JOURNAL OF FORMALIZED MATHEMATICS
Volume 2, Released 1990, Published 2003
Inst. of Computer Science, Univ. of Białystok

The Divisibility of Integers and Integer Relatively Primes [1]

Rafał Kwiatek
Warsaw University
Białystok

Grzegorz Zwara
Nicolaus Copernicus University
Toruń

Summary. We introduce the following notions: 1) the least common multiple of two integers (lcm(i, j)), 2) the greatest common divisor of two integers (gcd(i, j)), 3) the relative prime integer numbers, 4) the prime numbers. A few facts concerning the above items, among them a so-called Fundamental Theorem of Arithmetic, are introduced.

MML Identifier: `INT_2`.

WWW: `http://mizar.org/JFM/Vol2/int_2.html`

The articles [6], [3], [2], [4], [1], and [5] provide the notation and terminology for this paper.

In this paper a, b are natural numbers.

We now state four propositions:

(3)[1] $0 \mid a$ iff $a = 0$.

(4) $a = 0$ or $b = 0$ iff $\mathrm{lcm}(a,b) = 0$.

(5) $a = 0$ and $b = 0$ iff $\gcd(a,b) = 0$.

(6) $a \cdot b = \mathrm{lcm}(a,b) \cdot \gcd(a,b)$.

We adopt the following rules: m, n denote natural numbers and a, b, c, a_1, b_1 denote integers.

We now state a number of propositions:

(8)[2] $-n$ is a natural number iff $n = 0$.

(9) -1 is a natural number.

(10) $0 \mid a$ iff $a = 0$.

(11) $a \mid -a$ and $-a \mid a$.

(12) If $a \mid b$, then $a \mid b \cdot c$.

(13) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(14)(i) $a \mid b$ iff $a \mid -b$,

(ii) $a \mid b$ iff $-a \mid b$,

(iii) $a \mid b$ iff $-a \mid -b$, and

(iv) $a \mid -b$ iff $-a \mid b$.

[1] Supported by RPBP.III-24.B5.

[1] The propositions (1) and (2) have been removed.

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

(15) If $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.

(16) $a \mid 0$ and $1 \mid a$ and $-1 \mid a$.

(17) If $a \mid 1$ or $a \mid -1$, then $a = 1$ or $a = -1$.

(18) If $a = 1$ or $a = -1$, then $a \mid 1$ and $a \mid -1$.

(19) $a \equiv b (\mathrm{mod}\, c)$ iff $c \mid a - b$.

(20) $|a|$ is a natural number.

(21) $a \mid b$ iff $|a| \mid |b|$.

Let us consider a, b. The functor $\mathrm{lcm}(a,b)$ yielding an integer is defined by:

(Def. 2)[3] $\mathrm{lcm}(a,b) = \mathrm{lcm}(|a|,|b|)$.

Let us observe that the functor $\mathrm{lcm}(a,b)$ is commutative.

Next we state four propositions:

(23)[4] $\mathrm{lcm}(a,b)$ is a natural number.

(25)[5] $a \mid \mathrm{lcm}(a,b)$.

(26) $b \mid \mathrm{lcm}(a,b)$.

(27) For every c such that $a \mid c$ and $b \mid c$ holds $\mathrm{lcm}(a,b) \mid c$.

Let us consider a, b. The functor $a \gcd b$ yields an integer and is defined as follows:

(Def. 3) $a \gcd b = \gcd(|a|,|b|)$.

Let us notice that the functor $a \gcd b$ is commutative.

We now state several propositions:

(29)[6] $a \gcd b$ is a natural number.

(31)[7] $a \gcd b \mid a$.

(32) $a \gcd b \mid b$.

(33) For every c such that $c \mid a$ and $c \mid b$ holds $c \mid a \gcd b$.

(34) $a = 0$ or $b = 0$ iff $\mathrm{lcm}(a,b) = 0$.

(35) $a = 0$ and $b = 0$ iff $a \gcd b = 0$.

Let us consider a, b. We say that a and b are relative prime if and only if:

(Def. 4) $a \gcd b = 1$.

Let us note that the predicate a and b are relative prime is symmetric.

One can prove the following propositions:

(38)[8] If $a \neq 0$ or $b \neq 0$, then there exist a_1, b_1 such that $a = (a \gcd b) \cdot a_1$ and $b = (a \gcd b) \cdot b_1$ and a_1 and b_1 are relative prime.

[3] The definition (Def. 1) has been removed.
[4] The proposition (22) has been removed.
[5] The proposition (24) has been removed.
[6] The proposition (28) has been removed.
[7] The proposition (30) has been removed.
[8] The propositions (36) and (37) have been removed.

(39) If a and b are relative prime, then $c \cdot a \operatorname{gcd} c \cdot b = |c|$ and $c \cdot a \operatorname{gcd} b \cdot c = |c|$ and $a \cdot c \operatorname{gcd} c \cdot b = |c|$ and $a \cdot c \operatorname{gcd} b \cdot c = |c|$.

(40) If $c \mid a \cdot b$ and a and c are relative prime, then $c \mid b$.

(41) If a and c are relative prime and b and c are relative prime, then $a \cdot b$ and c are relative prime.

In the sequel p, q, k, l denote natural numbers.
Let us consider p. We say that p is prime if and only if:

(Def. 5) $p > 1$ and for every n such that $n \mid p$ holds $n = 1$ or $n = p$.

Let us consider m, n. We say that m and n are relative prime if and only if:

(Def. 6) $\gcd(m, n) = 1$.

One can prove the following propositions:

(44)[9] 2 is prime.

(46)[10] There exists p such that p is not prime.

(47) If p is prime and q is prime, then p and q are relative prime or $p = q$.

In this article we present several logical schemes. The scheme *Ind1* deals with a natural number $\mathcal{A}$ and a unary predicate $\mathcal{P}$, and states that:

For every k such that $k \geq \mathcal{A}$ holds $\mathcal{P}[k]$

provided the following requirements are met:

- $\mathcal{P}[\mathcal{A}]$, and
- For every k such that $k \geq \mathcal{A}$ and $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$.

The scheme *Comp Ind1* deals with a natural number $\mathcal{A}$ and a unary predicate $\mathcal{P}$, and states that:

For every k such that $k \geq \mathcal{A}$ holds $\mathcal{P}[k]$

provided the parameters meet the following condition:

- For every k such that $k \geq \mathcal{A}$ and for every n such that $n \geq \mathcal{A}$ and $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$.

The following proposition is true

(48) If $l \geq 2$, then there exists p such that p is prime and $p \mid l$.

REFERENCES

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

[2] Krzysztof Hryniewiecki. Basic properties of real numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/real_1.html`.

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

[4] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/int_1.html`.

[5] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/group_1.html`.

[9] The propositions (42) and (43) have been removed.
[10] The proposition (45) has been removed.

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

Received July 10, 1990

Published January 2, 2004