Euclid's Proof of the Infinitude of Primes

ℕaproche Formalization: Peter Koepke
University of Bonn

December 11, 2021

This paper contains a standard proof of Euclid's theorem that there are infinitely many prime numbers, following 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.

1 Importing Standard Preliminaries

[readtex preliminaries.ftl.tex]

2 Natural Numbers

Signature 1. A natural number is a mathematical object.

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

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

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 $m = n$.

Proof. Let $m \leq n \leq m$. Take a 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 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 $l * m < n * m$.

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 $<$ is ensured by:

Axiom 26. If $n < m$ then $n \prec m$.

Lemma 27. For every natural number n $n = 0$ or $1 \leq n$.

Proof. Proof by induction. □

Lemma 28. Let $m \neq 0$. Then $n \leq n * m$.

Proof. $1 \leq m$. □

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

Lemma 31. 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 $n = l * r$. □

Lemma 32. 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 33. n is prime iff n is nontrivial and for every divisor m of n $m = 1$ or $m = n$.

Lemma 34. Every nontrivial m has a prime divisor.

Proof. Proof by induction on m. □

7 Finite Sequences and Products

Definition 35. $\{m, \ldots, n\}$ is the class of natural numbers i such that $m \leq i \leq n$.

Axiom 36. $\{m, \ldots, n\}$ is a set.

Axiom 37. Assume F is a function and $x \in Dom(F)$. Then $F(x)$ is an object.

Definition 38. A sequence of length n is a function F such that $Dom(F) = \{1, \ldots, n\}$.

Let F_i stand for $F(i)$.

Definition 39. Let F be a sequence of length n. $\{F_1, \ldots, F_n\} = \{F_i | i \in Dom(F)\}$.

Signature 40. Let F be a sequence of length n such that $\{F_1, \ldots, F_n\} \subseteq \mathbb{N}$. $F_1 \cdots F_n$ is a natural number.

Axiom 41. (Factorproperty) Let F be a sequence of length n such that $F(i)$ is a nonzero natural number for every $i \in Dom(F)$. Then $F_1 \cdots F_n$ is nonzero and $F(i)$ divides $F_1 \cdots F_n$ for every $i \in Dom(F)$.

8 Finite and Infinite Sets

Let S denote a class.

Definition 42. S is finite iff $S = \{s_1, \ldots, s_n\}$ for some natural number n and some function s that is a sequence of length n.

Definition 43. S is infinite iff S is not finite.

9 Euclid's Theorem

Signature 44. $\mathbb{P}$ is the collection of prime natural numbers.

Theorem 45. (Euclid) $\mathbb{P}$ is infinite.

Proof. Assume that r is a natural number and p is a sequence of length r and $\{p_1, \ldots, p_r\}$ is a subclass of $\mathbb{P}$. p_i is a nonzero natural number for every $i \in \mathit{Domp}$. Consider $n = p_1 \cdots p_r + 1$. [dump on] $p_1 \cdots p_r$ is nonzero (by Factorproperty). n is nontrivial. 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. q is a divisor of $p_1 \cdots p_r$ (by Factorproperty, 1). Thus q divides 1. Contradiction. qed.

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