Formalizing Sets and Numbers, and some of Wiedijk's "100 Theorems" in Naproche

Peter Koepke, Mateusz Marcol and Patrick Schäfer
Mathematical Institute, University of Bonn, Germany

2023

[read `examples/lang/vocabulary.ftl.tex`] [read `examples/lang/macros.ftl.tex`]

Preliminary Remarks

The source file of this document is a LaTeX file which on one hand can be mathematically typeset into a readable pdf document, and which on the other hand can be input into the Naproche natural language proof checker. Naproche is part of the Isabelle prover IDE; installing the current version of Isabelle will also install Naproche. Opening and editing a `ftl.tex` *file like this one in Isabelle will automatically start the inbuilt Naproche proof checking.*

Apart from its mathematical content, the source file of about 3000 lines is testing the limits of the present Naproche system, its external automatic theorem provers (mostly E in our case), and the underlying hardware. The file has been checked successfully in about half an hour on mid-range consumer laptops. Checking, however, may fail, because ATP proof searches are restricted by wall-clock timeouts and depend significantly on system speed and state. It may be necessary to increase the standard timeout of 3 seconds to X = 10, 20, or more seconds by inserting `[timelimit X]` *commands, which we have done frequently. In stubborn cases, one has to insert further proof steps.*

Contents

1 Introduction **4**

2 Basic Notions **5**

3 Classes **6**

4 Maps **7**

5 Equinumerosity 9

6 Set-Theoretic Axioms 10

7 Ordered Pairs and Products 11

8 Cantor's Theorem (#63) 12

9 The Knaster-Tarski Fixed Point Theorem 12

10 The Schröder-Bernstein Theorem (#25) 13

11 The Real Field 14

12 Some Numbers 16

13 The Real Ordered Field 17

14 Upper and lower bounds 19

15 The rational numbers 20

16 Integers 20

17 The natural numbers 22

18 The Principle of Mathematical Induction (#74) 23

19 Sum of an Arithmetic Series (#68) 25

20 Exponentiation 26

21 Sum of a Geometric Series (#66) 27

22 Divisibility and Prime Numbers 28

23 The Greatest Common Divisor 29

24 Greatest Common Divisor Algorithm (#69) 30

25 Bezout's Identity (#60) 31

26 Irrationality of Roots of Prime Numbers (#1) 33

27 Finite and Infinite Sets 35

28 Number of Subsets of a Set (#52) 38

29 Finite Products 39

30 The Infinitude of Primes (#11) 39

1 Introduction

The ℕaproche system (for *Natural Proof Checking*) checks the logical correctness of texts written in an input language ForTheL (for *Formula Theory Language*) which ideally reads like common mathematical language. Proofs and proof structures should resemble the style of undergraduate textbooks. ℕaproche is a *natural proof assistant* intended to approximate and support ordinary mathematical practices. The inbuilt ontology of ℕaproche corresponds to classical foundations of mathematics in first-order logic and set theory.

ℕaproche is included in the Isabelle prover environment: installing Isabelle also installs ℕaproche; opening files with a `.ftl` or `.ftl.tex` extension in Isabelle/jEdit automatically activates proof-checking by ℕaproche, with feedback through the standard output buffer, highlighting, and pop-up windows. The ℕaproche installation contains a small library of formalization examples. The current document is one of the examples, available in `.ftl.tex` format for proof-checking and LaTeX typesetting, and as a typeset `.pdf` file.

This document serves several purposes: to demonstrate the ℕaproche concept within a longer formalization; to propose a logical and set-theoretical foundation for number systems in a build-up of mathematical notions with sets and classes, maps, relations and numbers; to prove several theorems from the well-known list of 100 theorems that F. Wiedijk has proposed as formalization benchmarks [7].

In our approach the ordered field $\mathbb{R}$ of real numbers is postulated axiomatically. We then construe the structures of integer and rational numbers as substructures of $\mathbb{R}$:

$$\mathbb{R} \supseteq \mathbb{Q} \supseteq \mathbb{Z} \supseteq \mathbb{N}.$$

This corresponds to the geometric intuition of a continuous line of numbers with distinguished elements 0 and 1, from which integer and rational numbers can be constructed. Technically, this has the advantage that real addition and multiplication can be *restricted* to those substructures, instead of *extending* operations to larger superstructures.

We list the ten "Wiedijk Theorems" contained in this document and the authors of the respective formalizations. Most formalizations build on earlier versions, also by other authors, some are inherited from ℕaproche's predecessor system SAD (for *System for Automated Deduction*) by A. Paskevich and others [6].

- #1: The Irrationality of the Square Root of 2
  Naproche formalization: Peter Koepke, Mateusz Marcol and Patrick Schäfer
- #11: The Infinitude of Primes
  Peter Koepke
- #25: The Schröder-Bernstein Theorem
  Alexander Holz, Marcel Schütz

- #52: Number of Subsets of a Set
  Patrick Schäfer
- #60: Bezout's Identity
  Mateusz Marcol, Patrick Schäfer
- #63: Cantor's Theorem
  Steffen Frerix
- #66: Sum of a Geometric Series
  Peter Koepke
- #66: Sum of an Arithmetic Series
  Peter Koepke
- #69: Greatest Common Divisor Algorithm
  Mateusz Marcol, Patrick Schäfer
- #74: The Principle of Mathematical Induction
  Peter Koepke

We shall continue to extend and improve the formalizations and upload new versions for inclusion into future releases of Isabelle.

We view the present state of ℕaproche and this paper as proof of concept for interactive theorem proving with natural language formalizations. To extend ℕaproche to a powerful comprehensive system like Mizar or Isabelle should in principle be possible, given sufficient time and manpower. We think, however, that it is more promising to equip established system with a natural language interface by adapting ℕaproche's translation techniques from natural mathematical language texts into formal logics.

2 Basic Notions

Some notions and their elementary properties are already built into ℕaproche and its input language ForTheL. There are mathematical *objects*, and *sets* and *classes* that contain mathematical objects. Sets are classes which are objects themselves and can thus be used in further mathematical constructions. *Functions* and *maps* map objects to objects, where functions are those maps which are themselves objects.

Modelling mathematical notions by objects corresponds to the intuition that numbers, points, etc. should not have internal set-theoretical structurings, in contrast to purely set-theoretical foundations of mathematics. This is also advantageous for automated proving since it prevents proof searches to dig into mathematically irrelevant internal structurings.

We begin by fixing some mathematical language. We import singular/plural forms of words that will be used in our formalizations (`examples/vocabulary.ftl.tex`). In the long run this should be replaced by employing a proper English

vocabulary. We also import some alternative formulations for useful mathematical phrases (`examples/macros.ftl.tex`).

On the basis of inbuilt assumptions we prove some lemmas that illustrate the ℕaproche ontology. Later we shall postulate further axioms known from the set theories of Kelley-Morse or Zermelo-Fraenkel.

The notions of set and class capture the naive intuition of set expressed by Georg Cantor:

> A set is a collection of definite, distinguishable objects of perception or thought conceived as a whole. The objects are called elements or members of the set.

This is reflected formally in the following two lemmas, stating that classes are built and determined by their elements which are mathematical objects.

Proposition 1. Let X be a class. Let x be an element of X. Then x is an object.

Lemma 2 (Extensionality Axiom). Let X, Y be classes. Assume that every element of X is an element of Y and every element of Y is an element of X. Then $X = Y$.

Maps are also built into ℕaproche, equipped with domains and an application operator $_(_)$.

Lemma 3. Let F be a map. Then $\mathrm{dom}(F)$ is a class.

Lemma 4. Let F be a map and x be an element of $\mathrm{dom}(F)$. Then $F(x)$ is an object.

Lemma 5 (Map Extensionality). Let F, G be maps. Assume $\mathrm{dom}(F) = \mathrm{dom}(G)$ and for all elements x of $\mathrm{dom}(F)$ we have $F(x) = G(x)$. Then $F = G$.

Sets are those classes that are themselves objects.

Lemma 6. Let X be a set. Then X is a class that is an object.

Lemma 7. Let X be a class that is an object. Then X is a set.

Similarly, functions are maps that are objects.

Lemma 8. Let F be a function. Then F is a map that is an object.

Lemma 9. Let F be a map that is an object. Then F is a function.

3 Classes

Classes are usually defined by abstraction terms {... | ...}. We indicate the beginnings of a theory of classes which could be extended much further.

Let S, T, U denote classes.

Definition 10. $\emptyset$ is the class that has no elements.

Let the empty class stand for $\emptyset$.

Definition 11. $\mathcal{V}$ is the class of all mathematical objects.

Let the universe stand for $\mathcal{V}$.

Definition 12. S is nonempty iff S has an element.

Definition 13. A subclass of S is a class T such that every $x \in T$ belongs to S.

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

Definition 14. The union of S and T is $\{x \mid x \in S \vee x \in T\}$.

Let $S \cup T$ stand for the union of S and T.

Definition 15. The intersection of S and T is $\{x \mid x \in S \wedge x \in T\}$.

Let $S \cap T$ stand for the intersection of S and T.

Definition 16. The set difference of S and T is $\{x \in S \mid x \notin T\}$.

Let $S \setminus T$ stand for the set difference of S and T.

These class operations satisfy algebraic properties of Boolean algebras like the following distributive law:

Proposition 17. Let B, C, D be classes. Then $B \cup (C \cap D) = (B \cup C) \cap (B \cup D)$.

We conclude with a few more definitions.

Definition 18. S is disjoint from T iff there is no element of S that is an element of T.

Definition 19. A family of sets is a class A such that every element of A is a set.

Definition 20. Let A be a family of sets. The union of A is $\{x | x \in y$ for some $y \in A\}$.

Let $\bigcup A$ stand for the union of A.

Lemma 21. Let A, B, C be sets such that $C \subseteq A$ and $C \subseteq B$. If $A \setminus C = B \setminus C$ then $A = B$.

4 Maps

Let S, T denote classes. Let F stand for maps.

Definition 22. A value of F is an object y such that $F(x) = y$ for some $x \in \mathrm{dom}(F)$.

Definition 23. Assume S is a subclass of the domain of F. $F[S] = \{F(x) \mid x \in S\}$.

Definition 24. Let F be a map. $\mathrm{ran}(F) = F[\mathrm{dom}(F)]$.

Let the image of F stand for $F[\mathrm{dom}(F)]$.

Definition 25. A map from S to T is a map F such that $\mathrm{dom}(F) = S$ and $F[S] \subseteq T$.

Let $F : S \to T$ stand for F is a map from S to T.

There are canonical operations on maps.

Signature 26. Let F, G be maps such that $\mathrm{ran}(G) \subseteq \mathrm{dom}(F)$. $F \circ G$ is a map H such that $\mathrm{dom}(H) = \mathrm{dom}(G)$ and $H(x) = F(G(x))$ for all $x \in \mathrm{dom}(H)$.

Lemma 27. Let F, G, H be maps such that $\mathrm{ran}(H) \subseteq \mathrm{dom}(G)$ and $\mathrm{ran}(G) \subseteq \mathrm{dom}(F)$. Then $(F \circ G) \circ H = F \circ (G \circ H)$.

Proof. $\mathrm{dom}((F \circ G) \circ H) = \mathrm{dom}(H)$. $\mathrm{dom}(G \circ H) = \mathrm{dom}(H)$. Let $U = G \circ H$.

$$\mathrm{dom}(F \circ (G \circ H)) = \mathrm{dom}(F \circ U) = \mathrm{dom}(U) = \mathrm{dom}(G \circ H) = \mathrm{dom}(H).$$

For every $x \in \mathrm{dom}(H)$ we have

$$((F \circ G) \circ H)(x) = F(G(H(x))) = (F \circ (G \circ H))(x).$$

□

Signature 28. Id is the map such that $\mathrm{dom}(Id) = \mathcal{V}$ and $Id(x) = x$ for all $x \in \mathcal{V}$.

Lemma 29. $Id : \mathcal{V} \to \mathcal{V}$.

Lemma 30. Let F be a map. Then $Id \circ F = F$.

Proof. Consider $G = Id \circ F$. $\mathrm{dom}(Id \circ F) = \mathrm{dom}(F)$. $((Id \circ F))(x) = F(x)$ for all $x \in \mathrm{dom}(F)$. □

Signature 31. Let F be a map and A be a class. $F \restriction A$ is the map G such that $\mathrm{dom}(G) = \mathrm{dom}(F) \cap A$ and $G(x) = F(x)$ for all $x \in \mathrm{dom}(G)$.

Lemma 32. Let F be a map. Then $F \circ (Id \restriction \mathrm{dom}(F)) = F$.

Proof. Consider $I = Id \restriction \mathrm{dom}(F)$. $\mathrm{dom}(F \circ (Id \restriction \mathrm{dom}(F))) = \mathrm{dom}(F \circ I) = \mathrm{dom}(I) = \mathrm{dom}(F)$. $(F \circ (Id \restriction \mathrm{dom}(F)))(x) = F(x)$ for all $x \in \mathrm{dom}(F)$. □

We distinguish several important kinds of maps.

Definition 33. A surjection from S onto T is a map f from S to T such that $f[S] = T$.

Definition 34. Let f be a map. f is injective iff $f(x) \neq f(y)$ for all distinct elements x, y of $\mathrm{dom}(f)$.

Lemma 35. Id is an injective surjection from $\mathcal{V}$ onto $\mathcal{V}$.

Lemma 36. Let F, G be injective maps such that $\mathrm{ran}(F) \subseteq \mathrm{dom}(G)$. Then $G \circ F$ is injective.

Lemma 37. Let S, T, U be classes. Let F be a surjection from S onto T and G be a surjection from T onto U. Then $G \circ F$ is a surjection from S onto U.

Proof. Then $(G \circ F)[S] = G[F[S]] = G[T] = U$. □

Signature 38. Let F be an injective map. F^{-1} is the map G such that $\mathrm{dom}(G) = \mathrm{ran}(F)$ and for all $v \in \mathrm{dom}(G)$ $G(v) \in \mathrm{dom}(F)$ and $F(G(v)) = v$.

Lemma 39. Let F be an injective map. Then $F^{-1} : \mathrm{ran}(F) \to \mathrm{dom}(F)$.

Definition 40. A bijection between S and T is an injective surjection from S onto T.

Lemma 41. Let S, T be classes. Let F be a bijection between S and T. Then F^{-1} is a bijection between T and S.

5 Equinumerosity

Bijective maps and functions are the basis for cardinality theory.

Let S, T, U denote classes.

Definition 42. S and T are equinumerous iff there exists a bijection between S and T.

Let $S \sim T$ stand for S and T are equinumerous.

We show that equinumerosity is an equivalence relation on classes and in particular on sets.

Lemma 43. $S \sim S$.

Proof. $Id \restriction S : S \to S$. $Id \restriction S$ is injective. $Id \restriction S$ is a surjection from S onto S. □

Lemma 44. Assume that $S \sim T$. Then $T \sim S$.

Lemma 45. Assume that $S \sim T \sim U$. Then $S \sim U$.

Lemma 46. Let A, B, C, D be classes such that A and B are disjoint and C

and D are disjoint. Assume that $A \sim C$ and $B \sim D$. Then $A \cup B \sim C \cup D$.

Proof. Take a bijection F between A and C. Take a bijection G between B and D.

Define

$$H(x) = \begin{cases} F(x) & : x \in A \\ G(x) & : x \in B \end{cases}$$

for $x \in A \cup B$. [timelimit 10]

H is a map from $A \cup B$ to $C \cup D$. [timelimit 3] H is a bijection between $A \cup B$ and $C \cup D$. □

6 Set-Theoretic Axioms

Many classes defined in mathematics are considered to be mathematical objects that can be used freely in further constructions. We defined sets to be classes that are objects. However, we cannot identify *all* classes with sets due to the famous Russell's paradox [3]. The proof is based on the important *diagonal argument*.

Let S denote a class.

Theorem 47 (Russell). There is a class that is not a set.

Proof. Define

$$R = \{x | x \text{ is a set and } x \notin x\}.$$

R is not a set. Indeed if R is a set then

$$R \in R \iff R \notin R.$$

□

As a reaction to Russell's theorem, Ernst Zermelo, Abraham Fraenkel and others have formulated axioms which postulate explicitly that certain classes are sets. We present the standard axioms without the axioms of infinity, choice and foundation. The infinity axiom will be introduced later by requiring that the (infinite) class of natural numbers is a set. The axioms of choice and foundation are not needed for our presentation. Note that the axiomatic strength introduced here corresponds to Kelley-Morse set theory, since classes can be formed using formulas with class quantifiers. We begin by restating the axiom of extensionality.

Lemma 48 (Extensionality Axiom). Let X, Y be classes. Assume that every element of X is an element of Y and every element of Y is an element of X. Then $X = Y$.

Axiom 49 (Set Existence Axiom). The empty class is a set.

Axiom 50 (Pairing Axiom). Let a, b be objects. Let $P = \{a, b\}$. Then P is a set.

Axiom 51 (Union Axiom). Let F be a set that is a family of sets. Then $\bigcup F$ is a set.

Axiom 52 (Separation Axiom). Assume that X is a set and T is a subclass of X. Then T is a set.

Definition 53. A subset of S is a set X such that $X \subseteq S$.

Definition 54. Let X be a set. The powerset of X is the collection of subsets of X.

Let $\mathcal{P}(X)$ denote the powerset of X.

Axiom 55 (Powerset Axiom). The powerset of any set is a set.

Axiom 56 (Replacement Axiom). Let F be a function. Let X be a subset of the domain of F. Then $F[X]$ is a set.

The treatment of functions and maps is similar to that of sets and classes, and we can postulate function-theoretic axioms like:

Axiom 57. Assume that f is a map and $\mathrm{dom}(f)$ is a set. Then f is a function.

7 Ordered Pairs and Products

Since we prefer objects over sets if possible, we do not work with Kuratowski-style set-theoretical ordered pairs, but introduce them as objects.

Lemma 58. Let x, y be objects. Then (x, y) is an object.

The universal property of ordered pairs is postulated as and axiom.

Axiom 59. For any objects a, b, c, d if $(a, b) = (c, d)$ then $a = c$ and $b = d$.

This allows to work with cartesian products. One could show from the Zermelo-Fraenkel axioms that $X \times Y$ is a set whenever X and Y are sets. But it is easier to postulate that as an axiom.

Let S, T denote classes.

Definition 60. $S \times T = \{(x, y) \mid x \in S \text{ and } y \in T\}$.

Axiom 61. Let X, Y be sets. Then $X \times Y$ is a set.

Lemma 62. Let x, y be objects. If (x, y) is an element of $S \times T$ then x is

an element of S and y is an element of T.

8 Cantor's Theorem (#63)

Despite its technical simplicity, Cantor's Theorem is the origin of infinitary and uncountable set theory. The diagonal argument of its proof has become a powerful and standard proof principle mainly in foundational theories.

Theorem (Cantor). Let M be a set. Then there is no surjection from M onto the powerset of M.

Proof. Assume the contrary. Take a surjection f from M onto the powerset of M. Define

$$N = \{x \in M \mid x \text{ is not an element of } f(x)\}.$$

Take an element z of M such that $f(z) = N$. Then

$$z \in N \iff z \notin f(z) = N.$$

Contradiction. □

9 The Knaster-Tarski Fixed Point Theorem

The Knaster-Tarski theorem is an important result in lattice theory [5, 1]. We prove the theorem for the $\subseteq$-relation on sets, in order to apply it in the subsequent section.

Definition 63. Let h be a map. A fixed point of h is an element u of $\mathrm{dom}(h)$ such that $h(u) = u$.

Definition 64. A map between families of sets is a map from some family of sets to some family of sets.

Definition. Let h be a map between families of sets. h preserves subsets iff for all $u, v \in \mathrm{dom}(h)$ we have

$$u \subseteq v \implies h(u) \subseteq h(v).$$

Theorem (Knaster-Tarski). Let x be a set. Let h be a map from $\mathcal{P}(x)$ to $\mathcal{P}(x)$ that preserves subsets. Then h has a fixed point.

Proof. Define $A = \{y \mid y \subseteq x \text{ and } y \subseteq h(y)\}$. [timelimit 10] Then A is a subset of $\mathcal{P}(x)$ and $\bigcup A \in \mathcal{P}(x)$. [timelimit 3]

(1) $\bigcup A \subseteq h(\bigcup A)$.

Proof. Let $u \in \bigcup A$. Take $y \in A$ such that $u \in y$. Then $u \in h(y) \subseteq h(\bigcup A)$. qed.

(2) $h(\bigcup A) \subseteq \bigcup A$.

Proof. $h(\bigcup A) \subseteq x$. $h(\bigcup A) \subseteq h(h(\bigcup A))$. $h(\bigcup A) \in A$. Thus $h(\bigcup A) \subseteq \bigcup A$. qed.

Then $\bigcup A$ is a fixed point of h (by 1, 2). □

10 The Schröder-Bernstein Theorem (#25)

The Schröder-Bernstein theorem, also called the Cantor-Schröder-Bernstein theorem, is important for developing the theory of infinite cardinals without the axiom of choice. We base the proof on the Tarski-Knaster theorem, following [4].

Theorem (Cantor-Schröder-Bernstein). Let x, y be sets. x and y are equinumerous iff there exists a injective map from x to y and there exists an injective map from y to x.

Proof. Case x and y are equinumerous. Take a bijection f between x and y. Then f^{-1} is a bijection between y and x. Hence f is an injective map from x to y and f^{-1} is an injective map from y to x. End.

Case there exists an injective map from x to y and there exists an injective map from y to x. Take an injective map f from x to y. Take an injective map g from y to x. We have $y \setminus f[a] \subseteq y$ for any $a \in \mathcal{P}(x)$.

(1) Define $h(a) = x \setminus g[y \setminus f[a]]$ for $a \in \mathcal{P}(x)$.

h is a map from $\mathcal{P}(x)$ to $\mathcal{P}(x)$. Indeed $h(a)$ is a subset of x for each subset a of x.

Let us show that h preserves subsets. Let u, v be subsets of x. $u, v \in \mathcal{P}(x)$. Assume $u \subseteq v$. Then $f[u] \subseteq f[v]$. Hence $y \setminus f[v] \subseteq y \setminus f[u]$. Thus $g[y \setminus f[v]] \subseteq g[y \setminus f[u]]$. Indeed $y \setminus f[v]$ and $y \setminus f[u]$ are subsets of y. Therefore $x \setminus g[y \setminus f[u]] \subseteq x \setminus g[y \setminus f[v]]$. Consequently $h(u) \subseteq h(v)$. End.

Hence we can take a fixed point c of h (by Knaster-Tarski).

(2) Define $F(u) = f(u)$ for $u \in c$.

We have $c = h(c)$ iff $x \setminus c = g[y \setminus f[c]]$. g^{-1} is a bijection between $\mathrm{ran}(g)$ and y. Thus $x \setminus c = g[y \setminus f[c]] \subseteq \mathrm{ran}(g)$. Therefore $x \setminus c$ is a subset of $\mathrm{dom}(g^{-1})$.

(3) Define $G(u) = g^{-1}(u)$ for $u \in x \setminus c$.

F is a bijection between c and $\mathrm{ran}(F)$. G is a bijection between $x \setminus c$ and $\mathrm{ran}(G)$.

Define

$$H(u) = \begin{cases} F(u) & : u \in c \\ G(u) & : u \notin c \end{cases}$$

for $u \in x$.

Let us show that H is a map from x to y. $\mathrm{dom}(H)$ is a set. Hence H is a map.

Let us show that every value of H is an element of y. Let v be a value of H. Take $u \in x$ such that $H(u) = v$. If $u \in c$ then $v = H(u) = F(u) = f(u) \in y$. If $u \notin c$ then $v = H(u) = G(u) = g^{-1}(u) \in y$. End. End.

(4) H is a surjection from x onto y. Indeed we can show that every element of y is a value of H. Let $v \in y$.

Case $v \in f[c]$. Take $u \in c$ such that $f(u) = v$. Then $F(u) = v$. End.

Case $v \notin f[c]$. Then $v \in y \setminus f[c]$. Hence $g(v) \in g[y \setminus f[c]]$. Thus $g(v) \in x \setminus h(c)$. We have $g(v) \in x \setminus c$. Therefore we can take $u \in x \setminus c$ such that $G(u) = v$. Then $v = H(u)$. End. End.

(5) H is injective. Indeed we can show that for all $u, v \in x$ if $u \neq v$ then $H(u) \neq H(v)$. Let $u, v \in x$. Assume $u \neq v$.

Case $u, v \in c$. Then $H(u) = F(u)$ and $H(v) = F(v)$. We have $F(u) \neq F(v)$. Hence $H(u) \neq H(v)$. End.

Case $u, v \notin c$. Then $H(u) = G(u)$ and $H(v) = G(v)$. We have $G(u) \neq G(v)$. Hence $H(u) \neq H(v)$. End.

Case $u \in c$ and $v \notin c$. Then $H(u) = F(u)$ and $H(v) = G(v)$. Hence $v \in g[y \setminus f[c]]$. We have $G(v) \in y \setminus F[c]$. Thus $G(v) \neq F(u)$. End.

Case $u \notin c$ and $v \in c$. Then $H(u) = G(u)$ and $H(v) = F(v)$. Hence $u \in g[y \setminus f[c]]$. We have $G(u) \in y \setminus f[c]$. Thus $G(u) \neq F(v)$. End. End.

Consequently H is a bijection between x and y (by 4, 5). Therefore x and y are equinumerous. End. □

11 The Real Field

We introduce the real numbers with their arithmetical operations and postulate that they satisfy standard field axioms. This is a partial axiomatisation. Only after the introduction of further axioms that specify the nested number systems

$$\mathbb{R} \supseteq \mathbb{Q} \supseteq \mathbb{Z} \supseteq \mathbb{N}.$$

and the relations between the numbersystems will it be clear that the reals introduced along this paper are isomorphic to the standard reals as completion of the rational numbers.

Signature 65. A real number is a mathematical object.

Definition 66. $\mathbb{R}$ is the collection of real numbers.

Axiom 67. $\mathbb{R}$ is a set.

Note that this axiom does not yet imply the existence of infinite sets, since under the axioms in this section $\mathbb{R}$ could still be some finite field. The following are standard axioms for commutative fields, where the additive and multiplicative inverses are given by functions $x \mapsto -x$ and $x \mapsto 1/x$.

Let x, y, z, w denote real numbers.

Signature 68. $x + y$ is a real number.

Let the sum of x and y denote $x + y$.

Signature 69. $x \cdot y$ is a real number.

Let the product of x and y denote $x \cdot y$.

Axiom 70. $x + y = y + x$.

Axiom 71. $(x + y) + z = x + (y + z)$.

Signature 72. 0 is a real number such that for every real number x $x + 0 = x$.

Signature 73. $-x$ is a real number such that $x + (-x) = 0$.

Axiom 74. $x \cdot y = y \cdot x$.

Axiom 75. $((x \cdot y)) \cdot z = x \cdot (y \cdot z)$.

Signature 76. 1 is a real number such that $1 \neq 0$ and for every real number x $1 \cdot x = x$.

Signature 77. Assume $x \neq 0$. $1/x$ is a real number such that $x \cdot (1/x) = 1$.

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

Axiom 78. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

We continue by proving some consequencen of the axioms. The selection of lemmas follows the *Foundations of Real Analysis* by Walter Rudin [2]. Note that in rare cases we need to use double brackets $((\dots))$ because of some parser bug.

Proposition 79. $((y \cdot x)) + (z \cdot x) = (y + z) \cdot x$.

Proposition 80. Let $x + y = x + z$. Then $y = z$.

Proof. $y = -x + (x + y) = -x + (x + z) = z$. □

Proposition 81. If $x + y = x$ then $y = 0$.

Proposition 82. If $x + y = 0$ then $y = -x$.

Proposition 83. $-(-x) = x$.

Proposition 84. Let x be nonzero and $x \cdot y = x \cdot z$. Then $y = z$.

Proof. $y = ((1/x) \cdot x) \cdot y = (1/x) \cdot (x \cdot y) = (1/x) \cdot (x \cdot z) = ((1/x) \cdot x) \cdot z = z$. □

Proposition 85. If x is nonzero and $x \cdot y = x$ then $y = 1$.

Proposition 86. If x is nonzero and $x \cdot y = 1$ then $y = 1/x$.

Proposition 87. If x is nonzero then $1/(1/x) = x$.

Proposition 88. $0 \cdot x = 0$.

Proposition 89. If x is nonzero and $y \neq 0$ then $x \cdot y \neq 0$.

Proposition 90. $(-x) \cdot y = -(x \cdot y)$.

Proof. $((x \cdot y)) + (-x \cdot y) = (x + (-x)) \cdot y = 0 \cdot y = 0$. □

Proposition 91. $-x = -1 \cdot x$.

Proposition 92. $(-x) \cdot (-y) = x \cdot y$.

Proof. $(-x) \cdot (-y) = -(x \cdot (-y)) = -((-y) \cdot x) = -(-(y \cdot x)) = y \cdot x = x \cdot y$. □

Let $x - y$ stand for $x + (-y)$. Let $\frac{x}{y}$ stand for $x \cdot (1/y)$.

We prove some lemmas for later use.

Lemma 93. Let $z \neq 0$. Then $x = \frac{z \cdot x}{z}$.

Lemma 94. $(1 - x) \cdot y = y - (x \cdot y)$.

Proof. $(1 - x) \cdot y = y + ((-x) \cdot y) = y - (x \cdot y)$. □

Lemma 95. Let $w \neq 0$. Then $\frac{x-y}{w} + \frac{y-z}{w} = \frac{x-z}{w}$.

Proof. $(x - y) + (y - z) = ((x - y) + y) - z = x - z$. □

Lemma 96. $-(x + y) = -x - y$.

Proof. $(x + y) + (-x - y) = (x - x) + (y - y) = 0$. □

12 Some Numbers

We introduce the standard notations for small natural numbers. Under the axioms so far, we could still have that$0 = 3$ because we could be working in a field of characteristic 3.

Definition 97. $2 = 1 + 1$.

Definition 98. $3 = 2 + 1$.

Definition 99. $4 = 3 + 1$.

Definition 100. $5 = 4 + 1$.

Definition 101. $6 = 5 + 1$.

Definition 102. $7 = 6 + 1$.

Definition 103. $8 = 7 + 1$.

Definition 104. $9 = 8 + 1$.

Definition 105. $10 = 9 + 1$.

Lemma 106. $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ are real numbers.

With these numbers we can prove some small "decimal arithmetic":

Lemma 107. $2 + 5 = 7$.

Lemma 108. $2 \cdot 5 = 10$.

Lemma 109. $5 \cdot 5 = (2 \cdot 10) + 5$.

[timelimit 10]

Lemma 110. Assume that $6 \neq 0$. Then $\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$.

Proof. $\frac{1}{2} + \frac{1}{3} = \frac{3}{6} + \frac{2}{6} = \frac{5}{6}$. □

[timelimit 3]

The assumption $6 \neq 0$ makes the fractions well-defined. Note that $6 \neq 0$ implies that $2, 3 \neq 0$.

13 The Real Ordered Field

We first introduce the weak order $\leq$ on $\mathbb{R}$ instead of the strong orders $<$. Although these orders are easily interdefinable, the choice can noticably influence automatic proof searches. $\leq$ is a linear order:

Let x, y, z, w denote real numbers.

Signature 111. $x \leq y$ is an atom.

Let $x \not\leq y$ stand for $\neg x \leq y$.

Let $x \geq y$ stand for $y \leq x$.

Axiom 112. $x \leq x$.

Axiom 113. If $x \leq y$ and $x \geq y$ then $x = y$.

Axiom 114. If $x \leq y$ and $y \leq z$ then $x \leq z$.

Axiom 115. $x \leq y$ or $x \geq y$.

The order makes $\mathbb{R}$ an ordered field:

Axiom 116. If $y \leq z$ then $x + y \leq x + z$ and $y + x \leq z + x$.

Axiom 117 (1 17 ii). If $x \geq 0$ and $y \leq z$ then $x \cdot y \leq x \cdot z$.

We define the strict order as an abbreviation.

Let $x < y$ stand for $x \leq y$ and $x \neq y$. Let $x \not< y$ stand for $\neg x < y$. Let $x > y$ stand for $y < x$.

Definition 118. x is positive iff $x > 0$.

Definition 119. x is negative iff $x < 0$.

Definition 120. x is nonnegative iff $x \geq 0$.

Lemma 121. $x \leq y$ iff $y \not< x$.

We prove some lemmas, following Rudin [2].

Proposition 122. $x > 0$ iff $-x < 0$.

Proposition 123. If $x \neq 0$ then $x \cdot x > 0$.

Proof. Assume $x \neq 0$. Case $x \geq 0$. Trivial. Case $x \leq 0$. Trivial. □

Proposition 124. $1 > 0$.

Proposition 125. $x \leq y$ iff $-x \geq -y$.

Proof. $x \leq y$ iff $x - y \leq 0$. $x - y \leq 0$ iff $-y = -x + (x - y) \leq -x$. □

Proposition 126. If $x < 0$ and $y < z$ then $x \cdot y > x \cdot z$.

Proof. Let $x < 0$ and $y < z$. $-x > 0$. $(-x) \cdot y < (-x) \cdot z$. $-(x \cdot y) < -(x \cdot z)$. □

Proposition 127. $-1 < 0$.

Proposition 128. $x - 1 < x$.

Proposition 129. $x < y < x + 1$ iff $0 < y - x < 1$.

Proof. $x < y$ iff $0 = x - x < y - x$. $y < x + 1$ iff $y - x < (x + 1) - x = 1$. □

Proposition 130. If $0 < y$ then $0 < 1/y$.

Lemma 131. 0=0.

Lemma 132 (syz). If $\neg x \leq y$ then $x \geq y$.

Proposition 133. Assume $0 < x \leq y$. Then $1/y \leq 1/x$.

Proof by contradiction. Assume the contrary. Then $\neg 1/y \leq 1/x$. Let $u = 1/y$ and $v = 1/x$. Then $1/y \geq 1/x$. Then $1/x < 1/y$. Then

$$1 = x \cdot (1/x) = (1/x) \cdot x \leq (1/x) \cdot y = y \cdot (1/x) < y \cdot (1/y) = 1.$$

Hence $1 < 1$. Contradiction. □

14 Upper and lower bounds

The real numbers are *complete*, which is often expressed via Dedekind cuts or Cauchy sequences. Here we use suprema and infima instead. We make the necessary definitions.

Let E denote a subset of $\mathbb{R}$. Let x, a, b denote real numbers.

Definition 134. An upper bound of E is a real number b such that for all elements x of E $x \leq b$.

Definition 135. E is bounded above iff E has an upper bound.

Definition 136. A lower bound of E is a real number b such that for all elements x of E $x \geq b$.

Definition 137. E is bounded below iff E has a lower bound.

Definition 138. A supremum of E is a real number a such that a is an upper bound of E and for all x if $x < a$ then x is not an upper bound of E.

Definition 139. Let E be bounded below. An infimum of E is a real number a such that a is a lower bound of E and for all x if $x > a$ then x is not a lower bound of E.

The crucial completeness axiom now reads:

Axiom 140 (existence supremum). Assume that E is nonempty and bounded above. Then E has a supremum.

By symmetry, the existence of suprema implies the existence of infima.

Definition 141. $E^- = \{-x \in \mathbb{R} \mid x \in E\}$.

Lemma 142. E^- is a subset of $\mathbb{R}$.

[timelimit 5]

Lemma 143. x is an upper bound of E iff $-x$ is a lower bound of E^-.

[timelimit 3]

Theorem 144. Assume that E is a nonempty subset of $\mathbb{R}$ such that E is bounded below. Then E has an infimum.

Proof. Take a lower bound a of E. $-a$ is an upper bound of E^-. Take a supremum b of E^-.

(1) $-b$ is an infimum of E.

Proof. $-b$ is a lower bound of E. Let c be a lower bound of E. Then $-c$ is an upper bound of E^-. Hence $b \leq -c$ and $c \leq -b$. qed. □

15 The rational numbers

We introduce the rational numbers as a subfield of $\mathbb{R}$.

Signature 145. A rational number is a real number.

Let p, q, r denote rational numbers.

Definition 146. $\mathbb{Q}$ is the collection of rational numbers.

Theorem 147. $\mathbb{Q}$ is a subset of $\mathbb{R}$.

In particular, $\mathbb{Q}$ is a set. We now stipulate that $\mathbb{Q}$ is closed under the field operations of $\mathbb{R}$.

Axiom 148. $0, 1$ are rational numbers.

Let p, q denote rational numbers.

Axiom 149. $p + q$, $p \cdot q$ are rational numbers.

Axiom 150. $-p$ is a rational number.

Axiom 151. Assume that $p \neq 0$. Then $1/p$ is a rational number.

The reals are "generated" from the rationals by suprema (or infima). We postulate:

Axiom 152. Let x be a real number. Then there exists a subset A of $\mathbb{Q}$ such that A is bounded above and x is the supremum of A.

Theorem 153. $\mathbb{R} = \{x \in \mathbb{R} \mid$ there exists $A \subseteq \mathbb{Q}$ such that A is bounded above and x is the supremum of $A\}$.

16 Integers

$\mathbb{Z}$ is introduced as a subring of $\mathbb{Q}$:

Signature 154. An integer is a rational number.

Definition 155. $\mathbb{Z}$ is the collection of integers.

Lemma 156. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

Lemma 157. $\mathbb{Z}$ is a set.

$\mathbb{Z}$ is closed under $+$, $\cdot$ and $-$.

Axiom 158. $0, 1$ are integers.

Let a, b denote integers.

Axiom 159. $a + b$, $a \cdot b$ are integers.

Axiom 160. $-a$ is an integer.

The axioms up to now are consistent with the unintended equality $\mathbb{Z} = \mathbb{Q} = \mathbb{R}$. The following two axioms are crucial to obtain the standard number systems. $\mathbb{Z}$ is a *discrete* ring:

Axiom 161. There is no integer a such that $0 < a < 1$.

But the discrete ring generates the rationals by fractions:

Axiom 162. Let p be a rational number. Then there exist integers m, n such that $n \neq 0$ and $p = \frac{m}{n}$.

[timelimit 5]

Lemma 163.

$$\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z} \wedge n \neq 0\}.$$

Proof. $\frac{m}{n} \in \mathbb{Q}$ where m, n are integers and $n \neq 0$. □

[timelimit 3]

Although $\mathbb{Z}$ is a small, indeed countable subring of $\mathbb{R}$, it is somehow "large" in $\mathbb{R}$.

Theorem 164 (Archimedes 1). $\mathbb{Z}$ is not bounded above.

Proof. Assume the contrary. $\mathbb{Z}$ is nonempty. Indeed 0 is an integer. Take a supremum b of $\mathbb{Z}$ (by existence supremum). Indeed $\mathbb{Z}$ is a subset of $\mathbb{R}$. Let us show that $b - 1$ is an upper bound of $\mathbb{Z}$. Let $x \in \mathbb{Z}$. $x + 1 \in \mathbb{Z}$. $x + 1 \leq b$. $x = (x + 1) - 1 \leq b - 1$. End. □

Theorem 165. $\mathbb{Z}$ is not bounded below.

Proof. Assume the contrary. Take a real number x that is a lower bound of $\mathbb{Z}$. Then $-x$ is an upper bound of $\mathbb{Z}$. Contradiction (by Archimedes 1). Indeed $\mathbb{Z}$ is bounded above. □

Theorem 166 (Archimedes 2). Let x be a real number. Then there is an integer a such that $x < a$.

Proof by contradiction. Assume the contrary. Then x is an upper bound

of $\mathbb{Z}$. Contradiction (by Archimedes 1). Indeed $\mathbb{Z}$ is bounded above. □

17 The natural numbers

Finally we have descended to the natural numbers.

Definition 167. A natural number is a nonnegative integer.

Definition 168. $\mathbb{N}$ is the collection of natural numbers.

Lemma 169. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

In particular we obtain the following theorem which in other set theoretic approaches is equivalent to the Axiom of Infinity.

Theorem 170 (Axiom of Infinity). $\mathbb{N}$ is a set.

The numbersystems $\mathbb{N}$, $\mathbb{Q}$ and $\mathbb{R}$ are strictly ascending with respect to $\subseteq$.

Let $x \subsetneq y$ stand for $x \subseteq y$ and $x \neq y$.

Theorem 171. $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q}$.

Proof. $-1 \notin \mathbb{N}$. $-1 \in \mathbb{Z}$. $\frac{1}{2} \notin \mathbb{Z}$. Indeed $0 < \frac{1}{2} < 1$. $\frac{1}{2} \in \mathbb{Q}$. □

Lemma 172. $\mathbb{Z} = \mathbb{N}^- \cup \mathbb{N}$.

Lemma 173. $\mathbb{N}^- \cap \mathbb{N} = \{0\}$.

We shall later prove that $\mathbb{Q} \subsetneq \mathbb{R}$ using the irrationality of $\sqrt{2}$. The following closure properties show that $\mathbb{N}$ is something like a half-ring.

Let l, m, n stand for natural numbers.

Lemma 174. 0 is a natural number.

Lemma 175. 1 is a natural number.

Lemma 176. $l + m$ is a natural number.

Lemma 177. $l \cdot m$ is a natural number.

Although we do not have additive inverses available in $\mathbb{N}$, we still have some cancellation properties known from rings.

Lemma 178. If $l + m = l + n$ or $m + l = n + l$ then $m = n$.

Lemma 179. Assume that l is nonzero. If $l \cdot m = l \cdot n$ or $m \cdot l = n \cdot l$ then $m = n$.

Together with the principle of mathematical induction the next lemma expresses that $\mathbb{N}$ is an inductive type that is generated by 0 and the successor operation $+1$.

Lemma 180. Let n be a natural number. Then $n = 0$ or $n = m + 1$ for some natural number m.

Proof. Case $n = 0$. Trivial.

Case $n \neq 0$. Let $m = n - 1$. m is a natural number and $n = m + 1$. End. □

Lemma 181. For every natural number n $n = 0$ or $1 \leq n$.

Lemma 182. If $m + n = 0$ then $m = 0$ and $n = 0$.

On $\mathbb{N}$, $\leq$ is definable using addition.

Lemma 183. If $m \geq n$ then $m - n$ is a natural number.

Lemma 184. Assume $m \leq n$. Then there exists a natural number l such that $m + l = n$.

Proof. $n - m$ is a natural number. $m + (n - m) = (n - m) + m = n$. □

Lemma 185. Assume there exists a natural number l such that $m+l = n$. Then $m \leq n$.

Lemma 186. Let $m \neq 0$. Then $n \leq n \cdot m$.

Proof. We have $1 \leq m$. $n = n \cdot 1 \leq n \cdot m$. □

Lemma 187. Let a, α, b, β be real numbers such that $a \leq \alpha$ and $b \leq \beta$. Then $a + b \leq \alpha + \beta$.

Proof. $a \leq \alpha$ and $a + b \leq \alpha + b$ and $\alpha + b \leq \alpha + \beta$. □

Lemma 188. Let a, b be integers such that $a < b$. Then $a + 1 \leq b$.

Proof. Assume the contrary. Let $c = a + 1$. $c > b$. Then $a < b < a + 1$. Thus $a - a = 0 < b - a < (a + 1) - a = 1$. Then $b - a$ is an integer and $0 < b - a < 1$. Contradiction. □

Lemma 189. Let a, b be integers such that $a > b$. Then $a - 1 \geq b$.

Proof. $a > b$. Then $-a < -b$. $-a+1 \leq -b$. $-(-a+1) \geq -(-b)$. $a-1 \geq b$. □

18 The Principle of Mathematical Induction (#74)

We prove the second-order Peano axiom for all subsets of $\mathbb{N}$. This implies the principle of *complete induction*: to prove a property $P(n)$ for all natural numbers n, prove $P(0)$ and the implication $P(n) \to P(n + 1)$.

Theorem 190 (Induction Theorem). Assume $A \subseteq \mathbb{N}$ and $0 \in A$ and for all $n \in A$ $n + 1 \in A$. Then $A = \mathbb{N}$.

Proof. Let us show that every element of $\mathbb{N}$ is an element of A. Let $n \in \mathbb{N}$. Assume the contrary. Define $F = \{j \in \mathbb{N} \mid j \notin A\}$. F is nonempty and F is bounded below. F is a subset of $\mathbb{R}$. Take an infimum a of F. Let us show that $a+1$ is a lower bound of F. Let $x \in F$. $x-1 \in \mathbb{Z}$.

Case $x-1<0$. Then $0<x<1$. Contradiction. End.

Case $x-1=0$. Then $x=1$ and $1 \notin A$. Contradiction. End.

Case $x-1>0$. Then $x-1 \in \mathbb{N}$. $x-1 \notin A$. Indeed $(x-1)+1=x \notin A$. $x-1 \in F$. $a \leq x-1$. $a+1 \leq (x-1)+1=x$. End. End.

Then $a+1>a$. Contradiction. End. □

Naproche provides a general mechanism for the organisation of inductive proofs. There is a reserved binary relation symbol $\prec$ which can be viewed as a universal inductive relation. The keyphrase *proof by induction* turns a universal claim $\forall x\ P(x)$ into the thesis

$$\forall x(\forall y(y \prec x \rightarrow\ P(y)) \rightarrow P(x))$$

expressing that P is inherited from $\prec$-predecessors. Therefore we can describe $\prec$ by:

Let n, m denote natural numbers.

Let m is inductively smaller than n stand for $m \prec n$.

The Induction Theorem justifies to embed the ordering of the natural numbers into $\prec$.

Axiom 191. If $n<m$ then n is inductively smaller than m.

We can now give a generic proof of mathematical induction which is typical of Naproche's approach.

Signature 192. $P(n)$ is an atom.

Theorem 193. Assume that $P(0)$ and for all natural numbers n if $P(n)$ then $P(n+1)$. Then $P(n)$ for all natural numbers n.

Proof by induction. Let n be a natural number.

Case $n=0$. Trivial.

Case $n \neq 0$. Then take a natural number m such that $n=m+1$. m is inductively smaller than n and $P(m)$. Hence $P(n)$. Qed. □

Induction also implies that the relation $<$ is well-founded on $\mathbb{N}$: every nonempty subset of $\mathbb{N}$ has a minimal element:

Theorem 194. Let X be a nonempty subset of $\mathbb{N}$. Then there is an element n of X such that n is the infimum of X.

Proof. Assume the contrary. Then for all elements n of X there is $x \in X$ such that $\neg n \leq x$.

(1) For all natural numbers n $n \notin X$.

Proof by induction. Let n be a natural number. Assume that $n \in X$. Take $x \in X$ such that $\neg n \leq x$. Then $x < n$. x is inductively smaller than n. Hence $x \notin X$. Contradiction. Qed.

Hence $X = \emptyset$. Contradiction.

□

19 Sum of an Arithmetic Series (#68)

Let a, d denote real numbers. Let n denote a natural number.

Signature 195. $\sum_{i=1}^{n}(a + d \cdot i)$ is a real number.

Axiom 196. $\sum_{i=1}^{1}(a + d \cdot i) = a + d$.

Axiom 197 (1). $\sum_{i=1}^{n+1}(a + d \cdot i) = \sum_{i=1}^{n}(a + d \cdot i) + (a + (d \cdot (n + 1)))$.

Lemma 198. Let b be a nonzero real number. $\frac{a}{b} \cdot d = a \cdot \frac{d}{b}$.

Theorem 199. For all nonzero natural numbers n

$$\sum_{i=1}^{n}(a + d \cdot i) = n \cdot (a + \frac{(n + 1) \cdot d}{2}).$$

Proof by induction on n. Let n be a nonzero natural number.

Case $n = 1$. Trivial.

Take a natural number m such that $m + 1 = n$. m is inductively smaller than n.

$$\sum_{i=1}^{m}(a + d \cdot i) = m \cdot (a + \frac{(m + 1) \cdot d}{2}).$$

Then

$$\sum_{i=1}^{n}(a + d \cdot i) = (m \cdot (a + \frac{(m + 1) \cdot d}{2})) + (a + (d \cdot (m + 1)))$$

(by 1).

[timelimit 10] Hence

$\sum_{i=1}^{n}(a + d \cdot i) =$

$((m \cdot a) + (m \cdot \frac{n \cdot d}{2})) + (a + (d \cdot n)) =$

$(((m \cdot a) + (m \cdot \frac{n \cdot d}{2})) + a) + (d \cdot n) =$

$(((m \cdot a) + a) + (m \cdot \frac{n \cdot d}{2})) + (d \cdot n) =$

$(((m \cdot a) + (1 \cdot a)) + (m \cdot \frac{n \cdot d}{2})) + (d \cdot n) =$

$((n \cdot a) + (m \cdot \frac{n \cdot d}{2})) + (d \cdot n).$

$((n \cdot a) + (m \cdot \frac{n \cdot d}{2})) + (d \cdot n) =$

$(n \cdot a) + ((m \cdot \frac{n \cdot d}{2}) + (d \cdot n)) =$

$(n \cdot a) + ((m \cdot \frac{n \cdot d}{2}) + (1 \cdot (d \cdot n))) =$

$(n \cdot a) + ((m \cdot \frac{n \cdot d}{2}) + (\frac{2}{2} \cdot (d \cdot n))).$

Then $(n \cdot a) + ((m \cdot \frac{n \cdot d}{2}) + (\frac{2}{2} \cdot (d \cdot n))) =$

$(n \cdot a) + ((m \cdot \frac{n \cdot d}{2}) + (2 \cdot \frac{n \cdot d}{2})) =$

$(n \cdot a) + ((m + 2) \cdot \frac{n \cdot d}{2}).$

Then $(n \cdot a) + ((m + 2) \cdot \frac{n \cdot d}{2}) = (n \cdot a) + ((n + 1) \cdot \frac{n \cdot d}{2}) =$

$(n \cdot a) + \frac{(n+1) \cdot (n \cdot d)}{2} = (n \cdot a) + \frac{((n+1) \cdot n) \cdot d}{2} =$

$(n \cdot a) + \frac{(n \cdot (n+1)) \cdot d}{2} = (n \cdot a) + \frac{n \cdot ((n+1) \cdot d)}{2} =$

$(n \cdot a) + (n \cdot \frac{((n+1) \cdot d)}{2}) = n \cdot (a + \frac{(n+1) \cdot d}{2})$. [timelimit 3] □

20 Exponentiation

Let x, y denote real numbers. Let i denote natural numbers.

Signature 200. x^i is a real number.

Axiom 201. $x^0 = 1$.

Axiom 202. $x^{i+1} = x^i \cdot x$.

Lemma 203. $x^1 = x$.

Lemma 204. $x^2 = x \cdot x$.

Lemma 205. $x \cdot x^i = x^{i+1}$.

Lemma 206. Let m be a natural number. For all natural numbers n m^n is a natural number.

Proof by induction on n. Let n be a natural number.

Case $n = 0$. $m^0 = 1 \in \mathbb{N}$. End.

Case $n \neq 0$. Take a natural number k such that $k = n - 1$. k is inductively smaller than n. m^k is a natural number. $m \cdot m^k = m^{k+1} = m^n$. Thus m^n is a natural number. End. □

Lemma 207. Let m be a nonzero natural number. For all natural numbers n $1 \leq m^n$.

Proof by induction on n. Let n be a natural number.

Case $n = 0$. $m^0 = 1$. $1 \leq 1$. End.

Case $n \neq 0$. Take a natural number k such that $k = n - 1$. k is inductively smaller than n. $1 \leq m^k$ and $1 \leq m$. Thus $1 \leq m \cdot m^k = m^{k+1} = m^n$. End. □

We prove two standard binomial formulas. The formulation is somewhat clumsy, since we are missing proper arithmetic parsing and rewriting.

[timelimit 10]

Lemma 208. $(x + y)^2 = (x^2 + (2 \cdot (x \cdot y))) + y^2$.

Proof. $(x + y) \cdot (x + y) = (x^2 + (x \cdot y)) + ((y \cdot x) + y^2) = (x^2 + ((x \cdot y) + (y \cdot x))) + y^2 = (x^2 + (2 \cdot (x \cdot y))) + y^2$. □

Lemma 209. $(x - y)^2 = (x^2 - (2 \cdot (x \cdot y))) + y^2$.

Proof. $(x-y)^2 = (x^2+(2\cdot(x\cdot(-y))))+(-y)^2 = (x^2+(2\cdot(x\cdot(-y))))+y^2 = (x^2 + (2 \cdot (-(x \cdot y)))) + (-y)^2 = (x^2 - (2 \cdot (x \cdot y))) + y^2$. □

[timelimit 3]

21 Sum of a Geometric Series (#66)

We treat the partial sums $\sum_{0 \leq i < n} x^i$ of a geometric series as a function in x and n which satisfies some recursive axioms:

Let x denote a real number. Let n denote a natural number.

Signature 210. $\sum_{0 \leq i < n} x^i$ is a real number.

Axiom 211. $\sum_{0 \leq i < 0} x^i = 0$.

Axiom 212. Let x be a real number and n be a natural number. Then $\sum_{0 \leq i < n+1} x^i = (\sum_{0 \leq i < n} x^i) + x^n$.

Theorem 213. Let $x \neq 1$. Then

$$\sum_{0 \leq i < n} x^i = \frac{1 - x^n}{1 - x}$$

for all natural numbers n.

Proof by induction on n.

$1 - x \neq 0$.

Let n be a natural number.

Case $n = 0$. Trivial.

Case $n \neq 0$. Take a natural number m such that $m+1 = n$. m is inductively smaller than $m + 1$ and $\sum_{0 \leq i < m} x^i = \frac{1-x^m}{1-x}$.

Take $a = x^m$ and $b = x^n$ and $c = 1 - x$. Then a, b, c are real numbers and $\sum_{0 \leq i < n} x^i = \frac{1-x^m}{1-x} + x^m = \frac{1-x^m}{1-x} + \frac{x^m \cdot (1-x)}{1-x} = \frac{1-x^m}{1-x} + \frac{(x^m \cdot 1)+(x^m \cdot (-x))}{1-x} = \frac{1-x^m}{1-x} + \frac{x^m+((-x)\cdot x^m)}{1-x} = \frac{1-x^m}{1-x} + \frac{x^m+(-(x\cdot x^m))}{1-x} = \frac{1-x^m}{1-x} + \frac{x^m-x^n}{1-x} = \frac{1-a}{c} + \frac{a-b}{c} = \frac{(1-a)+(a-b)}{c} = \frac{((1-a)+a)-b}{c} = \frac{(1+(-a+a))-b}{c} = \frac{1-b}{c} = \frac{1-x^n}{1-x}$. End. □

22 Divisibility and Prime Numbers

We prove some divisibility properties that will be useful further on.

Let m, n, l denote integers.

Definition 214. n divides m iff for some integer l $m = n \cdot l$.

Let $x|y$ denote x divides y. Let a divisor of x denote an integer that divides x.

Lemma 215. Assume $l|m|n$. Then $l|n$.

Proof. Take integers u, v such that $m = l \cdot u$ and $n = m \cdot v$. Then $n = l \cdot (u \cdot v)$. □

Lemma 216. Let $l|m$ and $l|m + n$. Then $l|n$.

Proof. Assume that l is nonzero. Take an integers p, q such that $m = l \cdot p$ and $m+n = l \cdot q$. Take $r = q-p$. We have $(l \cdot p)+(l \cdot r) = l \cdot q = m+n = (l \cdot p)+n$. Hence $n = l \cdot r$. □

Lemma 217. Let n, m be natural numbers such that n is nonzero and n divides m. Then $\frac{m}{n}$ is a natural number.

Lemma 218. Let m, n be natural numbers such that $n|m$. Then there exists a natural number l such that $n \cdot l = m$.

Proof. Case $n = 0$. Then $m = 0$. 0 is a natural number and $n \cdot 0 = m$. End.

Case $n \neq 0$. Take an integer l such that $n \cdot l = m$. Assume l is not a natural number. $n > 0$ and $l < 0$. Thus $n \cdot l < 0$. End. □

Lemma 219. Let m, n be natural numbers. If $n|m|n$ then $m = n$.

Proof. Assume $n|m|n$. If $n = 0$ then $m = 0$. Assume $n \neq 0$. Take natural numbers p, q such that $n \cdot p = m$ and $m \cdot q = n$. Then $n = m \cdot q = (n \cdot p) \cdot q = n \cdot (p \cdot q) = (p \cdot q) \cdot n$. $1 = p \cdot q$. Therefore $p = q = 1$. □

Lemma 220. Let m be a natural number such that $m \neq 0$. Let k be a divisor of m. Then $k \leq m$.

Proof. Assume the contrary. Then there is a natural number l such that $l > 0$ and $m = l \cdot k$. □

Proposition 221. Let k, l be natural number such that $k < l$ and $k > 0$. Then l is not a divisor of k.

Prime numbers are the mathematically most interesting class of natural numbers.

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

Definition 222. n is prime iff n is a nontrivial natural number and for every natural number m that divides n $m = 1$ or $m = n$.

Theorem 223. Every nontrivial natural number m has a prime divisor.

Proof by induction on m. Let m be a nontrivial natural number. Case m is a prime natural number. Trivial. Take a natural number n such that $n|m$ and $n \neq 1$ and $n \neq m$. n is a nontrivial natural number and $n < m$. n is inductively smaller than m. n has a prime divisor. □

23 The Greatest Common Divisor

Let m, n denote integers.

Signature 224. The greatest common divisor of m and n is a natural number.

Axiom 225. The greatest common divisor of m and n is a divisor of m and a divisor of n.

Axiom 226. Let d be a divisor of m and a divisor of n. Then d is a divisor of the greatest common divisor of m and n.

Lemma 227. Let z be an integer. z is the greatest common divisor of z and 0 or $-z$ is the greatest common divisor of z and 0.

Proof. Let d be the greatest common divisor of z and 0.

Case z is a natural number. z is a common divisor of z and 0. Then d divides z. z divides d. Thus $z = d$. End.

Case z is not a natural number. Then $-z$ is a natural number and $-z$ is

the greatest common divisor of $-z$ and 0. $-z$ is a common divisor of z and 0. Then $-z$ divides d and d divides $-z$. $d = -z$. End. □

Lemma 228. Let n, m be integers. The greatest common divisor of n and m is equal to the greatest common divisor of m and n.

Proof. Let d be the greatest common divisor of n and m. Let δ be the greatest common divisor of m and n. d is a common divisor of m and n. Thus d divides δ. δ is a common divisor of n and m. Thus δ divides d. $\delta = d$. □

Lemma 229. Let n be a natural number. n is the greatest common divisor of n and n.

Proof. n is a common divisor of n and n. Let d be the greatest common divisor of n and n. Then d divides n. n divides d. $d = n$. □

24 Greatest Common Divisor Algorithm (#69)

Let m, n denote natural numbers.

Proposition 230. Let m, n be natural numbers such that $m > n$. Let d be a divisor of m and a divisor of n such that $d > 0$. Then d is a divisor of $m - n$.

Proof. Take natural numbers u, v such that $m = d \cdot u$ and $n = d \cdot v$. Then $u \cdot d > v \cdot d$. Therefore $(u \cdot d) \cdot 1/d > (v \cdot d) \cdot 1/d$ and $u \cdot (d \cdot 1/d) > v \cdot (d \cdot 1/d)$. Thus $u > v$. Then $m - n = (d \cdot u) - (d \cdot v) = d \cdot (u - v)$. □

Proposition 231. Let m, n be natural numbers such that $m > n$. Let d be a divisor of $m-n$ and a divisor of n such that $d > 0$. Then d is a divisor of m.

Proof. Let k be $m - n$. k is a natural number. Take natural numbers u, v such that $k = d \cdot u$ and $n = d \cdot v$. Then $m = k+n = (d \cdot u)+(d \cdot v) = d \cdot (u+v)$. □

Lemma 232. Let m, n be natural numbers such that $m > n$. Then the greatest common divisor of m and n is the greatest common divisor of $m-n$ and n.

Proof. Case n=0. Trivial.

Case n ¿ 0. Take the greatest common divisor l of m and n and the greatest common divisor k of $m - n$ and n. 0 not divides n. Then $l > 0$ and $k > 0$.[timelimit 50] l is a divisor of $m - n$. k is a divisor of m. [timelimit 3] Hence l is a divisor of k and k is a divisor of l. Therefore $k = l$. End. □

Proposition 233. Let m, n be natural numbers such that $m < n$. Then

the greatest common divisor of m and n is the greatest common divisor of $n - m$ and m.

Signature 234. $\gcd(m, n)$ is a natural number.

Axiom 235. $\gcd(m, n) = \gcd(n, m)$.

Axiom 236. If $m = 0$ and n is a natural number then $\gcd(m, n) = n$.

Axiom 237. If $m > n$ then $\gcd(m, n) = \gcd(m - n, n)$.

Axiom 238. If $m < n$ then $\gcd(m, n) = \gcd(m, n - m)$.

Axiom 239. If $m = n$ then $\gcd(m, n) = \gcd(m - n, n)$.

Proposition 240. For all natural numbers m, n the greatest common divisor of m and n is $\gcd(m, n)$.

Proof by induction on $m + n$. Let m, n be natural numbers. Then $m + n$ is a natural number.

Case $m + n = 0$. Trivial.

Case $m + n > 0$. If $m = 0$ or $n = 0$ then $\gcd(m, n)$ is the greatest common divisor of m and n. Assume $m \neq 0$ and $n \neq 0$.[timelimit 20] If $m \leq n$ then $m+(n-m)$ is inductively smaller than $m+n$ and $\gcd(m, n) = \gcd(m, n-m)$ and the greatest common divisor of m and n is the greatest common divisor of m and $n - m$ and the greatest common divisor of m and n is $\gcd(m, n)$. [timelimit 3] If $m > n$ then $(m - n) + n$ is inductively smaller than $m + n$ and $\gcd(m, n) = \gcd(m - n, n)$ and the greatest common divisor of m and n is the greatest common divisor of $m - n$ and n. End. □

25 Bezout's Identity (#60)

Lemma 241. Let s, t be real numbers such that $s < t$. Then there exists a real number r such that $s < r < t$.

Proof. $\frac{s+t}{2}$ is a real number. [timelimit 30] $s + s < s + t$. $\frac{s+s}{2} < \frac{s+t}{2}$. $s = \frac{2}{2} \cdot s = \frac{2 \cdot s}{2} = \frac{s+s}{2} < \frac{s+t}{2}$. $s + t < t + t$ and $\frac{s+t}{2} < \frac{t+t}{2}$. $\frac{s+t}{2} < \frac{t+t}{2} = \frac{2 \cdot t}{2} = \frac{2}{2} \cdot t = t$. [timelimit 3] $s < \frac{s+t}{2} < t$. □

Let m, n denote integers.

Proposition 242. Let a be nonzero natural number. For every natural number m there exist a natural number k such that $0 \leq m - (k \cdot a) < a$.

Proof by induction on m. Let m be a natural number.

Case $m = 0$. $0 \leq 0 - (0 \cdot a) < a$. End.

Case $m > 0$. Let $\mu = m - 1$. μ is a natural number and μ is inductively smaller than m. Take a natural number k such that $0 \leq \mu - (k \cdot a) < a$. Then $\mu < m$ and $0 \leq \mu - (k \cdot a) < a$.

Let us show that $m-(k\cdot a)=a$ or $m-(k\cdot a)<a$. Assume the contrary. Let $b=m-(k\cdot a)$ and $c=(m-1)-(k\cdot a)$. $(m-1)-(k\cdot a)<a$. If $\neg b=a$ and $\neg b<a$ then $b>a$. Then $m-(k\cdot a)>a$. $(m-(k\cdot a))-1>a-1$. $(-1)+(m-(k\cdot a))>a-1$. $((-1)+m)-(k\cdot a)>a-1$. $(m-1)-(k\cdot a)>a-1$. $c>a-1$. Then $c\geq a$. Contradiction. End.

Case $m-(k\cdot a)=a$. k is a natural number. $0=a+(-a)=(m+(-(k\cdot a)))+(-a)=m+(-(k\cdot a)+(-a))=m+(-(k\cdot a)+((-1)\cdot a))=m+(((-k)\cdot a)+((-1)\cdot a))=m+(((-k)+(-1))\cdot a)=m+((-k-1)\cdot a)=m-(-(-k-1)\cdot a)$. $0\leq m-(-(-k-1)\cdot a)<a$. $-(-k-1)$ is a natural number. Indeed k is a natural number and $0>((-k)+(-1))=(-k-1)$. Then there exist a natural number l such that $0\leq m-(-(-k-1)\cdot a)<a$. End.

Case $m-(k\cdot a)<a$. Let $\nu=-(k\cdot a)$. $0\leq\mu+\nu<m+\nu$. $0\leq m-(k\cdot a)$. Then k is a natural number such that $0\leq m-(k\cdot a)<a$. End. End. □

Lemma 243 (lemma Bezout). Let a be nonzero natural number and m be an integer. Then there exists an integer k such that $0\leq m-(k\cdot a)<a$.

Proof. Case m is a natural number. Then there exists a natural number k such that $0\leq m-(k\cdot a)<a$. End.

Case m is not a natural number. Let $\mu=-m$. Then μ is a natural number. Take a natural number k such that $0\leq\mu-(k\cdot a)<a$. Let $\kappa=-k$. κ is an integer and $0\leq m-(\kappa\cdot a)<a$. End. □

Theorem 244 (Bezout). Let a,b be integers and δ be the greatest common divisor of a and b. Then there exist integer x and integer y such that $\delta=(a\cdot x)+(b\cdot y)$.

Proof. Case $a=0$. The greatest common divisor of b and a is equal to δ. Then $\delta=b$ or $\delta=-b$. 1 and -1 are integers. If $\delta=b$ then $\delta=(a\cdot 1)+(b\cdot 1)$. If $\delta=-b$ then $\delta=(a\cdot 1)+(b\cdot -1)$. End.

Case $b=0$. Then $\delta=a$ or $\delta=-a$. 1 and -1 are integers. If $\delta=a$ then $\delta=(a\cdot 1)+(b\cdot 1)$. If $\delta=-a$ then $\delta=(a\cdot -1)+(b\cdot 1)$. End.

Case $a\neq 0$ and $b\neq 0$. 0 not divides a. Thus $\delta\neq 0$. Define $S=\{(a\cdot e)+(b\cdot f)\mid e,f \text{ are integers and } (a\cdot e)+(b\cdot f)>0\}$. $a>0$ or $-a>0$. $((a\cdot 1)+(b\cdot 0))>0$ or $(a\cdot -1)+(b\cdot 0)>0$. If $((a\cdot 1)+(b\cdot 0))>0$ then $((a\cdot 1)+(b\cdot 0))\in S$. $((a\cdot 1)+(b\cdot 0))\in S$ or $(a\cdot -1)+(b\cdot 0)\in S$. S is nonempty.

Let us show that $S\subseteq\mathbb{N}$. Indeed we can show that for all $s\in S$ $s\in\mathbb{N}$. Let $s\in S$. Take integers e,f such that $s=(a\cdot e)+(b\cdot f)$. $a\cdot e\in\mathbb{Z}$ and $b\cdot f\in\mathbb{Z}$. Thus s is an integer. $s>0$. End.

S has an infimum. Take $d\in S$ such that d is the infimum of S. Take integers e,f such that $d=(a\cdot e)+(b\cdot f)$.

Let us show that d divides a. d is a nonzero natural number and a is

an integers. Take an integer k such that $0 \leq a - (k \cdot d) < d$ (by lemma Bezout). Take $r = a - (k \cdot d)$. $r = a - (k \cdot d) = a - (k \cdot ((a \cdot e) + (b \cdot f))) = a - ((k \cdot (a \cdot e)) + (k \cdot (b \cdot f))) = a + (-(k \cdot (a \cdot e)) - (k \cdot (b \cdot f)))$. Let $\phi = (-k \cdot e)$ and $\psi = (-k \cdot f)$. $-(k \cdot (a \cdot e)) = -(a \cdot (k \cdot e)) = a \cdot (-k \cdot e) = a \cdot \phi$. $-(k \cdot (b \cdot f)) = -(b \cdot (k \cdot f)) = b \cdot (-k \cdot f) = b \cdot \psi$. $r = (a + (a \cdot \phi)) + (b \cdot \psi)$. [timelimit 10] $(a + (a \cdot \phi)) + (b \cdot \psi) = (a \cdot (1 + \phi)) + (b \cdot \psi)$. [timelimit 3] $(1 + \phi)$ and ψ are integers. Thus $r \in S$ or $r = 0$. $0 \leq r < d$ and d is the infimum of S. Thus $r = 0$. $k \cdot d = a$. Therefore d divides a. End.

Let us show that d divides b. d is a nonzero natural number and b is an integers. Take an integer k such that $0 \leq b - (k \cdot d) < d$ (by lemma Bezout). Take $r = b - (k \cdot d)$. $r = b - (k \cdot d) = b - (k \cdot ((a \cdot e) + (b \cdot f))) = b - ((k \cdot (a \cdot e)) + (k \cdot (b \cdot f))) = b + (-(k \cdot (a \cdot e)) - (k \cdot (b \cdot f)))$. Let $\phi = (-k \cdot e)$ and $\psi = (-k \cdot f)$. $-(k \cdot (a \cdot e)) = -(a \cdot (k \cdot e)) = a \cdot (-k \cdot e) = a \cdot \phi$. $-(k \cdot (b \cdot f)) = -(b \cdot (k \cdot f)) = b \cdot (-k \cdot f) = b \cdot \psi$. $r = (b + (a \cdot \phi)) + (b \cdot \psi)$. [timelimit 10] $(b + (a \cdot \phi)) + (b \cdot \psi) = (a \cdot \phi) + (b + (b \cdot \psi)) = (a \cdot \phi) + (b \cdot (1 + \psi))$. [timelimit 3] ϕ and $(1 + \psi)$ are integers. Thus $r \in S$ or $r = 0$. $0 \leq r < d$ and d is the infimum of S. Thus $r = 0$. $k \cdot d = b$. Therefore d divides b. End.

d is a common divisor of a and b and a natural number.

Let us show that d is the greatest common divisor of a and b. Let c be the greatest common divisor of a and b. Take integers u, v such that $a = c \cdot u$ and $b = c \cdot v$. $d = (a \cdot e) + (b \cdot f) = ((c \cdot u) \cdot e) + ((c \cdot v) \cdot f) = (c \cdot (u \cdot e)) + (c \cdot (v \cdot f)) = c \cdot ((u \cdot e) + (v \cdot f))$. $((u \cdot e) + (v \cdot f))$ is an integer. c is a divisor of d and d is a divisor of c. Thus $d = c$. End.

Therefore $d = \delta$ and there exist integers i, j such that $\delta = (a \cdot i) + (b \cdot j)$. End. □

26 Irrationality of Roots of Prime Numbers (#1)

Let m, n denote natural numbers.

Lemma 245. The greatest common divisor of n and m is 0 iff $n = 0$ and $m = 0$.

Proof. Let us show that the greatest common divisor of 0 and 0 is 0. Assume the contrary. Let d be the greatest common divisor of 0 and 0. 0 is a divisor of 0 and 0 is not a divisor of d. Contradiction. End.

Let us show that if the greatest common divisor of n and m is 0 then $n = 0$ and $m = 0$. If $n \neq 0$ then 0 is not a divisor of n. If $m \neq 0$ then 0 is not a divisor of m. End. □

Let a prime number stand for a prime natural number.

Let p denote a prime number. Let n, m denote natural numbers. Let q

denote a rational number.

Definition 246. n and m are coprime iff n and m have no common prime divisor.

Lemma 247. If q is positive then there exist coprime natural numbers m, n such that $m \cdot q = n$.

Proof. Let q be positive.

Let us show that there exists a natural number a and nonzero natural number b such that $q = \frac{a}{b}$. Take an integer a and a nonzero integer b such that $q = \frac{a}{b}$.

Case $a = 0$ or a, b are natural numbers. Trivial.

Case ($a < 0$ and $b > 0$) or ($a > 0$ and $b < 0$). Then $\frac{a}{b} < 0$ and $q \geq 0$. Contradiction. End.

Case $a < 0$ and $b < 0$. Then $-a, -b \in \mathbb{N}$ and $q = \frac{-a}{-b}$. End. End. Take a natural number a and a nontrivial natural number b such that $q = \frac{a}{b}$.

Take the greatest common divisor d of a and b. b is nontrivial. Thus 0 not divides b and d is a nonzero natural number. Take $n = \frac{a}{d}$ and $m = \frac{b}{d}$. n, m are natural numbers.

Let us show that n, m are coprime.

Assume the contrary. The greatest common divisor of n and m is not 1. Take the greatest common divisor δ of n and m. Take $p = d \cdot \delta$, $\nu = \frac{n}{\delta}$ and $\mu = \frac{m}{\delta}$. p, ν, μ are natural numbers. $\nu \cdot p = \frac{n}{\delta} \cdot (\delta \cdot d) = n \cdot d = \frac{a}{d} \cdot d = a$ and $\mu \cdot p = \frac{m}{\delta} \cdot (\delta \cdot d) = m \cdot d = \frac{b}{d} \cdot d = b$. Thus p divides a and p divides b. $\delta \neq 1$. Therefore$p$ not divides d and d is not the greatest common divisor of a and b. Contradiction. End.

$q = \frac{n}{m}$ and $m \cdot q = n$. □

[timelimit 30]

Lemma 248. If p divides n^2 then p divides n.

Proof. Assume p divides n^2 and p not divides n. Thus the greatest common divisor of p and n is 1. Take integers s, t such that $(p \cdot s) + (n \cdot t) = 1$. $n = n \cdot 1 = n \cdot ((p \cdot s) + (n \cdot t)) = (n \cdot (p \cdot s)) + (n \cdot (n \cdot t))$. $n \cdot (p \cdot s), n \cdot (n \cdot t)$ are integers. p divides $n \cdot (p \cdot s)$. p divides $n \cdot (n \cdot t)$. Thus p divides $(n \cdot (p \cdot s)) + (n \cdot (n \cdot t))$ and p divides n. Contradiction. □

Theorem 249 (Pythagoras). $q^2 = p$ for no positive rational number q.

Proof by contradiction. Assume the contrary. Take a positive rational number q such that $p = q^2$. Take coprime natural numbers m, n such that $m \cdot q = n$. Then $(m \cdot q) \cdot (m \cdot q) = n^2$. Then $p \cdot m^2 = n^2$. Therefore p divides n. Take a natural number k such that $n = k \cdot p$. Then $p \cdot m^2 = p \cdot (k \cdot n)$.

Therefore $m^2 = k \cdot n$. Therefore m^2 is equal to $p \cdot k^2$. Hence p divides m. Contradiction. □

[timelimit 3]

27 Finite and Infinite Sets

Let m, n, k denote natural numbers.

Definition 250. $\{m, \ldots, n\}$ is the class of natural numbers i such that $m \leq i \leq n$.

Lemma 251. $\{m, \ldots, n\}$ is a set.

Proof. $\{m, \ldots, n\}$ is a subclass of $\mathbb{N}$. □

[timelimit 10]

Lemma 252. Assume that $m \leq n \leq k$. Then $\{m, \ldots, n\} \cup \{n+1, \ldots, k\} = \{m, \ldots, k\}$.

Proof. $\{m, \ldots, k\} \subseteq \{m, \ldots, n\} \cup \{n+1, \ldots, k\}$. Proof. Let $x \in \{m, \ldots, k\}$. x is an integer. $x \leq n$ or $n + 1 \leq x$. Proof. Assume the contrary. Then $n < x < n + 1$. $0 < x - n < 1$. End. $x \in \{m, \ldots, n\}$ or $x \in \{n + 1, \ldots, k\}$. End. □

Lemma 253. Assume that $m \leq n \leq k$. Then $\{m, \ldots, n\}$ and $\{n+1, \ldots, k\}$ are disjoint.

Lemma 254. Let $x \in \{1, \ldots, n + 1\} \setminus \{1, \ldots, n\}$. Then $x = n + 1$.

Proof. x is an integer. $x \leq n + 1$. $\neg x \leq n$. Assume that $x \neq n + 1$. $n < x < n + 1$. $0 < x - n < 1$. □

[timelimit 3] Let S denote a class.

Definition 255. S is finite iff S and $\{1, \ldots, n\}$ are equinumerous for some natural number n.

Lemma 256. Let S be finite. Then S is a set.

Proof. Take a natural number n such that S and $\{1, \ldots, n\}$ are equinumerous. Take a bijection f between $\{1, \ldots, n\}$ and S. Then $\{1, \ldots, n\}$ is a set and $S = f[\{1, \ldots, n\}]$. □

We show that the number n in the definition is uniquely determined.

Lemma 257. Let f be an injective map. Let S be a set. $f \restriction S$ is an injective map.

Lemma 258. For all natural numbers n for all natural numbers m for all injective maps f from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$ we have $m \leq n$.

Proof by induction on n. Let n be a natural number. Let m be a natural number. Let f be an injective map from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$.

Case $n = 0$. $\{1, \ldots, n\} = \emptyset$. Then $\{1, \ldots, m\} = \emptyset$ and $0 = m \leq n$. Qed.

Case $n \neq 0$. Take a natural number n' such that $n = n' + 1$.

Case $m = 0$. Then $m \leq n$. Trivial.

Case $m \neq 0$. Take a natural number m' such that $m = m' + 1$.

Case $f[\{1, \ldots, m'\}] \subseteq \{1, \ldots, n'\}$.

Take

$$g = f \restriction \{1, \ldots, m'\}.$$

Take $C = \{1, \ldots, m'\}$ and $D = \{1, \ldots, n'\}$. $f \restriction \{1, \ldots, m'\}$ is an injective map. $\mathrm{dom}(f \restriction \{1, \ldots, m'\}) = \{1, \ldots, m'\}$. $f[\{1, \ldots, m'\}] \subseteq \{1, \ldots, n'\}$. g is a map from C to D.

(1) $f \restriction \{1, \ldots, m'\}$ is an injective map from $\{1, \ldots, m'\}$ to $\{1, \ldots, n'\}$.

n' is inductively smaller than n. [timelimit 10] $m' \leq n'$ and $m \leq n$. Qed. [timelimit 3]

Case $\neg f[\{1, \ldots, m'\}] \subseteq \{1, \ldots, n'\}$.

Take $w \in f[\{1, \ldots, m'\}]$ such that $w \notin \{1, \ldots, n'\}$. $w \in f[\{1, \ldots, m'\}] \subseteq f[\{1, \ldots, m\}] \subseteq \{1, \ldots, n\}$. $w \in \{1, \ldots, n' + 1\} \setminus \{1, \ldots, n'\}$. $w = n$. Take $i \in \{1, \ldots, m'\}$ such that $f(i) = w$. Define

$$h(j) = \begin{cases} f(j) & : j \neq i \\ f(m) & : j = i \end{cases}$$

for $j \in \{1, \ldots, m'\}$. h is a map. $\mathrm{dom}(h) = \{1, \ldots, m'\}$.

(2) h is injective.

Proof. Let j, k be distinct elements of $\{1, \ldots, m'\}$. Let us show that $h(j) \neq h(k)$.

Case $j = i$. Then $k \neq i$. $k \neq m$. [timelimit 10] $h(j) = f(m) \neq f(k) = h(k)$. [timelimit 3] Qed.

Case $k = i$. Then $j \neq i$. $j \neq m$. [timelimit 10] $h(j) = f(j) \neq f(m) = h(k)$. [timelimit 3] Qed. Then $j \neq i$ and $k \neq i$. [timelimit 10] $h(j) = f(j) \neq f(k) = h(k)$. [timelimit 3] Qed. Qed.

(3) $h[\{1, \ldots, m'\}] \subseteq \{1, \ldots, n'\}$.

Proof. Let $j \in \{1, \ldots, m'\}$. $h(j) \in \{1, \ldots, n\}$. Proof. [timelimit 30] $h(j) = f(j) \in \{1, \ldots, n\}$ or $h(j) = f(m) \in \{1, \ldots, n\}$. [timelimit 3] Qed.

Let us show that $h(j) \in \{1, \ldots, n'\}$.

Proof. [timelimit 10] Case $j = i$.

$h(j) = f(m) \neq f(i) = w = n$. Indeed $m \neq i$.

End. [timelimit 3]

Then $j \neq i$. $h(j) = f(j) \neq f(i) = n$. Qed. Qed.

(4) h is an injective map from $\{1, \ldots, m'\}$ to $\{1, \ldots, n'\}$.

n' is inductively smaller than n. Then $m' \leq n'$ and $m \leq n$. Qed. Qed. Qed. □

Lemma 259. Let n, m be natural numbers and $\{1, \ldots, m\} \sim \{1, \ldots, n\}$. Then $m = n$.

Proof. There is an injective map from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$ and there is an injective map from $\{1, \ldots, n\}$ to $\{1, \ldots, m\}$. Then $m \leq n \leq m$. □

Signature 260. Let x be a finite set. $|x|$ is the natural number n such that x and $\{1, \ldots, n\}$ are equinumerous.

Lemma 261. Let x be a finite set. Let x and $\{1, \ldots, n\}$ be equinumerous. Then $|x| = n$.

Proof. $x \sim \{1, \ldots, |x|\}$ and $x \sim \{1, \ldots, n\}$. Thus $\{1, \ldots, |x|\} \sim \{1, \ldots, n\}$. □

Lemma 262. $|\{1, \ldots, n\}| = n$.

Lemma 263. Let n, m, i be natural numbers. Then $\{m, \ldots, n\} \sim \{m + i, \ldots, n + i\}$.

Proof. Define

$$H(k) = k + i$$

for $k \in \{m, \ldots, n\}$. [timelimit 30] H is a map from $\{m, \ldots, n\}$ to $\{m + i, \ldots, n + i\}$. H is injective. H is a surjection from $\{m, \ldots, n\}$ onto $\{m + i, \ldots, n + i\}$. Proof. Let $u \in \{m + i, \ldots, n + i\}$. $m + i \leq u \leq n + i$. $m = (m + i) - i \leq u - i \leq (n + i) - i = n$. Hence $u - i \in \{m, \ldots, n\}$. $H(u - i) = u$ and $u \in H[\{m, \ldots, n\}]$. Qed.[timelimit 3] □

Lemma 264. Let x, y be disjoint finite sets. Then $x \cup y$ is a finite set and $|x \cup y| = |x| + |y|$.

Proof. Take $m = |x|$ and $n = |y|$. $x \sim \{1, \ldots, m\}$. Consider $u = \{1, \ldots, n\}$ and $v = \{m, \ldots, m + n\}$. $y \sim \{1, \ldots, n\} \sim \{1 + m, \ldots, n + m\}$. $y \sim \{m+1, \ldots, m+n\}$.[timelimit 50] $x \cup y \sim \{1, \ldots, m\} \cup \{m+1, \ldots, m+n\} = \{1, \ldots, |x| + |y|\}$. [timelimit 10] $x \cup y \sim \{1, \ldots, |x| + |y|\}$. $|x \cup y| = |x| + |y|$. □

Definition 265. S is infinite iff S is not finite.

Definition 266. S is denumerable iff S and $\mathbb{N}$ are equinumerous.

28 Number of Subsets of a Set (#52)

Lemma 267. Let X be a finite set. $|X| = 0$ iff $X = \emptyset$.

Proof. Let us show that if $|X| = 0$ then $X = \emptyset$. Assume $|X| = 0$ and there exists an $x \in X$. Take $x \in X$ and bijection g between X and $\{1, \ldots, 0\}$. Then $g(x) \in \{1, \ldots, 0\} = \emptyset$. Contradiction. End.

If $X = \emptyset$ then $|X| = 0$. □

Definition 268. Let Y be a nonempty set and $y \in Y$. $\{y\}_Y$ is $\{\nu \in Y \mid \nu = y\}$.

Theorem 269. For all finite sets X and all natural numbers n if $|X| = n$ then $\mathcal{P}(X)$ is finite and $|\mathcal{P}(X)| = 2^n$.

Proof by induction on n. Let X be a finite set and n be a natural number. Assume $|X| = n$.

Case $n = 0$. $\{1, \ldots, 0\} = \emptyset$. Thus $X = \emptyset$. For all $x \in \mathcal{P}(\emptyset)$ $x = \emptyset$. Define $h(x) = 1$ for $x \in \mathcal{P}(\emptyset)$. h is a bijection between $\mathcal{P}(\emptyset)$ and $\{1, \ldots, 1\}$. Hence $|\mathcal{P}(X)| = 1$ and $2^0 = 1$. End.

Case $n \neq 0$. Take a natural number m such that $m = n-1$. m is inductively smaller than n. There exists a bijection between X and $\{1, \ldots, n\}$ and $1 \in \{1, \ldots, n\}$. Thus X is nonempty. Take a bijection g between X and $\{1, \ldots, n\}$. Take $\xi \in X$ such that $g(\xi) = n$.

Define $M = \{x \mid x \in \mathcal{P}(X) \text{ and } \xi \in x\}$. Define $N = \{x \mid x \in \mathcal{P}(X) \text{ and } \xi \notin x\}$. $M \cup N = \mathcal{P}(X)$. M, N are disjoint.

Take $Y = X \setminus \{\xi\}_X$. $Y \subseteq X$. Let us show that Y is finite and $|Y| = m$. Take $f = g \restriction Y$. g is injective. Thus f is injective.

Let us show that $f[Y] \subseteq \{1, \ldots, m\}$. $f[Y] \subseteq \{1, \ldots, n\}$ and $f(\gamma) = n$ for no $\gamma \in Y$. Thus $f[Y] \subseteq \{1, \ldots, m\}$. End.

(2) f is a surjection from Y onto $\{1, \ldots, m\}$. Indeed we can show that every element of $\{1, \ldots, m\}$ is a value of f. Let $y \in \{1, \ldots, m\}$. $\{1, \ldots, m\} \subseteq \{1, \ldots, n\}$. g is a surjection from X onto $\{1, \ldots, n\}$. Take $x \in X$ such that $g(x) = y$. $y \neq n$ and $x \neq \xi$. $x \in Y$ and $f(x) = g(x) = y$. End. QED.

Let us show that M and N are finite and $|\mathcal{P}(Y)| = |M| = |N|$. We can show that there exists a bijection between M and N. Define $f(x) = x \setminus \{\xi\}_X$ for $x \in M$.

We can show that f is injective. Let $x, y \in M$. Assume $f(x) = f(y)$. $\{\xi\}_X \subseteq x$ and $\{\xi\}_X \subseteq y$. $x \setminus \{\xi\}_X = y \setminus \{\xi\}_X$. Thus $x = y$. End.

We can show that $f[M] \subseteq N$. Let $x \in M$ and $y = f(x)$. $y = x \setminus \{\xi\}_X$. $y \subseteq X$ and $\xi \notin y$. Thus $y \in N$. End.

(2) f is a surjection from M onto N. Indeed we can show that every

element of N is a value of f. Let $y \in N$ and $x = y \cup \{\xi\}_X$. $x \subseteq X$ and $\xi \in x$. $x \in M$. $f(x) = (y \cup \{\xi\}_X) \setminus \{\xi\}_X = y \setminus \{\xi\}_X = y$. End. End.

We can show that $\mathcal{P}(Y) \subseteq N$. Let $y \in \mathcal{P}(Y)$. $y \subseteq X$ and $\xi \notin y$. $y \in N$. End.

We can show that $N \subseteq \mathcal{P}(Y)$. Let $y \in N$. $\xi \notin y$. $y \subseteq Y$. $y \in \mathcal{P}(Y)$. End.

$\mathcal{P}(Y) = N$. $\mathcal{P}(Y)$ is finite. N is finite and M is finite. Thus $|\mathcal{P}(Y)| = |N| = |M|$. QED.

$|\mathcal{P}(Y)| = 2^m$. Hence $|M| = |N| = 2^m$. $|M| + |N| = |M \cup N| = |\mathcal{P}(X)|$. Let $w = 2^m$. $|M| + |N| = 2^m + 2^m = (1 \cdot 2^m) + (1 \cdot 2^m) = (1 + 1) \cdot 2^m = 2 \cdot 2^m = 2^{m+1} = 2^n$. Therefore $\mathcal{P}(X)$ is finite and $|\mathcal{P}(X)| = 2^n$. End. □

29 Finite Products

Let n denote a natural number.

Definition 270. A sequence of length n is a function F such that $\mathrm{dom}(F) = \{1, \ldots, n\}$.

Let F_i stand for $F(i)$.

Definition 271. Let F be a sequence of length n. $\{F_1, \ldots, F_n\} = \{F_i | i \in \mathrm{dom}(F)\}$.

Signature 272. 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 273 (Factorproperty). Let F be a sequence of length n such that $F(i)$ is a nonzero natural number for every $i \in \mathrm{dom}(F)$. Then $F_1 \cdots F_n$ is nonzero and $F(i)$ divides $F_1 \cdots F_n$ for every $i \in \mathrm{dom}(F)$.

30 The Infinitude of Primes (#11)

Signature 274. $\mathbb{P}$ is the collection of prime natural numbers.

Theorem 275 (Euclid). $\mathbb{P}$ is infinite.

Proof by contradiction. Assume that $\mathbb{P}$ is finite. Take a natural number r such that $\{1, \ldots, r\}$ and $\mathbb{P}$ are equinumerous. Take a bijection p between $\{1, \ldots, r\}$ and $\mathbb{P}$. p is a sequence of length r and $\mathbb{P} = \{p_1, \ldots, p_r\}$.

(1) p_i is a nonzero natural number for every $i \in \mathrm{dom}(p)$.

Consider $n = p_1 \cdots p_r + 1$. [timelimit 10] $p_1 \cdots p_r$ is nonzero and n is nontrivial. [timelimit 3] Take a prime divisor q of n.

(2) $q \notin \{p_1, \ldots, p_r\}$.

Proof by contradiction. Take a natural number i such that $1 \leq i \leq r$ and $q = p_i$. q is a divisor of n. $i \in \mathrm{dom}(p)$. p_i is a divisor of $p_1 \cdots p_r$ (by Factorproperty, 1). Thus q divides 1. [timelimit 10] Contradiction. qed. [timelimit 3] □

References

[1] Bronisław Knaster. "Un théorème sur les fonctions d'ensembles". In: *Ann. Soc. Polon. Math* 6 (1928), pp. 133–134.

[2] Walter Rudin. *Principles of Mathematical Analysis*. McGraw Hill, 1953.

[3] Bertrand Russell. *The Principles of Mathematics*. Cambridge University Press, 1903.

[4] Bernd S. W. Schröder. "The fixed point property for ordered sets". In: *Arabian Journal of Mathematics* 1 (2012), pp. 529–547.

[5] Alfred Tarski. "A lattice-theoretical fixpoint theorem and its applications". In: *Pacific Journal of Mathematics* 5 (2 1955), pp. 285–309.

[6] *The SAD Proof Checker*. URL: http://nevidal.org/sad.en.html.

[7] Freek Wiedijk. *Formalizing 100 Theorems*. URL: https://www.cs.ru.nl/~freek/100 (visited on 10/14/2023).