Formalizing Divisibility Rules as a Student Case Study

Adam Naumowicz

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

Abstract. We would like to present some results of a student case study administered as a part of an interactive theorem proving elective course for computer science students. The students' task was to prove in Mizar the divisibility rules for selected primes based on the decimal representation of natural numbers. The formalized proofs were quite elementary, so a project like this could be carried out by a group of students without particularly strong mathematical background. In this paper we give a short overview of definitions that had to be introduced for the case study and present the way the divisibility rules were eventually formulated by the students. After that we discuss an example of a more interesting proof case, i.e. the divisibility by 11 rule.

1 Introduction

The initial motivation for formalizing in Mizar the divisibility rules for selected primes stemmed from the fact that the well-known divisibility rule for the number three appeared on the "Formalizing 100 Theorems" list[1]. Despite the fact that this theorem is elementary, it had not been available in the Mizar Mathematical Library (MML). Therefore, we decided to formalize that particular divisibility rule and also build a general formal framework of concepts to enable expressing other similar properties. To this end we first proved that every natural number can be uniquely represented as a base-b numeral, for arbitrary b. As the immediate application, we proved divisibility criteria in the base-10 numeral system for initial prime numbers in the NUMERAL1 article [2]. This formed the basis of formalization projects for a group of computer science students at the University of Bialystok. The results of the work can be found in the NUMERAL2 article [3], which extends MML with the formalizations of the divisibility criteria for next prime numbers up to 101.

2 Background Notions

The basic notions that the students could use in their formalization concerned the unique representation of natural numbers in a positional numeral system

[1] The divisibility by three rule is listed as item no. 85. The complete list maintained by Freek Wiedijk is available at http://www.cs.ru.nl/F.Wiedijk/100.

with an arbitrary base. The binary representation of integers (more appropriate for various computer science applications) had previously been developed in the ARITHM series of Mizar articles [4]. For the current task, we needed to focus on a more general representation allowing to utilize decimal digits commonly used in elementary mathematics. The formalization presented to the students was based on the proof by Sierpinski [6]. Given a sequence of natural numbers (d, treated as digits) and a value b denoting a base of the positional system, we introduced the Mizar functor $value(d, b)$ as follows:

```
definition
  let d be XFinSequence of NAT;
  let b be Nat;
  func value(d,b) -> Nat means
  ex d1 being XFinSequence of NAT st (dom d1 = dom d &
  for i being Nat st i in dom d1 holds
   d1.i = (d.i)*(b|^i)) & it = Sum d1;
end;
```

Considerably more difficult it is to define the next definition which asserts that any natural number can be represented using an arbitrary base.

```
definition
  let n,b be Nat;
  assume b>1;
  func digits(n,b) -> XFinSequence of NAT means
     value(it,b)=n & it.(len (it)-1) <> 0 &
     for i being Nat st i in dom it holds
      0 <= it.i & it.i < b if n <> 0 otherwise it = <%0%>;
end;
```

The proof of its existence requires a rather simple inductive proof. Its uniqueness, however, is more involved. Its proof takes over 1000 lines of Mizar code and forms the main part of the NUMERAL1 article. These definitions allowed to express the divisibility by three rule:

```
theorem
  for n being Nat holds 3 divides n iff 3 divides Sum digits(n,10);
```

2.1 More Divisibility Rules

With the formal apparatus working as expected, the students could formalize more examples of divisibility rules. Some of them are well-known from the school curriculum, others are less known, but equally simple. For example Wikipedia lists rules for numbers (not only primes) up to 20 and for some other selected numbers not exceeding 1000. The paper [1] appeared to be an even more complete source – the author provided a listing of unified divisibility rules for the complete list of 1000 first prime numbers based on the observation that if p is an integer not divisible by 2 or by 5, then p divides an arbitrary integer n if it divides

$$n' = (n - n \bmod 10)/10 - (f - A \times p) \times (n \bmod 10) =$$

$$(n - p \times (k - 10 \times A) \times (n \bmod 10))/10,$$

where $f = ((p \times k) - 1)/10$, A is any integer (positive, negative, or 0), and for $p > 0$, $k = [3 \times (p \bmod 10) - 2] \bmod 16$.

Various values of the A parameter can be used to customize the rules. Assuming $A = 0$, the Mizar formalization of this observation for any base b can be expressed by this theorem:

```
theorem
  for p being prime Nat, n,f,b being Nat st
  (ex k being Nat st b*f + 1 = p*k)
  & b > 1 &  p,b are_coprime holds p divides n iff p divides
  value(mid(digits(n,b),2,len(digits(n,b))),b) - f*digits(n,b).0;
```

As an example of how a particular divisibility rule was stated, we show below the rule instantiated for seven:

```
theorem
  7 divides n iff 7 divides
  value(mid(digits(n,10),2,len(digits(n,10))),10)-2*digits(n,10).0;
```

The *mid* function used above simpy forms a subsequence of a given sequence by specifying the first and last index. One can observe that given the above pattern, the formalization of consecutive divisibility rules becomes rather simple and schematic. If there was a proof that a given number is prime, it would be possible to easily follow the same steps and state a rule as given in [1]. However, producing all the proofs for the complete list of 1000 first prime numbers would have a very limited practical value. This is why we decided to restrict ourselves to the prime numbers up to 101 and re-use the lemmas already formalized in the Mizar library thanks to the article NAT_4 [5] which established the primality of many numbers. The proofs for the missing prime numbers within the assumed range were developed with ease by the students in an almost automatic fashion.

2.2 The Divisibility Rule for 11

Apart from the facts that followed the very same pattern, a slightly more challenging task was to formalize a well-known and mathematically elegant divisibility rule for eleven which is based on the alternating sum of the digits of a given number. To be able to state the fact we had to prove first that the summation of digits can be achieved with a needed permutation of the digits:

```
theorem
  for F being XFinSequence
  for X,Y being set st X misses Y
  ex P being Permutation of dom SubXFinS(F,X\/Y) st
  SubXFinS(F,X\/Y) * P = SubXFinS(F,X) ^ SubXFinS(F,Y);
```

The value of the summation should not depend on the way we group the digits. The use of the $SubXFinS$ function allows to create subsequences made of elements which do not have to be consecutive in the original sequence. The next step was to prove that the consecutive natural numbers which are indices of the representing digits contribute either an even number, or an odd number. This allowed to finally formulate the divisibility rule for 11, i.e. that it is enough to consider the difference between the sums of digits in the decimal representation that correspond to even and odd positions, respectively:

```
theorem
11 divides n iff 11 divides
Sum SubXFinS(digits(n,10),EvenNAT)-Sum SubXFinS(digits(n,10),OddNAT);
```

3 Conclusion

We reported on the Mizar formalization of an example of elementary mathematics which was achieved in a student classroom context. The concepts developed and general theorems proved for this development can be useful for further Mizar formalizations, not necessarily related to divisibility rules as such. The formalized proofs were quite elementary (plain natural reasoning or involving simple inductive argument), so a project like this could be carried out successfully by any group of students with some mathematical background. On the other hand, the formalization adds to the didactic utility of the Mizar Mathematical Library, because for the library to be widely used for educational purposes it is essential that elementary mathematical facts should either be present in it, or it should be fairly straightforward to formalize them.

References

1. C.C. Briggs, Simple divisibility rules for the 1st 1000 prime numbers, arXiv preprint arXiv:math/0001012, 2000.
2. Adam Naumowicz, On the representation of natural numbers in positional numeral systems, Formalized Mathematics, 14(4), pp. 221-223, 2006, DOI:10.2478/v10037-006-0025-9.
3. Adam Naumowicz and Radosaw Piliszek, More on Divisibility Criteria for Selected Primes, Formalized Mathematics, 21(2), pp. 87-94, 2013, DOI: 10.2478/forma-2013-0010.
4. Takaya Nishiyama and Yasuho Mizuhara, Binary Arithmetics, Formalized Mathematics, 4(1), pp. 83-86, 1993.
5. Marco Riccardi, Pocklington's Theorem and Bertrand's Postulate, Formalized Mathematics, 14(2), pp. 47-52, 2006, DOI: 10.2478/v10037-006-0007-y.
6. Wacław Sierpiski, Elementary Theory of Numbers, PWN, Warsaw, 1964.