FORMALIZED MATHEMATICS
Vol.1, No.5, November–December 1990
Université Catholique de Louvain

The Divisibility of Integers and Integer Relatively Primes [1]

Rafał Kwiatek
Nicolaus Copernicus University
Toruń

Grzegorz Zwara
Warsaw University
Białystok

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 Foundamental Theorem of Arithmetic, are introduced.

MML Identifier: `INT_2`.

The papers [2], [1], and [3] provide the terminology and notation for this paper. In the sequel a, b will be natural numbers. Next we state several propositions:

(1) $\mathrm{lcm}(a,b) = \mathrm{lcm}(b,a)$.

(2) $\mathrm{gcd}(a,b) = \mathrm{gcd}(b,a)$.

(3) $0 \mid a$ if and only if $a = 0$.

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

(5) $a = 0$ and $b = 0$ if and only if $\mathrm{gcd}(a,b) = 0$.

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

We follow the rules: m, n are natural numbers and a, b, c, a_1, b_1 are integers. Let us consider n. The functor $+n$ yields an integer and is defined by:

(Def.1) $+n = n$.

Next we state a number of propositions:

(7) $+n = n$.

(8) $-n$ is a natural number if and only if $n = 0$.

(9) -1 is not a natural number.

(10) $+0 \mid a$ if and only if $a = 0$.

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

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

ISSN 0777–4028

(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) $a \mid b$ if and only if $a \mid -b$ but $a \mid b$ if and only if $-a \mid b$ but $a \mid b$ if and only if $-a \mid -b$ but $a \mid -b$ if and only if $-a \mid b$.

(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) $a \equiv b (\operatorname{mod} c)$ if and only if $c \mid a - b$.

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

Let us consider a. Then $|a|$ is a natural number.

We now state the proposition

(21) $a \mid b$ if and only if $|a| \mid |b|$.

Let us consider a, b. The functor $\operatorname{lcm}(a, b)$ yields an integer and is defined as follows:

(Def.2) $\operatorname{lcm}(a, b) = \operatorname{lcm}(|a|, |b|)$.

The following propositions are true:

(22) $\operatorname{lcm}(a, b) = \operatorname{lcm}(|a|, |b|)$.

(23) $\operatorname{lcm}(a, b)$ is a natural number.

(24) $\operatorname{lcm}(a, b) = \operatorname{lcm}(b, a)$.

(25) $a \mid \operatorname{lcm}(a, b)$.

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

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

Let us consider a, b. The functor $\gcd(a, b)$ yields an integer and is defined by:

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

One can prove the following propositions:

(28) $\gcd(a, b) = \gcd(|a|, |b|)$.

(29) $\gcd(a, b)$ is a natural number.

(30) $\gcd(a, b) = \gcd(b, a)$.

(31) $\gcd(a, b) \mid a$.

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

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

(34) $a = 0$ or $b = 0$ if and only if $\operatorname{lcm}(a, b) = 0$.

(35) $a = 0$ and $b = 0$ if and only if $\gcd(a, b) = 0$.

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

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

Next we state several propositions:

(36) a and b are relatively prime if and only if $\gcd(a, b) = 1$.

(37) If a and b are relatively prime, then b and a are relatively prime.

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

(39) If a and b are relatively prime, then $\gcd(c \cdot a, c \cdot b) = |c|$ and $\gcd(c \cdot a, b \cdot c) = |c|$ and $\gcd(a \cdot c, c \cdot b) = |c|$ and $\gcd(a \cdot c, b \cdot c) = |c|$.

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

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

In the sequel p, q, k, l will 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 $n = p$.

The following proposition is true

(42) p is prime if and only if $p > 1$ 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 relatively prime if and only if:

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

We now state several propositions:

(43) m and n are relatively prime if and only if $\gcd(m, n) = 1$.

(44) 2 is prime.

(45) There exists p such that p is prime.

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

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

In this article we present several logical schemes. The scheme *Ind1* concerns 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 conditions:

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

The scheme *Comp_Ind1* concerns 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 have the following property:

- 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 $\mathcal{P}[k]$.

Next we state the proposition

(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. *Formalized Mathematics*, 1(**1**):41–46, 1990.

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

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

Received July 10, 1990