FORMALIZED MATHEMATICS
2006, Vol. **14**, No. **1**, Pages 29–36
DOI: 10.2478/v10037-006-0005-0

On the Properties of the Möbius Function

Magdalena Jastrzębska[1]
Institute of Mathematics
University of Białystok
Akademicka 2, 15-267 Białystok, Poland

Adam Grabowski[2]
Institute of Mathematics
University of Białystok
Akademicka 2, 15-267 Białystok, Poland

Summary. We formalized some basic properties of the Möbius function which is defined classically as

$$\mu(n) = \begin{cases} 1, \text{ if } n = 1, \\ 0, \text{ if } p^2|n \text{ for some prime } p, \\ (-1)^r, \text{ if } n = p_1 p_2 \cdots p_r, \text{ where } p_i \text{ are distinct primes.} \end{cases}$$

as e.g., its multiplicativity. To enable smooth reasoning about the sum of this number-theoretic function, we introduced an underlying many-sorted set indexed by the set of natural numbers. Its elements are just values of the Möbius function.

The second part of the paper is devoted to the notion of the radical of number, i.e. the product of its all prime factors.

The formalization (which is very much like the one developed in Isabelle proof assistant connected with Avigad's formal proof of Prime Number Theorem) was done according to the book [13].

MML identifier: `MOEBIUS1`, version: `7.7.01 4.60.940`

The notation and terminology used here are introduced in the following papers: [26], [31], [12], [6], [3], [4], [1], [24], [2], [19], [18], [29], [32], [8], [9], [5], [17], [16], [28], [33], [22], [23], [11], [14], [20], [10], [15], [27], [25], [7], [30], and [21].

[1]This is a part of the author's MSc thesis.

[2]This work has been partially supported by the KBN grant 4 T11C 039 24 and the FP6 IST grant TYPES No. 510996.

ISSN 1426–2630

1. Preliminaries

The scheme *LambdaNATC* deals with an element $\mathcal{A}$ of $\mathbb{N}$, a set $\mathcal{B}$, and a unary functor $\mathcal{F}$ yielding a set, and states that:

> There exists a function f from $\mathbb{N}$ into $\mathcal{B}$ such that $f(0) = \mathcal{A}$ and
> for every non zero natural number x holds $f(x) = \mathcal{F}(x)$

provided the parameters have the following properties:

- $\mathcal{A} \in \mathcal{B}$, and
- For every non zero natural number x holds $\mathcal{F}(x) \in \mathcal{B}$.

One can check that there exists a natural number which is non prime and non zero.

One can prove the following propositions:

(1) For every non zero natural number n such that $n \neq 1$ holds $n \geq 2$.

(2) For all natural numbers k, n, i such that $1 \leq k$ holds $i \in \operatorname{Seg} n$ iff $k \cdot i \in \operatorname{Seg}(k \cdot n)$.

(3) For all natural numbers m, n such that m and n are relative prime holds $m > 0$ or $n > 0$.

(4) For every non prime natural number n such that $n \neq 1$ there exists a prime number p such that $p \mid n$ and $p \neq n$.

(5) For every natural number n such that $n \neq 1$ there exists a prime number p such that $p \mid n$.

(6) For every prime number p and for every non zero natural number n holds $p \mid n$ iff $p\text{-count}(n) > 0$.

(7) $\operatorname{support} \operatorname{PPF}(1) = \emptyset$.

(8) For every prime number p holds $\operatorname{support} \operatorname{PPF}(p) = \{p\}$.

In the sequel m, n are natural numbers.

We now state the proposition

(9) For every prime number p such that $n \neq 0$ and $m \leq p\text{-count}(n)$ holds $p^m \mid n$.

Let us observe that every natural number which is odd is also non zero.

The following propositions are true:

(10) For every natural number a and for every prime number p such that $p^2 \mid a$ holds $p \mid a$.

(11) Let p be a prime natural number and m, n be non zero natural numbers. If m and n are relative prime and $p^2 \mid m \cdot n$, then $p^2 \mid m$ or $p^2 \mid n$.

(12) For every real bag N over $\mathbb{N}$ such that $\operatorname{support} N = \{n\}$ holds $\sum N = N(n)$.

Let us mention that $\operatorname{CFS}(\emptyset)$ is empty.

The following propositions are true:

(13) Let p be a prime number. Suppose $p \mid n$. Then $\{d; d$ ranges over natural numbers: $d > 0 \ \wedge \ d \mid n \ \wedge \ p \mid d\} = \{p \cdot d; d$ ranges over natural numbers: $d > 0 \ \wedge \ d \mid n \div p\}$.

(14) For every non zero natural number n there exists a natural number k such that $\operatorname{support} \mathrm{PPF}(n) \subseteq \operatorname{Seg} k$.

(15) For every non zero natural number n and for every prime number p such that $p \notin \operatorname{support} \mathrm{PPF}(n)$ holds $p\text{-count}(n) = 0$.

(16) Let k be a natural number and n be a non zero natural number. If $\operatorname{support} \mathrm{PPF}(n) \subseteq \operatorname{Seg}(k+1)$ and $\operatorname{support} \mathrm{PPF}(n) \not\subseteq \operatorname{Seg} k$, then $k+1$ is a prime number.

(17) For all non zero natural numbers m, n such that for every prime number p holds $p\text{-count}(m) \leq p\text{-count}(n)$ holds $\operatorname{support} \mathrm{PPF}(m) \subseteq \operatorname{support} \mathrm{PPF}(n)$.

(18) Let k be a natural number and n be a non zero natural number. Suppose $\operatorname{support} \mathrm{PPF}(n) \subseteq \operatorname{Seg}(k+1)$. Then there exists a non zero natural number m and there exists a natural number e such that $\operatorname{support} \mathrm{PPF}(m) \subseteq \operatorname{Seg} k$ and $n = m \cdot (k+1)^e$ and for every prime number p holds if $p \in \operatorname{support} \mathrm{PPF}(m)$, then $p\text{-count}(m) = p\text{-count}(n)$ and if $p \notin \operatorname{support} \mathrm{PPF}(m)$, then $p\text{-count}(m) \leq p\text{-count}(n)$.

(19) For all non zero natural numbers m, n such that for every prime number p holds $p\text{-count}(m) \leq p\text{-count}(n)$ holds $m \mid n$.

2. Squarefree Numbers

Let x be a natural number. We say that x is square-containing if and only if:

(Def. 1) There exists a prime number p such that $p^2 \mid x$.

One can prove the following proposition

(20) Let n be a natural number. Given a non zero natural number p such that $p \neq 1$ and $p^2 \mid n$. Then n is square-containing.

Let x be a natural number. We introduce x is squarefree as an antonym of x is square-containing.

The following propositions are true:

(21) 0 is square-containing.

(22) 1 is squarefree.

(23) Every prime number is squarefree.

Let us observe that every element of $\mathbb{N}$ which is prime is also squarefree.

The subset SCNAT of $\mathbb{N}$ is defined as follows:

(Def. 2) For every natural number n holds $n \in \mathrm{SCNAT}$ iff n is squarefree.

Let us mention that there exists a natural number which is squarefree and there exists a natural number which is square-containing.

One can check that every natural number which is square and non trivial is also square-containing.

We now state several propositions:

(24) If n is squarefree, then for every prime number p holds p-count$(n) \leq 1$.

(25) If $m \cdot n$ is squarefree, then m is squarefree.

(26) If m is squarefree and $n \mid m$, then n is squarefree.

(27) Let p be a prime number and m, d be natural numbers. If m is squarefree and $p \mid m$ and $d \mid m \div p$, then $d \mid m$ and $p \nmid d$.

(28) For every prime number p and for all natural numbers m, d such that $p \mid m$ and $d \mid m$ and $p \nmid d$ holds $d \mid m \div p$.

(29) Let p be a prime number and m be a natural number. Suppose m is squarefree and $p \mid m$. Then $\{d; d \text{ ranges over natural numbers: } 0 < d \wedge d \mid m \wedge p \nmid d\} = \{d; d \text{ ranges over natural numbers: } 0 < d \wedge d \mid m \div p\}$.

3. Möbius Function

Let n be a natural number. The functor $\mu(n)$ yielding a real number is defined by:

(Def. 3)(i) $\mu(n) = 0$ if n is square-containing,

(ii) there exists a non zero natural number n' such that $n' = n$ and $\mu(n) = (-1)^{\text{card support PPF}(n')}$, otherwise.

One can prove the following four propositions:

(30) $\mu(1) = 1$.

(31) $\mu(2) = -1$.

(32) $\mu(3) = -1$.

(33) For every natural number n such that n is squarefree holds $\mu(n) \neq 0$.

Let n be a squarefree natural number. Observe that $\mu(n)$ is non zero.

We now state several propositions:

(34) For every prime number p holds $\mu(p) = -1$.

(35) For all non zero natural numbers m, n such that m and n are relative prime holds $\mu(m \cdot n) = \mu(m) \cdot \mu(n)$.

(36) For every prime number p and for every natural number n such that $1 \leq n$ and $n \cdot p$ is squarefree holds $\mu(n \cdot p) = -\mu(n)$.

(37) For all non zero natural numbers m, n such that m and n are not relative prime holds $\mu(m \cdot n) = 0$.

(38) For every natural number n holds $n \in \text{SCNAT}$ iff $\mu(n) \neq 0$.

4. Natural Divisors

Let n be a natural number. The functor NatDivisors n yields a subset of $\mathbb{N}$ and is defined by:

(Def. 4) NatDivisors $n = \{k; k \text{ ranges over elements of } \mathbb{N}: k \neq 0 \wedge k \mid n\}$.

We now state two propositions:

(39) For all natural numbers n, k holds $k \in$ NatDivisors n iff $0 < k$ and $k \mid n$.

(40) For every non zero natural number n holds NatDivisors $n \subseteq$ Seg n.

Let n be a non zero natural number. Note that NatDivisors n is finite and has non empty elements.

One can prove the following proposition

(41) NatDivisors $1 = \{1\}$.

5. The Sum of Values of Möbius Function

Let X be a set. The functor SMoebius X yielding a many sorted set indexed by $\mathbb{N}$ is defined as follows:

(Def. 5) support SMoebius $X = X \cap$ SCNAT and for every natural number k such that $k \in$ support SMoebius X holds (SMoebius X)$(k) = \mu(k)$.

Let X be a set. One can check that SMoebius X is real-yielding.

Let X be a finite set. Note that SMoebius X is finite-support.

One can prove the following three propositions:

(42) $\sum$ SMoebius NatDivisors $1 = 1$.

(43) For all finite subsets X, Y of $\mathbb{N}$ such that X misses Y holds support SMoebius $X \cup$ support SMoebius $Y =$ support(SMoebius $X +$ SMoebius Y).

(44) For all finite subsets X, Y of $\mathbb{N}$ such that X misses Y holds SMoebius$(X \cup Y) =$ SMoebius $X +$ SMoebius Y.

6. Prime Factors of a Number

Let n be a non zero natural number. The functor PFactors n yields a many sorted set indexed by Prime and is defined by:

(Def. 6) support PFactors $n =$ support PFExp(n) and for every natural number p such that $p \in$ support PFExp(n) holds (PFactors n)$(p) = p$.

Let n be a non zero natural number. Note that PFactors n is finite-support and natural-yielding.

One can prove the following propositions:

(45) PFactors $1 =$ EmptyBag Prime .

(46) For every prime number p holds $\mathrm{PFactors}\, p \cdot \langle p \rangle = \langle p \rangle$.

(47) For every prime number p and for every non zero natural number n holds $\mathrm{PFactors}(p^n) \cdot \langle p \rangle = \langle p \rangle$.

(48) For every prime number p and for every non zero natural number n such that $p\text{-count}(n) = 0$ holds $(\mathrm{PFactors}\, n)(p) = 0$.

(49) For every non zero natural number n and for every prime number p such that $p\text{-count}(n) \neq 0$ holds $(\mathrm{PFactors}\, n)(p) = p$.

(50) For all non zero natural numbers m, n such that m and n are relative prime holds $\mathrm{PFactors}(m \cdot n) = \mathrm{PFactors}\, m + \mathrm{PFactors}\, n$.

(51) Let n be a non zero natural number and A be a finite subset of $\mathbb{N}$. Suppose $A = \{k; k \text{ ranges over elements of } \mathbb{N}\colon\ 0 < k \ \wedge\ k \mid n \ \wedge\ k \text{ is square-containing}\}$. Then $\mathrm{SMoebius}\, A = \mathrm{EmptyBag}\, \mathbb{N}$.

7. The Radical of a Number

Let n be a non zero natural number. The functor $\mathrm{Rad}(n)$ yields a natural number and is defined as follows:

(Def. 7) $\mathrm{Rad}(n) = \prod \mathrm{PFactors}\, n$.

The following proposition is true

(52) For every non zero natural number n holds $\mathrm{Rad}(n) > 0$.

Let n be a non zero natural number. Observe that $\mathrm{Rad}(n)$ is non zero.

One can prove the following propositions:

(53) For every prime number p holds $p = \mathrm{Rad}(p)$.

(54) For every prime number p and for every non zero natural number n holds $\mathrm{Rad}(p^n) = p$.

(55) For every non zero natural number n holds $\mathrm{Rad}(n) \mid n$.

(56) For every prime number p and for every non zero natural number n holds $p \mid n$ iff $p \mid \mathrm{Rad}(n)$.

(57) For every non zero natural number k such that k is squarefree holds $\mathrm{Rad}(k) = k$.

(58) For every non zero natural number n holds $\mathrm{Rad}(n) \leq n$.

(59) For every prime number p and for every non zero natural number n holds $p\text{-count}(\mathrm{Rad}(n)) \leq p\text{-count}(n)$.

(60) For every non zero natural number n holds $\mathrm{Rad}(n) = 1$ iff $n = 1$.

(61) For every prime number p and for every non zero natural number n holds $p\text{-count}(\mathrm{Rad}(n)) \leq 1$.

Let n be a non zero natural number. Note that $\mathrm{Rad}(n)$ is squarefree.

One can prove the following propositions:

(62) For every non zero natural number n holds $\mathrm{Rad}(\mathrm{Rad}(n)) = \mathrm{Rad}(n)$.

(63) Let n be a non zero natural number and p be a prime number. Then $\{k; k \text{ ranges over elements of } \mathbb{N}\colon\ 0 < k \ \wedge\ k \mid \mathrm{Rad}(n) \ \wedge\ p \mid k\} \subseteq \mathrm{Seg}\, n$.

(64) Let n be a non zero natural number and p be a prime number. Then $\{k; k \text{ ranges over elements of } \mathbb{N}\colon\ 0 < k \ \wedge\ k \mid \mathrm{Rad}(n) \ \wedge\ p \nmid k\} \subseteq \mathrm{Seg}\, n$.

(65) For all non zero natural numbers k, n holds $k \mid n$ and k is squarefree iff $k \mid \mathrm{Rad}(n)$.

(66) Let n be a non zero natural number. Then $\{k; k \text{ ranges over natural numbers}\colon\ 0 < k \ \wedge\ k \mid n \ \wedge\ k \text{ is squarefree}\} = \{k; k \text{ ranges over natural numbers}\colon\ 0 < k \ \wedge\ k \mid \mathrm{Rad}(n)\}$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek. Sequences of ordinal numbers. *Formalized Mathematics*, 1(**2**):281–290, 1990.
[5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[6] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[7] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[11] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[12] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[13] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1980.
[14] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.
[15] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.
[16] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.
[17] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[18] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[19] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[20] Library Committee of the Association of Mizar Users. Binary operations on numbers. *To appear in Formalized Mathematics*.
[21] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**):49–58, 2004.
[22] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[23] Christoph Schwarzweller and Andrzej Trybulec. The evaluation of multivariate polynomials. *Formalized Mathematics*, 9(**2**):331–338, 2001.

[24] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.
[25] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[26] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[27] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[28] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[29] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[30] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[33] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received March 21, 2006