Negation

Negations are statements of the form

$$\boxed{\text{not } P}$$

or, in other words,

$$\boxed{P \text{ is not the case}}$$

or

$$\boxed{P \text{ is absurd}}$$

or

$$\boxed{P \text{ leads to contradiction}}$$

or, in symbols,

$$\boxed{\neg P}$$

A first proof strategy for negated goals and assumptions:

If possible, reexpress the negation in an *equivalent* form and use instead this other statement.

Logical equivalences

$$
\begin{array}{rcl}
\neg\big(\,P \Longrightarrow Q\,\big) & \iff & P \wedge \neg Q \\
\neg\big(\,P \iff Q\,\big) & \iff & P \iff \neg Q \\
\neg\big(\forall x.\, P(x)\big) & \iff & \exists x.\, \neg P(x) \\
\neg\big(P \wedge Q\big) & \iff & (\neg P) \vee (\neg Q) \\
\neg\big(\exists x.\, P(x)\big) & \iff & \forall x.\, \neg P(x) \\
\neg\big(P \vee Q\big) & \iff & (\neg P) \wedge (\neg Q) \\
\neg\big(\neg P\big) & \iff & P \\
\neg P & \iff & (P \Rightarrow \textbf{false})
\end{array}
$$

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

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

PROOF: Let P and Q be statements

Assume $P \Rightarrow Q$

Assume $Q \Rightarrow$ false $(\Longleftrightarrow \neg Q)$

Therefore $P \Rightarrow$ false $(\Longleftrightarrow \neg P)$

$\boxtimes$

Proof by contradiction

The strategy for proof by contradiction:

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

Proof pattern:

In order to prove

$$P$$

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,

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

PROOF: Let P and Q be statements.

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

Assume P (2)

RTP: Q

By contradiction, assume $\neg Q$ (3)

From (3) and (1), we have $\neg P$ (4)

From (2) and (4), we obtain a contradiction.

Therefore Q holds. ☒

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: Let x be a positive real number.

($\Leftarrow$) Vacuous. = Trivial = Straightforward = Easy = ...

($\Rightarrow$) Assume x is rational. That is,

$\exists$ a, b int. $x = a/b$. (#)

RTP: (†)

By contradiction,

Assume: $\neg[\exists$ pos. int. m, n. $x = m/n$
$\wedge \neg(\exists$ prime p. $p \mid m \wedge p \mid n)]$

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

Equivalently

Assume: $\forall$ pos. int. m, n.

$$x = m/n \Rightarrow \exists \text{ prime } p.\ p \mid m \wedge p \mid n.$$

Let a_0, b_0 be pos. int. such that $x = a_0/b_0$ (using assumption (#))

By instantiation and MP,

$$\exists \text{ prime } p_0.\ p_0 \mid a_0 \wedge p_0 \mid b_0$$

Therefore

$$\exists\, a_1, b_1 \text{ pos. int. } a_0 = p_0 \cdot a_1 \wedge b_0 = p_0 \cdot b_1$$

Moreover $x = a_0/b_0 = p_0 \cdot a_1 / p_0 \cdot b_1 = a_1/b_1$

Therefore $\exists\, p_1$ prime $p_1 \mid a_1 \wedge p_1 \mid b_1$

Again $\exists\, a_2, b_2 .\ a_1 = p_1 \cdot a_2 \wedge b_1 = p_1 \cdot b_2$

So $x = a_1/b_1 = p_1 \cdot a_2 / p_1 \cdot b_2 = a_2/b_2$

NB: $a_0 = p_0 \cdot a_1 = p_0 \cdot p_1 \cdot a_2$

$b_0 = p_0 \cdot b_1 = p_0 \cdot p_1 \cdot b_2$

Iterating the argument: $a_0 = p_0 \cdot a_1 = p_0 \cdot p_1 \cdot a_2 = p_0 \cdot p_1 \cdot p_2 \cdot a_3$

$= p_0 \cdot p_1 \cdot p_2 \cdots p_n \cdot a_{n+1} \geq 2^n \cdot a_{n+1}$

For arbitrary n, we have $a_0 \geq 2^n$

In particular for $n = a_0$, $a_0 \geq 2^{a_0}$

a contradiction ↯ $\boxtimes$

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

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

- Multiplication

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

neutral element

operation

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

associativity.

- 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

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

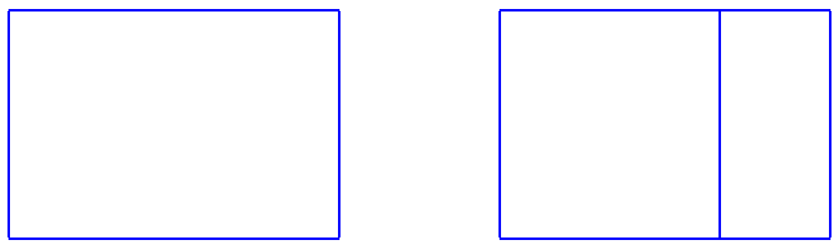
- Commutativity law

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

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

- Distributive law

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



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

Cancellation

The additive and multiplicative structures of natural numbers further satisfy the following laws.

- Additive cancellation

  For all natural numbers k, m, n,

  $$k + m = k + n \implies m = n \quad .$$

- Multiplicative cancellation

  For all natural numbers k, m, n,

  if $k \neq 0$ then $k \cdot m = k \cdot n \implies m = n \quad .$

Inverses

Definition 42

1. *A number* x *is said to admit an* additive inverse *whenever there exists a number* y *such that* $x + y = 0$.

2. *A number* x *is said to admit a* multiplicative inverse *whenever there exists a number* y *such that* $x \cdot y = 1$.

Extending the system of natural numbers to: (i) admit all additive inverses and then (ii) also admit all multiplicative inverses for non-zero numbers yields two very interesting results:

(i) the *integers*

$$\mathbb{Z} \;:\quad \ldots -n\,,\ \ldots\,,\ -1\,,\ 0\,,\ 1\,,\ \ldots\,,\ n\,,\ \ldots$$

which then form what in the mathematical jargon is referred to as a *commutative ring*, and

(ii) the *rationals* $\mathbb{Q}$ which then form what in the mathematical jargon is referred to as a *field*.

The division theorem and algorithm

Theorem 43 (Division Theorem) *For every natural number* m *and positive natural number* n*, there exists a unique pair of integers* q *and* r *such that* $q \geq 0$, $0 \leq r < n$, *and* $m = q \cdot n + r$.