!}{1 \times p!} = 1$$

$$\implies \binom{p}{m} \equiv 1 \pmod{p}$$

Lemma 28: congruence at non-ends of combinations

Goal: $(\forall p \text{ prime}, m \in \mathbb{Z})\ 0 < m < p \implies \binom{p}{m} \equiv 0 \pmod{p}$

Assume:
1. p prime
2. $m \in \mathbb{Z}$
3. $0 < m < p$

New goal: $\binom{p}{m} \equiv 0 \pmod{p}$

Missing: Euclid's Lemma
p prime $\implies (p|(a \times b) \implies p|a \vee p|b)$

Assume:
4. $\binom{p}{m} \in \mathbb{Z}$ by magic
5. $\neg p|m!$
6. $\neg p|(p-m)!$

$$\begin{aligned} p \times (p-1)! &= \binom{p}{m} \times (p-m)! \times m! \\ \implies p&|\binom{p}{m} \times (p-m)! \times m! \\ \implies p&|\binom{p}{m} \text{ by (5), (6) and (Euclid's Lemma)} \\ \implies &\binom{p}{m} \equiv 0 \pmod{p} \end{aligned}$$

Proposition 29: congruence of combinations

Goal: $(\forall p \text{ prime}, m \in \mathbb{Z})\ , 0 \leq m \leq p \implies \binom{p}{m} \equiv 0 \pmod{p} \vee \binom{p}{m} \equiv 1 \pmod{p}$

Assume:
1. p prime, $m \in \mathbb{Z}$
2. $0 \leq m \leq p$

New goal: $\binom{p}{m} \equiv 0 \pmod{p} \vee \binom{p}{m} \equiv 1 \pmod{p}$

Assume:
3. $(m = 0 \vee m = p) \vee 0 < m < p$

Case: $m = 0 \vee m = p$

Case: $0 < m < p$

Subgoal:
$\binom{p}{m} \equiv 0 \pmod p \vee \binom{p}{m} \equiv 1 \pmod p$

$$\binom{p}{m} \equiv 1 \pmod p \text{ by (L27)}$$
$$\implies \binom{p}{m} \equiv 0 \pmod p \vee \binom{p}{m} \equiv 1 \pmod p$$

Subgoal:
$\binom{p}{m} \equiv 0 \pmod p \vee \binom{p}{m} \equiv 1 \pmod p$

$$\binom{p}{m} \equiv 0 \pmod p \text{ by (L28)}$$
$$\implies \binom{p}{m} \equiv 0 \pmod p \vee \binom{p}{m} \equiv 1 \pmod p$$

Definition: binomial theorem

$$(\forall p \in \mathbb{N}, m, n)\ (m+n)^p = \sum_{k=0}^{p} \binom{p}{k} m^{p-k} n^k$$

Corollary 33: the freshman's dream

Goal: $(\forall m, n \in \mathbb{N}, p \text{ prime})\ (m+n)^p \equiv m^p + n^p \pmod p$

Assume:
1. $m, n \in \mathbb{N}, p$ prime

New goal: $(m+n)^p \equiv m^p + n^p \pmod p$

Informal

$$(m+n)^p = \binom{p}{0} m^p + \sum_{k=1}^{p-1} m^{p-k} n^k + \binom{p}{p} n^p$$

$$\implies (m^p + n^p) + \sum_{k=1}^{p-1} m^{p-k} n^k \equiv m^p + n^p + 0 \pmod p \text{ by (L28)}$$
$$\implies (m+n)^p \equiv m^p + n^p \pmod p$$

Formal proof requires induction.

Corollary 34: the dropout lemma

Goal: $(\forall m \in \mathbb{N}, p \text{ prime})\ (m+1)^p \equiv m^p + 1 \pmod p$

Assume:
1. $m \in \mathbb{N}, p$ prime

New goal: $(m+1)^p \equiv m^p + 1 \pmod p$

$$(\forall m \in \mathbb{N})\ (m+1)^p \equiv m^p + 1^p \pmod p \text{ by (C33)}$$
$$\implies (\forall m \in \mathbb{N})\ (m+1)^p \equiv m^p + 1 \pmod p$$

Proposition 35: the many dropout lemma

Goal: $(\forall m, i \in \mathbb{N}, p \text{ prime})\ (m+i)^p \equiv m^p + i \pmod p$

Assume:
1. $m, i \in \mathbb{N}, p$ prime

New goal: $(m+i)^p \equiv m^p + i \pmod p$

Informal

$$
\begin{aligned}
&(m+i)^p = \Big(m + \underbrace{1+1+1+1}_{i\text{ times}}\Big)^p \\
\implies &((m+i-1)+1)^p \equiv (m+i-1)^p + 1 \pmod p \\
\implies &((m+i-2)+1)^p \equiv (m+i-2)^p + 1 + 1 \pmod p) \\
\vdots \implies &(m+1)^p \equiv m^p + \underbrace{1+1+1+1}_{i\text{ times}} \pmod p \\
\implies &(m+i)^p \equiv m^p + i \pmod p \text{ by transitivity}
\end{aligned}
$$

The formal proof requires induction.

Theorem 36: Fermat's little theorem, clause 1

Goal: $(\forall i \in \mathbb{N}, p \text{ prime})\ i^p \equiv i \pmod p$

Assume:
1. $i \in \mathbb{N}, p$ prime

New goal: $i^p \equiv i \pmod p$

$$
\begin{aligned}
&(0+i)^p \equiv 0^p + i \pmod p \text{ by (P35)} \\
\implies &i^p \equiv i \pmod p
\end{aligned}
$$

Logical equivalences

$$
\begin{aligned}
\neg(P \implies Q) &\iff P \wedge \neg Q \\
\neg(P \iff Q) &\iff P \iff \neg Q \\
\neg(P \wedge Q) &\iff \neg P \vee \neg Q \\
\neg(P \vee Q) &\iff \neg P \wedge \neg Q \\
\neg((\forall x)\ P(x)) &\iff (\exists x)\ \neg P(x) \\
\neg((\exists x)\ P(x)) &\iff (\forall x)\ P(x) \\
\neg(\neg P) &\iff P \\
\neg P &\iff (P \implies \text{false})
\end{aligned}
$$

Theorem 37: contrapositive forward

Goal: $(P \implies Q) \implies (\neg Q \implies \neg P)$

Assume:
1. P, Q statement
2. $P \implies Q$
3. $\neg Q$
4. P

New goal: false

$$
\begin{aligned}
&Q \text{ by (2) and (4) as (5)} \\
\implies &\text{false by (3) and (5)}
\end{aligned}
$$

Theorem 39: contrapositive reverse

Goal: $(\neg Q \implies \neg P) \implies (P \implies Q)$

Assume:
1. $\neg Q \implies \neg P$
2. P

New goal: Q

Assume:
3. $\neg Q$ by contradiction

New goal: false

$$\begin{aligned} &\neg P \text{ by (1) and (3) as (4)} \\ \implies &\text{false by (2) and (4)} \end{aligned}$$

Corollary 40: contrapositive bi-implication

Goal: $(P \implies Q) \iff (\neg Q \implies \neg P)$

Subgoal: $(P \implies Q) \implies (\neg Q \implies \neg P)$ Exact (T37)	Subgoal: $(P \implies Q) \impliedby (\neg Q \implies \neg P)$ Exact (T38)

Corollary 41: square root irrational

Goal: $(\forall x)\ x$ irrational $\wedge\ x > 0 \implies \sqrt{x}$ irrational

Assume:
1. x irrational $\wedge\ x > 0$

New goal: $\sqrt{x}$ irrational

Assume:
2. $\sqrt{x}$ rational by contradiction

New goal: false

$$\begin{aligned} &(\exists p,q \in \mathbb{Z})\ \sqrt{x} = p/q \\ \implies &(\exists p,q, \in \mathbb{Z})\ x = \left(\sqrt{x}\right)^2 = p^2/q^2 \\ \implies &(\exists p',q' \in \mathbb{Z})\ x = p'/q' \\ \implies &x \text{ rational} \\ \implies &\text{false by (1)} \end{aligned}$$

Lemma 42: rational lowest terms

Lemma 42.1: positive integers cannot be a product of infinitely many primes

Informal

Goal: $(\forall a \in \mathbb{Z}^+, p_1, p_2, \ldots, p_\infty \text{ prime})\ a \neq p_1 \times p_2 \times \cdots \times p_\infty$

Assume:
1. $a \in Z^+, p_1, p_2, \ldots, p_\infty$ prime
2. $a = p_1 \times p_2 \times \cdots \times p_\infty$ by contradiction

New goal: false

$$
\begin{aligned}
&a \geq 2^{\infty} \text{ by 2 is the smallest prime} \\
\implies &a \notin \mathbb{Z}^{+} \text{ by all integers are finite} \\
\implies &\text{false by (1)}
\end{aligned}
$$

Goal: $(\forall x \in \mathbb{R} \land x > 0)\ x \text{ rational} \iff (\exists m{,}n \in \mathbb{Z}^{+})\ x = m/n \land (\neg(\exists p \text{ prime})\ p|m \land p|n)$

Assume:
1. $x \in \mathbb{R} \land x > 0$

New goal: $x \text{ rational} \iff (\exists m{,}n \in \mathbb{Z}^{+})\ x = m/n \land (\neg(\exists p \text{ prime})\ p|m \land p|n)$

Subgoal: $(\exists m{,}n \in \mathbb{Z}^{+})\ x = m/n \land (\neg(\exists p \text{ prime})\ p|m \land p|n) \implies x \text{ rational}$

$$
\begin{aligned}
&(\exists m{,}n \in \mathbb{Z}^{+})\ x = m/n \land (\neg(\exists p \text{ prime})\ p|m \land p|n) \\
\implies &(\exists m{,}n \in \mathbb{Z})\ x = m/n \\
\iff &x \text{ rational}
\end{aligned}
$$

Subgoal: $x \text{ rational} \implies (\exists m{,}n \in \mathbb{Z}^{+})\ x = m/n \land (\neg(\exists p \text{ prime})\ p|m \land p|n)$

Assume:
2. $x \text{ rational} : (\exists a{,}b \in \mathbb{Z}^{+})\ x = a/b$

New goal: $(\exists m{,}n \in \mathbb{Z}^{+})\ x = m/n \land (\neg(\exists p \text{ prime})\ p|m \land p|n)$

Assume:
3. $(\forall m{,}n \in \mathbb{Z}^{+})\ x \neq m/n \lor (\exists p \text{ prime})\ p|m \land p|n$ by contradiction

New goal: false

$$
\begin{aligned}
&(\forall m{,}n \in \mathbb{Z}^{+})\ x = m/n \implies (\exists p \text{ prime})\ p|m \land p|n \text{ by (3)} \\
\implies &(\exists p_0 \text{ prime})\ p_0|a \land p_0|b \text{ by (2)} \\
\implies &(\exists a_0{,}b_0 \in \mathbb{Z}^{+})\ a = p_0 \times a_0 \land b = p_0 \times b_0 \\
\implies &(\exists p_1 \text{ prime})\ p_1|a_0 \land p_1|b_0 \text{ by setting } x = a_0/b_0 \\
\implies &(\exists a_1{,}b_1 \in \mathbb{Z}^{+})\ a = p_0 \times p_1 \times a_1 \land b = p_0 \times p_1 \times b_1 \\
&\vdots
\end{aligned}
$$

false, positive integers cannot be written as a product of infinitely many primes by (L42.1).

Definition: commutative laws
$(A, e, \otimes)$ satisfies commutative laws iff

$$a \otimes b = b \otimes a$$

Definition: monoid laws
$(A, e, \otimes)$ satisfies monoid laws iff

$$0 \otimes e = e = e \otimes 0$$
$$(a \otimes b) \otimes c = a \otimes (b \otimes c)$$

A monoid is commutative if $(A, e, \otimes)$ satisfies the commutative laws.

Defintion: natural numbers

```
type N =
| zero
| succ of N
```

- $(\mathbb{N}, 0 +)$ is a commutative monoid.
- $(\mathbb{N}, 1, \times)$ is a commutative monoid.