JOURNAL OF FORMALIZED MATHEMATICS
Volume 3, Released 1991, Published 2003
Inst. of Computer Science, Univ. of Białystok

The Lattice of Natural Numbers and The Sublattice of it. The Set of Prime Numbers.

Marek Chmur
Warsaw University
Białystok

Summary. Basic properties of the least common multiple and the greatest common divisor. The lattice of natural numbers ($\mathrm{L}_{\mathbb{N}}$) and the lattice of natural numbers greater than zero ($\mathrm{L}_{\mathbb{N}^+}$) are constructed. The notion of the sublattice of the lattice of natural numbers is given. Some facts about it are proved. The last part of the article deals with some properties of prime numbers and with the notions of the set of prime numbers and the *n*-th prime number. It is proved that the set of prime numbers is infinite.

MML Identifier: `NAT_LAT`.

WWW: `http://mizar.org/JFM/Vol3/nat_lat.html`

The articles [10], [6], [12], [11], [1], [9], [2], [14], [4], [3], [7], [13], [5], and [8] provide the notation and terminology for this paper.

In this paper n, m, l, k, j denote natural numbers.

One can prove the following proposition

(2)[1] If $l \geq 1$, then $k \cdot l \geq k$.

Let us consider n. Then $n!$ is a natural number.

One can prove the following propositions:

(3) If $l \geq 1$ and $n \geq k \cdot l$, then $n \geq k$.

(5)[2] If $l \neq 0$, then $l \mid l!$.

(8)[3] If $n \neq 0$, then $\frac{n+1}{n} > 1$.

(9) $\frac{k}{k+1} < 1$.

(10) For every natural number l holds $l! \geq l$.

(12)[4] For all m, n such that $m \neq 1$ holds if $m \mid n$, then $m \nmid n+1$.

(13) $j \mid l$ and $j \mid l+1$ iff $j = 1$.

[1] The proposition (1) has been removed.
[2] The proposition (4) has been removed.
[3] The propositions (6) and (7) have been removed.
[4] The proposition (11) has been removed.

(15)[5] For all k, j such that $j \neq 0$ holds $j \mid (j+k)!$.

(16) If $j \leq l$ and $j \neq 0$, then $j \mid l!$.

(17) For all l, j such that $j \neq 1$ and $j \neq 0$ holds if $j \mid l!+1$, then $j > l$.

(19)[6] $\mathrm{lcm}(m, \mathrm{lcm}(n,k)) = \mathrm{lcm}(\mathrm{lcm}(m,n),k)$.

(20) $m \mid n$ iff $\mathrm{lcm}(m,n) = n$.

(23)[7] $n \mid m$ and $k \mid m$ iff $\mathrm{lcm}(n,k) \mid m$.

(26)[8] $\mathrm{lcm}(m,1) = m$.

(27) $\mathrm{lcm}(m,n) \mid m \cdot n$.

(28) $\gcd(m, \gcd(n,k)) = \gcd(\gcd(m,n),k)$.

(30)[9] If $n \mid m$, then $\gcd(n,m) = n$.

(32)[10] $m \mid n$ and $m \mid k$ iff $m \mid \gcd(n,k)$.

(35)[11] $\gcd(m,1) = 1$.

(36) $\gcd(m,0) = m$.

(37) $\mathrm{lcm}(\gcd(m,n),n) = n$.

(38) $\gcd(m, \mathrm{lcm}(m,n)) = m$.

(39) $\gcd(m, \mathrm{lcm}(m,n)) = \mathrm{lcm}(\gcd(n,m),m)$.

(40) If $m \mid n$, then $\gcd(m,k) \mid \gcd(n,k)$.

(41) If $m \mid n$, then $\gcd(k,m) \mid \gcd(k,n)$.

(42) If $m > 0$, then $\gcd(0,m) > 0$.

(43) If $n > 0$, then $\gcd(n,m) > 0$.

(44) If $m > 0$ and $n > 0$, then $\mathrm{lcm}(m,n) > 0$.

(45) $\mathrm{lcm}(\gcd(n,m), \gcd(n,k)) \mid \gcd(n, \mathrm{lcm}(m,k))$.

(46) If $m \mid l$, then $\mathrm{lcm}(m, \gcd(n,l)) \mid \gcd(\mathrm{lcm}(m,n),l)$.

(47) $\gcd(n,m) \mid \mathrm{lcm}(n,m)$.

The binary operation $\mathrm{hcf}_{\mathbb{N}}$ on $\mathbb{N}$ is defined as follows:

(Def. 3)[12] $\mathrm{hcf}_{\mathbb{N}}(m, n) = \gcd(m,n)$.

The binary operation $\mathrm{lcm}_{\mathbb{N}}$ on $\mathbb{N}$ is defined by:

(Def. 4) $\mathrm{lcm}_{\mathbb{N}}(m, n) = \mathrm{lcm}(m,n)$.

In the sequel p, q are elements of $\langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$.

Let m be an element of $\langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$. The functor ${}^{@}m$ yields a natural number and is defined by:

---

[5] The proposition (14) has been removed.
[6] The proposition (18) has been removed.
[7] The propositions (21) and (22) have been removed.
[8] The propositions (24) and (25) have been removed.
[9] The proposition (29) has been removed.
[10] The proposition (31) has been removed.
[11] The propositions (33) and (34) have been removed.
[12] The definitions (Def. 1) and (Def. 2) have been removed.

(Def. 5) $^{@}m = m$.

Next we state three propositions:

(48) $p \sqcup q = \mathrm{lcm}(^{@}p, ^{@}q)$.

(49) $p \sqcap q = \mathrm{gcd}(^{@}p, ^{@}q)$.

(52)[13] For all elements a, b of $\langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$ such that $a \sqsubseteq b$ holds $^{@}a \mid {}^{@}b$.

The element $\mathbf{0}_{\mathbb{L}_{\mathbb{N}}}$ of $\langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$ is defined as follows:

(Def. 6) $\mathbf{0}_{\mathbb{L}_{\mathbb{N}}} = 1$.

The element $\mathbf{1}_{\mathbb{L}_{\mathbb{N}}}$ of $\langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$ is defined as follows:

(Def. 7) $\mathbf{1}_{\mathbb{L}_{\mathbb{N}}} = 0$.

One can prove the following two propositions:

(55)[14] $^{@}(\mathbf{0}_{\mathbb{L}_{\mathbb{N}}}) = 1$.

(56) For every element a of $\langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$ holds $\mathbf{0}_{\mathbb{L}_{\mathbb{N}}} \sqcap a = \mathbf{0}_{\mathbb{L}_{\mathbb{N}}}$ and $a \sqcap \mathbf{0}_{\mathbb{L}_{\mathbb{N}}} = \mathbf{0}_{\mathbb{L}_{\mathbb{N}}}$.

The lattice $\mathbb{L}_{\mathbb{N}}$ is defined as follows:

(Def. 8) $\mathbb{L}_{\mathbb{N}} = \langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$.

One can verify that $\mathbb{L}_{\mathbb{N}}$ is strict.
In the sequel p, q, r are elements of $\mathbb{L}_{\mathbb{N}}$.
We now state several propositions:

(60)[15] $\mathbb{L}_{\mathbb{N}}$ is a lower bound lattice.

(61) $\mathrm{lcm}_{\mathbb{N}}(p, q) = \mathrm{lcm}_{\mathbb{N}}(q, p)$.

(62) $\mathrm{hcf}_{\mathbb{N}}(q, p) = \mathrm{hcf}_{\mathbb{N}}(p, q)$.

(63) $\mathrm{lcm}_{\mathbb{N}}(p, \mathrm{lcm}_{\mathbb{N}}(q, r)) = \mathrm{lcm}_{\mathbb{N}}(\mathrm{lcm}_{\mathbb{N}}(p, q), r)$.

(64) $\mathrm{lcm}_{\mathbb{N}}(p, \mathrm{lcm}_{\mathbb{N}}(q, r)) = \mathrm{lcm}_{\mathbb{N}}(\mathrm{lcm}_{\mathbb{N}}(q, p), r)$ and $\mathrm{lcm}_{\mathbb{N}}(p, \mathrm{lcm}_{\mathbb{N}}(q, r)) = \mathrm{lcm}_{\mathbb{N}}(\mathrm{lcm}_{\mathbb{N}}(p, r), q)$ and $\mathrm{lcm}_{\mathbb{N}}(p, \mathrm{lcm}_{\mathbb{N}}(q, r)) = \mathrm{lcm}_{\mathbb{N}}(\mathrm{lcm}_{\mathbb{N}}(r, q), p)$ and $\mathrm{lcm}_{\mathbb{N}}(p, \mathrm{lcm}_{\mathbb{N}}(q, r)) = \mathrm{lcm}_{\mathbb{N}}(\mathrm{lcm}_{\mathbb{N}}(r, p), q)$.

(65) $\mathrm{hcf}_{\mathbb{N}}(p, \mathrm{hcf}_{\mathbb{N}}(q, r)) = \mathrm{hcf}_{\mathbb{N}}(\mathrm{hcf}_{\mathbb{N}}(p, q), r)$.

(66) $\mathrm{hcf}_{\mathbb{N}}(p, \mathrm{hcf}_{\mathbb{N}}(q, r)) = \mathrm{hcf}_{\mathbb{N}}(\mathrm{hcf}_{\mathbb{N}}(q, p), r)$ and $\mathrm{hcf}_{\mathbb{N}}(p, \mathrm{hcf}_{\mathbb{N}}(q, r)) = \mathrm{hcf}_{\mathbb{N}}(\mathrm{hcf}_{\mathbb{N}}(p, r), q)$ and $\mathrm{hcf}_{\mathbb{N}}(p, \mathrm{hcf}_{\mathbb{N}}(q, r)) = \mathrm{hcf}_{\mathbb{N}}(\mathrm{hcf}_{\mathbb{N}}(r, q), p)$ and $\mathrm{hcf}_{\mathbb{N}}(p, \mathrm{hcf}_{\mathbb{N}}(q, r)) = \mathrm{hcf}_{\mathbb{N}}(\mathrm{hcf}_{\mathbb{N}}(r, p), q)$.

(67) $\mathrm{hcf}_{\mathbb{N}}(q, \mathrm{lcm}_{\mathbb{N}}(q, p)) = q$ and $\mathrm{hcf}_{\mathbb{N}}(\mathrm{lcm}_{\mathbb{N}}(p, q), q) = q$ and $\mathrm{hcf}_{\mathbb{N}}(q, \mathrm{lcm}_{\mathbb{N}}(p, q)) = q$ and $\mathrm{hcf}_{\mathbb{N}}(\mathrm{lcm}_{\mathbb{N}}(q, p), q) = q$.

(68) $\mathrm{lcm}_{\mathbb{N}}(q, \mathrm{hcf}_{\mathbb{N}}(q, p)) = q$ and $\mathrm{lcm}_{\mathbb{N}}(\mathrm{hcf}_{\mathbb{N}}(p, q), q) = q$ and $\mathrm{lcm}_{\mathbb{N}}(q, \mathrm{hcf}_{\mathbb{N}}(p, q)) = q$ and $\mathrm{lcm}_{\mathbb{N}}(\mathrm{hcf}_{\mathbb{N}}(q, p), q) = q$.

The subset $\mathbb{N}^{+}$ of $\mathbb{N}$ is defined by:

(Def. 9) For every natural number n holds $n \in \mathbb{N}^{+}$ iff $0 < n$.

[13] The propositions (50) and (51) have been removed.
[14] The propositions (53) and (54) have been removed.
[15] The propositions (57)–(59) have been removed.

One can check that $\mathbb{N}^+$ is non empty.

Let D be a non empty set, let S be a non empty subset of D, and let N be a non empty subset of S. We see that the element of N is an element of S.

Let D be a subset of $\mathbb{R}$. Observe that every element of D is real.

Let D be a subset of $\mathbb{N}$. Observe that every element of D is real.

A positive natural number is an element of $\mathbb{N}^+$.

Let k be a natural number. Let us assume that $k > 0$. The functor ${}^{@}k$ yielding an element of $\mathbb{N}^+$ is defined by:

(Def. 10) ${}^{@}k = k$.

Let k be an element of $\mathbb{N}^+$. The functor ${}^{@}k$ yields a positive natural number and is defined by:

(Def. 11) ${}^{@}k = k$.

In the sequel m, n denote positive natural numbers.

The binary operation $\mathrm{hcf}_{\mathbb{N}^+}$ on $\mathbb{N}^+$ is defined by:

(Def. 12) $\mathrm{hcf}_{\mathbb{N}^+}(m, n) = \gcd(m,n)$.

The binary operation $\mathrm{lcm}_{\mathbb{N}^+}$ on $\mathbb{N}^+$ is defined by:

(Def. 13) $\mathrm{lcm}_{\mathbb{N}^+}(m, n) = \mathrm{lcm}(m,n)$.

In the sequel p, q are elements of $\langle \mathbb{N}^+, \mathrm{lcm}_{\mathbb{N}^+}, \mathrm{hcf}_{\mathbb{N}^+} \rangle$.

Let m be an element of $\langle \mathbb{N}^+, \mathrm{lcm}_{\mathbb{N}^+}, \mathrm{hcf}_{\mathbb{N}^+} \rangle$. The functor ${}^{@}m$ yielding a positive natural number is defined by:

(Def. 14) ${}^{@}m = m$.

The following propositions are true:

(69) $p \sqcup q = \mathrm{lcm}({}^{@}p, {}^{@}q)$.

(70) $p \sqcap q = \gcd({}^{@}p, {}^{@}q)$.

The lattice $\mathbb{L}_{\mathbb{N}^+}$ is defined as follows:

(Def. 15) $\mathbb{L}_{\mathbb{N}^+} = \langle \mathbb{N}^+, \mathrm{lcm}_{\mathbb{N}^+}, \mathrm{hcf}_{\mathbb{N}^+} \rangle$.

One can check that $\mathbb{L}_{\mathbb{N}^+}$ is strict.

Let L be a lattice. A lattice is called a sublattice of L if it satisfies the conditions (Def. 16).

(Def. 16)(i) The carrier of it $\subseteq$ the carrier of L,

(ii) the join operation of it $=$ (the join operation of L)$\restriction$[: the carrier of it, the carrier of it :], and

(iii) the meet operation of it $=$ (the meet operation of L)$\restriction$[: the carrier of it, the carrier of it :].

Let L be a lattice. Observe that there exists a sublattice of L which is strict.

One can prove the following propositions:

(75)[16] Every lattice L is a sublattice of L.

(76) $\mathbb{L}_{\mathbb{N}^+}$ is a sublattice of $\mathbb{L}_{\mathbb{N}}$.

In the sequel n, i, k, k_1, k_2, m, l denote natural numbers.

The subset Prime of $\mathbb{N}$ is defined by:

(Def. 17) For every natural number n holds $n \in$ Prime iff n is prime.

[16] The propositions (71)–(74) have been removed.

Let us observe that there exists a natural number which is prime.

A prime number is a prime natural number.

In the sequel p, f are prime numbers.

Let us consider p. The functor $\mathrm{Prime}(p)$ yields a subset of $\mathbb{N}$ and is defined as follows:

(Def. 19)[17] For every natural number q holds $q \in \mathrm{Prime}(p)$ iff $q < p$ and q is prime.

Next we state a number of propositions:

(77) $\mathrm{Prime}(p) \subseteq \mathrm{Prime}$.

(78) For every prime number q such that $p < q$ holds $\mathrm{Prime}(p) \subseteq \mathrm{Prime}(q)$.

(79) $\mathrm{Prime}(p) \subseteq \mathrm{Seg}\, p$.

(80) $\mathrm{Prime}(p)$ is finite.

(81) For every l there exists p such that p is prime and $p > l$.

(84)[18] $\mathrm{Prime} \neq \emptyset$.

(85) $\{k : k < 2 \ \wedge \ k \text{is prime}\} = \emptyset$.

(86) For every p holds $\{k : k < p \ \wedge \ k \text{is prime}\} \subseteq \mathbb{N}$.

(87) For every m holds $\{k : k < m \ \wedge \ k \text{is prime}\} \subseteq \mathrm{Seg}\, m$.

(88) For every m holds $\{k : k < m \ \wedge \ k \text{is prime}\}$ is finite.

(89) For every prime number f holds $f \notin \{k : k < f \ \wedge \ k \text{is prime}\}$.

(90) For every f holds $\{k : k < f \ \wedge \ k \text{is prime}\} \cup \{f\}$ is finite.

(91) For all prime numbers f, g such that $f < g$ holds $\{k_1 : k_1 < f \ \wedge \ k_1 \text{is prime}\} \cup \{f\} \subseteq \{k_2 : k_2 < g \ \wedge \ k_2 \text{is prime}\}$.

(92) For every k such that $k > m$ holds $k \notin \{k_1 : k_1 < m \ \wedge \ k_1 \text{is prime}\}$.

Let us consider n. The functor $\mathrm{pr}(n)$ yields a prime number and is defined by:

(Def. 20) There exists a finite set B such that $B = \{k : k < \mathrm{pr}(n) \ \wedge \ k \text{is prime}\}$ and $n = \mathrm{card}\, B$.

The following propositions are true:

(93) $\mathrm{Prime}(p) = \{k : k < p \ \wedge \ k \text{is prime}\}$.

(94) Prime is infinite.

(95) For every i such that i is prime and for all m, n such that $i \mid m \cdot n$ holds $i \mid m$ or $i \mid n$.

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/card_1.html`.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/nat_1.html`.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finseq_1.html`.

[4] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/binop_1.html`.

[5] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funct_1.html`.

[17] The definition (Def. 18) has been removed.

[18] The propositions (82) and (83) have been removed.

[6] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/zfmisc_1.html.

[7] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finset_1.html.

[8] Rafał Kwiatek. Factorial and Newton coefficients. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/newton.html.

[9] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/int_2.html.

[10] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. http://mizar.org/JFM/Axiomatics/tarski.html.

[11] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. http://mizar.org/JFM/Addenda/numbers.html.

[12] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/subset_1.html.

[13] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relat_1.html.

[14] Stanisław Żukowski. Introduction to lattice theory. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/lattices.html.

Received April 26, 1991

Published January 2, 2004