

# Euclid's Proof of the Infinitude of Primes, Formalized in Naproche

Andrei Paskevich and Peter Koepke  
U Paris-Saclay and U Bonn

February 20, 2021

This paper contains a standard proof of Euclid's theorem that there are infinitely many prime numbers. We follow the first proof given in *Proofs from THE BOOK* by Martin Aigner and Günter M. Ziegler, Springer Verlag. Before the proof we set up a language and axioms for natural number arithmetic, define divisibility and prime numbers, introduce some set theoretic background and define finite sets, sequences and products.

On an older laptop with an Intel Pentium N3710 processor Naproche takes around 75 seconds to check this text.

## 1 Naproche Settings and Notation

```
[printprover on][dump on]
[synonym number/-s] [synonym divide/-s] [synonym set/-s] [synonym
element/-s] [synonym belong/-s] [synonym subset/-s]
```

## 2 Natural Numbers

In order to be able to form classes and sets of natural numbers natural numbers are introduced as “small” objects.

Let  $x$  is small stand for  $x$  is setsized.

**Signature 1.** A natural number is a small object.

Let  $i, k, l, m, n, p, q, r$  denote natural numbers.

**Lemma 2.**  $i$  is small.

**Signature 3.** 0 is a natural number.

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

**Signature 4.** 1 is a nonzero natural number.

**Signature 5.**  $m + n$  is a natural number.

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

**Axiom 7.**  $m + n = n + m$ .

**Axiom 8.**  $(m + n) + l = m + (n + l)$ .

**Axiom 9.**  $m + 0 = m = 0 + m$ .

**Axiom 10.**  $m * n = n * m$ .

**Axiom 11.**  $(m * n) * l = m * (n * l)$ .

**Axiom 12.**  $m * 1 = m = 1 * m$ .

**Axiom 13.**  $m * 0 = 0 = 0 * m$ .

**Axiom 14.**  $m*(n+l) = (m*n)+(m*l)$  and  $(n+l)*m = (n*m)+(l*m)$ .

**Axiom 15.** If  $l + m = l + n$  or  $m + l = n + l$  then  $m = n$ .

**Axiom 16.** Assume that  $l$  is nonzero. If  $l * m = l * n$  or  $m * l = n * l$  then  $m = n$ .

**Axiom 17.** If  $m + n = 0$  then  $m = 0$  and  $n = 0$ .

### 3 The Natural Order

**Definition 18.**  $m \leq n$  iff there exists a natural number  $l$  such that  $m + l = n$ .

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

**Definition 19.** 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 20.**  $m \leq m$ .

**Lemma 21.** If  $m \leq n \leq m$  then  $m = n$ .

**Lemma 22.** If  $m \leq n \leq l$  then  $m \leq l$ .

**Axiom 23.**  $m \leq n$  or  $n < m$ .

**Lemma 24.** Assume that  $l < n$ . Then  $m+l < m+n$  and  $l+m < n+m$ .

**Lemma 25.** Assume that  $m$  is nonzero and  $l < n$ . Then  $m * l < m * n$  and  $l * m < n * m$ .

**Axiom 26.**  $n = 0$  or  $n = 1$  or  $1 < n$ .

**Lemma 27.** If  $m \neq 0$  then  $n \leq n * m$ .

## 4 Induction

Naproche provides a special binary relation symbol  $\prec$  for a universal inductive relation: if at any point  $m$  property  $P$  is inherited at  $m$  provided all  $\prec$ -predecessors of  $m$  satisfy  $P$ , then  $P$  holds everywhere. Induction along  $\prec$  is ensured by:

**Axiom 28.** If  $n < m$  then  $n \prec m$ .

## 5 Division

**Definition 29.**  $n$  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 30.** Let  $l|m$  and  $l|m + n$ . Then  $l|n$ .

*Proof.* Assume that  $l$  is nonzero. Take  $p$  such that  $m = l * p$ . Take  $q$  such that  $m + n = l * q$ .

Let us show that  $p \leq q$ . Proof by contradiction. Assume the contrary. Then  $q < p$ .  $m + n = l * q < l * p = m$ . Contradiction. qed.

Take  $r = q - p$ . We have  $(l * p) + (l * r) = l * q = m + n = (l * p) + n$ . Hence  $n = l * r$ .  $\square$

**Lemma 31.** Let  $m|n \neq 0$ . Then  $m \leq n$ .

## 6 Primes

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

**Definition 32.**  $n$  is prime iff  $n$  is nontrivial and for every divisor  $m$  of  $n$   $m = 1$  or  $m = n$ .

**Lemma 33.** Every nontrivial  $k$  has a prime divisor.

*Proof.* Proof by induction. □

## 7 Classes

Let  $S, T$  stand for classes. Let  $x$  belongs to  $S$  stand for  $x$  is an element of  $S$ .

**Definition 34.** A subclass of  $S$  is a class  $T$  such that every element of  $T$  belongs to  $S$ .

Let  $T \subseteq S$  stand for  $T$  is a subclass of  $S$ .

We extend the built-in ontology of Naproche according to the following principles for elements and sets:

**Axiom 35.** Every element of every class is small.

**Axiom 36.** Every set is a small class and every small class is a set.

**Definition 37.**  $\mathbb{N}$  is the class of natural numbers.

## 8 Finite Sequences and Products

**Definition 38.**  $\{m, \dots, n\}$  is the class of natural numbers  $i$  such that  $m \leq i \leq n$ .

**Axiom 39.**  $\{m, \dots, n\}$  is a set.

**Axiom 40.** Assume  $F$  is a function and  $x \in \text{Dom}(F)$ . Then  $F(x)$  is small.

**Definition 41.** A sequence of length  $n$  is a function  $F$  such that  $\text{Dom}(F) = \{1, \dots, n\}$ .

Let  $F_i$  stand for  $F(i)$ .

**Definition 42.** Let  $F$  be a sequence of length  $n$ .  $\{F_1, \dots, F_n\} =$

$\{F_i | i \in \text{Dom}(F)\}$ .

**Signature 43.** Let  $F$  be a sequence of length  $n$  such that  $\{F_1, \dots, F_n\} \subseteq \mathbb{N}$ .  $F_1 \cdots F_n$  is a natural number.

**Axiom 44. (Factorproperty)** Let  $F$  be a sequence of length  $n$  such that  $F(i)$  is a nonzero natural number for every  $i \in \text{Dom}(F)$ . Then  $F_1 \cdots F_n$  is nonzero and  $F(i)$  divides  $F_1 \cdots F_n$  for every  $i \in \text{Dom}(F)$ .

## 9 Finite and Infinite Sets

**Definition 45.**  $S$  is finite iff  $S = \{F_1, \dots, F_n\}$  for some natural number  $n$  and some function  $F$  that is a sequence of length  $n$ .

**Definition 46.**  $S$  is infinite iff  $S$  is not finite.

## 10 Euclid's Theorem

**Signature 47.**  $\mathbb{P}$  is the class of prime natural numbers.

**Theorem 48. (Euclid)**  $\mathbb{P}$  is infinite.

*Proof.* Assume that  $r$  is a natural number and  $p$  is a sequence of length  $r$  and  $\{p_1, \dots, p_r\}$  is a subclass of  $\mathbb{P}$ .

(1)  $p_i$  is a nonzero natural number for every  $i$  such that  $1 \leq i \leq r$ .

Consider  $n = p_1 \cdots p_r + 1$ . Take a prime divisor  $q$  of  $n$ .

Let us show that  $q \neq p_i$  for all  $i$  such that  $1 \leq i \leq r$ .

Proof by contradiction. Assume that  $q = p_i$  for some natural number  $i$  such that  $1 \leq i \leq r$ .  $q$  is a divisor of  $n$  and  $q$  is a divisor of  $p_1 \cdots p_r$  (by Factorproperty, 1). Thus  $q$  divides 1. Contradiction. qed.

Hence  $\{p_1, \dots, p_r\}$  is not the class of prime natural numbers.  $\square$