FORMALIZED MATHEMATICS
Vol.2, No.4, September–October 1991
Université Catholique de Louvain

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 fact 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.

The papers [15], [6], [18], [14], [7], [17], [9], [1], [11], [2], [16], [12], [5], [4], [8], [13], [10], and [3] provide the terminology and notation for this paper. In the sequel n, m, l, k, j will be natural numbers. We now state two propositions:

(1) For all natural numbers m, n holds $m \mid m \cdot n$ and $n \mid m \cdot n$.

(2) For all k, l such that $l \geq 1$ holds $k \cdot l \geq k$.

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

The following propositions are true:

(3) For all n, k, l such that $l \geq 1$ holds if $n \geq k \cdot l$, then $n \geq k$.

(4) $k = 0$ or $k \geq 1$.

(5) For every l such that $l \neq 0$ holds $l \mid l!$.

(6) $k \neq k + 1$.

(8)[1] For every n such that $n \neq 0$ holds $\frac{n+1}{n} > 1$.

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

[1] The proposition (7) has been removed.

ISSN 0777–4028

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

(12)[2] For all m, n such that $m \neq 1$ holds if $m \mid n$, then $m \nmid n+1$.

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

(14) For every l there exists j such that $j \mid l!$.

(15) 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 $j > l$.

(18) For all natural numbers m, n holds $\mathrm{lcm}(m,n) = \mathrm{lcm}(n,m)$.

(19) For all natural numbers m, n, k holds $\mathrm{lcm}(m, \mathrm{lcm}(n,k)) = \mathrm{lcm}(\mathrm{lcm}(m,n),k)$.

(20) For all natural numbers m, n holds $m \mid n$ if and only if $\mathrm{lcm}(m,n) = n$.

(21) $m \mid \mathrm{lcm}(m,n)$ and $n \mid \mathrm{lcm}(m,n)$.

(22) $\mathrm{lcm}(m,m) = m$.

(23) $n \mid m$ and $k \mid m$ if and only if $\mathrm{lcm}(n,k) \mid m$.

(24) $\mathrm{lcm}(m,n) \mid 0$.

(25) $1 \mid \mathrm{lcm}(m,n)$.

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

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

(28) For all natural numbers m, n, k holds $\gcd(m, \gcd(n,k)) = \gcd(\gcd(m,n),k)$.

(29) $\gcd(m,n) \mid m$ and $\gcd(m,n) \mid n$.

(30) For all natural numbers m, n such that $n \mid m$ holds $\gcd(n,m) = n$.

(31) $\gcd(m,m) = m$.

(32) $m \mid n$ and $m \mid k$ if and only if $m \mid \gcd(n,k)$.

(33) $\gcd(m,n) \mid 0$.

The following propositions are true:

(34) $1 \mid \gcd(m,n)$.

(35) $\gcd(m,1) = 1$.

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

(37) For all natural numbers m, n holds $\mathrm{lcm}(\gcd(m,n),n) = n$.

(38) For all natural numbers m, n holds $\gcd(m, \mathrm{lcm}(m,n)) = m$.

(39) For all natural numbers m, n holds $\gcd(m, \mathrm{lcm}(m,n)) = \mathrm{lcm}(\gcd(n,m),m)$.

(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) For every m such that $m > 0$ holds $\gcd(0,m) > 0$.

(43) For all m, n such that $m > 0$ and $n > 0$ holds $\gcd(n,m) > 0$.

(44) For all m, n such that $m > 0$ and $n > 0$ holds $\mathrm{lcm}(m,n) > 0$.

[2] The proposition (11) has been removed.

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

(46) For all m, n, l such that $m \mid l$ holds $\mathrm{lcm}(m,\gcd(n,l)) \mid \gcd(\mathrm{lcm}(m,n),l)$.

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

Let m be an element of $\mathbb{N}$ **qua** a non-empty set. The functor ${}^{@}m$ yielding a natural number is defined by:

(Def.1) ${}^{@}m = m$.

Let m be a natural number. The functor ${}^{@}m$ yielding an element of $\mathbb{N}$ **qua** a non-empty set is defined as follows:

(Def.2) ${}^{@}m = m$.

We now define two new functors. The binary operation $\mathrm{hcf}_{\mathbb{N}}$ on $\mathbb{N}$ is defined by:

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

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 denote elements of the carrier of $\langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$. Let m be an element of the carrier of $\langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$. The functor ${}^{@}m$ yielding a natural number is defined as follows:

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

We now state several propositions:

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

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

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

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

(52) For all elements a, b of the carrier 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 the carrier 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 the carrier of $\langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$ is defined by:

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

We now state three propositions:

(55)[3] ${}^{@}(\mathbf{0}_{\mathbb{L}_{\mathbb{N}}}) = 1$.

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

(57) There exists an element z of the carrier of $\langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$ such that for every element x of the carrier of $\langle \mathbb{N}, \mathrm{lcm}_{\mathbb{N}}, \mathrm{hcf}_{\mathbb{N}} \rangle$ holds $z \sqcap x = z$.

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

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

The following proposition is true

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

[3] The propositions (53) and (54) have been removed.

In the sequel p, q, r will denote elements of the carrier of $\mathbb{L}_{\mathbb{N}}$. One can prove the following propositions:

(60)[4] $\mathbb{L}_{\mathbb{N}}$ 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) (i) $\mathrm{lcm}_{\mathbb{N}}(p, \mathrm{lcm}_{\mathbb{N}}(q, r)) = \mathrm{lcm}_{\mathbb{N}}(\mathrm{lcm}_{\mathbb{N}}(q, p), r)$,
(ii) $\mathrm{lcm}_{\mathbb{N}}(p, \mathrm{lcm}_{\mathbb{N}}(q, r)) = \mathrm{lcm}_{\mathbb{N}}(\mathrm{lcm}_{\mathbb{N}}(p, r), q)$,
(iii) $\mathrm{lcm}_{\mathbb{N}}(p, \mathrm{lcm}_{\mathbb{N}}(q, r)) = \mathrm{lcm}_{\mathbb{N}}(\mathrm{lcm}_{\mathbb{N}}(r, q), p)$,
(iv) $\mathrm{lcm}_{\mathbb{N}}(p, \mathrm{lcm}_{\mathbb{N}}(q, r)) = \mathrm{lcm}_{\mathbb{N}}(\mathrm{lcm}_{\mathbb{N}}(r, p), q)$.

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

(66) (i) $\mathrm{hcf}_{\mathbb{N}}(p, \mathrm{hcf}_{\mathbb{N}}(q, r)) = \mathrm{hcf}_{\mathbb{N}}(\mathrm{hcf}_{\mathbb{N}}(q, p), r)$,
(ii) $\mathrm{hcf}_{\mathbb{N}}(p, \mathrm{hcf}_{\mathbb{N}}(q, r)) = \mathrm{hcf}_{\mathbb{N}}(\mathrm{hcf}_{\mathbb{N}}(p, r), q)$,
(iii) $\mathrm{hcf}_{\mathbb{N}}(p, \mathrm{hcf}_{\mathbb{N}}(q, r)) = \mathrm{hcf}_{\mathbb{N}}(\mathrm{hcf}_{\mathbb{N}}(r, q), p)$,
(iv) $\mathrm{hcf}_{\mathbb{N}}(p, \mathrm{hcf}_{\mathbb{N}}(q, r)) = \mathrm{hcf}_{\mathbb{N}}(\mathrm{hcf}_{\mathbb{N}}(r, p), q)$.

(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 $n \in \mathbb{N}^+$ if and only if $0 < n$.

Let D be a non-empty set, and 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.

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

Let k be a natural number satisfying the condition: $k > 0$. The functor ${}^{@}k$ yields an element of $\mathbb{N}^+$ **qua** a non-empty set and is defined by:

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

Let k be an element of $\mathbb{N}^+$ **qua** a non-empty set. The functor ${}^{@}k$ yields a positive natural number and is defined as follows:

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

In the sequel m, n denote positive natural numbers. We now define two new functors. 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 as follows:

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

In the sequel p, q will denote elements of the carrier of $\langle \mathbb{N}^+, \mathrm{lcm}_{\mathbb{N}^+}, \mathrm{hcf}_{\mathbb{N}^+} \rangle$. Let m be an element of the carrier of $\langle \mathbb{N}^+, \mathrm{lcm}_{\mathbb{N}^+}, \mathrm{hcf}_{\mathbb{N}^+} \rangle$. The functor ${}^{@}m$ yields a positive natural number and is defined as follows:

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

[4] The proposition (59) has been removed.

One can prove the following four propositions:

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

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

(71) $\mathrm{lcm}_{\mathbb{N}^+}(p, q) = p \sqcup q$.

(72) $\mathrm{hcf}_{\mathbb{N}^+}(p, q) = p \sqcap q$.

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

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

Next we state the proposition

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

Let L be a lattice. A lattice is said to be a sublattice of L if:

(Def.16) the carrier of it $\subseteq$ the carrier of L and the join operation of it $=$ (the join operation of L) $\restriction$ [: the carrier of it, the carrier of it :] and the meet operation of it $=$ (the meet operation of L) $\restriction$ [: the carrier of it, the carrier of it :].

The following two propositions are true:

(75)[5] For every lattice L holds 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 will denote natural numbers. The set Prime of natural numbers is defined as follows:

(Def.17) for every natural number n holds $n \in$ Prime if and only if n is prime.

A natural number is said to be a prime number if:

(Def.18) it $\in$ Prime.

In the sequel p, q denote prime numbers and f denotes a prime number. Let us consider p. The functor Prime(p) yields sets of natural numbers and is defined by:

(Def.19) for every natural number q holds $q \in$ Prime(p) if and only if $q < p$ and q is prime.

Next we state a number of propositions:

(77) Prime(p) $\subseteq$ Prime.

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

(79) Prime(p) $\subseteq$ Seg p.

(80) Prime(p) is finite.

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

(82) For every q such that q is prime there exists p such that p is prime and $p > q$.

(83) Prime $\subseteq \mathbb{N}$.

(84) Prime $\neq \emptyset$.

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

[5] The proposition (74) has been removed.

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

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

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

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

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

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

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

Let us consider n. The functor $\mathrm{pr}(n)$ yielding a prime number is defined as follows:

(Def.20) $n = \operatorname{card}\{k : k < \mathrm{pr}(n) \wedge k$ is prime$\}$.

One can prove the following two propositions:

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

(94) Prime is not finite.

The following proposition is true

(95) For every i such that i is prime 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. *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. Sequences of ordinal numbers. *Formalized Mathematics*, 1(**2**):281–290, 1990.

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

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

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

[7] Marek Chmur. The lattice of real numbers. The lattice of real functions. *Formalized Mathematics*, 1(**4**):681–684, 1990.

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

[9] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

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

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

[12] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.

[13] Henryk Oryszczyszyn and Krzysztof Prażmowski. Real functions spaces. *Formalized Mathematics*, 1(**3**):555–561, 1990.

[14] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.

[15] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

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

[17] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

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

Received April 26, 1991