FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 153–162, 2013
DOI: 10.2478/forma-2013-0017

VERSITA
degruyter.com/view/j/forma

On Square-Free Numbers

Adam Grabowski
Institute of Informatics
University of Białystok
Akademicka 2, 15-267 Białystok
Poland

Summary. In the article the formal characterization of square-free numbers is shown; in this manner the paper is the continuation of [19]. Essentially, we prepared some lemmas for convenient work with numbers (including the proof that the sequence of prime reciprocals diverges [1]) according to [18] which were absent in the Mizar Mathematical Library. Some of them were expressed in terms of clusters' registrations, enabling automatization machinery available in the Mizar system. Our main result of the article is in the final section; we proved that the lattice of positive divisors of a positive integer n is Boolean if and only if n is square-free.

MSC: 11A51 03B35

Keywords: square-free numbers; prime reciprocals; lattice of natural divisors

MML identifier: `MOEBIUS2`, version: `8.1.02 5.18.1182`

The notation and terminology used in this paper have been introduced in the following articles: [8], [2], [3], [30], [34], [6], [9], [16], [10], [11], [39], [27], [31], [42], [36], [19], [4], [23], [15], [26], [5], [12], [22], [37], [17], [20], [7], [41], [13], [25], [33], [32], [38], [40], [21], and [14].

1. Preliminaries

Let a, b be non zero natural numbers. Let us observe that $\gcd(a, b)$ is non zero and $\operatorname{lcm}(a, b)$ is non zero.

Let n be a natural number. Note that $0 -' n$ reduces to 0.

Now we state the propositions:

(1) Let us consider natural numbers n, i. If $n \geqslant 2^{2 \cdot i + 2}$, then $\frac{n}{2} \geqslant 2^i \cdot \sqrt{n}$.

(2) Let us consider a natural number n. Then $\operatorname{support} \operatorname{PFExp}(n) \subseteq \mathbb{P}$.

ISSN 1426–2630(Print), 1898-9934(Online)

Let us consider a non zero natural number n. Now we state the propositions:

(3) $n - (n \operatorname{div} 2) \cdot 2 \leqslant 1$.

(4) $(n \operatorname{div} 2) \cdot 2 \leqslant n$.

Now we state the propositions:

(5) Let us consider non zero natural numbers a, b. Suppose a and b are not relatively prime. Then there exists a non zero natural number k such that

(i) $k \neq 1$, and

(ii) $k \mid a$, and

(iii) $k \mid b$.

(6) Let us consider non zero natural numbers n, a. If $a \mid n$, then $n \operatorname{div} a \neq 0$.

(7) Let us consider natural numbers i, j. If i and j are relatively prime, then $\operatorname{lcm}(i, j) = i \cdot j$.

Let f be a natural-valued finite sequence. Let us note that $\prod f$ is natural.

2. Prime Numbers

Now we state the propositions:

(8) $\operatorname{pr}(0) = 2$.

(9) $\mathbb{P}(3) = \{2\}$. Proof: For every natural number q, $q \in \{2\}$ iff $q < 3$ and q is prime by [27, (28)], [4, (13)]. □

(10) $\operatorname{pr}(1) = 3$. The theorem is a consequence of (9).

(11) $\mathbb{P}(5) = \{2, 3\}$. Proof: For every natural number q, $q \in \{2, 3\}$ iff $q < 5$ and q is prime by [27, (28)], [17, (41)], [4, (13)]. □

(12) $\operatorname{pr}(2) = 5$. The theorem is a consequence of (11).

(13) $\mathbb{P}(6) = \{2, 3, 5\}$. Proof: $\{2, 3, 5\} \subseteq \mathbb{N}$. For every natural number q, $q \in \{2, 3, 5\}$ iff $q < 6$ and q is prime by [27, (28)], [17, (41), (59)]. □

(14) $\mathbb{P}(7) = \{2, 3, 5\}$. Proof: $\{2, 3, 5\} \subseteq \mathbb{N}$. For every natural number q, $q \in \{2, 3, 5\}$ iff $q < 7$ and q is prime by [27, (28)], [17, (41), (59)]. □

(15) $\operatorname{pr}(3) = 7$. The theorem is a consequence of (14).

(16) $\mathbb{P}(11) = \{2, 3, 5, 7\}$. Proof: $\{2, 3, 5, 7\} \subseteq \mathbb{N}$. For every natural number q, $q \in \{2, 3, 5, 7\}$ iff $q < 11$ and q is prime by [27, (28)], [17, (41), (59)]. □

(17) $\operatorname{pr}(4) = 11$. The theorem is a consequence of (16).

(18) $\mathbb{P}(13) = \{2, 3, 5, 7, 11\}$. Proof: $\{2, 3, 5, 7, 11\} \subseteq \mathbb{N}$. For every natural number q, $q \in \{2, 3, 5, 7, 11\}$ iff $q < 13$ and q is prime by [27, (28)], [17, (41), (59)]. □

(19) $\operatorname{pr}(5) = 13$.

(20) Let us consider natural numbers m, n. Then

(i) $\mathbb{P}(m) \subseteq \mathbb{P}(n)$, or

(ii) $\mathbb{P}(n) \subseteq \mathbb{P}(m)$.

(21) Let us consider natural numbers n, m. Then $n < m$ if and only if $\mathrm{pr}(n) < \mathrm{pr}(m)$. PROOF: For every natural numbers n, m such that $n < m$ holds $\mathrm{pr}(n) < \mathrm{pr}(m)$ by [2, (11)], [26, (69)], [4, (39)]. □

3. PRIME RECIPROCALS

In this paper n, i denote natural numbers.

The functor $\mathrm{inv}_{\mathbb{P}}$ yielding a sequence of real numbers is defined by

(Def. 1) Let us consider a natural number i. Then $it(i) = \frac{1}{\mathrm{pr}(i)}$.

Let f be a sequence of real numbers. We introduce f is divergent as an antonym for f is convergent.

Let us note that $\mathrm{inv}_{\mathbb{P}}$ is decreasing and lower bounded and $\mathrm{inv}_{\mathbb{P}}$ is convergent.

The functor $\mathrm{inv}_{\mathbb{N}}$ yielding a sequence of real numbers is defined by

(Def. 2) Let us consider a natural number i. Then $it(i) = \frac{1}{i}$.

Let us note that $\mathrm{inv}_{\mathbb{N}}$ is non-negative yielding and $\mathrm{inv}_{\mathbb{N}}$ is convergent.

Now we state the propositions:

(22) $\lim \mathrm{inv}_{\mathbb{N}} = 0$.

(23) $\mathrm{inv}_{\mathbb{P}}$ is a subsequence of $\mathrm{inv}_{\mathbb{N}}$. The theorem is a consequence of (21). PROOF: Define $\mathcal{F}(\text{natural number}) = \mathrm{pr}(\$_1)$. Consider f being a sequence of real numbers such that for every natural number i, $f(i) = \mathcal{F}(i)$ from [24, Sch. 1]. For every natural number n, $f(n)$ is an element of $\mathbb{N}$. For every natural numbers n, m such that $n < m$ holds $f(n) < f(m)$. $\mathrm{inv}_{\mathbb{P}} = \mathrm{inv}_{\mathbb{N}} \cdot f$ by [10, (13)]. □

Let f be a non-negative yielding sequence of real numbers. One can verify that every subsequence of f is non-negative yielding and $\mathrm{inv}_{\mathbb{P}}$ is non-negative yielding.

Now we state the proposition:

(24) $\lim \mathrm{inv}_{\mathbb{P}} = 0$.

Observe that $(\sum_{\alpha=0}^{\kappa}(\mathrm{inv}_{\mathbb{P}})(\alpha))_{\kappa\in\mathbb{N}}$ is non-decreasing as a sequence of real numbers.

Now we state the proposition:

(25) Let us consider a non-negative yielding sequence f of real numbers. Suppose f is summable. Let us consider a real number p. Suppose $p > 0$. Then there exists an element i of $\mathbb{N}$ such that $\sum(f \upharpoonright i) < p$.

4. Square Factors

Let n be a non zero natural number. The functor SqFactors n yielding a many sorted set indexed by $\mathbb{P}$ is defined by

(Def. 3) (i) support it = support PFExp(n), and

(ii) for every natural number p such that $p \in$ support PFExp(n) holds $it(p) = p^{(p\text{-count}(n)) \operatorname{div} 2}$.

Let us observe that SqFactors n is finite-support and natural-valued.

Note that every element of support SqFactors n is natural.

The functor SqF n yielding a natural number is defined by the term

(Def. 4) $\prod$ SqFactors n.

Now we state the proposition:

(26) Let us consider a bag f of $\mathbb{P}$. Then $\prod f \neq 0$.

Let n be a non zero natural number. Let us observe that SqF n is non zero.

Let p be a prime number. The functor SqFDiv p yielding a subset of $\mathbb{N}$ is defined by

(Def. 5) Let us consider a natural number n. Then $n \in it$ if and only if n is square-free and for every prime number i such that $i \mid n$ holds $i \leqslant p$.

In the sequel p denotes a prime number.

Now we state the propositions:

(27) $1 \in$ SqFDiv p. Proof: For every prime number i such that $i \mid 1$ holds $i \leqslant p$ by [21, (15)]. □

(28) $0 \notin$ SqFDiv p.

Let us note that there exists a natural number which is square-free and non zero.

Let us consider p. One can verify that there exists a bag of Seg p which is positive yielding.

Now we state the propositions:

(29) Let us consider a positive yielding bag f of Seg p. Then dom f = support f. Proof: Seg $p \subseteq$ support f by [10, (3)]. □

(30) dom CFS(Seg p) = Seg p.

(31) Let us consider a finite set A. Then dom CFS(A) = Seg $\overline{\overline{A}}$.

(32) Let us consider a positive yielding bag g of Seg p. If $g = p \mapsto p$, then $g = g \cdot$ CFS(support g). The theorem is a consequence of (29) and (30). Proof: Set $g = f \cdot$ CFS(Seg p). For every element x such that $x \in$ dom g holds $g(x) = p \mapsto p(x)$ by [10, (12)], [35, (7)], [10, (3)]. □

(33) Let us consider a positive yielding bag f of Seg p. If $f = p \mapsto p$, then $\prod f = p^p$. The theorem is a consequence of (32).

Let us consider a non zero natural number n. Now we state the propositions:

(34) If $n \in \operatorname{SqFDiv} p$, then $\operatorname{support} \operatorname{PFExp}(n) \subseteq \operatorname{Seg} p$.

(35) If $n \in \operatorname{SqFDiv} p$, then $\overline{\overline{\operatorname{support} \operatorname{PFExp}(n)}} \leqslant p$.

Now we state the propositions:

(36) Let us consider a square-free non zero natural number n. Then $\operatorname{rng} \operatorname{PFExp}(n) \subseteq \{0, 1\}$.

(37) Let us consider non zero natural numbers m, n. If $\operatorname{PFExp}(m) = \operatorname{PFExp}(n)$, then $m = n$. PROOF: For every element x such that $x \in \operatorname{dom} \operatorname{PPF}(m)$ holds $(\operatorname{PPF}(m))(x) = (\operatorname{PPF}(n))(x)$ by [23, (33)]. □

Let p be a prime number. Observe that $\operatorname{SqFDiv} p$ is non empty.

Note that every element of $\operatorname{SqFDiv} p$ is non empty.

The functor $2^{\mathbb{P}}(p)$ yielding a set is defined by the term

(Def. 6) $2^{\operatorname{Seg} p \cap \mathbb{P}}$.

Let us note that $2^{\mathbb{P}}(p)$ is finite.

The functor $\operatorname{Hom}_{\mathbb{P}}(p)$ yielding a function from $\operatorname{SqFDiv} p$ into $2^{\mathbb{P}}(p)$ is defined by

(Def. 7) Let us consider an element x of $\operatorname{SqFDiv} p$. Then $it(x) = \operatorname{PFExp}(x) \restriction (\operatorname{Seg} p \cap \mathbb{P})$.

Observe that $\operatorname{Hom}_{\mathbb{P}}(p)$ is one-to-one.

Now we state the proposition:

(38) $\overline{\overline{\operatorname{SqFDiv} p}} \subseteq \overline{\overline{2^{\mathbb{P}}(p)}}$.

Let p be a prime number. One can verify that $\operatorname{SqFDiv} p$ is finite.

Now we state the propositions:

(39) $\overline{\overline{\operatorname{SqFDiv} p}} \leqslant 2^p$.

(40) If $n \neq 0$ and $p^i \mid n$, then $i \leqslant p\text{-count}(n)$.

(41) If $n \neq 0$ and for every prime number p, $p\text{-count}(n) \leqslant 1$, then n is square-free. The theorem is a consequence of (40).

(42) Let us consider a prime number p and a non zero natural number n. If $p\text{-count}(n) = 0$, then $(\operatorname{SqFactors} n)(p) = 0$.

(43) Let us consider a non zero natural number n and a prime number p. Suppose $p\text{-count}(n) \neq 0$. Then $(\operatorname{SqFactors} n)(p) = p^{(p\text{-count}(n)) \operatorname{div} 2}$.

(44) Let us consider non zero natural numbers m, n. Suppose m and n are relatively prime. Then $\operatorname{SqFactors}(m \cdot n) = \operatorname{SqFactors} m + \operatorname{SqFactors} n$. The theorem is a consequence of (42) and (43).

(45) Let us consider a non zero natural number n. Then $\operatorname{SqF} n \mid n$. The theorem is a consequence of (44). PROOF: Define $\mathcal{F}$(non zero natural number) $= \prod \operatorname{SqFactors} \$_1$. Define $\mathcal{G}$(non zero natural number) $= \operatorname{SqFactors} \$_1$. Define $\mathcal{P}$[natural number] $\equiv$ for every non zero natural number n such that $\operatorname{support} \mathcal{G}(n) \subseteq \operatorname{Seg} \$_1$ holds $\mathcal{F}(n) \mid n$. For every natural number

k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (1)], [4, (13)], [23, (34), (42)]. $\mathcal{P}[0]$ by [23, (20)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. □

Let n be a non zero natural number. One can check that PFactors n is prime-factorization-like.

Let us consider a bag f of $\mathbb{P}$. Now we state the propositions:

(46) There exists a finite sequence g of elements of $\mathbb{N}$ such that
  (i) $\prod f = \prod g$, and
  (ii) $g = f \cdot \mathrm{CFS}(\mathrm{support}\, f)$.

(47) If $f(p) = p^n$, then $p^n \mid \prod f$.

(48) If $f(p) = p^n$, then $p\text{-count}(\prod f) \geqslant n$.

5. Extracting Square-containing and Square-free Part of a Number

Let n be a non zero natural number. The functor TSqFactors n yielding a many sorted set indexed by $\mathbb{P}$ is defined by

(Def. 8) (i) support it = support PFExp(n), and
  (ii) for every natural number p such that $p \in$ support PFExp(n) holds $it(p) = p^{2\cdot((p\text{-count}(n)) \operatorname{div} 2)}$.

Now we state the proposition:

(49) Let us consider a non zero natural number n. Then TSqFactors n = (SqFactors n)^2. Proof: For every element x such that $x \in$ dom TSqFactors n holds (TSqFactors n)(x) = (SqFactors n)^2(x) by [26, (9), (11)]. □

Let n be a non zero natural number. Let us observe that TSqFactors n is finite-support and natural-valued.

The functor TSqF n yielding a natural number is defined by the term

(Def. 9) $\prod$ TSqFactors n.

Observe that TSqF n is non zero.

Now we state the propositions:

(50) Let us consider a prime number p and a non zero natural number n. If $p\text{-count}(n) = 0$, then (TSqFactors n)(p) = 0.

(51) Let us consider a non zero natural number n and a prime number p. Suppose $p\text{-count}(n) \neq 0$. Then (TSqFactors n)(p) = $p^{2\cdot((p\text{-count}(n)) \operatorname{div} 2)}$.

(52) Let us consider non zero natural numbers m, n. Suppose m and n are relatively prime. Then TSqFactors($m \cdot n$) = TSqFactors m + TSqFactors n. The theorem is a consequence of (50) and (51).

Let n be a non zero natural number. One can check that support TSqFactors n is natural-membered.

Now we state the proposition:

(53) Let us consider a non zero natural number n. Then TSqF $n \mid n$. The theorem is a consequence of (4) and (52). PROOF: Define $\mathcal{F}$(non zero natural number) $= \prod$ TSqFactors \$1. Define $\mathcal{G}$(non zero natural number) = TSqFactors \$1. Define $\mathcal{P}$[natural number] $\equiv$ for every non zero natural number n such that support $\mathcal{G}(n) \subseteq$ Seg \$1 holds $\mathcal{F}(n) \mid n$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (1)], [4, (13)], [23, (34), (42)]. $\mathcal{P}[0]$ by [23, (20)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. □

Let n be a non zero natural number. Let us note that n div TSqF n is square-free as a natural number.

Now we state the propositions:

(54) Let us consider non zero natural numbers n, k. If $k \neq 1$ and $k^{\mathbf{2}} \mid n$, then n is square-containing.

(55) Let us consider a square-free non zero natural number n and a non zero natural number a. If $a \mid n$, then a and n div a are relatively prime. The theorem is a consequence of (5) and (54). PROOF: n div $a \neq 0$ by [29, (12)]. Consider k being a non zero natural number such that $k \neq 1$ and $k \mid a$ and $k \mid n$ div a. □

6. BINARY OPERATIONS

Now we state the propositions:

(56) Let us consider non empty sets A, C, a commutative binary operation L on A, and a binary operation L_1 on C. If $C \subseteq A$ and $L_1 = L \restriction C$, then L_1 is commutative. PROOF: For every elements a, b of C, $L_1(a,b) = L_1(b,a)$ by [14, (87)], [10, (49)]. □

(57) Let us consider non empty sets A, C, an associative binary operation L on A, and a binary operation L_1 on C. If $C \subseteq A$ and $L_1 = L \restriction C$, then L_1 is associative. PROOF: For every elements a, b, c of C, $L_1(a, L_1(b,c)) = L_1(L_1(a,b),c)$ by [14, (87)], [10, (49), (47)]. □

Let C be a non empty set, L be a commutative binary operation on C, and M be a binary operation on C. Note that $\langle C, L, M\rangle$ is join-commutative.

Let L be a binary operation on C and M be a commutative binary operation on C. Let us observe that $\langle C, L, M\rangle$ is meet-commutative.

Let L be an associative binary operation on C and M be a binary operation on C. Note that $\langle C, L, M\rangle$ is join-associative.

Let L be a binary operation on C and M be an associative binary operation on C. Let us observe that $\langle C, L, M\rangle$ is meet-associative.

7. On the Natural Divisors

Now we state the proposition:

(58) Let us consider a non zero natural number n. Then the set of positive divisors of $n \subseteq \mathbb{N}^+$.

Let us consider a non zero natural number n and natural numbers x, y. Now we state the propositions:

(59) Suppose x, $y \in$ the set of positive divisors of n. Then $\mathrm{lcm}(x, y) \in$ the set of positive divisors of n.

(60) Suppose x, $y \in$ the set of positive divisors of n. Then $\gcd(x, y) \in$ the set of positive divisors of n.

Let n be a non zero natural number. Note that the set of positive divisors of n is non empty and $\gcd_{\mathbb{N}}$ is commutative and associative and $\mathrm{lcm}_{\mathbb{N}}$ is commutative and associative.

Now we state the propositions:

(61) $\gcd_{\mathbb{N}^+} = \gcd_{\mathbb{N}} \restriction \mathbb{N}^+$. Proof: Set $h_1 = \gcd_{\mathbb{N}^+}$. Set $h = \gcd_{\mathbb{N}}$. Set $N = \mathbb{N}^+$. $h_1 = h\restriction(N \times N)$ by [41, (62)], [10, (49), (2)]. □

(62) $\mathrm{lcm}_{\mathbb{N}^+} = \mathrm{lcm}_{\mathbb{N}} \restriction \mathbb{N}^+$. Proof: Set $h_1 = \mathrm{lcm}_{\mathbb{N}^+}$. Set $h = \mathrm{lcm}_{\mathbb{N}}$. Set $N = \mathbb{N}^+$. $h_1 = h\restriction(N \times N)$ by [41, (62)], [10, (49), (2)]. □

Let us observe that $\gcd_{\mathbb{N}^+}$ is commutative and $\mathrm{lcm}_{\mathbb{N}^+}$ is commutative and $\gcd_{\mathbb{N}^+}$ is associative and $\mathrm{lcm}_{\mathbb{N}^+}$ is associative.

8. The Lattice of Natural Divisors

Let n be a non zero natural number. The lattice of positive divisors of n yielding a strict sublattice of $\mathbb{L}_{\mathbb{N}^+}$ is defined by

(Def. 10) The carrier of it = the set of positive divisors of n.

One can check that the carrier of the lattice of positive divisors of n is natural-membered.

Now we state the proposition:

(63) Let us consider a non zero natural number n and elements a, b of the lattice of positive divisors of n. Then

(i) $a \sqcup b = \mathrm{lcm}(a, b)$, and

(ii) $a \sqcap b = \gcd(a, b)$.

Let n be a non zero natural number and p, q be elements of the lattice of positive divisors of n. We identify $\mathrm{lcm}(p, q)$ with $p \sqcup q$. We identify $\gcd(p, q)$ with $p \sqcap q$. Let us note that the lattice of positive divisors of n is non empty.

Note that the lattice of positive divisors of n is distributive and bounded.

Now we state the proposition:

(64) Let us consider a non zero natural number n. Then

(i) $\top_\alpha = n$, and

(ii) $\bot_\alpha = 1$,

where α is the lattice of positive divisors of n. PROOF: Set $L =$ the lattice of positive divisors of n. Reconsider $T = n$ as an element of L. For every element a of L, $T \sqcup a = T$ and $a \sqcup T = T$ by [26, (44)], [19, (39)]. □

Let n be a square-free non zero natural number. One can verify that the lattice of positive divisors of n is Boolean.

Let n be a non zero natural number. One can verify that every element of the lattice of positive divisors of n is non zero.

Now we state the proposition:

(65) Let us consider a non zero natural number n. Then the lattice of positive divisors of n is Boolean if and only if n is square-free. The theorem is a consequence of (64) and (7). PROOF: Set $L =$ the lattice of positive divisors of n. If L is Boolean, then n is square-free by [26, (81)], [19, (39)], [28, (7)]. □

REFERENCES

[1] M. Aigner and G. M. Ziegler. *Proofs from THE BOOK*. Springer-Verlag, Berlin Heidelberg New York, 2004.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

[4] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[5] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[7] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

[8] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[9] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[10] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[11] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[12] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[13] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[14] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[15] Marek Chmur. The lattice of natural numbers and the sublattice of it. The set of prime numbers. *Formalized Mathematics*, 2(**4**):453–459, 1991.

[16] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[17] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.

[18] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1980.

[19] Magdalena Jastrzębska and Adam Grabowski. On the properties of the Möbius function. *Formalized Mathematics*, 14(**1**):29–36, 2006. doi:10.2478/v10037-006-0005-0.

[20] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

[21] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**): 573–577, 1997.

[22] Artur Korniłowicz. On the real valued functions. *Formalized Mathematics*, 13(**1**):181–187, 2005.

[23] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.

[24] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[25] Jarosław Kotowicz. Convergent sequences and the limit of sequences. *Formalized Mathematics*, 1(**2**):273–275, 1990.

[26] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[27] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[28] Xiquan Liang, Li Yan, and Junjie Zhao. Linear congruence relation and complete residue systems. *Formalized Mathematics*, 15(**4**):181–187, 2007. doi:10.2478/v10037-007-0022-7.

[29] Robert Milewski. Natural numbers. *Formalized Mathematics*, 7(**1**):19–22, 1998.

[30] Adam Naumowicz. Conjugate sequences, bounded complex sequences and convergent complex sequences. *Formalized Mathematics*, 6(**2**):265–268, 1997.

[31] Hiroyuki Okazaki and Yasunari Shidama. Uniqueness of factoring an integer and multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$. *Formalized Mathematics*, 16(**2**):103–107, 2008. doi:10.2478/v10037-008-0015-1.

[32] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[33] Konrad Raczkowski and Andrzej Nędzusiak. Series. *Formalized Mathematics*, 2(**4**):449–452, 1991.

[34] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

[35] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.

[36] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[37] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.

[38] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[39] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[40] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[41] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[42] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

Received July 12, 2013