A ℕaproche Teaser

Peter Koepke

June 3, 2025

Abstract

This is an introduction to the ℕaproche proof system [1] which accepts and checks readable texts written in a (controlled) natural mathematical language, with natural proof structurings.

The LaTeXsource of the present file can be loaded into Isabelle 2024 (see [2]) which then automatically calls the ℕaproche proof checking component of the Isabelle distribution. Depending on hardware this file can be proof-checked within 1 or 2 minutes.

Contents

0.1 Introduction

Most formalizations in today's interactive proof systems are not "readable" by mathematicians, since they resemble computer programs for building proofs from proof commands. In contrast, the system ℕaproche (for Natural Proof Checking) uses the (extendible) controlled natural language ForTheL (Formula Theory Language) as its input language (see also [3]). ForTheL is embedded in LaTeX and can readily be typeset by pdfLaTeX.

ℕaproche can be viewed as a system that transforms ForTheL statements into proof tasks that are sent out to an external automated theorem prover (ATP) like the E first-order prover [4] or Vampire [5]. A

ForTheL text is correct if all generated proof tasks can be discharged automatically.

Our short yet self-contained text starts from first principles and develops the theory of natural numbers is as far as required for the final result which is Euclid's Lemma. Ideally foundational theories would be provided by some library but the existing libraries and library mechanisms in ℕaproche are still rudimentary.

Our formalization of natural numbers is an initial segment of a larger ℕaproche formalization of perfectoid *rings* which are main components of Peter Scholze's *perfectoid spaces*.

This text is written as a file `EuclidsLemma.ftl.tex` in the LaTeX dialect of ℕaproche and typeset by pdf-LaTeX. `EuclidsLemma.ftl.tex` can be checked in the ℕaproche program by opening the file in the Isabelle 2024 generic proof assistant [2] (there were unexpected problems in integrating ℕaproche into the current Isabelle 2025).

0.2 Getting Started

ℕaproche proof checking constitutes a major computational process: each statement generates several first-order proof tasks each of which can take several seconds of ATP proving. To ease the proving process one can insert intermediate proof steps or increase the resources available to the external automated theorem prover.

Let us fix the ATP and its parameters:

```
[prover eprover]

[timelimit 2]

[memorylimit 8000]
```

These are ℕaproche system commands that choose E as the ATP, which is the default anyway; set the ATP timeout to 2 seconds (default = 3); and allow up to 8000 Megabytes of working memory per prover call (default = 2048).

ℕaproche commands and formalizations are enclosed in `\begin{forthel}` ... `\end{forthel}` environments and printed out on a grey background. Everything else is interpreted as "literate" commentary that is not subject to the logical checking by the system.

We expand our mathematical language by some singular/plural pairs (vocabulary) by importing a library file which contains ℕaproche commands of the form

```
[synonym number/-s]
```

:

[readtex meta-inf/source/vocabulary.ftl.tex]

We also introduce some alternative phrases for mathematical properties (macros) by import a file with ”alias” commands of the form

```
Let $x$ and $y$ are distinct stand for $x \neq y$.
```

:

[readtex meta-inf/source/macros.ftl.tex]

0.3 Natural Numbers

Our formalization axiomatically builds up a small yet familiar mathematical environment of natural numbers. The 𝕟aproche default environment contains mathematical *objects*. We introduce further types by **Signature**, **Definition** and **Axiom** commands.

Natural numbers are introduced as objects of type “natural number” and characterized by arithmetical axioms, instead of constructing them set-theoretically. This correponds to widespread intuitions that numbers are indivisible “atomic” objects.

The following 𝕟aproche commands introduce the notion (or type) of natural numbers. Together with an induction axiom to be stated later, natural numbers can be understood as the inductive type generated by 0 and +1.

Signature 1. A natural number is a mathematical object.

Let n, m, k, l, i, j denote natural numbers.

Definition 2. $\mathbb{N}$ is the collection of natural numbers.

Axiom 3 (Axiom of Infinity). $\mathbb{N}$ is a set.

Signature 4. 0 is a natural number.

Let x is nonzero stand for $x \neq 0$.

Signature 5. 1 is a nonzero natural number.

Signature 6. $m + n$ is a natural number.

Axiom 7. If n is a nonzero natural number then $n = m + 1$ for some natural number m.

We postulate basic arithmetic properties of $\mathbb{N}$ axiomatically, although they could also be proved inductively.

Signature 8. $m * n$ is a natural number.

Axiom 9. $m + n = n + m$.

Axiom 10. $(m + n) + l = m + (n + l)$.

Axiom 11. $m + 0 = m = 0 + m$.

Axiom 12. $m * n = n * m$.

Axiom 13. $(m * n) * l = m * (n * l)$.

Axiom 14. $m * 1 = m = 1 * m$.

Axiom 15. $m * 0 = 0 = 0 * m$.

Axiom 16. $m * (n + l) = (m * n) + (m * l)$ and $(n + l) * m = (n * m) + (l * m)$.

Axiom 17. If $l + m = l + n$ or $m + l = n + l$ then $m = n$.

Axiom 18. Assume that l is nonzero. If $l*m = l*n$ or $m*l = n*l$ then $m = n$.

Axiom 19. If $m + n = 0$ then $m = 0$ and $n = 0$.

We name two more natural numbers:

Definition 20. $2 = 1 + 1$.

Definition 21. $3 = 2 + 1$.

0.4 The Natural Order

Definition 22. $m \leq n$ iff there exists a natural number l such that $m + l = n$.

Let $m < n$ stand for $m \leq n$ and $m \neq n$. Let $n > m$ stand for $m < n$. Let $n \geq m$ stand for $m \leq n$.

Definition 23. Assume that $n \leq m$. $m - n$ is a natural number l such that $n + l = m$.

The following three lemmas show that $\leq$ is a partial order:

Lemma 24. $m \leq m$.

Lemma 25. If $m \leq n \leq m$ then $m = n$.

Proof. Let $m \leq n \leq m$. Take natural numbers k, l such that $n = m + k$ and $m = n + l$. Then $m = m + (k + l)$ and $k + l = 0$ and $k = 0$. Hence $m = n$. □

Lemma 26. If $m \leq n \leq l$ then $m \leq l$.

We axiomatically postulate monotonicity properties for the arithmetical operations.

Axiom 27. $m \leq n$ or $n < m$.

Lemma 28. Assume that $l < n$. Then $m + l < m + n$ and $l + m < n + m$.

Lemma 29. Assume that m is nonzero and $l < n$. Then $m * l < m * n$ and $l * m < n * m$.

0.5 Induction

ℕaproche provides an in-built binary relation symbol $\prec$ as a universal inductive relation: if

> (inheritance property) at any point m property P holds at m provided all $\prec$-predecessors of m satisfy P

then

> P holds everywhere.

ℕaproche has a proof tactic "by induction [on ...]", which reduces the inductive proof goal "P holds everywhere" to proving the inheritance property for P.

Initially, there is no specification of $\prec$. The induction proof method for some concrete relation is made available by embedding that relation into $\prec$. Therefore we axiomatically embed the natural order into $\prec$.

Axiom 30. If $m < n$ then $m \prec n$.

Let m is inductively smaller than n stand for $m \prec n$.

As a first example of induction we show:

Lemma 31. For every natural number n: $n = 0$ or $1 \leq n$.
Proof by induction. Let n be a natural number. Case $n = 0$. Trivial.

Take $n' = n - 1$. □

Lemma 32. If $m \leq n + 1$ then $m \leq n$ or $m = n + 1$.

Lemma 33. Let $m \neq 0$. Then $n \leq n * m$.

Proof. $1 \leq m$. □

Here are some intuitive facts about the numbers $0, 1, 2, 3$:

Lemma 34. If $m \leq 0$ then $m = 0$.

Lemma 35. If $m \leq 1$ then $m = 0$ or $m = 1$.

Lemma 36. If $m \leq 2$ then $m = 0$ or $m = 1$ or $m = 2$.

Lemma 37. $0 < 1 < 2 < 3$.

0.6 Division

Definition 38. n divides m iff for some l: $m = n * l$.

Let $x|y$ denote x divides y. Let a divisor of x denote a natural number that divides x.

Lemma 39. Assume $l|m|n$. Then $l|n$.

Lemma 40. Let $l|m$ and $l|m + n$. Then $l|n$.

Proof. Case l is nonzero. Take a natural number q such that $m = l * q$. Take a natural number r such that $m + n = l * r$.

Let us show that $q \leq r$.

Proof by contradiction. Assume the contrary. Then $r < q$. $m + n = l * r < l * q = m$. Contradiction. qed.

Take $s = r - q$. We have $(l * q) + (l * s) = l * r = m + n = (l * q) + n$. Hence $n = l * s$. qed. □

Lemma 41. Let $m|n \neq 0$. Then $m \leq n$.

Definition 42. n is even iff 2 divides n.

Let n is odd stand for n is not even.

Lemma 43. For all natural numbers n n is even or $n = (2 * m) + 1$ for some m.

Proof by induction. Let n be a natural number.

Case $n = 0$. Trivial.

Take $n' = n - 1$.

Case n' is even. Take a natural number m' such that $n' = 2 * m'$. Then $n = (2 * m) + 1$ for some m. qed.

Take a natural number m' such that $n' = (2 * m') + 1$. Then $n = ((2 * m') + 1) + 1 = 2 * (m' + 1)$. Hence n is even.

□

0.7 Prime Numbers

[dump on] Let p, d denote natural numbers.

Let n is nontrivial stand for $n \neq 0$ and $n \neq 1$.

Definition 44. p is prime iff p is nontrivial and for every divisor d of p $d = 1$ or $d = p$.

Let a prime number stand for a natural number that is prime.

Lemma 45. 2 is prime.

Lemma 46. Every even prime number is equal to 2.

Lemma 47. 3 is prime.

Lemma 48. Every nontrivial natural number has a prime divisor.

Proof by induction. □

0.8 Euclid's Lemma

We need that prime numbers are prime elements in the ring of integers, or the halfring of natural numbers. The following argument is taken over almost verbatim from the Wikipedia article on Euclid's Lemma [6].

Definition 49. m and n are coprime iff every common divisor of m and n is equal to 1.

Lemma 50. If m and m are coprime then $m = 1$.

Let a, b denote natural numbers.

Lemma 51. For all nonzero natural numbers n, a, b if $n | a * b$ and n and a are coprime then n divides b.

Proof by induction on $a * b$.

Let n, a, b be nonzero natural numbers such that $n | a * b$ and n and a are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n | b$. qed.

Case $a > n$. Then $q \geq b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$. Thus n divides b. qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n-a$ divides $a*(b-q)$. $n-a$ and a are coprime. $a*(b-q) < a*b$. $a*(b-q)$ is inductively smaller than $a*b$. Thus $n-a$ divides $b-q$.

Take a natural number r such that $b-q = r*(n-a)$.

$(n-a)*q = (n*q)-(a*q) = (a*b)-(a*q) = a*(b-q) = a*(r*(n-a)) = (a*r)*(n-a)$.

$n-a \neq 0$ and $q = a*r$.

$a*(n*r) = n*(a*r) = n*q = a*b$.

Then $n*r = b$ and n divides b. □

Theorem 52 (Euclids Lemma). Let p be a prime number and $p|m*n$. Then $p|m$ or $p|n$.

References

[1] Anonymous

[2] The Isabelle homepage: `https://isabelle.in.tum.de/`

[3] Andrei Paskevich: The syntax and semantics of the ForTheL language. `http://nevidal.org/download/forthel.pdf`, 2007.

[4] Stephan Schulz: The E Theorem Prover. `http://wwwlehre.dhbw-stuttgart.de/~sschulz/E/E.html`

[5] The Vampire homepage: `https://vprover.github.io/`

[6] Wikipedia entry “Euclid’s Lemma”: `https://en.wikipedia.org/wiki/Euclid\%27s_lemma`