

There are infinitely many primes

September 9, 2014

I. Foundations

We work with *sets* and with *elements*. Let A, X, Y, Z denote sets, and let x, y, z denote elements. An *element* of X is an element. Let x *belongs to* X , or x *is in* X , or $x \in X$ stand for x is an element of X . \emptyset is a set that has no elements. X is *empty* stands for $X = \emptyset$, and X is *nonempty* stands for $X \neq \emptyset$. A *subset* of Y is defined to be a set such that every element of X belongs to Y . $X \subseteq Y$ stands for X is a subset of Y .

We can show that $X \subseteq X$ (reflexivity); $X \subseteq Y \subseteq Z \rightarrow X \subseteq Z$ (transitivity); and $X \subseteq Y \subseteq X \rightarrow X = Y$ (symmetry).

We also work with functions. Let f, g, h denote functions. The *domain* of f , $\text{dom } f$, is a set. For $x \in \text{dom } f$ $f(x)$ is an element. Let f_x stand for $f(x)$. For $X \subseteq \text{dom } f$ define $f[X] = \{f(x) \mid x \in X\}$. Let $\text{ran } f$, or the *range* of f stand for $f[\text{dom } f]$. A function *from* X denotes a function f such that $\text{dom } f = X$. A function *from* X *to* Y denotes a function f such that $\text{dom } f = X$ and $\text{ran } f \subseteq Y$. $f: X$ means that f is a function from X , and $f: X \rightarrow Y$ means that f is a function from X to Y .

If $x \in \text{dom } f$ then trivially $f(x) \in \text{ran } f$.

For $X \subseteq \text{dom } f$ define $f \upharpoonright X$ to be a function g from X such that $g(x) = f(x)$ for every $x \in X$.

We work with *numbers*. Let i, j, k, l, m, n, q, r denote numbers. \mathbb{N} is defined to be the set of numbers. 0 is a number. Let x is *nonzero* stand for $x \neq 0$. 1 is a nonzero number. The *sum* of m and n , $m + n$, is a number. The *product* of m and n , $m \cdot n$, is a number. We presuppose

- the associativity of addition: $(m + n) + l = m + (n + l)$;
- the neutrality of 0: $m + 0 = 0 + m = m$;
- the commutativity of addition: $m + n = n + m$;

- the associativity of multiplication: $(m \cdot n) \cdot l = m \cdot (n \cdot l)$;
- the neutrality of 1: $m \cdot 1 = 1 \cdot m = m$;
- $m \cdot 0 = 0 = 0 \cdot m$;
- the commutativity of multiplication: $m \cdot n = n \cdot m$;
- distributivity: $m \cdot (n + l) = (m \cdot n) + (m \cdot l)$, and $(n + l) \cdot m = (n \cdot m) + (l \cdot m)$;
- additive cancellation: if $l + m = l + n$ or $m + l = n + l$ then $m = n$;
- multiplicative cancellation: Assume that l is nonzero. Then $l + m = l + n$ or $m + l = n + l$ implies $m = n$;
- if $m + n = 0$ then $m = 0$ and $n = 0$.

We can show that if $m \cdot n = 0$ then $m = 0$ or $n = 0$.

Define $m \leq n$ iff there exists l such that $m + l = n$. For $m \leq n$ define $(n - m)$ to be a number such that $m + l = n$. Let $m < n$ stand for $m \neq n$ and $m \leq n$.

Obviously, $m \leq m$; $m \leq n \leq l \rightarrow m \leq l$; and $m \leq n \leq m \rightarrow m = n$. Furthermore, $m \leq n$ or $n < m$; for $l < n$ we have $m + l < m + n$ and $l + m < n + m$; and for m nonzero and $l < n$ we have $m \cdot l < m \cdot n$ and $l \cdot m < n \cdot m$. We presuppose that for every number n we have $n = 0$ or $n = 1$ or $1 < n$. We can prove that $m \neq 0$ implies $n \leq n \cdot m$. Indeed observe that $1 \leq m$.

We can carry out inductions on the relation $<$.

Define $\{m, \dots, n\} = \{i \in \mathbb{N} \mid m \leq i \leq n\}$. For a function f such that $\{m, \dots, n\} \subseteq \text{dom } f$ let $\{f_m, \dots, f_n\} = \{f(i) \mid m \leq i \leq n\}$. We say that f lists X in n steps iff $\text{dom } f = \{1, \dots, n\}$ and $X = \{f_m, \dots, f_n\}$. X is called *finite* iff there is a function f and a number n such that f lists X in n steps. X is called *infinite* iff X is not finite.

II. Prime Numbers

1. Divisibility

We define that m divides n , $m|n$, iff for some l $n = m \cdot l$. A *divisor* of n is defined as a number that divides n . For m nonzero and $m|n$, $\frac{n}{m}$ is defined as a number l such that $n = m \cdot l$.

Obviously, $l|m \mid n \rightarrow l|n$ (transitivity of divisibility); and if $l|m$ and $l|n$ then $l|m + n$. Indeed if l is nonzero then $m + n = l \cdot (\frac{m}{l} + \frac{n}{l})$.

Lemma 1. *DivMin.* Let $l|m$ and $l|m + n$. Then $l|n$.

Proof. Assume that l, n are nonzero. Take i such that $m = l \cdot i$. Take j such that $m + n = l \cdot j$.

Let us show that $i \leq j$. Assume the contrary. Then $j < i$. $m + n = l \cdot j < l \cdot i = m$. $m \leq m + n$. $m = m + n$. $n = 0$. Contradiction.

Take $k = j - i$. We have $(l \cdot i) + (l \cdot k) = (l \cdot i) + n$. Hence $n = l \cdot k$. □

We can show: if $m|n \neq 0$, then $m \leq n$.

Lemma 2. *DivAsso.* Let l be nonzero and divide m . Then $n \cdot \frac{m}{l} = \frac{n \cdot m}{l}$.

Proof. $(l \cdot n) \cdot \frac{m}{l} = l \cdot \frac{n \cdot m}{l}$. □

Define $\mathbb{N}^+ = \{n \in \mathbb{N} \mid n \neq 0\}$.

For $f: \{m, \dots, n\} \rightarrow \mathbb{N}^+$ consider $\prod_{i=m}^n f_i$ which is an element of \mathbb{N}^+ . We presuppose that for $f: \{m, \dots, n\} \rightarrow \mathbb{N}^+$ and $m \leq j \leq n$, f_j divides $\prod_{i=m}^n f_i$.

2. Primes

Let m is *trivial* stand for $m=0$ or $m=1$. Let m is *nontrivial* stand for $m \neq 0$ and $m \neq 1$. We call a number q *prime* iff q is nontrivial and for every divisor m of q we have $m=1$ or $m=q$. We say that m is *compound* for m is not prime.

Lemma 3. *PrimDiv. Every nontrivial k has a prime divisor.*

Proof by induction on k . Let k be nontrivial. Case k is prime. Obvious. Case k is compound. Take a divisor m of k such that $m \neq 1$ and $m \neq k$. $m \neq 0$. m is nontrivial and $m \ll k$. Take a prime divisor n of m . n is a prime divisor of k . end. qed.

Theorem 4. *The set of prime numbers is infinite.*

Proof. Let A be a finite set of prime numbers. Take a function p and a number r such that p lists A in r steps. $\text{ran } p \subseteq \mathbb{N}^+$. $\prod_{i=1}^r p_i \neq 0$. Take $n = \prod_{i=1}^r p_i + 1$. n is nontrivial. Take a prime divisor q of n .

Let us show that q is not an element of A . Assume the contrary. Take i such that $(1 \leq i \leq r \text{ and } q = p_i)$. p_i divides $\prod_{i=1}^r p_i$ (by MultProd). Then q divides 1 (by DivMin). Contradiction. qed.

Hence A is not the set of prime numbers. □