There are infinitely many primes

October 4, 2014

Suggestions:

Ad hoc extensions to SAD, to be used as proof of concept for a subsequent project of extensive structural changes and extensions to the ForTheL language.

Work with the established top level sections of SAD. Complement the official form with some abbreviated forms. Try to keep the sentence structure close to the official form, so that the changes to the SAD code are only superficial.

E.g. "Work with X" can be derived from the official "Signature. X is a notion." by replacing "Signature." by "Work with" and "is a notion" by " ". Or a listing of axiom can be carried out by sentences of the form " - the_commutativity_of_addition: $m + n = n + m$" instead of "Axiom the_commutativity_of_addition. $m + n = n + m$." again by replacing "Axiom" by "-" and the first "." by ":".

These changes have to be be carried out so that the function of each sentence is uniquely identifiable by human readers and by the system.

Later, the controlled language ForTheL is to be turned into a controlled language with grammatical correctness requirements and a rich spectrum of common mathematical phrases.

Examples:

Signature extensions: Signature. Let ... . Let ... . X is a notion.

One sentence version: (We) (also) Work with X. Fix the relation ... . The constant X is a number ... . We require that an element is a ... . The term $f(x)$ is a set. The *domain* is ... (Here, the introduction is signaled by *italics*.

Short version with premises: Given (that) ... fix the relation/constant/term.

Axiom: Axiom. Let ... . Let ... . Statement.

One sentence version: (We) presuppose that Statement.

Short version with premises: For ... postulate that .... .

List of axioms: " - the_commutativity_of_addition: $m+n=n+m$", see above.

Definitions: Definition. Let ... . Let ... . Statement.

One sentence version: (We) define .... .

Short version with premises: Define, for ..., t=... . Define, for ..., ...

List of definitions: " .....

Claims:

"Note that .... ." anstelle von "We have ...."

"Obviously/Trivially ..." (To be used when no proof is given)

...

Induction. SAD handles inductions with a inbuilt special relation, which nevertheless has to be invoked by a signature extension:

Signature IH. m -<- n is an atom. Axiom IH. m < n => m -<- n.

These commands could be be invoked instead by something like: "We can carry out inductions on the relation $<$."

In the case of natural numbers, the Axiom IH is a version of the induction axiom (schema) of first-order Peano arithmetic.

I. Foundations

We work with *sets*. Let A, X, Y, Z denote sets. We also work with *elements*. Let x, y, z denote elements. We require that an *element* of X is an element. Let x *belongs to* X stand for x is an element of X. Let x *is in* X stand for x is an element of X. Let $x \in X$ stand for x is an element of X. The constant $\emptyset$ is a set that has no elements. X is *empty* stands for $X = \emptyset$. X is *nonempty* stands for $X \neq \emptyset$. Define a *subset* of Y as 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 (a) $X \subseteq X$ (reflexivity). (b) $X \subseteq Y \subseteq Z \to X \subseteq Z$ (transitivity). (c) $X \subseteq Y \subseteq X \to X = Y$ (symmetry).

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

Note that if $x \in \operatorname{dom} f$ then $f(x) \in \operatorname{ran} f$.

Define for $X \subseteq \operatorname{dom} f$ the term $f \restriction X$ 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. Define $\mathbb{N}$ to be the set of numbers. The constant 0 is a number. Let x is *nonzero* stand for $x \neq 0$. The constant 1 is a nonzero number. The term $m+n$ is a number. Let the *sum* of m and n stand for $m+n$. The term $m \cdot n$ is a number. Let the *sum* of m and n stand for $m \cdot n$. We assume the following axioms.

- 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 $m+l=n$. Define for $m\leq n$ the expression $n-m$ to be a number such that $m+l=n$. Let $m<n$ stand for $m\neq n$ and $m\leq n$.

Obviously, $m\leqslant m$; $m\leqslant n\leqslant l\rightarrow m\leq l$; 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 $n\leqslant n\cdot m$. Indeed observe that $1\leqslant m$.

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

Define $\{m,\ ...,\ n\}=\{i\in\mathbb{N}\mid m\leq i\leq n\}$. For a function f such that $\{m,\ ...,\ n\}\subseteq \mathrm{dom}\ f$ let $\{f_m,\ ...,\ f_n\}=\{f(i)\mid m\leq i\leq n\}$. We say that f *lists* X *in* n *steps* iff $\mathrm{dom}\ f=\{1,\ ...,\ n\}$ and $X=\{f_m,...,f_n\}$. 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, $l|m|\ n\rightarrow l|n$ (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 $f\colon \{m, ..., n\} \to \mathbb{N}^+$ consider $\prod_{i=m}^{n} f_i$ which is an element of $\mathbb{N}^+$. We presuppose that for f: $\{m, ..., n\} -> \mathbb{N}^+$ 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 $m \prec\!\!\prec k$. 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. 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 ($1 \leq i \leq r$ 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. □