FORMALIZED MATHEMATICS
Volume 6, Number 4, 1997
University of Białystok

The Chinese Remainder Theorem

Andrzej Kondracki
AMS Management Systems Poland
Warsaw

Summary. The article is a translation of the first chapters of a book *Wstęp do teorii liczb* (Eng. *Introduction to Number Theory*) by W. Sierpiński, WSiP, Biblioteczka Matematyczna, Warszawa, 1987. The first few pages of this book have already been formalized in MML. We prove the Chinese Remainder Theorem and Thue's Theorem as well as several useful number theory propositions.

MML Identifier: WSIERP_1.

The terminology and notation used in this paper are introduced in the following articles: [20], [16], [9], [14], [18], [1], [10], [13], [12], [15], [11], [17], [21], [6], [7], [2], [5], [3], [8], [4], and [19].

For simplicity, we follow the rules: x, y, z, w denote real numbers, a, b, c, d, e, f, g denote natural numbers, k, l, m, n, m_1, n_1 denote integers, and q denotes a rational number.

The following propositions are true:

(1) If $y \neq 0$, then $(\frac{x}{y})^a = \frac{x^a}{y^a}$.

(2) $x^2 = x \cdot x$ and $(-x)^2 = x^2$.

(3) $(-x)^{2 \cdot a} = x^{2 \cdot a}$ and $(-x)^{2 \cdot a+1} = -x^{2 \cdot a+1}$.

(4) If $x \neq 0$, then $x^a_{\mathbb{Z}} = x^a$.

(5) If $x \geqslant 0$ and $y \geqslant 0$ and $d > 0$ and $x^d = y^d$, then $x = y$.

(6) $x > \max(y, z)$ iff $x > y$ and $x > z$.

(7) If $x \leqslant 0$ and $y \geqslant z$, then $y - x \geqslant z$ and $y \geqslant z + x$.

(8) If $x \leqslant 0$ and $y > z$ or $x < 0$ and $y \geqslant z$, then $y > z + x$ and $y - x > z$.

Let us consider a, b. Then $\gcd(a, b)$ is a natural number. Let us observe that the functor $\gcd(a, b)$ is commutative.

Let us consider m, n. Then $m \gcd n$ is an integer. Let us observe that the functor $m \gcd n$ is commutative.

ISSN 1426–2630

Let us consider k, a. Then k^a is an integer.

Let us consider a, b. Then a^b is a natural number.

We now state a number of propositions:

(9) If $k \mid m$ and $k \mid n$, then $k \mid m+n$.

(10) If $k \mid m$ and $k \mid n$, then $k \mid m \cdot m_1 + n \cdot n_1$.

(11) If $m \gcd n = 1$ and $k \gcd n = 1$, then $m \cdot k \gcd n = 1$.

(12) If $\gcd(a,b) = 1$ and $\gcd(c,b) = 1$, then $\gcd(a \cdot c, b) = 1$.

(13) $0 \gcd m = |m|$ and $1 \gcd m = 1$.

(14) 1 and k are relative prime.

(15) If k and l are relative prime, then k^a and l are relative prime.

(16) If k and l are relative prime, then k^a and l^b are relative prime.

(17) If $k \gcd l = 1$, then $k \gcd l^b = 1$ and $k^a \gcd l^b = 1$.

(18) $|m| \mid k$ iff $m \mid k$.

(19) If $a \mid b$, then $a^c \mid b^c$.

(20) If $a \mid 1$, then $a = 1$.

(21) If $d \mid a$ and $\gcd(a,b) = 1$, then $\gcd(d,b) = 1$.

(22) If $k \neq 0$, then $k \mid l$ iff $\frac{l}{k}$ is an integer.

(23) If $a \leqslant b - c$, then $a \leqslant b$ and $c \leqslant b$.

In the sequel f_1, f_2, f_3 are finite sequences.

Next we state two propositions:

(24) If $a \in \operatorname{Seg} \operatorname{len} f_2$, then $a \in \operatorname{Seg} \operatorname{len}(f_2 \frown f_3)$.

(25) If $a \in \operatorname{Seg} \operatorname{len} f_3$, then $\operatorname{len} f_2 + a \in \operatorname{Seg} \operatorname{len}(f_2 \frown f_3)$.

Let f_4 be a finite sequence of elements of $\mathbb{R}$ and let us consider a. Then $f_4(a)$ is a real number.

Let f_5 be a finite sequence of elements of $\mathbb{Z}$ and let us consider a. Then $f_5(a)$ is an integer.

Let f_6 be a finite sequence of elements of $\mathbb{N}$ and let us consider a. Then $f_6(a)$ is a natural number.

Let D be a non empty set and let D_1 be a non empty subset of D. We see that the finite sequence of elements of D_1 is a finite sequence of elements of D.

Let D be a non empty set, let D_1 be a non empty subset of D, and let f_7, f_8 be finite sequences of elements of D_1. Then $f_7 \frown f_8$ is a finite sequence of elements of D_1.

Let D be a non empty set and let D_1 be a non empty subset of D. Then $\varepsilon_{(D_1)}$ is an empty finite sequence of elements of D_1.

$\mathbb{Z}$ is a non empty subset of $\mathbb{R}$.

For simplicity, we adopt the following convention: D, D_1 are non empty sets, v_1, v_2, v_3 are sets, f_6 is a finite sequence of elements of $\mathbb{N}$, f_5, f_9 are finite sequences of elements of $\mathbb{Z}$, and f_4 is a finite sequence of elements of $\mathbb{R}$.

Let us consider f_5. Then $\sum f_5$ is an integer. Then $\prod f_5$ is an integer.

Let us consider f_6. Then $\sum f_6$ is a natural number. Then $\prod f_6$ is a natural number.

Let us consider a, f_1. The functor $f_1 {\sim} a$ yielding a finite sequence is defined as follows:

(Def. 1)(i) $f_1 {\sim} a = f_1$ if $a \notin \operatorname{dom} f_1$,

(ii) $\operatorname{len}(f_1 {\sim} a) + 1 = \operatorname{len} f_1$ and for every b holds if $b < a$, then $(f_1 {\sim} a)(b) = f_1(b)$ and if $b \geqslant a$, then $(f_1 {\sim} a)(b) = f_1(b+1)$, otherwise.

Let us consider D, let us consider a, and let f_1 be a finite sequence of elements of D. Then $f_1 {\sim} a$ is a finite sequence of elements of D.

Let us consider D, let D_1 be a non empty subset of D, let us consider a, and let f_1 be a finite sequence of elements of D_1. Then $f_1 {\sim} a$ is a finite sequence of elements of D_1.

One can prove the following propositions:

(26) $\langle v_1 \rangle {\sim} 1 = \varepsilon$ and $\langle v_1, v_2 \rangle {\sim} 1 = \langle v_2 \rangle$ and $\langle v_1, v_2 \rangle {\sim} 2 = \langle v_1 \rangle$ and $\langle v_1, v_2, v_3 \rangle {\sim} 1 = \langle v_2, v_3 \rangle$ and $\langle v_1, v_2, v_3 \rangle {\sim} 2 = \langle v_1, v_3 \rangle$ and $\langle v_1, v_2, v_3 \rangle {\sim} 3 = \langle v_1, v_2 \rangle$.

(27) If $1 \leqslant a$ and $a \leqslant \operatorname{len} f_4$, then $\sum (f_4 {\sim} a) + f_4(a) = \sum f_4$.

(28) If $a \in \operatorname{Seg} \operatorname{len} f_6$ and $f_6(a) \neq 0$, then $\frac{\prod f_6}{f_6(a)}$ is a natural number.

(29) $\operatorname{num} q$ and $\operatorname{den} q$ are relative prime.

(30) If $q \neq 0$ and $q = \frac{k}{a}$ and $a \neq 0$ and k and a are relative prime, then $k = \operatorname{num} q$ and $a = \operatorname{den} q$.

(31) If there exists q such that $a = q^b$, then there exists k such that $a = k^b$.

(32) If there exists q such that $a = q^d$, then there exists b such that $a = b^d$.

(33) If $e > 0$ and $a^e \mid b^e$, then $a \mid b$.

(34) There exist m, n such that $\gcd(a, b) = a \cdot m + b \cdot n$.

(35) There exist m_1, n_1 such that $m \gcd n = m \cdot m_1 + n \cdot n_1$.

(36) If $m \mid n \cdot k$ and $m \gcd n = 1$, then $m \mid k$.

(37) If $\gcd(a, b) = 1$ and $a \mid b \cdot c$, then $a \mid c$.

(38) If $a \neq 0$ and $b \neq 0$, then there exist c, d such that $\gcd(a, b) = a \cdot c - b \cdot d$.

(39) If $f > 0$ and $g > 0$ and $\gcd(f, g) = 1$ and $a^f = b^g$, then there exists e such that $a = e^g$ and $b = e^f$.

In the sequel x, y, z, t denote integers.

Next we state several propositions:

(40) There exist x, y such that $m \cdot x + n \cdot y = k$ iff $m \gcd n \mid k$.

(41) Suppose $m \neq 0$ and $n \neq 0$ and $m \cdot m_1 + n \cdot n_1 = k$. Let given x, y. If $m \cdot x + n \cdot y = k$, then there exists t such that $x = m_1 + t \cdot \frac{n}{m \gcd n}$ and $y = n_1 - t \cdot \frac{m}{m \gcd n}$.

(42) If $\gcd(a, b) = 1$ and $a \cdot b = c^d$, then there exist e, f such that $a = e^d$ and $b = f^d$.

(43) For every d such that for every a such that $a \in \operatorname{Seg} \operatorname{len} f_6$ holds $\gcd(f_6(a), d) = 1$ holds $\gcd(\prod f_6, d) = 1$.

(44) Suppose $\operatorname{len} f_6 \geqslant 2$ and for all b, c such that $b \in \operatorname{Seg} \operatorname{len} f_6$ and $c \in \operatorname{Seg} \operatorname{len} f_6$ and $b \neq c$ holds $\gcd(f_6(b), f_6(c)) = 1$. Let given f_5. Suppose $\operatorname{len} f_5 = \operatorname{len} f_6$. Then there exists f_9 such that $\operatorname{len} f_9 = \operatorname{len} f_6$ and for every b such that $b \in \operatorname{Seg} \operatorname{len} f_6$ holds $f_6(b) \cdot f_9(b) + f_5(b) = f_6(1) \cdot f_9(1) + f_5(1)$.

(45) If $x < y$ and $z \geqslant w$ or $x \leqslant y$ and $z > w$ or $x < y$ and $z > w$, then $x - z < y - w$.

(46) If $a \neq 0$ and $a \gcd k = 1$, then there exist b, e such that $0 \neq b$ and $0 \neq e$ and $b \leqslant \sqrt{a}$ and $e \leqslant \sqrt{a}$ and $a \mid k \cdot b + e$ or $a \mid k \cdot b - e$.

References

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

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

[3] Grzegorz Bancerek and Piotr Rudnicki. Two programs for **scm**. Part I - preliminaries. *Formalized Mathematics*, 4(**1**):69–72, 1993.

[4] Józef Białas and Yatsuka Nakamura. Dyadic numbers and T_4 topological spaces. *Formalized Mathematics*, 5(**3**):361–366, 1996.

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

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

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

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

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

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

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

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

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

[14] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

[15] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

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

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

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

[19] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

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

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

Received December 30, 1997