Dataset Description: Formalization of Elementary Number Theory in Mizar

Adam Naumowicz

Institute of Informatics
University of Białystok, Poland
adamn@mizar.org

CICM 2020, July 28, 2020

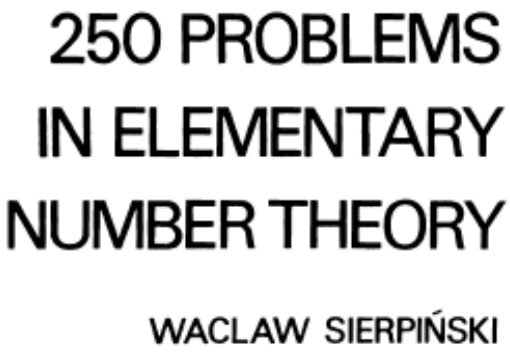
Motivation

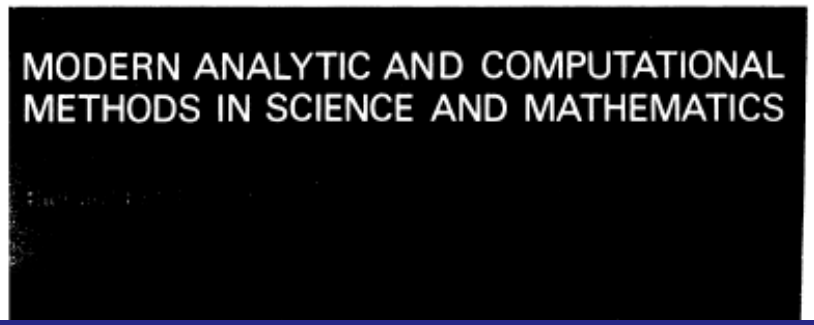
- The centrally maintained library of formalizations developed using MIZAR , the Mizar Mathematical Library (MML), contains over $60,000$ theorems and $12,000$ definitions
- The data is organized into more than $1,300$ files representing *articles* on various topics (as such, the huge and somewhat eclectic library does not appear to be the best resource for introducing the Mizar way of formalizing mathematics to new users or facilitating introductory Mizar-based courses for math students)
- There is a need for developing a set of easy to comprehend Mizar data files which can provide a better starting point for educational activities

About this Dataset

- Our dataset is based on examples from elementary number theory (which has an initially relatively steep learning curve, few prerequisites and provides a great selection of self-contained proofs)
- Number theory proofs very often carry an extra recreational component (such tasks are in line with the educational entertainment approach to learning which helps perceive the formalization as a challenging but rewarding activity)
- We believe that thanks to mastering the elementary techniques and familiarizing with the theory's basic methods one can be prepared to approach the study and/or formalization of further, more advanced problems.

Mathematical Content





Mathematical Content

250 PROBLEMS
IN ELEMENTARY
NUMBER THEORY

by

W. SIERPIŃSKI

Polish Academy of Sciences

AMERICAN ELSEVIER PUBLISHING COMPANY, INC.
NEW YORK

PWN—POLISH SCIENTIFIC PUBLISHERS
WARSZAWA

1970

A Humble Tribute to Sierpinski

- Sierpinski had numerous contributions to many fields of mathematics, but number theory was his first main area of interest
- Sierpinski's prolific and diverse research resulted in over 700 papers and 50 books
- The content of the book covers the following chapters:
  I. Divisibility of Numbers,
  II. Relatively Prime Numbers,
  III. Arithmetic Progressions,
  IV. Prime and Composite Numbers,
  V. Diophantine Equations,
  VI. Miscellanea.

Dataset Basics

- Our initial dataset uses data corresponding to ten first problems from the first chapter
- Unlike other sources used in many Mizar formalization projects this material comprises self-contained and relatively short proofs, so the work on the formalization can easily be split, given necessary formal environment and necessary hints
- They can form a number of similar yet slightly different tasks which can be solved/formalized independently by individuals or in groups

Dataset Organization

- The data is located in directories: nump001 – nump010 corresponding to ten initial problems from Sierpinski's book
- Each directory contains subdirectories with:
  - a bare statement (`statement/numpOXYt.miz`)
  - a proof sketch (`sketch/numpOXYs.miz`)
  - a full proof (`proof/numpOXYp.miz`)

  and an extra file `references` (extracted theorems and schemes) to consult before attempting the proof
- Each `*.miz` file contains its environment
- The sketches are proof skeletons which, apart from the problem statement, contain a working proof structure which can be filled in as is, or modified by hand within the restriction of a given environment
- Proof sketches have all references removed (including references to local labels, but the labels are left in the source)
- Moreover, `then` linking is preserved to keep the proof flow resembling the informal original

Formalization Tips

- In some cases, following Sierpinski's proofs directly requires introducing a few lemmas (not readily available in the current MML) in order not to complicate the proof itself
- Users may find it useful to try the `::$V-` and `::$V+` pragmas to skip proof checking over certain parts of the file
- The proof sketches could also be fed into ATP-based MizAR automation within the Emacs mode to automate proof search
- The source files can be HTML-ized once they get processed by the Mizar verifier

Problem Encoding in Mizar

6. Prove the theorem, due to Kraïtchik, asserting that $13|2^{70}+3^{70}$.

```
:: Problem 6 (due to Kraitchik)
theorem
  13 divides 2|^70 + 3|^70;
```

Problem Encoding in MIZAR - Style Variation

3. Prove that there exists infinitely many positive integers n such that $4n^2 + 1$ is divisible both by 5 and 13.

```
:: Problem 3
theorem
  {n where n is positive Integer:
  5 divides 4*(n|^2) + 1 & 13 divides 4*(n|^2) + 1} is
       infinite;
```

Problem Encoding in MIZAR - Some Issues

9. Prove that for every positive integer n the number $3(1^5 + 2^5 + ... + n^5)$ is divisible by $1^3 + 2^3 + ... + n^3$.

```
:: Problem 9
  for s1,s2 being XFinSequence of NAT, n being Nat st
  (len s1=n+1 & for i being Nat st i in dom s1 holds
      s1.i=i|^5) &
  (len s2=n+1 & for i being Nat st i in dom s2 holds
      s2.i=i|^3)
  holds Sum s2 divides 3*Sum s1;
```

Things to note:

- Mizar rendering employs 0-based finite sequences to represent the ellipses available in traditional mathematics,
- This encoding is slightly more general than the original statement, because it also covers the trivial case of $n = 0$ (so n does not have to be strictly positive) since 0^3 divides 0^5 according to the definition of the reflexive 'divides' predicate

First problem – statement

1. Find all positive integers n such that n^2+1 is divisible by $n+1$.

```
:: Problem 1
theorem
  for n being positive Integer holds n+1 divides n^2 + 1 iff
       n = 1;
```

First problem – statement with environment

```
environ
 vocabularies ARYTM_3, XXREAL_0, INT_1, SQUARE_1;
 notations XCMPLX_0, XXREAL_0, INT_1, SQUARE_1;
 constructors SQUARE_1, SERIES_1;
 registrations ORDINAL1, XREAL_0, INT_1, PYTHTRIP;
 requirements REAL, NUMERALS, SUBSET;

begin :: Problem 1
theorem
  for n being positive Integer holds n+1 divides n^2 + 1 iff
       n = 1;
```

First problem – proof sketch

```
environ
 vocabularies CARD_1, ARYTM_1, ARYTM_3, XXREAL_0, RELAT_1, INT_1, SQUARE_1;
 notations NUMBERS, XCMPLX_0, XXREAL_0, INT_1, SQUARE_1;
 constructors SQUARE_1, SERIES_1;
 registrations ORDINAL1, XREAL_0, NAT_1, INT_1, PYTHTRIP;
 requirements REAL, NUMERALS, SUBSET, ARITHM;
 equalities SQUARE_1;
 theorems INT_1, INT_2, INT_5, XREAL_1, XXREAL_0;

begin :: Problem 1
theorem
  for n being positive Integer holds n+1 divides n^2 + 1 iff n = 1;
  proof
    let n be positive Integer;
    thus n+1 divides n^2 + 1 implies n = 1
    proof
      assume n+1 divides n^2 + 1;
      then A1: n+1 divides n*(n+1)-(n-1);
      n+1 divides n*(n+1);
      then A2: n+1 divides n-1;
      assume A3: n<>1;
      n >= 0+1;
      then n > 1;
      then n-1 > 1-1;
      then n+1 <= n-1;
      then n+1-n <= n-1-n;
      hence contradiction;
    end;
    assume n=1;
    hence n+1 divides n^2 + 1;
  end;
```

First problem – complete proof

```
environ
 vocabularies CARD_1, ARYTM_1, ARYTM_3, XXREAL_0, RELAT_1, INT_1, SQUARE_1;
 notations NUMBERS, XCMPLX_0, XXREAL_0, INT_1, SQUARE_1;
 constructors SQUARE_1, SERIES_1;
 registrations ORDINAL1, XREAL_0, NAT_1, INT_1, PYTHTRIP;
 requirements REAL, NUMERALS, SUBSET, ARITHM;
 equalities SQUARE_1;
 theorems INT_1, INT_2, INT_5, XREAL_1, XXREAL_0;

begin :: Problem 1
theorem
  for n being positive Integer holds n+1 divides n^2 + 1 iff n = 1;
  proof
    let n be positive Integer;
    thus n+1 divides n^2 + 1 implies n = 1
    proof
      assume n+1 divides n^2 + 1;
      then A1: n+1 divides n*(n+1)-(n-1);
      n+1 divides n*(n+1) by INT_1:def 3;
      then A2: n+1 divides n-1 by A1,INT_5:2;
      assume A3: n<>1;
      n >= 0+1 by INT_1:7;
      then n > 1 by A3,XXREAL_0:1;
      then n-1 > 1-1 by XREAL_1:9;
      then n+1 <= n-1 by A2,INT_2:27;
      then n+1-n <= n-1-n by XREAL_1:9;
      hence contradiction;
    end;
    assume n=1;
    hence n+1 divides n^2 + 1;
  end;
```

Characteristics of Dataset Problems

Problem #	Size (in lines)	References extracted	Lemmas required	Schemes used	Other comments
1	39	6	-	-	-
2	105	10	2	-	-
3	80	17	-	Infinite sequence existence	- -
4	58	14	-	-	-
5	77	30	-	-	Fermat's little theorem
6	54	19	-	-	Fermat's little theorem (due to Kraichik)
7	93	27	-	-	Fermat's little theorem
8	163	31	2	Induction	0-based finite sequences
9	69	12	-	Infinite sequence existence	0-based finite sequences
10	159	32	2	-	1-based finite sequences

Accessing the Dataset

- The dataset is available for download as a compressed `number.zip` archive from `http://mizar.uwb.edu.pl/~softadm/number/`
- All the files are compatible with the current official Mizar ver. 8.1.09 bundled with MML ver. 5.57.1355
- The underlying Mizar article is now also available in the MML as article NUMBER01

Conclusion and Future Work

The described dataset was created to serve the following main purposes:

- facilitating theorem proving education (including self-education),
- promoting proof methodology based on gap filing proof development/refinement,
- providing simple data for proof exchange and comparison of different formalization environments and frameworks, and
- being a starting point for further, more advanced number theory developments

There are several ways we can make this dataset grow and become more generally useful:

- continue completing the proofs from the divisibility of numbers chapter,
- start the formalization work (in parallel) on other chapters, or
- formulate a number of next theorems in each chapter to boost development by others/students