JOURNAL OF FORMALIZED MATHEMATICS
Volume 9, Released 1997, Published 2003
Inst. of Computer Science, Univ. 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`.

WWW: `http://mizar.org/JFM/Vol9/wsierp_1.html`

The articles [11], [16], [2], [12], [14], [1], [8], [10], [13], [17], [5], [4], [6], [7], [15], [3], and [9] provide the notation and terminology for this paper.

For simplicity, we adopt the following rules: x, y, z 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:

(2)[1] $x^2 = x \cdot x$ and $(-x)^2 = x^2$.

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

(5)[2] If $x \geq 0$ and $y \geq 0$ and $d > 0$ and $x^d = y^d$, then $x = y$.

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

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

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

Let us consider k, a. Observe that k^a is integer.

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

Next we 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 $1 \gcd m = 1$.

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

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

(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 $k \operatorname{gcd} l = 1$, then $k \operatorname{gcd} l^b = 1$ and $k^a \operatorname{gcd} l^b = 1$.

(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 $a \leq b - c$, then $a \leq b$ and $c \leq b$.

In the sequel f_1 denotes a finite sequence.

Let f be a finite sequence of elements of $\mathbb{Z}$ and let a be a set. Note that $f(a)$ is integer.

Let f_2 be a finite sequence of elements of $\mathbb{N}$ and let us consider a. Then $f_2(a)$ is a natural number.

Let D be a non empty set, let D_1 be a non empty subset of D, and let f_3, f_4 be finite sequences of elements of D_1. Then $f_3 \frown f_4$ 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 use the following convention: D is a non empty set, v, v_1, v_2, v_3 are sets, f_2 is a finite sequence of elements of $\mathbb{N}$, f_5, f_6 are finite sequences of elements of $\mathbb{Z}$, and f_7 is a finite sequence of elements of $\mathbb{R}$.

Let us consider f_5. Then $\sum f_5$ is an element of $\mathbb{Z}$. Then $\prod f_5$ is an element of $\mathbb{Z}$.

Let us consider f_2. Then $\sum f_2$ is a natural number. Then $\prod f_2$ is a natural number.

Let us consider a, f_1. Then $(f_1)_{\restriction a}$ can be characterized by the condition:

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

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

Let us consider D, let us consider a, and let f_1 be a finite sequence of elements of D. Then $(f_1)_{\restriction a}$ 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 $(f_1)_{\restriction a}$ is a finite sequence of elements of D_1.

We now state a number of propositions:

(26)[3] $\langle v_1 \rangle_{\restriction 1} = \emptyset$ and $\langle v_1, v_2 \rangle_{\restriction 1} = \langle v_2 \rangle$ and $\langle v_1, v_2 \rangle_{\restriction 2} = \langle v_1 \rangle$ and $\langle v_1, v_2, v_3 \rangle_{\restriction 1} = \langle v_2, v_3 \rangle$ and $\langle v_1, v_2, v_3 \rangle_{\restriction 2} = \langle v_1, v_3 \rangle$ and $\langle v_1, v_2, v_3 \rangle_{\restriction 3} = \langle v_1, v_2 \rangle$.

(27) If $a \in \operatorname{dom} f_7$, then $\sum((f_7)_{\restriction a}) + f_7(a) = \sum f_7$.

(28) If $a \in \operatorname{dom} f_2$, then $\frac{\prod f_2}{f_2(a)}$ 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 $a = b^d$.

[3] The propositions (24) and (25) have been removed.

(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, t denote integers.
We now 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 $a \in \operatorname{dom} f_2$ holds $\gcd(f_2(a), d) = 1$ holds $\gcd(\prod f_2, d) = 1$.

(44) Suppose $\operatorname{len} f_2 \geq 2$ and for all b, c such that $b \in \operatorname{dom} f_2$ and $c \in \operatorname{dom} f_2$ and $b \neq c$ holds $\gcd(f_2(b), f_2(c)) = 1$. Let given f_5. Suppose $\operatorname{len} f_5 = \operatorname{len} f_2$. Then there exists f_6 such that $\operatorname{len} f_6 = \operatorname{len} f_2$ and for every b such that $b \in \operatorname{dom} f_2$ holds $f_2(b) \cdot f_6(b) + f_5(b) = f_2(1) \cdot f_6(1) + f_5(1)$.

(46)[4] If $a \neq 0$ and $a \gcd k = 1$, then there exist b, e such that $0 \neq b$ and $0 \neq e$ and $b \leq \sqrt{a}$ and $e \leq \sqrt{a}$ and $a \mid k \cdot b + e$ or $a \mid k \cdot b - e$.

(47) $\operatorname{dom}((f_1)_{\restriction a}) \subseteq \operatorname{dom} f_1$.

(48) $(\langle v \rangle \frown f_1)_{\restriction 1} = f_1$ and $(f_1 \frown \langle v \rangle)_{\restriction \operatorname{len} f_1 + 1} = f_1$.

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] Grzegorz Bancerek. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal1.html.

[3] Grzegorz Bancerek. Joining of decorated trees. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/trees_4.html.

[4] 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.

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

[6] Czesław Byliński. The sum and product of finite sequences of real numbers. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/rvsum_1.html.

[7] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Journal of Formalized Mathematics*, 4, 1992. http://mizar.org/JFM/Vol4/matrix_2.html.

[8] Andrzej Kondracki. Basic properties of rational numbers. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/rat_1.html.

[9] Jarosław Kotowicz and Yatsuka Nakamura. Introduction to Go-Board — part I. *Journal of Formalized Mathematics*, 4, 1992. http://mizar.org/JFM/Vol4/goboard1.html.

[4] The proposition (45) has been removed.

[10] 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.

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

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

[13] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers operations: min, max, square, and square root. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/square_1.html.

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

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

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

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

Received December 30, 1997

Published January 2, 2004