Fermat's Little Theorem

The Many Dropout Lemma (Proposition 35) gives the first part of the following very important theorem as a corollary.

Theorem 36 (Fermat's Little Theorem) *For all natural numbers* i *and primes* p*,*

1. $\mathrm{i}^{\mathrm{p}} \equiv \mathrm{i} \pmod{\mathrm{p}}$*, and*
2. $\mathrm{i}^{\mathrm{p}-1} \equiv 1 \pmod{\mathrm{p}}$ *whenever* i *is not a multiple of* p*.*

$i \not\equiv 0 \pmod{p}$

The fact that the first part of Fermat's Little Theorem implies the second one will be proved later on .

Every natural number i not a multiple of a prime number p has a *reciprocal* modulo p, namely i^{p-2}, as $i \cdot (i^{p-2}) \equiv 1 \pmod{p}$.

Btw

1. Fermat's Little Theorem has applications to:
   (a) primality testing[a],
   (b) the verification of floating-point algorithms, and
   (c) cryptographic security.

[a] For instance, to establish that a positive integer $\mathtt{m}$ is not prime one may proceed to find an integer $\mathtt{i}$ such that $\mathtt{i}^{\mathtt{m}} \not\equiv \mathtt{i} \pmod{\mathtt{m}}$.

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

$$
\begin{aligned}
\neg(P \Longrightarrow Q) &\iff P \wedge \neg Q \\
\neg(P \Longleftrightarrow Q) &\iff P \Longleftrightarrow \neg Q \\
\neg(\forall x.\, P(x)) &\iff \exists x.\, \neg P(x) \\
\neg(P \wedge Q) &\iff (\neg P) \vee (\neg Q) \\
\neg(\exists x.\, P(x)) &\iff \forall x.\, \neg P(x) \\
\neg(P \vee Q) &\iff (\neg P) \wedge (\neg Q) \\
\neg(\neg P) &\iff P \\
\neg P &\iff (P \Rightarrow \mathbf{false})
\end{aligned}
$$

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

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

PROOF: Assume P, Q statements.

Assume: ① $P \Rightarrow Q$

Assume: $\neg Q \Leftrightarrow$ ② $(Q \Rightarrow \text{false})$

From ① and ②, we have $(P \Rightarrow \text{false}) \Leftrightarrow \neg P$.

as required.

Proof by contradiction

Amongst the equivalences for negation, we have postulated the somewhat controversial:

$$\neg\neg P \iff P$$

which is *classically* accepted.

In this light,

to prove P or equivalently $\neg\neg P$

one may equivalently

prove $\neg P \implies \mathbf{false}$;

$\Downarrow$

$(\neg P \Rightarrow \text{false})$

that is,

assuming $\neg P$ leads to contradiction.

This technique is known as *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,

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

PROOF: Let P, Q be statements.

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

Assume: (2) P

RTP: Q.

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

Then from (1) and (3), we have (4) $\neg P \Leftrightarrow (P \Rightarrow \text{false})$

Therefore, from (2) and (4) we have a contradiction.

So, by proof by contradiction, we have Q as required ☒

Proof by contrapositive

Corollary 40 *For all statements* P *and* Q*,*

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

Btw Using the above equivalence to prove an implication is known as *proof by contrapositive*.

Corollary 41 *For every positive irrational number* x*, the real number* $\sqrt{x}$ *is irrational.*

$(x \text{ irrational} \Rightarrow \sqrt{x} \text{ irrational}) \Leftrightarrow (\sqrt{x} \text{ rational} \Rightarrow x \text{ rational})$

Lemma 42 *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 pos. real number.

($\Rightarrow$) ($\dagger$) $\Rightarrow$ x rational ✓

($\Leftarrow$) Assume: x rational; That is, ① $x = a/b$ for some pos. int. a and b.

RTP: ($\dagger$)

By contradiction, assume $\neg(\dagger)$

Equivalently,

$$\neg(\exists \text{pos.int } m,n.\ x = m/n \wedge \neg(\exists \text{prime } p.\ p \mid m \wedge p \mid n))$$

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

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

$$\Leftrightarrow (2)\ \forall \text{pos.int } m,n.\ x = m/n \Rightarrow \exists \text{ prime } p.\ p \mid m \wedge p \mid n$$

By ①, $x = a/b$ for pos. int a, b.
and together with ② we have $\exists$ prime. $p_0 \mid a \wedge p \mid b$.
$a = p_0 \cdot a_0$ and $b = p_0 \cdot b_0$ for pos. int. a_0 and b_0.
Then, ③ $x = a_0/b_0$ and together with ② we have
$\exists$ prime p_1. $p_1 \mid a_0 \wedge p_1 \mid b_0$.

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

So $a_0 = p_1 \cdot a_1$, $b_0 = p_1 \cdot b_1$ for pos. int. a_1 and b_1

Note $a = p_0 \cdot a_0 = p_0 \cdot p_1 \cdot a_1$ and $b = p_0 \cdot b_0 = p_0 \cdot p_1 \cdot b_1$

Also so $x = a_1/b_1$ so by (2) $\exists$ prime p_2. $p_2 | a_1 \wedge p_2 | b_1$.

That is $a_1 = p_2 \cdot a_2 \wedge b_1 = p_2 \cdot b_2$ for pos. int a_2, b_2.

Note $a = p_0 \cdot p_1 \cdot p_2 \cdot a_2$ and $b = p_0 \cdot p_1 \cdot p_2 \cdot b_2$.

Iterating the argument, we have

$a = p_0 \cdot p_1 \cdot p_2 \cdots \cdot p_\ell \cdot a_\ell$ for primes p_i and a pos. int. a_ℓ.

for an ℓ as large as desired.

In particular $a \geq 2^a$ taking $\ell = a$ which is absurd

$\boxtimes$

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*

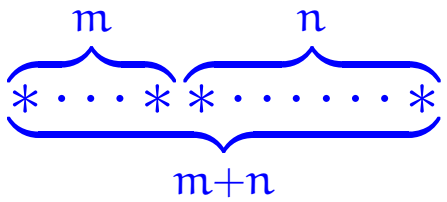
$$\mathbb{N} : \quad 0 , \quad 1 , \quad \ldots , \quad n , \quad n+1 , \quad \ldots$$

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

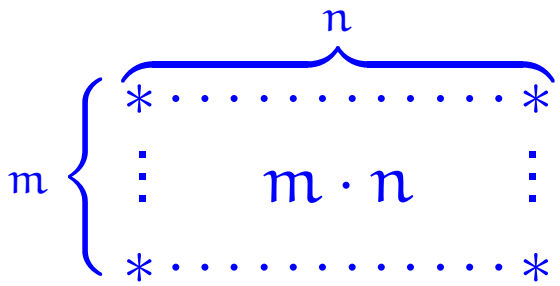
```
datatype
  N = zero | succ of N
```

The basic operations of this number system are:

- Addition



- Multiplication



We can unambiguously write

$a_1 + a_2 + \cdots + a_\ell$

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

- Monoid laws

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

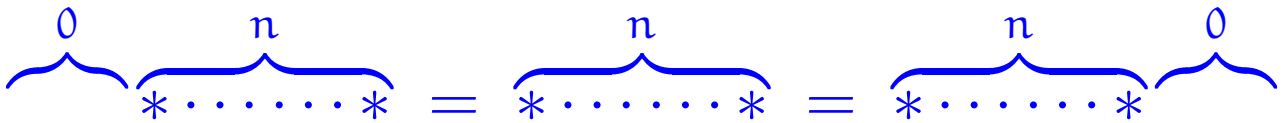
- Commutativity law

$$m + n = n + m$$

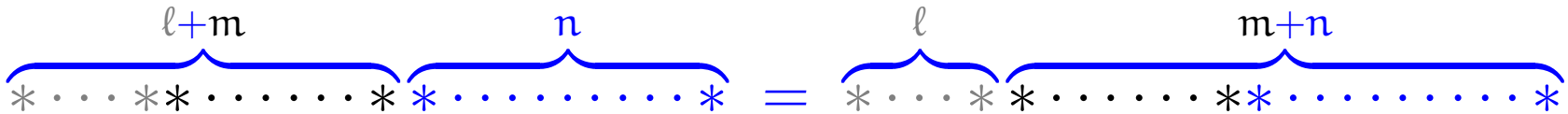
and as such is what in the mathematical jargon is referred to as a *commutative monoid*.

Commutative monoid laws

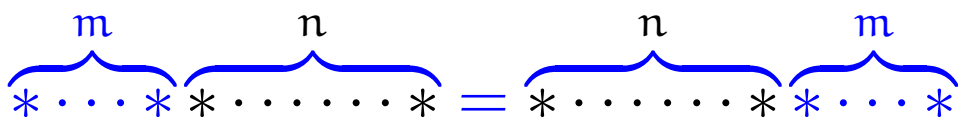
- Neutral element laws



- Associativity law



- Commutativity law



Monoids

Definition 43 *A* monoid *is an algebraic structure with*

- *a* neutral element*, say* e*,*
- *a* binary operation*, say* $\bullet$*,*

satisfying

- neutral element laws*:* $e \bullet x = x = x \bullet e$
- associativity law*:* $(x \bullet y) \bullet z = x \bullet (y \bullet z)$ $\rightsquigarrow$ $x_1 \bullet \cdots \bullet x_\ell$

Monoids

Definition 43 *A* monoid *is an algebraic structure with*

- *a* neutral element*, say* e*,*
- *a* binary operation*, say* $\bullet$*,*

satisfying

- neutral element laws*:* $e \bullet x = x = x \bullet e$
- associativity law*:* $(x \bullet y) \bullet z = x \bullet (y \bullet z)$

A monoid is commutative *if:*

- commutativity*:* $x \bullet y = y \bullet x$

is satisfied.

Example:
α lists
$e = nil$
$\bullet = @$

satisfied
for α = unit

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

- Monoid laws

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

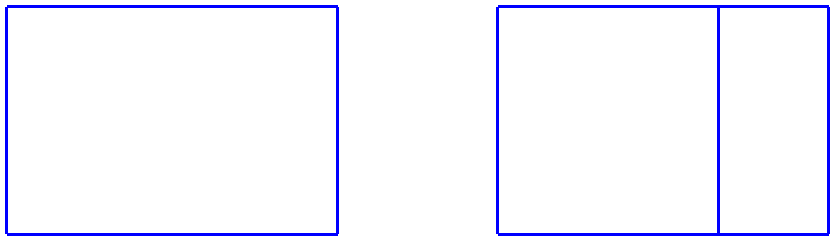
- Commutativity law

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

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

- Distributive laws

$$\begin{aligned} l \cdot 0 &= 0 \\ l \cdot (m + n) &= l \cdot m + l \cdot n \end{aligned}$$



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