

**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

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

**Definition: real numbers**

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

- $(\exists m, n \in \mathbb{Z}) x = m/n \iff x$  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
- $x \text{ nonnegative} \wedge x \in \mathbb{Z} \iff x \in \mathbb{N}$

**Proposition 10: rational square root**

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

**Proof**

Assume:

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

New goal:  $x$  rational

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

**Definition: modus ponens**

$P \wedge (P \implies Q) \implies Q$

**Theorem 11: implication transitivity**

$$(\forall P_1, P_2, P_3 \text{ statement}) (P_1 \Rightarrow P_2 \wedge P_2 \Rightarrow P_3) \Rightarrow (P_1 \Rightarrow P_3)$$

**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: bi-implication**

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

**Definition: divisibility**

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

**Definition: congruence**

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

**Proposition 16: parity as congruence**

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

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

Assume:

1.  $n$  even

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

$$n \text{ even} \Leftrightarrow (\exists k \in \mathbb{Z}) n = 2 \times k$$

$$\Leftrightarrow (\exists k \in \mathbb{Z}) (n - 0) = 2 \times k$$

$$\Leftrightarrow n \equiv 0 \pmod{2}$$

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

Assume:

1.  $n$  odd

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

$$n \text{ odd} \Leftrightarrow (\exists k \in \mathbb{Z}) n = 2 \times k + 1$$

$$\Leftrightarrow (\exists k \in \mathbb{Z}) (n - 1) = 2 \times k$$

$$\Leftrightarrow n \equiv 1 \pmod{2}$$

**Proposition 18: linearity of congruence**

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

Assume:

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

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

Assume:

3.  $a \equiv b \pmod{m}$

4.  $n \in \mathbb{Z}^+$

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

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

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

Assume:

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

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

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

### Definition

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

### Theorem 19: divisibility of prime products

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

Assume:

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

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

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

Assume:

$$2. 6|n$$

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

Subgoal:  $3|n$

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

Subgoal:  $2|n$

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

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

Assume:

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

New goal:  $6|n$

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

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

Assume:

1.  $l, m, n \in \mathbb{Z}$
2.  $l|m \wedge m|n$

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

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

### Proposition 24: unique existence of proper congruence

#### Lemma 24.1: congruence transitivity

Goal:  $n \equiv x \pmod{m} \wedge n \equiv y \pmod{m} \implies x \equiv y \pmod{m}$

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:  $x \equiv y \pmod{m}$

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

Let  $P(z) : 0 \leq z < m \wedge n \equiv z \pmod{m}$

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

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

Assume:

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

New goal:  $((\exists z) P(z)) \wedge ((\forall x, y) P(x) \wedge P(y) \implies x = y)$

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

**Missing**

This goal is not proved

Subgoal:  $(\forall x, y) P(x) \wedge P(y) \implies x = y$

Assume:

3.  $x, y$  exists
4.  $0 \leq x < m \wedge n \equiv x \pmod{m}$
5.  $0 \leq y < m \wedge n \equiv y \pmod{m}$

New goal:  $x = y$

**Missing**

$$-1 < i < 1 \implies i = 0$$

$$-m < -y \leq 0 \text{ by (4) as (6)}$$

$$-m < x - y < m \text{ by (4) and (6) as (7)}$$

$$x \equiv y \pmod{m} \text{ by (4), (5) and (L24.1)}$$

$$\iff (\exists i \in \mathbb{Z}) x - y = i \times m$$

$$\iff (\exists i \in \mathbb{Z}) -m < i \times m < m \text{ by (7)}$$

$$\iff (\exists i \in \mathbb{Z}) -1 < i < 1 \text{ by cancellation}$$

$$\iff i = 0 \text{ by magic}$$

$$\implies x - y = 0$$

$$\iff x = y$$

### Proposition 25: parity of square

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

Assume:

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

New goal:  $n^2 \equiv 0 \pmod{4} \vee n^2 \equiv 1 \pmod{4}$

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

**Missing**

$$0 \leq z < 2 \implies z = 0 \vee z = 1$$

Assume:

$$2. z = 0 \vee z = 1$$

Case  $z = 0$

$$\begin{aligned} \text{Subgoal: } n &\equiv 0 \pmod{2} \implies \\ n^2 &\equiv 0 \pmod{4} \vee n^2 \equiv 1 \pmod{4} \end{aligned}$$

Assume:

$$3. n \equiv 0 \pmod{2}$$

New goal:

$$n^2 \equiv 0 \pmod{4} \vee n^2 \equiv 1 \pmod{4}$$

$$(\exists i \in \mathbb{Z}) n = i \times 2$$

$$\implies (\exists i \in \mathbb{Z}) n^2 = i^2 \times 4$$

$$\implies (\exists j \in \mathbb{Z}) n^2 = j \times 4$$

$$\implies n^2 \equiv 0 \pmod{4}$$

$$\implies n^2 \equiv 0 \pmod{4} \vee n^2 \equiv 1 \pmod{4}$$

Case  $z = 1$

$$\begin{aligned} \text{Subgoal: } n &\equiv 1 \pmod{2} \implies \\ n^2 &\equiv 0 \pmod{4} \vee n^2 \equiv 1 \pmod{4} \end{aligned}$$

Assume:

$$3. n \equiv 1 \pmod{2}$$

New goal:

$$n^2 \equiv 0 \pmod{4} \vee n^2 \equiv 1 \pmod{4}$$

$$(\exists i \in \mathbb{Z}) n = i \times 2 + 1$$

$$\implies (\exists i \in \mathbb{Z}) n^2 = 4 \times (i^2 + i) + 1$$

$$\implies (\exists j \in \mathbb{Z}) n^2 = 4 \times j + 1$$

$$\implies n^2 \equiv 1 \pmod{4}$$

$$\implies n^2 \equiv 0 \pmod{4} \vee n^2 \equiv 1 \pmod{4}$$

**Lemma 27: congruence at ends of combinations****Definition: combinations**

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

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

**Note**

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

Assume:

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

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

Assume:

$$3. m = 0 \vee m = p$$

Case  $m = 0$

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

Assume:

$$4. m = 0$$

Case  $m = p$

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

Assume:

$$4. m = p$$

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

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

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

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

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

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

### Lemma 28: congruence at non-ends of combinations

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

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

$$p \text{ prime} \Rightarrow (p|(a \times b) \Rightarrow p|a \vee p|b)$$

Assume:

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

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

### Proposition 29: congruence of combinations

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

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

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

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

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

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

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

**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.  $m, n \in \mathbb{N}, p \text{ prime}$

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

**Informal**

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

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

$$\Rightarrow (m + n)^p \equiv m^p + n^p \pmod{p}$$

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.  $m \in \mathbb{N}, p \text{ prime}$

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

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

$$\Rightarrow (\forall m \in \mathbb{N}) (m + 1)^p \equiv m^p + 1 \pmod{p}$$

**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.  $m, i \in \mathbb{N}, p \text{ prime}$

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

**Informal**

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

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.  $i \in \mathbb{N}, p \text{ prime}$

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**

$$\begin{aligned}
 \neg(P \implies Q) &\iff P \wedge \neg Q \\
 \neg(P \iff Q) &\iff P \not\iff \neg Q \\
 \neg(P \wedge Q) &\iff \neg P \vee \neg Q \\
 \neg(P \vee Q) &\iff \neg P \wedge \neg Q \\
 \neg(\forall x) P(x) &\iff (\exists x) \neg P(x) \\
 \neg(\exists x) P(x) &\iff (\forall x) \neg P(x) \\
 \neg(\neg P) &\iff P \\
 \neg P &\iff (P \implies \text{false})
 \end{aligned}$$

**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

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

**Theorem 39: contrapositive reverse**Goal:  $(\neg Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow Q)$ 

Assume:

1.  $\neg Q \Rightarrow \neg P$
2.  $P$

New goal:  $Q$ 

Assume:

3.  $\neg Q$  by contradiction

New goal: false

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

**Corollary 40: contrapositive bi-implication**Goal:  $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$ 

Subgoal:  $(P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)$   
 Exact (T37)

Subgoal:  $(P \Rightarrow Q) \Leftarrow (\neg Q \Rightarrow \neg P)$   
 Exact (T38)

**Corollary 41: square root irrational**Goal:  $(\forall x) x \text{ irrational} \wedge x > 0 \Rightarrow \sqrt{x} \text{ irrational}$ 

Assume:

1.  $x \text{ irrational} \wedge x > 0$

New goal:  $\sqrt{x}$  irrational

Assume:

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

New goal: false

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

**Lemma 42: rational lowest terms**

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

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

Assume:

1.  $a \in \mathbb{Z}^+, p_1, p_2, \dots, p_\infty \text{ prime}$
2.  $a = p_1 \times p_2 \times \dots \times p_\infty$  by contradiction

New goal: false

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

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

Assume:

$$1. x \in \mathbb{R} \wedge x > 0$$

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

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

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

Assume:

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

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

Assume:

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

New goal: false

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

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

$$\begin{aligned} 0 \otimes e &= e = e \otimes 0 \\ (a \otimes b) \otimes c &= a \otimes (b \otimes c) \end{aligned}$$

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

### Definition: semiring

$(A, e_1, \oplus, e_2, \otimes)$  is a semiring if

- $(A, e_1, \oplus)$  is a commutative monoid.
- $(A, e_1, \otimes)$  is a monoid.
- $\otimes$  is distributive over  $\oplus$ :  $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

A semiring is commutative if  $\otimes$  is.

### Definition: cancellation

- $\oplus$  allows cancellation by  $c$  on the left if  $c \oplus x = c \oplus y \implies x = y$
- $\oplus$  allows cancellation by  $c$  on the right if  $x \oplus c = y \oplus c \implies x = y$
- $\oplus$  allows cancellation by  $c$  if it allows cancellation both on the left and on the right.

### Defintion: natural numbers

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

- $(\mathbb{N}, 0 +, 1, \times)$  is a commutative semiring.
- $+$  supports cancellation by any  $c$
- $\times$  supports cancellation by any  $c \neq 0$

### Definition: inverse

$(\exists l \in A) l \oplus x = e \implies x$  admits an inverse to the left

$(\exists r \in A) x \oplus r = e \implies x$  admits an inverse to the right

$x$  admits an inverse to the left and right  $\implies x$  admits an inverse

## Proposition 47: equality of inverses

Goal:  $(\forall (A, e, \oplus) \text{ monoid}) x \text{ admits an inverse} \implies l = r$

Assume:

1.  $(A, e, \oplus)$  monoid
2.  $(\exists l) l \oplus x = e$
3.  $(\exists r) x \oplus r = e$

New goal:  $l = r$

$$\begin{aligned} l &= l \oplus e \\ &= l \oplus (x \oplus r) \\ &= (l \oplus x) \oplus r \text{ commutative by monoid property} \\ &= e \oplus r \\ &= r \end{aligned}$$

**Definition: group**

- A group is a monoid which every element has an inverse.
- The group is commutative if the monoid is commutative.

**Definition: additive and multiplicative inverses**

- $x$  admits an additive inverse if  $(\exists y) x + y = 0$
- $x$  admits a multiplicative inverse if  $(\exists y) x \times y = 1$

**Definition: ring**

A ring  $(A, e_1, \oplus, e_2, \otimes)$  is a semiring where  $(A, e_1, \oplus)$  is a group.

The ring is commutative if  $(A, e_2, \otimes)$  is.

**Definition: field**

A field  $(A, e_1, \oplus, e_2, \otimes)$  is a commutative ring where every element besides 0 has an inverse with respect to  $\otimes$ .

**Definition: integers and rationals**

- The integers  $\mathbb{Z}$  admits all additive inverses,  $(\mathbb{Z}, 0, +, 1, \times)$  is a commutative ring.
- The rationals  $\mathbb{Q}$  also admits all multiplicative inverses,  $(\mathbb{Q}, 0, +, 1, \times)$  is a field.

**Theorem 53: division theorem**

Let  $P(q, r) : q \geq 0 \wedge 0 \leq r \leq n \wedge q \times n = r$

Goal:  $(\forall m, n \in \mathbb{N}) (\exists! q, !r \in \mathbb{Z}) P(q, r)$

Assume:

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

New goal:  $((\exists q, r \in \mathbb{Z}) P(q, r)) \wedge (P(q, r) \wedge P(q', r') \Rightarrow q = q' \wedge r = r')$

Subgoal:  $(\exists q, r \in \mathbb{Z}) P(q, r)$

**Missing**

This goal is not proved.

Subgoal:  $P(q, r) \wedge P(q', r') \Rightarrow q = q' \wedge r = r'$

Assume:

2.  $q \geq 0 \wedge 0 \leq r < n \wedge q \times n + r = m$
3.  $q' \geq 0 \wedge 0 \leq r' < n \wedge q' \times n + r' = m$

Goal:  $q = q' \wedge r = r'$

$$0 \leq r < n \wedge -n < r \leq 0$$

$$\Rightarrow -n < r - r' < n \text{ by (2) and (3) as (4)}$$

$$m - r = q \times n \Rightarrow m \equiv r \pmod{n} \text{ by (2)}$$

$$m - r' = q' \times n \Rightarrow m \equiv r' \pmod{n} \text{ by (3)}$$

$$\Rightarrow r \equiv r' \pmod{n} \text{ by (L24.1)}$$

$$\Rightarrow (\exists i \in \mathbb{Z}) r - r' = i \times n$$

$$\Rightarrow i = 0 \wedge r = r' \text{ by (4)}$$

$$\Rightarrow q = q' \text{ by cancellation}$$

**Definition: quo and rem**

For the  $q$  and  $r$  associated by  $m = q \times n + r$

- $\text{quo}(m, n) = q$
- $\text{rem}(m, n) = r$

And satisfies the property  $m = \text{quo}(m, n) \times n + \text{rem}(m, n)$

**Theorem 56: existence of quotient and remainder**

```
let divalg m n =
  let diviter q r =
    if r < n then (q, r)
    else diviter (q + 1) (r - n)
  in diviter 0 m
```

Goal:  $\text{divalg}$  terminates  $\wedge$  ( $\text{divalg}$  terminates with  $(q_0, r_0) \Rightarrow r_0 < n \wedge m = q_0 \times n + r_0$ )

Subgoal:  $\text{divalg}$  terminates

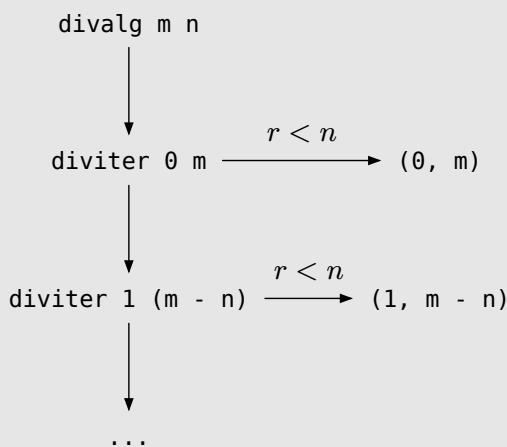
**Note**

This goal is also called **total correctness**.

**Informal**

$r \in \mathbb{N}$  decreases in each step, which is bounded below. This cannot continue forever.

It must terminate.



Subgoal:

$\text{divalg}$  terminates with  $(q_0, r_0) \Rightarrow r_0 < n \wedge m = q_0 \times n + r_0$

**Note**

This goal is also called **partial correctness**.

Assume:

1.  $\text{divalg}$  terminates with  $(q_0, r_0)$

New goal:  $r_0 < n \wedge m = q_0 \times n + r_0$

**Informal**

In the  $n$ th call of  $\text{diviter}$

1.  $\text{diviter } 0 \ m : m = q_0 \times n + r_0$  by trivial, if  $r_0 < n$  terminate. Otherwise
2.  $\text{diviter } q_1 \ r_1 \ m = q_1 \times n + r_1$  by trivial, if  $r_1 < n$  terminate. Otherwise
3. ...

$$m = (q + 1) \times n + (r - n)$$

If the property holds for one point of the computation, then it holds for the next point of computation, this is called **proof by invariant**.

**Proposition 57: uniqueness of remainder**

Goal:  $k \equiv l \pmod{m} \Leftrightarrow \text{rem}(k, m) = \text{rem}(l, m)$

Subgoal:  $\text{rem}(k, m) = \text{rem}(l, m) \Rightarrow k \equiv l \pmod{m}$

Assume:

$$1. \text{ rem}(k, m) = \text{rem}(l, m)$$

New goal:  $k \equiv l \pmod{m}$

$$\begin{aligned} & (\exists q, r \in \mathbb{N}) \ k = q \times m + r \text{ by (1)} \\ & (\exists q', r' \in \mathbb{N}) \ l = q' \times m + r' \text{ by (1)} \\ \implies & k - l = (q - q') \times m + (r - r') \\ \implies & (\exists a \in \mathbb{N}) \ k - l = a \times m \\ \implies & k \equiv l \pmod{m} \end{aligned}$$

Subgoal:  $k \equiv l \pmod{m} \implies \text{rem}(k, m) \wedge \text{rem}(l, m)$

Assume:

$$1. \ k \equiv l \pmod{m}$$

New goal:  $\text{rem}(k, m) = \text{rem}(l, m)$

$$\begin{aligned} & (\exists a \in \mathbb{Z}) \ k - l = a \times m \\ \implies & (\exists q, r, q', r' \in \mathbb{Z}) \ (q \times m + r) - (q' \times m + r') = a \times m \text{ by (T56)} \\ \implies & r - r' = (a - q + q') \times m \\ \implies & r - r' = 0 \times m \text{ by bound } (-m) < r - r' < m \\ \implies & r = r' \end{aligned}$$

### Corollary 58.1: congruence with remainder

Goal:  $(\forall m \in \mathbb{N}) \ n \equiv \text{rem}(n, m) \pmod{m}$

Assume:

$$1. \ m \in \mathbb{N}$$

New goal:  $n \equiv \text{rem}(n, m) \pmod{m}$

$$\begin{aligned} & (\exists a \in \mathbb{Z}) \ n = m \times \text{quo}(n, m) + \text{rem}(n, m) \\ \implies & n - \text{rem}(n, m) = m \times \text{quo}(n, m) \\ \implies & n \equiv \text{rem}(n, m) \pmod{m} \end{aligned}$$

### Corollary 58.2: existence of modulus integer

Goal:  $(\forall k \in \mathbb{Z}) \ (\exists! [k]_m) \ 0 \leq [k]_m < m \wedge k \equiv [k]_m \pmod{m}$

Subgoal:  $(\forall k \in \mathbb{N}) \ (\exists! [k]_m) \ 0 \leq [k]_m < m \wedge k \equiv [k]_m \pmod{m}$

Assume:

$$1. \ k \in \mathbb{N}$$

New goal:  $(\exists! [k]_m) \ 0 \leq [k]_m < m \wedge k \equiv [k]_m \pmod{m}$

Let  $[k]_m = \text{rem}(k, m)$ .

Let  $P(k) : 0 \leq [k]_m < m \wedge k \equiv [k]_m \pmod{m}$

New goal:  $P([k]_m) \wedge (P(a) \wedge P(b) \implies a = b)$

<p>Subgoal:  <math>0 \leq [k]_m &lt; m \wedge k \equiv [k]_m \pmod{m}</math>  Exact by (T56) and (P57).</p>	<p>Subgoal: <math>P(a) \wedge P(b) \implies a = b</math>  Assume:  2. <math>0 \leq a &lt; m \wedge k \equiv a \pmod{m}</math>  3. <math>0 \leq b &lt; m \wedge k \equiv b \pmod{m}</math>  New goal: <math>a = b</math>  <math>-m &lt; a - b &lt; m</math> by (2) and (3)  <math>(\exists i \in \mathbb{Z}) a - b = i \times m</math> by (2) and (3)  <math>\implies i = 0 \wedge a = b</math> by bounds</p>
,	

<p>Subgoal: <math>(\forall k \in \mathbb{Z}^-) (\exists! [k]_m) 0 \leq [k]_m &lt; m \wedge k \equiv [k]_m \pmod{m}</math></p> <p>Assume:</p> <p>1. <math>k \in \mathbb{Z}^-</math></p> <p>New goal: <math>(\exists! [k]_m) 0 \leq [k]_m &lt; m \wedge k \equiv [k]_m \pmod{m}</math></p> <p><math>(\exists i \in \mathbb{Z}) k + i \times m \geq 0</math> by magic</p> <p><math>k + i \times m \equiv k \pmod{m}</math> by trivial</p> <p>Then get the goal by setting <math>k' = k + i \times m</math> using the previous subgoal.</p>
---

### Definition: modular arithmetic

$$k +_m l = [k + l]_m = \text{rem}(k + l, m)$$

$$k \times_m l = [k \times l]_m = \text{rem}(k \times l, m)$$

### Proposition 62: modular arithmetic is a commutative ring

Goal:  $(\mathbb{Z}_m, 0, +_m, 1, \times_m)$  is a commutative ring

<p>Subgoal: <math>(\mathbb{Z}_m, 0, +_m)</math> is a commutative monoid</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 5px;">Property</th><th style="text-align: left; padding: 5px;">Proof</th></tr> </thead> <tbody> <tr> <td style="padding: 5px;">Commutative</td><td style="padding: 5px;"><math>a_m +_m b_m = \text{rem}(a_m + b_m) = b_m +_m a_m</math></td></tr> <tr> <td style="padding: 5px;">Neutral element</td><td style="padding: 5px;"><math>0_m +_m a_m = a_m = a_m + 0_m</math></td></tr> <tr> <td style="padding: 5px;">Associativity</td><td style="padding: 5px;"><math>(a_m +_m b_m) +_m c_m = \text{rem}(a_m + b_m + c_m) = a_m +_m (b_m +_m c_m)</math></td></tr> </tbody> </table>		Property	Proof	Commutative	$a_m +_m b_m = \text{rem}(a_m + b_m) = b_m +_m a_m$	Neutral element	$0_m +_m a_m = a_m = a_m + 0_m$	Associativity	$(a_m +_m b_m) +_m c_m = \text{rem}(a_m + b_m + c_m) = a_m +_m (b_m +_m c_m)$
Property	Proof								
Commutative	$a_m +_m b_m = \text{rem}(a_m + b_m) = b_m +_m a_m$								
Neutral element	$0_m +_m a_m = a_m = a_m + 0_m$								
Associativity	$(a_m +_m b_m) +_m c_m = \text{rem}(a_m + b_m + c_m) = a_m +_m (b_m +_m c_m)$								

<p>Subgoal: <math>(\mathbb{Z}_m, 1, \times_m)</math> is a commutative monoid</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 5px;">Property</th><th style="text-align: left; padding: 5px;">Proof</th></tr> </thead> <tbody> <tr> <td style="padding: 5px;">Commutative</td><td style="padding: 5px;"><math>a_m \times_m b_m = \text{rem}(a_m \times b_m) = b_m \times_m a_m</math></td></tr> <tr> <td style="padding: 5px;">Neutral element</td><td style="padding: 5px;"><math>1_m \times_m a_m = a_m = a_m \times 1_m</math></td></tr> <tr> <td style="padding: 5px;">Associativity</td><td style="padding: 5px;"><math>(a_m \times_m b_m) \times_m c_m = \text{rem}(a_m \times b_m \times c_m) = a_m \times_m (b_m \times_m c_m)</math></td></tr> </tbody> </table>		Property	Proof	Commutative	$a_m \times_m b_m = \text{rem}(a_m \times b_m) = b_m \times_m a_m$	Neutral element	$1_m \times_m a_m = a_m = a_m \times 1_m$	Associativity	$(a_m \times_m b_m) \times_m c_m = \text{rem}(a_m \times b_m \times c_m) = a_m \times_m (b_m \times_m c_m)$
Property	Proof								
Commutative	$a_m \times_m b_m = \text{rem}(a_m \times b_m) = b_m \times_m a_m$								
Neutral element	$1_m \times_m a_m = a_m = a_m \times 1_m$								
Associativity	$(a_m \times_m b_m) \times_m c_m = \text{rem}(a_m \times b_m \times c_m) = a_m \times_m (b_m \times_m c_m)$								

Subgoal:  $(\mathbb{Z}_m, 0, +_m, 1, \times_m)$  is a semiring

Apply subgoals (1) and (2).

New goal: distributivity  $a_m \times (b_m +_m c_n) = a_m \times_m b_m +_m a_m \times_m c_m$

$$\begin{aligned} a_m \times (b_m +_m c_n) &\equiv a_m \times (b_m +_m c_m) \pmod{m} \\ &\equiv a_m \times (b_m + c_m) \pmod{m} \\ &\equiv a_m \times b_m + a_m \times c_m \pmod{m} \\ &\equiv a_m \times_m b_m +_m a_m \times_m c_m \pmod{m} \end{aligned}$$

Subgoal:  $(\mathbb{Z}_m, 0, +)$  is a group

Apply subgoal (1).

New goal:  $(\forall x_m \in \mathbb{Z}_m) (\exists y_m \in \mathbb{Z}_m) [x_m +_m y_m] = 0$

Assume:

$$1. \quad x_m \in \mathbb{Z}_m$$

$$\text{Let } y_m = [-x_m]_m$$

$$\text{New goal: } x_m +_m y_m = 0$$

$$\begin{aligned} x_m +_m y_m &\equiv x_m + [-x]_m \pmod{m} \\ &\equiv x_m + (m - x_m) \pmod{m} \text{ by trivial } \equiv m \pmod{m} \\ &\equiv 0 \pmod{m} \end{aligned}$$

Sugboal:  $(\mathbb{Z}_m, 0, +_m, 1, \times_m)$  is a commutative ring.

Exact by subgoal (2) and (4).

### Proposition 63: condition for reciprocal

Goal:  $(\forall m \in \mathbb{Z}^+, k \in \mathbb{Z}_m) ((\exists l \in \mathbb{Z}_m) k \times_m l = 1) \iff ((\exists i, j \in \mathbb{Z}) k \times i + m \times j = 1)$

Assume:

$$1. \quad m \in \mathbb{Z}^+, k \in \mathbb{Z}_m$$

Subgoal:  $((\exists l \in \mathbb{Z}_m) k \times_m l = 1) \implies ((\exists i, j \in \mathbb{Z}) k \times i + m \times j = 1)$

Assume:

$$2. \quad (\exists l \in \mathbb{Z}_m) k \times_m l = 1$$

$$\text{New goal: } (\exists i, j \in \mathbb{Z}) k \times i + m \times j = 1$$

$$\text{Let } i = k$$

$$\text{New goal: } (\exists j \in \mathbb{Z}) k \times l + m \times j = 1$$

$$\begin{aligned} &(\exists l \in \mathbb{Z}_m) k \times l \equiv 1 \pmod{m} \\ &\implies (\exists a \in \mathbb{Z}) k \times l - 1 = m \times a \\ &\implies (\exists j \in \mathbb{Z}) k \times l + m \times j = 1 \end{aligned}$$

Subgoal:  $((\exists i, j \in \mathbb{Z}) k \times i + m \times j = 1) \implies ((\exists l \in \mathbb{Z}_m) k \times_m l = 1)$

Assume:

$$2. (\exists i, j \in \mathbb{Z}) k \times i + m \times j = 1$$

New goal:  $(\exists l \in \mathbb{Z}_m) k \times_m l = 1$

$$(\exists i, j \in \mathbb{Z}) k \times i - 1 = m \times (-j)$$

$$(\exists i, a \in \mathbb{Z}) k \times i - 1 = m \times a$$

$$k \times i \equiv 1 \pmod{m}$$

$$k \times_m [i]_m = 1$$

### Definition: linear combination

$r \in \mathbb{Z}$  is a linear combination of  $m, n \in \mathbb{Z}$  if

$$(\exists s, t \in \mathbb{Z}) s \times m + t \times n = r$$

### Proposition 65: condition for reciprocal (linar combination)

Goal:  $(\forall k \in \mathbb{Z}_m) ((\exists l \in \mathbb{Z}_m) k \times_m l = 1) \iff 1$  is a linear combination of  $m$  and  $k$

Exact by (P63).

### Definition: sets

- $x \in A$  if  $x$  is an element in  $A$
- $A = B \iff ((\forall x) x \in A \iff x \in B)$
- $\{x \in A \mid P(x)\} = \{x \in A \mid Q(x)\} \iff ((\forall x \in A) P(x) \iff Q(x))$