

# Naproche - Talking to ATPs

BY PETER KOEPKE

Mathematical Institute and Hausdorff Center for Mathematics, University of Bonn



**EuroProofNet School on Natural Formal Mathematics**

Bonn, 2 June 2025

## Abstract

Interactive Theorem Proving (ITP) can be seen as a process where a human user steers an Automated Theorem Prover (ATP) to certify proof steps sufficient for the theorem under consideration. Steering is achieved by various languages which are connected by logically correct translation mechanisms. In the Naproche system, these languages contain the ordinary language of mathematics, the controlled natural language ForTheL, enriched first-order logic, and the ATP input language TPTP.



## A Naproche Teaser

Peter Koepke

June 2, 2025

*Simple introduction of natural numbers and prime numbers*

### **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.

# An example Naproche text

## Contents

1	Introduction	1	<i>Simple introduction of natural numbers and prime numbers</i>
2	Getting Started	2	
3	Natural Numbers	3	
4	The Natural Order	4	
5	Induction	5	
6	Division	6	
7	Prime Numbers	7	
8	Euclid's Lemma	7	

## An example Naproche text

*Simple introduction of natural numbers and prime numbers*

*Leading up to Euclid's Lemma*

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

# An example Naproche text

## 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.*

□

*Simple introduction of natural numbers and prime numbers*

*Leading up to Euclid's Lemma*

*Detailed analysis of Lemma 48*

## Lemma 48

### 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.*

□

*Mathematical statement in natural language*

*Considered as fully formal statement by Naproche*

*Fully formal material on gray background*

*Other “literate” material on white background*

# Lemma 48

□

## 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.* □

## 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  $q \geq b$ .

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

*Mathematical statement in natural language*

*Considered as fully formal statement by Naproche*

*Fully formal material on gray background*

*Other “literate” material on white background*

# A mathematical view on the text

## 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.*

□

*Textbook-like introduction of prime numbers*

- *pretyping of variables  $p, d$*
- *definition of prime*
- *prime number as a linguistic alternative*
- *illustrative lemmas 45-47 whose proofs are “left to the reader”*
- *Lemma 48 is an interesting result with the proof hint “by induction”*



# The typesetting view

```
486 \subsection{Prime Numbers}
487
488 \begin{forthel}
489 [dump on]
490 Let  $p, d$  denote natural numbers.
491
492 Let  $n$  is nontrivial stand for  $n \neq 0$  and  $n \neq 1$ .
493
494 \begin{definition}
495  $p$  is prime iff  $p$  is nontrivial and
496 for every divisor  $d$  of  $p$   $d = 1$  or  $d = p$ .
497 \end{definition}
498 Let a prime number stand for a natural number that is prime.
499
500 \begin{lemma}  $2$  is prime.
501 \end{lemma}
502
503 \begin{lemma}
504 Every even prime number is equal to  $2$ .
505 \end{lemma}
506
507 \begin{lemma}  $3$  is prime.
508 \end{lemma}
509
510 \begin{lemma}
511 Every nontrivial natural number has a prime divisor.
512 \end{lemma}
513 \begin{proof}[by induction]
514 %Let  $n$  be a nontrivial natural number.
515 %Assume that  $n$  is not prime.
516 %Take a divisor  $m$  of  $n$  such that  $m \neq 1$  and  $m \neq n$ .
517 % $m$  is inductively smaller than  $n$ .
518 %Every prime divisor of  $m$  is a prime divisor of  $n$ .
519 \end{proof}
520 \end{forthel}
```

Readable output generated from  
 $L^A T_E X$  by pdfLaTeX

- simple  $L^A T_E X$

- *forthel* environments for strictly  
formal text

- ordinary  $L^A T_E X$  environments for def-  
initions, lemmas and proofs

-  $L^A T_E X$  file ([...fnt1.org](http://www.fnt1.org)) is the  
input to the Naproche system

# Working with Isabelle documents in Isabelle



## Isabelle

[Home](#)[Overview](#)[Installation](#)[Documentation](#)

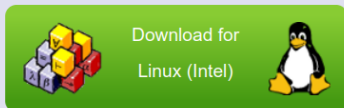
### Site Mirrors:

[Cambridge \(.uk\)](#)  
[Munich \(.de\)](#)  
[Sydney \(.au\)](#)  
[Potsdam, NY \(.us\)](#)

## What is Isabelle?

Isabelle is a generic proof assistant. It allows mathematical formulas to be expressed in a formal language and provides tools for proving those formulas in a logical calculus. Isabelle was originally developed at the [University of Cambridge](#) and [Technische Universität München](#), but now includes numerous contributions from institutions and individuals worldwide. See the [Isabelle overview](#) for a brief introduction.

## Now available: Isabelle2024 (May 2024)



[Download for Linux \(Intel\)](#) - [Download for Linux \(ARM\)](#) - [Download for Windows](#) - [Download for macOS](#)

### Hardware requirements:

- *Small experiments*: 4 GB memory, 2 CPU cores
- *Medium applications*: 8 GB memory, 4 CPU cores
- *Large projects*: 16 GB memory, 8 CPU cores
- *Extra-large projects*: 64 GB memory, 16 CPU cores

### Some notable changes:

- More robust and scalable support for distributed build clusters.
- Official support for ARM64 on Linux (notably Docker on Apple Silicon).
- HOL: various improvements of theory libraries, notably in HOL-Analysis.
- HOL: updates and improvements of Sledgehammer.

# Working with Isabelle documents in Isabelle2024



## Isabelle

[Home](#)[Overview](#)[Installation](#)[Documentation](#)

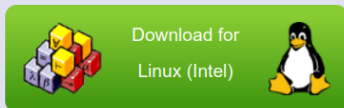
### Site Mirrors:

[Cambridge \(.uk\)](#)  
[Munich \(.de\)](#)  
[Sydney \(.au\)](#)  
[Potsdam, NY \(.us\)](#)

## What is Isabelle?

Isabelle is a generic proof assistant. It allows mathematical formulas to be expressed in a formal language and provides tools for proving those formulas in a logical calculus. Isabelle was originally developed at the [University of Cambridge](#) and [Technische Universität München](#), but now includes numerous contributions from institutions and individuals worldwide. See the [Isabelle overview](#) for a brief introduction.

## Now available: Isabelle2024 (May 2024)



[Download for Linux \(Intel\)](#) - [Download for Linux \(ARM\)](#) - [Download for Windows](#) - [Download for macOS](#)

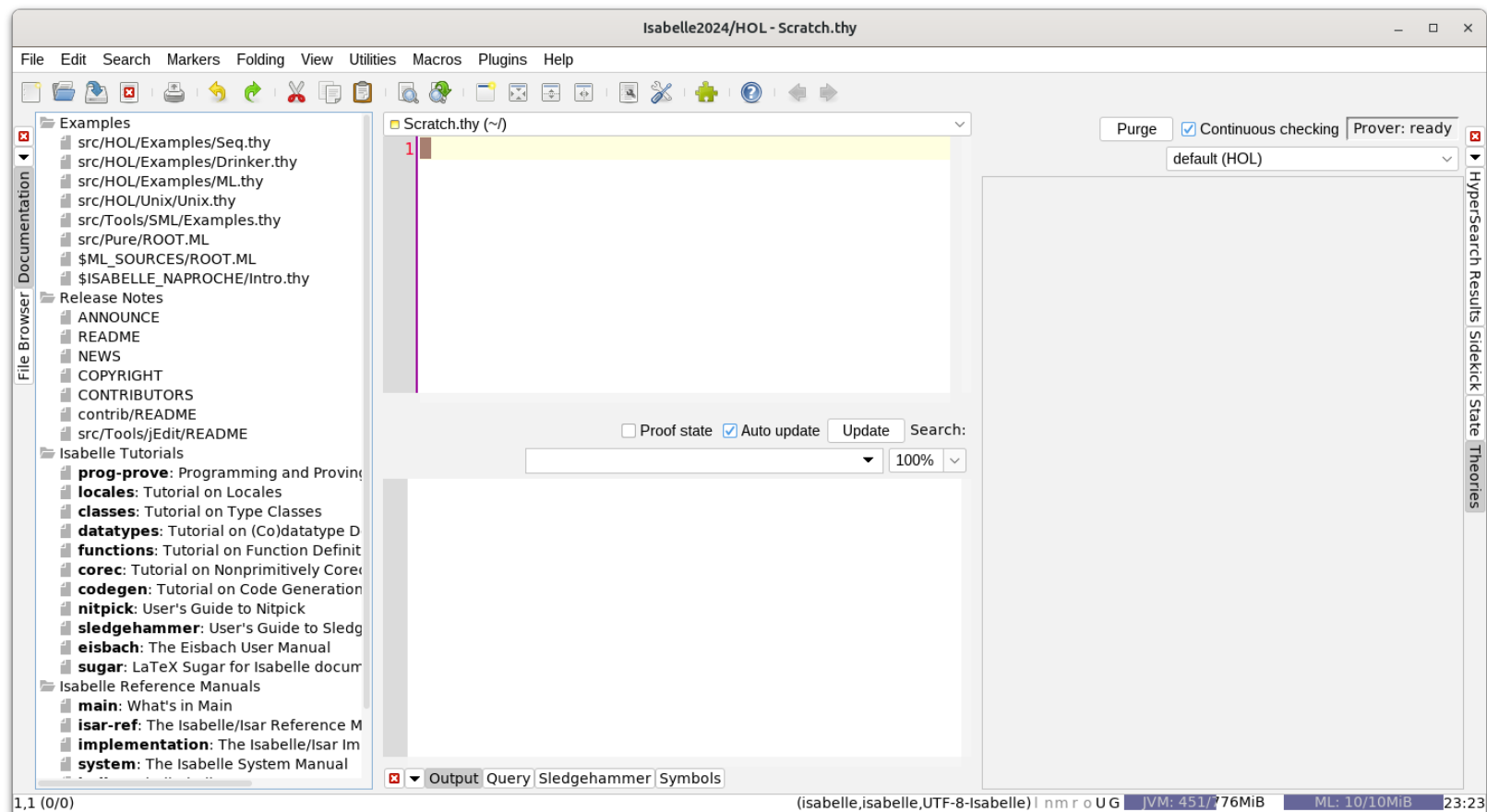
### Hardware requirements:

- *Small experiments*: 4 GB memory, 2 CPU cores
- *Medium applications*: 8 GB memory, 4 CPU cores
- *Large projects*: 16 GB memory, 8 CPU cores
- *Extra-large projects*: 64 GB memory, 16 CPU cores

### Some notable changes:

- More robust and scalable support for distributed build clusters.
- Official support for ARM64 on Linux (notably Docker on Apple Silicon).
- HOL: various improvements of theory libraries, notably in HOL-Analysis.
- HOL: updates and improvements of Sledgehammer.

# Working with Isabelle documents in Isabelle



# Working with Isabelle documents in Isabelle

The screenshot shows the Isabelle2024/HOL - EuclidsLemma02\_24.ftl.tex editor interface. The main window displays the source code of a lemma and its proof. The left sidebar shows the file browser with a tree structure of files and folders. The right sidebar shows the search results and state theories. The bottom status bar displays the current line and column, the document encoding, and the memory usage of the JVM and ML components.

File Isabelle2024/HOL - EuclidsLemma02\_24.ftl.tex

File Edit Search Markers Folding View Utilities Macros Plugins Help

File Browser Documentation

- Examples
  - src/HOL/Examples/Seq.thy
  - src/HOL/Examples/Drinker.thy
  - src/HOL/Examples/ML.thy
  - src/HOL/Unix/Unix.thy
  - src/Tools/SML/Examples.thy
  - src/Pure/ROOT.ML
  - SML\_SOURCES/ROOT.ML
  - \$ISABELLE\_NAPROCHE/Intro.thy
- Release Notes
  - ANNOUNCE
  - README
  - NEWS
  - COPYRIGHT
  - CONTRIBUTORS
  - contrib/README
  - src/Tools/jEdit/README
- Isabelle Tutorials
  - prog-prove**: Programming and Proving
  - locales**: Tutorial on Locales
  - classes**: Tutorial on Type Classes
  - datatypes**: Tutorial on (Co)datatype D
  - functions**: Tutorial on Function Definit
  - corec**: Tutorial on Nonprimively Corec
  - codegen**: Tutorial on Code Generation
  - nitpick**: User's Guide to Nitpick
  - sledgehammer**: User's Guide to Sledg
  - eisbach**: The Eisbach User Manual
  - sugar**: LaTeX Sugar for Isabelle docum
- Isabelle Reference Manuals
  - main**: What's in Main
  - isar-ref**: The Isabelle/Isar Reference M
  - implementation**: The Isabelle/Isar Im
  - system**: The Isabelle System Manual

EuclidsLemma02\_24.ftl.tex (~HOME/C/25/06/SoNaLF)

```
506
507 \begin{lemma}  $\$3\$$  is prime.
508 \end{lemma}
509
510 \begin{lemma}
511 Every nontrivial natural number has a prime di
512 \end{lemma}
513 \begin{proof}[by induction]
514 %Let  $\$n\$$  be a nontrivial natural number.
515 %Assume that  $\$n\$$  is not prime.
516 %Take a divisor  $\$m\$$  of  $\$n\$$  such that  $\$m \neq 1$ 
```

Purge ☒ Continuous checking Prover: ready

default (HOL)

☐ ZFC\_Rudiments ☐ Naproche

☐ Proof state ☒ Auto update Update Search: 100%

[Reasoner] (file "/home/peter/HOME/C/25/06/SoNaLF/ verification successful  
[Main] (file "/home/peter/HOME/C/25/06/SoNaLF/Euc sections 205 - goals 59 - trivial 0 - proved 125  
[Main] (file "/home/peter/HOME/C/25/06/SoNaLF/Euc symbols 680 - checks 658 - trivial 630 - proved 2  
[Main] (file "/home/peter/HOME/C/25/06/SoNaLF/Euc parser 00:00.29 - reasoner 00:00.31 - simplifier  
[Main] (file "/home/peter/HOME/C/25/06/SoNaLF/Euc total 00:56.05

Output Query Sledgehammer Symbols

520,14 (12199/14757) (latex,none,UTF-8-Isabelle) | nm r o U G JVM: 270/512MiB ML: 29/285MiB 23:26

## 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.*



*Textbook-like introduction of prime numbers*

- *Lemma 48 has a short proof “by induction”*
- *Proof is carried out by the E Automated Theorem Prover (ATP)*
- *What is the prover task given to E?*

# Inspecting the interaction of Naproche and E in Isabelle: *dump on*

The screenshot shows the Isabelle2024 HOL editor interface. The main window displays a proof script in `EuclidsLemma02_24.ftl.tex` with the following content:

```
504 Every even prime number is equal to $2$.
505 \end{lemma}
506
507 \begin{lemma} $3$ is prime.
508 \end{lemma}
509 \dump on
510 \begin{lemma}
511 Every nontrivial natural number has a prime di
512 \end{lemma}
513 \begin{proof}[by induction]
514 %Let $n$ be a nontrivial natural number.
```

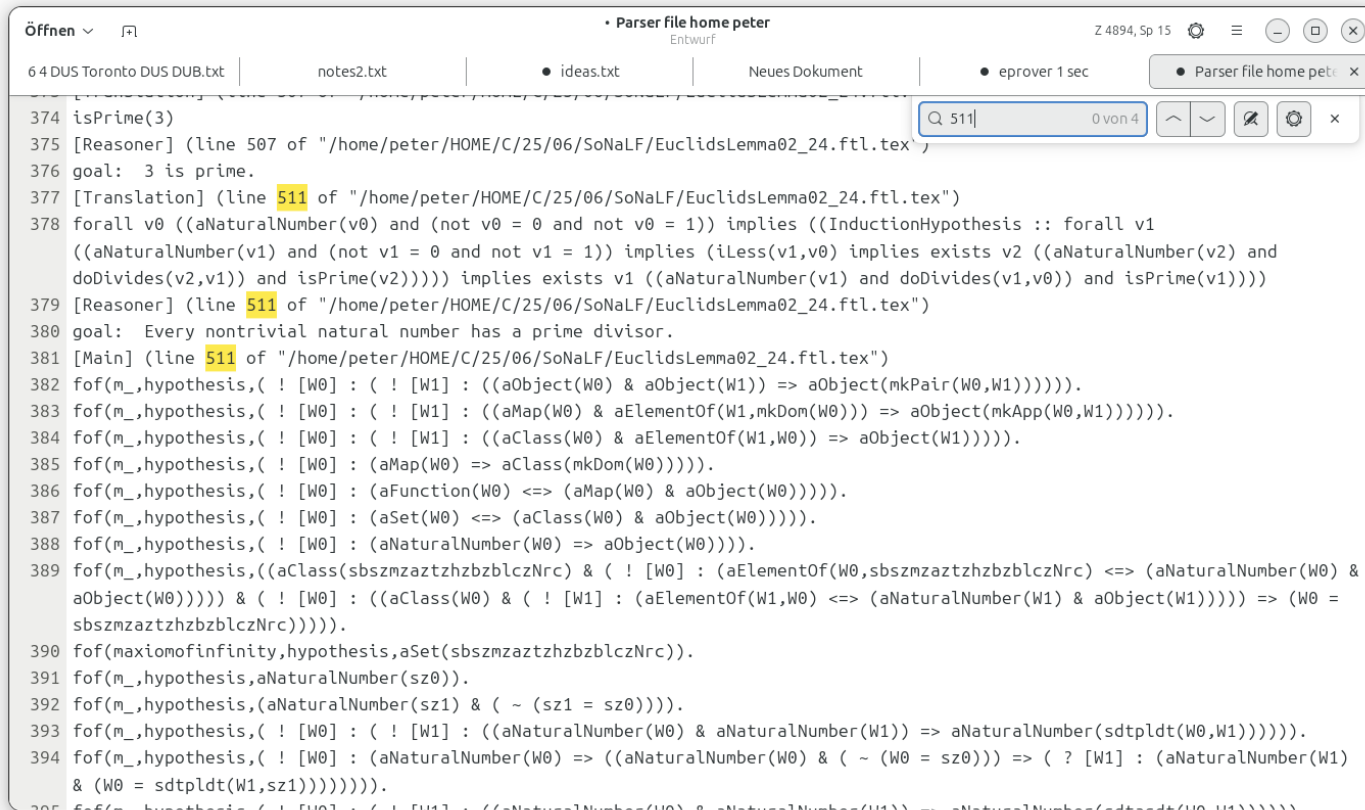
On the right side, the **Prover** section shows `Continuous checking` is enabled and the prover is `ready`. Below it, the **Theories** section shows `ZFC_Rudiments` and `Naproche` are loaded.

The **Output** pane at the bottom shows the following messages:

```
[Parser] (file "/home/peter/Isabelle2024/contrib/
parsing successful
[Parser] (file "/home/peter/Isabelle2024/contrib/
parsing successful
[Parser] (file "/home/peter/Isabelle2024/contrib/
parsing successful
[Reasoner] (file "/home/peter/HOME/C/25/06/SoNaLF
verification started
[Translation] (line 165 of "/home/peter/HOME/C/25
forall v0 ((HeadTerm :: aNaturalNumber(v0)) impli
[Translation] (line 171 of "/home/peter/HOME/C/25
forall v0 ((HeadTerm :: v0 = \mathbb{N})) iff (aCl
```

The status bar at the bottom indicates the current position is `509,10 (11837/14757)` and the system is running `(latex,none,UTF-8-Isabelle) | nm r o U G` with `JVM: 299/$12MiB` and `ML: 175/431MiB`.

# First-order translation and translation into TPTP prover format

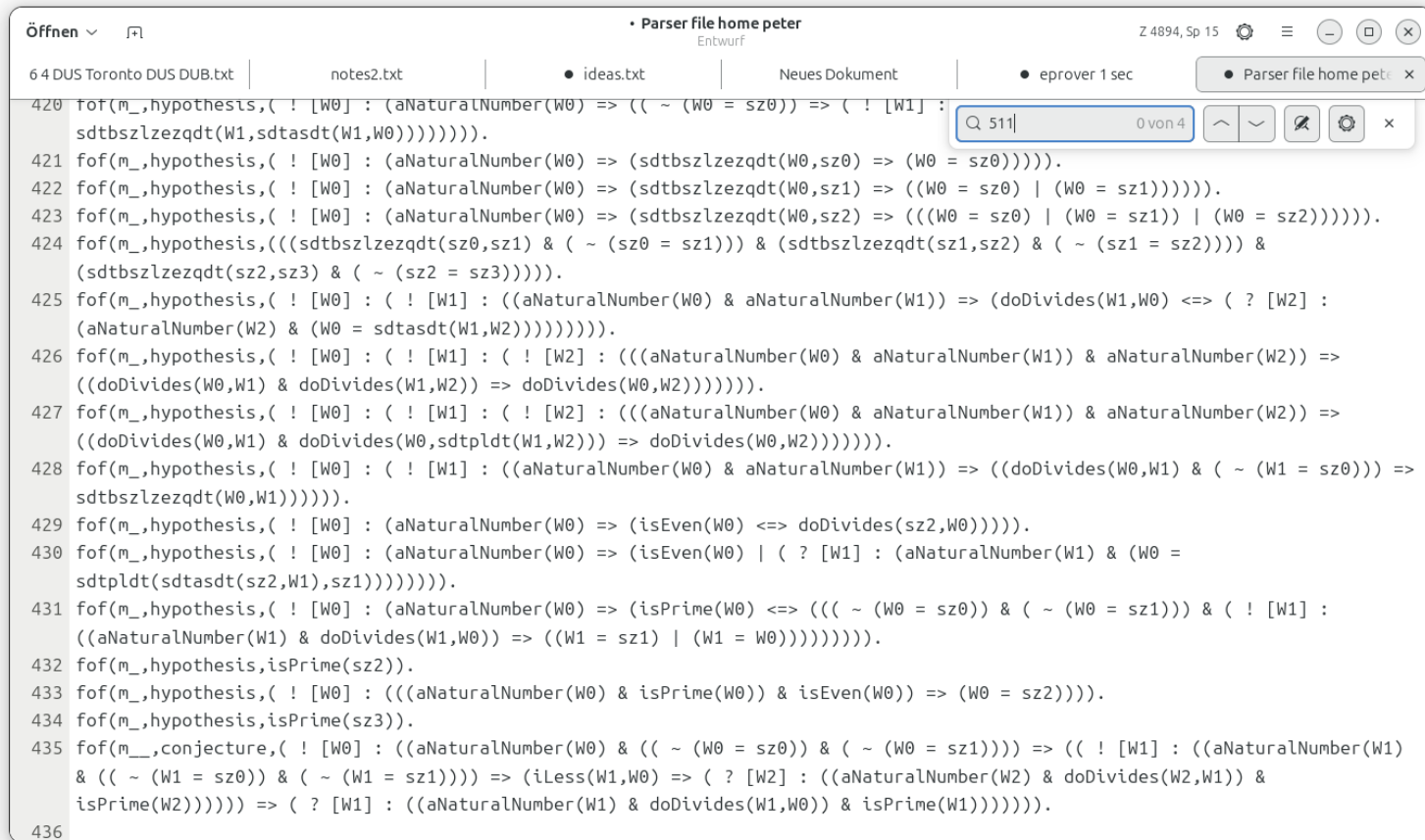


```
Öffnen ▾  Parser file home peter  Z 4894, Sp 15  Entwurf
6 4 DUS Toronto DUS DUB.txt | notes2.txt | • ideas.txt | Neues Dokument | • eprover 1 sec | • Parser file home pete x

374 isPrime(3)
375 [Reasoner] (line 507 of "/home/peter/HOME/C/25/06/SoNaLF/EuclidsLemma02_24.ftl.tex")
376 goal: 3 is prime.
377 [Translation] (line 511 of "/home/peter/HOME/C/25/06/SoNaLF/EuclidsLemma02_24.ftl.tex")
378 forall v0 ((aNaturalNumber(v0) and (not v0 = 0 and not v0 = 1)) implies ((InductionHypothesis :: forall v1
    ((aNaturalNumber(v1) and (not v1 = 0 and not v1 = 1)) implies (iLess(v1,v0) implies exists v2 ((aNaturalNumber(v2) and
    doDivides(v2,v1)) and isPrime(v2)))))) implies exists v1 ((aNaturalNumber(v1) and doDivides(v1,v0)) and isPrime(v1))))
379 [Reasoner] (line 511 of "/home/peter/HOME/C/25/06/SoNaLF/EuclidsLemma02_24.ftl.tex")
380 goal: Every nontrivial natural number has a prime divisor.
381 [Main] (line 511 of "/home/peter/HOME/C/25/06/SoNaLF/EuclidsLemma02_24.ftl.tex")
382 fof(m_,hypothesis,( ! [W0] : ( ! [W1] : ((aObject(W0) & aObject(W1)) => aObject(mkPair(W0,W1)))))).
383 fof(m_,hypothesis,( ! [W0] : ( ! [W1] : ((aMap(W0) & aElementOf(W1,mkDom(W0))) => aObject(mkApp(W0,W1)))))).
384 fof(m_,hypothesis,( ! [W0] : ( ! [W1] : ((aClass(W0) & aElementOf(W1,W0)) => aObject(W1))))).
385 fof(m_,hypothesis,( ! [W0] : (aMap(W0) => aClass(mkDom(W0))))).
386 fof(m_,hypothesis,( ! [W0] : (aFunction(W0) <=> (aMap(W0) & aObject(W0))))).
387 fof(m_,hypothesis,( ! [W0] : (aSet(W0) <=> (aClass(W0) & aObject(W0))))).
388 fof(m_,hypothesis,( ! [W0] : (aNaturalNumber(W0) => aObject(W0))))).
389 fof(m_,hypothesis,((aClass(sbszmzaztzhzbzblczNrc) & ( ! [W0] : (aElementOf(W0,sbszmzaztzhzbzblczNrc) <=> (aNaturalNumber(W0) &
    aObject(W0)))) & ( ! [W0] : ((aClass(W0) & ( ! [W1] : (aElementOf(W1,W0) <=> (aNaturalNumber(W1) & aObject(W1)))) => (W0 =
    sbszmzaztzhzbzblczNrc)))))).
390 fof(maxiomofinfinity,hypothesis,aSet(sbszmzaztzhzbzblczNrc)).
391 fof(m_,hypothesis,aNaturalNumber(sz0)).
392 fof(m_,hypothesis,(aNaturalNumber(sz1) & ( ~ (sz1 = sz0)))).
393 fof(m_,hypothesis,( ! [W0] : ( ! [W1] : ((aNaturalNumber(W0) & aNaturalNumber(W1)) => aNaturalNumber(sdtpldt(W0,W1)))))).
394 fof(m_,hypothesis,( ! [W0] : (aNaturalNumber(W0) => ((aNaturalNumber(W0) & ( ~ (W0 = sz0))) => ( ? [W1] : (aNaturalNumber(W1)
    & (W0 = sdtpldt(W1,sz1)))))))).
395 fof(m_,hypothesis,( ! [W0] : ( ! [W1] : ((aNaturalNumber(W0) & aNaturalNumber(W1)) => aNaturalNumber(sdtpldt(W0,W1))))))
```



# First-order translation and translation into TPTP prover format



The screenshot shows a web-based interface for a TPTP prover. The title bar indicates the file is 'Parser file home peter' and the status is 'Entwurf'. The interface includes a tabbed editor with tabs for '6 4 DUS Toronto DUS DUB.txt', 'notes2.txt', 'ideas.txt', 'Neues Dokument', and 'eprover 1 sec'. The main text area contains a list of logical formulas, each preceded by a line number from 420 to 436. The formulas are written in a notation where 'f' represents function symbols, 'p' represents predicate symbols, and variables are denoted by letters like W0, W1, W2, sz0, sz1, sz2, sz3. The formulas are organized into groups: lines 420-421 and 422-423 are hypotheses; lines 424-425 and 426-427 are hypotheses; lines 428-429 and 430-431 are hypotheses; line 432 is a hypothesis; line 433 is a hypothesis; line 434 is a hypothesis; and line 435 is a conjecture. A search bar at the top right of the text area shows '511' and '0 von 4' results. The line number 436 is visible at the bottom left of the text area.

```
420 fof(m_hypothesis,( ! [W0] : (aNaturalNumber(W0) => (( ~ (W0 = sz0)) => ( ! [W1] :  
    sdtbszlzezqdt(W1,sdtasdt(W1,W0)))))).  
421 fof(m_hypothesis,( ! [W0] : (aNaturalNumber(W0) => (sdtbszlzezqdt(W0,sz0) => (W0 = sz0)))).  
422 fof(m_hypothesis,( ! [W0] : (aNaturalNumber(W0) => (sdtbszlzezqdt(W0,sz1) => ((W0 = sz0) | (W0 = sz1)))).  
423 fof(m_hypothesis,( ! [W0] : (aNaturalNumber(W0) => (sdtbszlzezqdt(W0,sz2) => (((W0 = sz0) | (W0 = sz1)) | (W0 = sz2)))).  
424 fof(m_hypothesis,(((sdtbszlzezqdt(sz0,sz1) & ( ~ (sz0 = sz1))) & (sdtbszlzezqdt(sz1,sz2) & ( ~ (sz1 = sz2))) &  
    (sdtbszlzezqdt(sz2,sz3) & ( ~ (sz2 = sz3)))).  
425 fof(m_hypothesis,( ! [W0] : ( ! [W1] : ((aNaturalNumber(W0) & aNaturalNumber(W1)) => (doDivides(W1,W0) <=> ( ? [W2] :  
    (aNaturalNumber(W2) & (W0 = sdtasdt(W1,W2)))))).  
426 fof(m_hypothesis,( ! [W0] : ( ! [W1] : ( ! [W2] : (((aNaturalNumber(W0) & aNaturalNumber(W1)) & aNaturalNumber(W2)) =>  
    ((doDivides(W0,W1) & doDivides(W1,W2)) => doDivides(W0,W2)))))).  
427 fof(m_hypothesis,( ! [W0] : ( ! [W1] : ( ! [W2] : (((aNaturalNumber(W0) & aNaturalNumber(W1)) & aNaturalNumber(W2)) =>  
    ((doDivides(W0,W1) & doDivides(W0,sdtpldt(W1,W2)) => doDivides(W0,W2)))))).  
428 fof(m_hypothesis,( ! [W0] : ( ! [W1] : ((aNaturalNumber(W0) & aNaturalNumber(W1)) => ((doDivides(W0,W1) & ( ~ (W1 = sz0))) =>  
    sdtbszlzezqdt(W0,W1)))))).  
429 fof(m_hypothesis,( ! [W0] : (aNaturalNumber(W0) => (isEven(W0) <=> doDivides(sz2,W0)))).  
430 fof(m_hypothesis,( ! [W0] : (aNaturalNumber(W0) => (isEven(W0) | ( ? [W1] : (aNaturalNumber(W1) & (W0 =  
    sdtpldt(sdtasdt(sz2,W1),sz1)))))).  
431 fof(m_hypothesis,( ! [W0] : (aNaturalNumber(W0) => (isPrime(W0) <=> ((( ~ (W0 = sz0)) & ( ~ (W0 = sz1))) & ( ! [W1] :  
    ((aNaturalNumber(W1) & doDivides(W1,W0)) => ((W1 = sz1) | (W1 = W0)))))).  
432 fof(m_hypothesis,isPrime(sz2)).  
433 fof(m_hypothesis,( ! [W0] : (((aNaturalNumber(W0) & isPrime(W0)) & isEven(W0)) => (W0 = sz2))).  
434 fof(m_hypothesis,isPrime(sz3)).  
435 fof(m_conjecture,( ! [W0] : ((aNaturalNumber(W0) & (( ~ (W0 = sz0)) & ( ~ (W0 = sz1)))) => (( ! [W1] : ((aNaturalNumber(W1)  
    & (( ~ (W1 = sz0)) & ( ~ (W1 = sz1)))) => (iLess(W1,W0) => ( ? [W2] : ((aNaturalNumber(W2) & doDivides(W2,W1)) &  
    isPrime(W2)))))) => ( ? [W1] : ((aNaturalNumber(W1) & doDivides(W1,W0)) & isPrime(W1))))).  
436
```

# Naproche's input to E

...

```
fof(m_,hypothesis,( ! [W0] : (aNaturalNumber(W0) => (isPrime(W0)
<=> ((( ~ (W0 = sz0)) & ( ~ (W0 = sz1))) & ( ! [W1] :
((aNaturalNumber(W1) & doDivides(W1,W0)) => ((W1 = sz1) | (W1 =
W0)))))))).
```

```
fof(m_,hypothesis,isPrime(sz2)).
```

```
fof(m_,hypothesis,( ! [W0] : (((aNaturalNumber(W0) & isPrime(W0))
& isEven(W0)) => (W0 = sz2)))).
```

```
fof(m_,hypothesis,isPrime(sz3)).
```

```
fof(m_,conjecture,( ! [W0] : ((aNaturalNumber(W0) & (( ~ (W0 =
sz0)) & ( ~ (W0 = sz1)))) => (( ! [W1] : ((aNaturalNumber(W1) &
(( ~ (W1 = sz0)) & ( ~ (W1 = sz1)))) => (iLess(W1,W0) => ( ? [W2]
: ((aNaturalNumber(W2) & doDivides(W2,W1)) & isPrime(W2)))))
=> ( ? [W1] : ((aNaturalNumber(W1) & doDivides(W1,W0)) &
isPrime(W1)))))).
```

"original"

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

**Lemma 2.** 2 is prime.

**Lemma 3.** Every even prime number is equal to 2.

**Lemma 4.** 3 is prime.

**Lemma 5.** Every nontrivial  $n$  has a prime divisor.

# The “by induction” proof tactic

## 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.

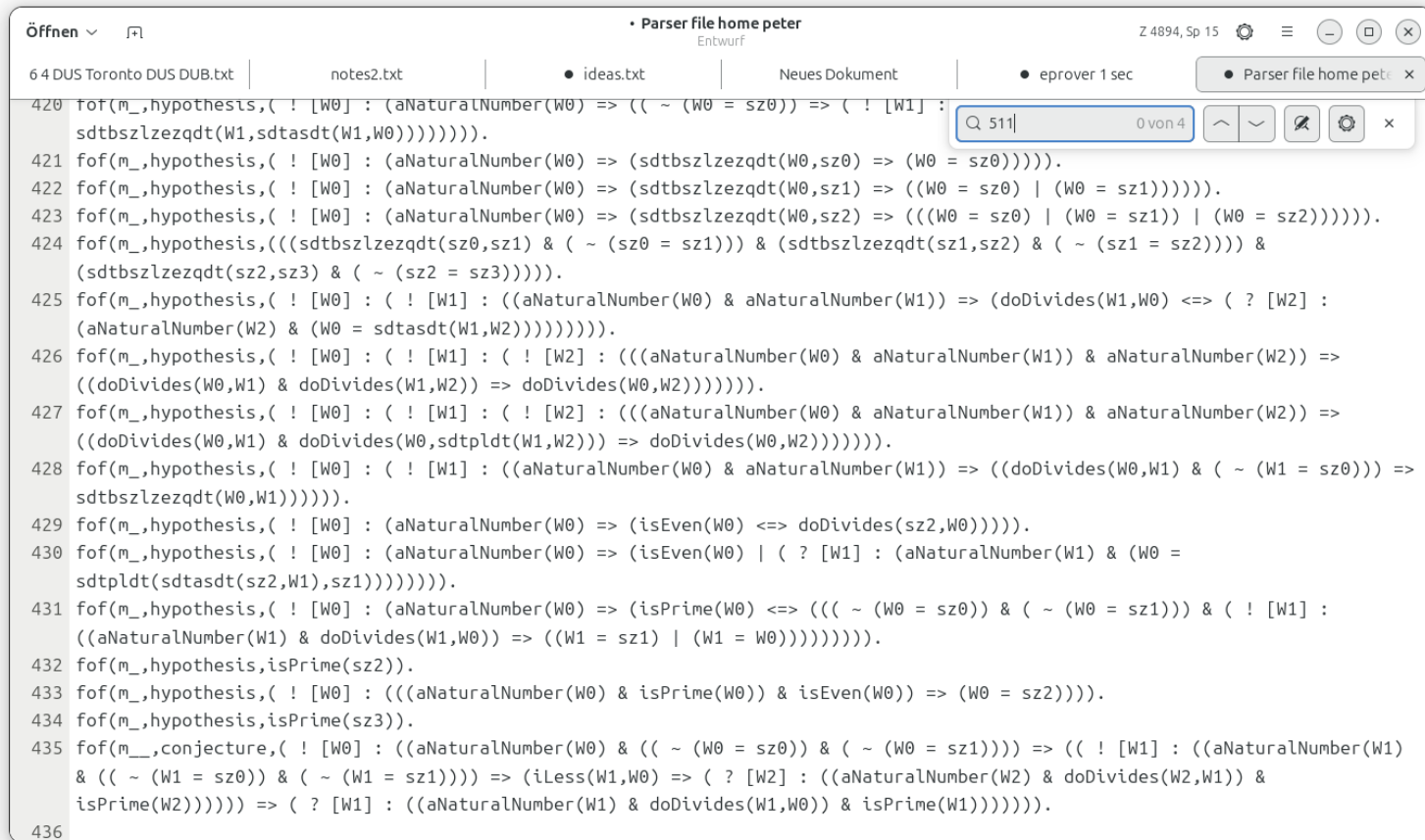
Naproche has a proof tactic “by induction [on ...]”, which reduces the inductive proof goal “ $P$  holds everywhere” to proving the inheritance property for  $P$ .

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  $m \prec n$ .

# Induction in TPTP: iLess as $\Leftarrow$



```
420 fof(m_hypothesis, ( ! [W0] : (aNaturalNumber(W0) => (( ~ (W0 = sz0)) => ( ! [W1] :  
    sdtbszlzezqdt(W1, sdtasdt(W1, W0))))))).  
421 fof(m_hypothesis, ( ! [W0] : (aNaturalNumber(W0) => (sdtbszlzezqdt(W0, sz0) => (W0 = sz0)))).  
422 fof(m_hypothesis, ( ! [W0] : (aNaturalNumber(W0) => (sdtbszlzezqdt(W0, sz1) => ((W0 = sz0) | (W0 = sz1))))).  
423 fof(m_hypothesis, ( ! [W0] : (aNaturalNumber(W0) => (sdtbszlzezqdt(W0, sz2) => (((W0 = sz0) | (W0 = sz1)) | (W0 = sz2))))).  
424 fof(m_hypothesis, (((sdtbszlzezqdt(sz0, sz1) & ( ~ (sz0 = sz1))) & (sdtbszlzezqdt(sz1, sz2) & ( ~ (sz1 = sz2)))) &  
    (sdtbszlzezqdt(sz2, sz3) & ( ~ (sz2 = sz3)))).  
425 fof(m_hypothesis, ( ! [W0] : ( ! [W1] : ((aNaturalNumber(W0) & aNaturalNumber(W1)) => (doDivides(W1, W0) <=> ( ? [W2] :  
    (aNaturalNumber(W2) & (W0 = sdtasdt(W1, W2))))))).  
426 fof(m_hypothesis, ( ! [W0] : ( ! [W1] : ( ! [W2] : (((aNaturalNumber(W0) & aNaturalNumber(W1)) & aNaturalNumber(W2)) =>  
    ((doDivides(W0, W1) & doDivides(W1, W2)) => doDivides(W0, W2)))))).  
427 fof(m_hypothesis, ( ! [W0] : ( ! [W1] : ( ! [W2] : (((aNaturalNumber(W0) & aNaturalNumber(W1)) & aNaturalNumber(W2)) =>  
    ((doDivides(W0, W1) & doDivides(W0, sdtpldt(W1, W2)) => doDivides(W0, W2)))))).  
428 fof(m_hypothesis, ( ! [W0] : ( ! [W1] : ((aNaturalNumber(W0) & aNaturalNumber(W1)) => ((doDivides(W0, W1) & ( ~ (W1 = sz0))) =>  
    sdtbszlzezqdt(W0, W1))))).  
429 fof(m_hypothesis, ( ! [W0] : (aNaturalNumber(W0) => (isEven(W0) <=> doDivides(sz2, W0)))).  
430 fof(m_hypothesis, ( ! [W0] : (aNaturalNumber(W0) => (isEven(W0) | ( ? [W1] : (aNaturalNumber(W1) & (W0 =  
    sdtpldt(sdtasdt(sz2, W1), sz1)))))).  
431 fof(m_hypothesis, ( ! [W0] : (aNaturalNumber(W0) => (isPrime(W0) <=> ((( ~ (W0 = sz0)) & ( ~ (W0 = sz1))) & ( ! [W1] :  
    ((aNaturalNumber(W1) & doDivides(W1, W0)) => ((W1 = sz1) | (W1 = W0))))))).  
432 fof(m_hypothesis, isPrime(sz2)).  
433 fof(m_hypothesis, ( ! [W0] : (((aNaturalNumber(W0) & isPrime(W0)) & isEven(W0)) => (W0 = sz2))).  
434 fof(m_hypothesis, isPrime(sz3)).  
435 fof(m_conjecture, ( ! [W0] : ((aNaturalNumber(W0) & (( ~ (W0 = sz0)) & ( ~ (W0 = sz1)))) => (( ! [W1] : ((aNaturalNumber(W1)  
    & (( ~ (W1 = sz0)) & ( ~ (W1 = sz1)))) => (iLess(W1, W0) => ( ? [W2] : ((aNaturalNumber(W2) & doDivides(W2, W1)) &  
    isPrime(W2)))))) => ( ? [W1] : ((aNaturalNumber(W1) & doDivides(W1, W0)) & isPrime(W1))))).  
436
```

# Naproche's input to E

...

```
fof(m_,hypothesis,( ! [W0] : (aNaturalNumber(W0) => (isPrime(W0)
<=> ((( ~ (W0 = sz0)) & ( ~ (W0 = sz1))) & ( ! [W1] :
((aNaturalNumber(W1) & doDivides(W1,W0)) => ((W1 = sz1) | (W1 =
W0)))))))).
```

```
fof(m_,hypothesis,isPrime(sz2)).
```

```
fof(m_,hypothesis,( ! [W0] : (((aNaturalNumber(W0) & isPrime(W0))
& isEven(W0)) => (W0 = sz2)))).
```

```
fof(m_,hypothesis,isPrime(sz3)).
```

```
fof(m_,conjecture,( ! [W0] : ((aNaturalNumber(W0) & (( ~ (W0 =
sz0)) & ( ~ (W0 = sz1)))) => (( ! [W1] : ((aNaturalNumber(W1) &
(( ~ (W1 = sz0)) & ( ~ (W1 = sz1)))) => (iLess(W1,W0) => ( ? [W2]
: ((aNaturalNumber(W2) & doDivides(W2,W1)) & isPrime(W2)))))
=> ( ? [W1] : ((aNaturalNumber(W1) & doDivides(W1,W0)) &
isPrime(W1)))))).
```

"original"

**Definition 6.**  $p$  is prime iff  $p$  is nontrivial and for every divisor  $d$  of  $p$   $d = 1$  or  $d = p$ .

**Lemma 7.** 2 is prime.

**Lemma 8.** Every even prime number is equal to 2.

**Lemma 9.** 3 is prime.

**Lemma 10.** Every nontrivial  $n$  has a prime divisor.

# E fails without “by induction”; some statistics

Isabelle2024/HOL - EuclidsLemma02\_24.ftl.tex (modified)

File Edit Search Markers Folding View Utilities Macros Plugins Help

Examples

- src/HOL/Examples/Seq.thy
- src/HOL/Examples/Drinker.thy
- src/HOL/Examples/ML.thy
- src/HOL/Unix/Unix.thy
- src/Tools/SML/Examples.thy
- src/Pure/ROOT.ML
- \$ML\_SOURCES/ROOT.ML
- \$ISABELLE\_NAPROCHE/Intro.thy

Release Notes

- ANNOUNCE
- README
- NEWS
- COPYRIGHT

CONTRIBUTORS

- contrib/README
- src/Tools/jEdit/README

Isabelle Tutorials

- prog-prove**: Programming and Proving
- locales**: Tutorial on Locales
- classes**: Tutorial on Type Classes
- datatypes**: Tutorial on (Co)datatype Definitions
- functions**: Tutorial on Function Definitions
- corec**: Tutorial on Nonprimitively Corecursive Functions
- codegen**: Tutorial on Code Generation
- nitpick**: User's Guide to Nitpick
- sledgehammer**: User's Guide to Sledgehammer
- eisbach**: The Eisbach User Manual
- sugar**: LaTeX Sugar for Isabelle documents

Isabelle Reference Manuals

- main**: What's in Main
- isar-ref**: The Isabelle/Isar Reference Manual
- implementation**: The Isabelle/Isar Implementation
- system**: The Isabelle System Manual
- jedit**: Isabelle/jEdit

Demo Documents

- Old Isabelle Manuals
- Original jEdit Documentation

EuclidsLemma02\_24.ftl.tex (~HOME/C/25/06/SoNaLF/)

```
507 \begin{lemma}  $\$3$  is prime.
508 \end{lemma}
509 [dump on]
510 \begin{lemma}
511 Every nontrivial natural number has a prime divisor.
512 \end{lemma}
513 %\begin{proof}[by induction]
514 %Let  $\$n$  be a nontrivial natural number.
515 %Assume that  $\$n$  is not prime.
516 %Take a divisor  $\$m$  of  $\$n$  such that  $\$m \neq 1$  and  $\$m \neq n$ .
517 % $\$m$  is inductively smaller than  $\$n$ .
518 %Every prime divisor of  $\$m$  is a prime divisor of  $\$n$ .
519 %\end{proof}
520 \end{forthe!}
521
522 \subsection{Euclid's Lemma}
523
524 We need that prime numbers are prime
```

☐ Proof state ☒ Auto update Update Search: 100%

fof(m\_\_\_\_, conjecture, (doDivides(xp,xm) | doDivides(xp,xn))).

[Reasoner] (file "/home/peter/HOME/C/25/06/SoNaLF/EuclidsLemma02\_24.ftl.tex")  
verification failed  
[Main] (file "/home/peter/HOME/C/25/06/SoNaLF/EuclidsLemma02\_24.ftl.tex")  
sections 205 - goals 59 - failed 1 - trivial 0 - proved 124 - equations 0  
[Main] (file "/home/peter/HOME/C/25/06/SoNaLF/EuclidsLemma02\_24.ftl.tex")  
symbols 671 - checks 649 - trivial 621 - proved 28 - unfolds 827  
[Main] (file "/home/peter/HOME/C/25/06/SoNaLF/EuclidsLemma02\_24.ftl.tex")  
parser 00:00.31 - reasoner 00:00.31 - simplifier 00:00.00 - prover 00:13.32/00:00  
[Main] (file "/home/peter/HOME/C/25/06/SoNaLF/EuclidsLemma02\_24.ftl.tex")  
total 00:13.95  
ERROR

☒ Output Query Sledgehammer Symbols

(latex,none,UTF-8-Isabelle) | nm r o U G JVM: 173/512MiB ML: 5/497MiB 23:55

# The linguistic view: analyzing mathematical language

## 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.*



- *simple (argumentative) sentences with symbolic material*
- *L<sup>A</sup>T<sub>E</sub>X conventions*
- *grammatical analysis*
- *parsing*
- *softly typed language*
- *translating into first-order logic*

# Phrase structure grammar

every nontrivial natural number has a prime divisor

*statement*  $\rightarrow$  *subject predicate*

*subject*  $\rightarrow$  every nontrivial natural number

*predicate*  $\rightarrow$  has a prime divisor



# The syntax and semantics of the ForTheL language\*

Andrei Paskevich

Université Paris XII — Val de Marne, Créteil, France

Kiev National Taras Shevchenko University, Kiev, Ukraine

December 2007

## Contents

<b>1</b>	<b>Formal Theory Language</b>	<b>3</b>
1.1	Introduction . . . . .	3
1.2	Lexical structure . . . . .	4
1.3	Syntax of a statement . . . . .	5
1.3.1	Syntactic primitives . . . . .	6
1.3.2	Notions . . . . .	7
1.3.3	Terms . . . . .	9
1.3.4	Predicates . . . . .	10
1.3.5	Statements . . . . .	12

# A simplified fragment of the ForTheL phrase structure grammar

every nontrivial natural number has a prime divisor

*simpleStatement*  $\rightarrow$  *terms* *doesPredicate* {and *doesPredicate*}

*terms*  $\rightarrow$  *term* {(, | and) *term*}

*term*  $\rightarrow$  *quantifiedNotion* | *definiteTerm*

*quantifiedNotion*  $\rightarrow$  (every | each | all | any) *notion*

*notion*  $\rightarrow$  *classNoun* | ...

*classNoun*  $\rightarrow$  {*leftAttribute*} *primClassNoun* [*rightAttribute*]

*primClassNoun*  $\rightarrow$  natural number

*doesPredicate*  $\rightarrow$  (has | have) *hasPredicate*

*hasPredicate*  $\rightarrow$  [ a | an | the ] *possessedNoun* {and [ a | an | the ] *possessedNoun*} | no *possessedNoun*

*possessedNoun*  $\rightarrow$  {*leftAttribute*} *primPossessedNoun*

*primPossessedNoun*  $\rightarrow$  (divisor | divisors) [*names*] — derived from the phrase “divisor of”

*leftAttribute*  $\rightarrow$  nontrivial | prime | ...

# The ForTheL phrase structure grammar is implemented in Naproche

every nontrivial natural number has a prime divisor

*simpleStatement*  $\rightarrow$  *terms doesPredicate* {and *doesPredicate*}

simple :: FTL Formula

simple = label "simple statement" \$ do

(q, ts) <- terms

p <- conjChain doesPredicate

q <\$> dig p ts

...

*doesPredicate*  $\rightarrow$  (has | have) *hasPredicate*

doesPredicate :: FTL Formula

doesPredicate = label "does predicate" \$

(... <|> hasP <|> ...

where

...

hasP = has >> hasPredicate

...

## 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  $b \geq q$ .

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

## 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  $n$  are coprime then  $m \nmid n$ .

Let  $a, b$  denote natural numbers.

**Lemma 51.** For all nonzero natural numbers  $n, a, b$  if  $n \mid a * b$  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  $n \mid a * b$  and  $n$  and  $a$  are coprime. Take a natural number  $q$  such that  $n * q = a * b$ .

Case  $n = a$ . Then  $n = 1$  and  $n \mid b$ . 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  $b \geq q$ .

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

### By induction [\[ edit \]](#)

The following proof is inspired by Euclid's version of [Euclidean algorithm](#), which proceeds by using only subtractions.

Suppose that  $n \mid ab$  and that  $n$  and  $a$  are coprime (that is, their greatest common divisor is 1). One has to prove that  $n$  divides  $b$ . Since  $n \mid ab$ , there exists an integer  $q$  such that

$$nq = ab.$$

Without loss of generality, one can suppose that  $n, q, a$ , and  $b$  are positive, since the divisibility relation is independent of the signs of the involved integers.

To prove the theorem by [strong induction](#), we suppose that it has been proved for all smaller values of  $ab$ . There are three cases:

1. If  $n = a$ , coprimality implies  $n = 1$ , and  $n$  divides  $b$  trivially.
2. If  $n < a$ , then subtracting  $nb$  from both sides gives

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

Thus,  $n$  divides  $(a - n)b$ . Since we assumed that  $n$  and  $a$  are coprime, it follows that  $a - n$  and  $n$  must be coprime. (If not, their greatest common divisor  $d$  would divide their sum  $a$  as well as  $n$ , contradicting our assumption.)

The conclusion therefore follows by induction hypothesis, since  $0 < (a - n)b < ab$ .

3. If  $n > a$  then subtracting  $aq$  from both sides gives

## Naïve texts can be readable like textbook mathematics:

**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  $b \geq q$ .

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

## Perspectives

- to increase the coverage of  $\mathbb{N}$ aproche ...
- to build a more efficient  $\mathbb{N}$ aproche on a set-theoretical basis (Adrian De Lon) ...
- to transfer the  $\mathbb{N}$ aproche approach to other proof systems ...
- to use LLMs for language translation and other language processing ...

# Thank you!

<https://naproche.github.io/>

<https://isabelle.in.tum.de/website-Isabelle2024/>