Recall $\neg P = P \Rightarrow \text{false}$

Theorem 37 *For all statements* P *and* Q,

$$(P \implies Q) \implies (\neg Q \implies \neg P) \ .$$

PROOF: Let P and Q be statements.

① Assume $P \Rightarrow Q$

② Assume $\neg Q$; that is, $Q \Rightarrow$ false

RTP: $\neg P$

$\boxed{?}$ $(\neg Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow Q)$?

③ Assume: P

RTP: false

From ① & ③, by MP, we have Q ④

From ② & ④, by MP, we have false

$\boxtimes$

Proof by contradiction

The strategy for proof by contradiction:

To prove a goal P by contradiction is to prove the equivalent statement $\underbrace{\neg P \implies \mathbf{false}}_{\neg\neg P}$

instead of proving P we prove $\neg\neg P$.

classical

$P \iff \neg\neg P$

$(P \vee \neg P) \iff true$

Proof by contradiction

The strategy for proof by contradiction:

To prove a goal P by contradiction is to prove the equivalent statement $\neg\mathrm{P} \implies \mathbf{false}$

Proof pattern:

In order to prove

$$\mathrm{P}$$

1. Write: We use proof by contradiction. So, suppose P is false.
2. Deduce a logical contradiction.
3. Write: This is a contradiction. Therefore, P must be true.

Scratch work:

Before using the strategy

Assumptions	Goal
	P
$\vdots$	

After using the strategy

Assumptions	Goal
	contradiction
$\vdots$	
$\neg P$	

Theorem 39 *For all statements* P *and* Q,

$$(\neg \mathrm{Q} \implies \neg \mathrm{P}) \implies (\mathrm{P} \implies \mathrm{Q}) \quad .$$

PROOF: Let P, Q be statements.

(1) Assume $\neg Q \Rightarrow \neg P$

(2) Assume: P

RTP: Q

By contradiction (3) Assume $\neg Q$

From (1) & (3) by MP, we have (4) $\neg P$

From (2) & (4), we have a contradiction.

Hence, by contradiction, Q holds. $\boxtimes$

Lemma 41 *A positive real number* x *is rational iff*

$$\exists \textit{ positive integers } m, n : \quad x = m/n \wedge \neg(\exists \textit{ prime } p : p \mid m \wedge p \mid n) \qquad (\dagger)$$

PROOF: ($\Leftarrow$) Exercise.

($\Rightarrow$) Let x be a positive real.

Assume x is rational; that is, there are positive integers i and j such that $x = i/j$.

RTP: ($\dagger$)

We proceed by contradiction, Assuming $\neg(\dagger)$ we will derive an absurdity.

$$(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$$

Examine

$$\neg(t)$$

$$\Leftrightarrow \left(\forall \text{ pos. int. } m, n. \quad \neg\left(x = m/n\right) \vee \left(\exists \text{ prime } p : p \mid m \wedge p \mid n\right)\right)$$

$$\Leftrightarrow (*) \left(\forall \text{ pos. int. } m, n. \quad x = m/n \Rightarrow \exists \text{ prime } p : p \mid m \wedge p \mid n \right)$$

Recap: Assuming (*) we need establish a contradiction.

Idea

$$x = i/j \overset{(*)}{\Longrightarrow} x = p_0 \cdot i_0 / p_0 \cdot j_0 \qquad i = p_0 \cdot i_0$$

$$x = i_0/j_0 \Longrightarrow x = p_1 i_1 / p_1 j_1 \qquad i_0 = p_1 i_1$$

$$x = i_1/j_1 \Longrightarrow x = p_2 \cdot i_2 / p_2 \cdot j_2 \qquad i_1 = p_2 \cdot i_2$$

$$\vdots$$

if $k = i$ this is absurd

$$i = p_0 \cdot i_0 = p_0 \cdot p_1 \cdot i_1 = p_0 \cdot p_1 \cdot p_2 \cdot i_2 =$$

$$= \cdots = p_0 \cdot p_1 \cdot p_2 \cdots\cdots p_k \cdot i_k \geq 2^{k+1}$$

Numbers

Objectives

- Get an appreciation for the abstract notion of number system, considering four examples: natural numbers, integers, rationals, and modular integers.

- Prove the correctness of three basic algorithms in the theory of numbers: the division algorithm, Euclid's algorithm, and the Extended Euclid's algorithm.

- Exemplify the use of the mathematical theory surrounding Euclid's Theorem and Fermat's Little Theorem in the context of public-key cryptography.

- To understand and be able to proficiently use the Principle of Mathematical Induction in its various forms.

Natural numbers

In the beginning there were the *natural numbers*

$$\mathbb{N} \ : \quad 0 \, , \quad 1 \, , \quad \ldots \, , \quad n \, , \quad n+1 \, , \quad \ldots$$

generated from *zero* by successive increment; that is, put in ML:

```
datatype
  N = zero | succ of N
```

The basic operations of this number system are:

- Addition

$$\underbrace{\overbrace{*\cdots*}^{\mathfrak{m}}\overbrace{*\cdots\cdots*}^{\mathfrak{n}}}_{\mathfrak{m}+\mathfrak{n}}$$

- Multiplication

$$\mathfrak{m}\left\{\begin{array}{ccc} \multicolumn{3}{c}{\overbrace{*\cdots\cdots\cdots\cdots*}^{\mathfrak{n}}} \\ \vdots & \mathfrak{m}\cdot\mathfrak{n} & \vdots \\ * & \cdots\cdots\cdots & * \end{array}\right.$$

0 is a neutral element
for +

The *additive structure* $(\mathbb{N}, 0, +)$ of natural numbers with zero and addition satisfies the following:

the notation $l+m+n$ makes sense!

- Monoid laws

$$0+n=n=n+0 \quad , \quad (l+m)+n=l+(m+n)$$

- Commutativity law

$$m+n=n+m$$

and as such is what in the mathematical jargon is referred to as a *commutative monoid*.

Also the *multiplicative structure* $(\mathbb{N}, 1, \cdot)$ of natural numbers with one and multiplication is a commutative monoid:

- Monoid laws

$$1 \cdot n = n = n \cdot 1 \quad , \quad (l \cdot m) \cdot n = l \cdot (m \cdot n)$$

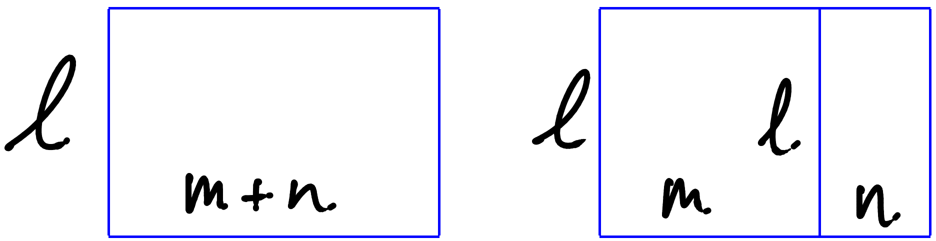
- Commutativity law

$$m \cdot n = n \cdot m$$

The additive and multiplicative structures interact nicely in that they satisfy the

- Distributive law

$$l \cdot (m + n) \;=\; l \cdot m + l \cdot n$$



and make the overall structure $(\mathbb{N}, 0, +, 1, \cdot)$ into what in the mathematical jargon is referred to as a *commutative semiring*.