FORMALIZED MATHEMATICS
Vol. **16**, No. **3**, Pages 247–252, **2008**

Modular Integer Arithmetic[1]

Christoph Schwarzweller
Institute of Computer Science
University of Gdańsk
Wita Stwosza 57, 80-952 Gdańsk, Poland

Summary. In this article we show the correctness of integer arithmetic based on Chinese Remainder theorem as described e.g. in [11]: Integers are transformed to finite sequences of modular integers, on which the arithmetic operations are performed. Retransformation of the results to the integers is then accomplished by means of the Chinese Remainder theorem. The method presented is a typical example for computing in homomorphic images.

MML identifier: `INT_6`, version: `7.9.01 4.103.1019`

The terminology and notation used here are introduced in the following articles: [10], [9], [8], [2], [7], [5], [4], [3], [6], and [1].

1. Preliminaries

Let f be a finite sequence. Note that $f{\restriction}0$ is empty.

Let f be a complex-valued finite sequence and let n be a natural number. Observe that $f{\restriction}n$ is complex-valued.

Let f be an integer-valued finite sequence and let n be a natural number. Note that $f{\restriction}n$ is integer-valued.

Let f be an integer-valued finite sequence and let n be a natural number. Observe that $f_{\lfloor n}$ is integer-valued.

Let i be an integer. Observe that $\langle i \rangle$ is integer-valued.

Let f, g be integer-valued finite sequences. Note that $f \frown g$ is integer-valued.

One can prove the following propositions:

[1] This work has been partially supported by grant BW 5100-5-0293-7.

ISSN 1426–2630(p), 1898-9934(e)

(1) For all complex-valued finite sequences f_1, f_2 holds $\mathrm{len}(f_1 + f_2) = \min(\mathrm{len}\, f_1, \mathrm{len}\, f_2)$.

(2) For all complex-valued finite sequences f_1, f_2 holds $\mathrm{len}(f_1 - f_2) = \min(\mathrm{len}\, f_1, \mathrm{len}\, f_2)$.

(3) For all complex-valued finite sequences f_1, f_2 holds $\mathrm{len}(f_1\, f_2) = \min(\mathrm{len}\, f_1, \mathrm{len}\, f_2)$.

(4) Let m_1, m_2 be complex-valued finite sequences. Suppose $\mathrm{len}\, m_1 = \mathrm{len}\, m_2$. Let k be a natural number. If $k \leq \mathrm{len}\, m_1$, then $(m_1\, m_2){\restriction}k = (m_1{\restriction}k)\,(m_2{\restriction}k)$.

Let F be an integer-valued finite sequence. Note that $\sum F$ is integer and $\prod F$ is integer.

Next we state several propositions:

(5) Let f be a complex-valued finite sequence and i be a natural number. If $i + 1 \leq \mathrm{len}\, f$, then $(f{\restriction}i) \frown \langle f(i+1) \rangle = f{\restriction}(i+1)$.

(6) For every complex-valued finite sequence f such that there exists a natural number i such that $i \in \mathrm{dom}\, f$ and $f(i) = 0$ holds $\prod f = 0$.

(7) For all integers n, a, b holds $(a - b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n$.

(8) For all integers i, j, k such that $i \mid j$ holds $k \cdot i \mid k \cdot j$.

(9) Let m be an integer-valued finite sequence and i be a natural number. If $i \in \mathrm{dom}\, m$ and $m_i \neq 0$, then $\frac{\prod m}{m_i}$ is an integer.

(10) Let m be an integer-valued finite sequence and i be a natural number. If $i \in \mathrm{dom}\, m$, then there exists an integer z such that $z \cdot m_i = \prod m$.

(11) Let m be an integer-valued finite sequence and i, j be natural numbers. If i, $j \in \mathrm{dom}\, m$ and $j \neq i$ and $m_j \neq 0$, then $\frac{\prod m}{m_i \cdot m_j}$ is an integer.

(12) Let m be an integer-valued finite sequence and i, j be natural numbers. Suppose i, $j \in \mathrm{dom}\, m$ and $j \neq i$ and $m_j \neq 0$. Then there exists an integer z such that $z \cdot m_i = \frac{\prod m}{m_j}$.

2. More on Greatest Common Divisors

Next we state a number of propositions:

(13) For every integer i holds $|i| \mid i$ and $i \mid |i|$.

(14) For all integers i, j holds $i \gcd j = i \gcd |j|$.

(15) For all integers i, j such that i and j are relative prime holds $\mathrm{lcm}(i, j) = |i \cdot j|$.

(16) For all integers i, j, k holds $i \cdot j \gcd i \cdot k = |i| \cdot (j \gcd k)$.

(17) For all integers i, j holds $i \cdot j \gcd i = |i|$.

(18) For all integers i, j, k holds $i \gcd j \gcd k = i \gcd j \gcd k$.

(19) For all integers i, j, k such that i and j are relative prime holds $i \gcd j \cdot k = i \gcd k$.

(20) For all integers i, j such that i and j are relative prime holds $i \cdot j \mid \operatorname{lcm}(i, j)$.

(21) For all integers x, y, i, j such that i and j are relative prime holds if $x \equiv y \pmod{i}$ and $x \equiv y \pmod{j}$, then $x \equiv y \pmod{i \cdot j}$.

(22) For all integers i, j such that i and j are relative prime there exists an integer s such that $s \cdot i \equiv 1 \pmod{j}$.

3. Chinese Remainder Sequences

Let f be an integer-valued finite sequence. We introduce f is multiplicative-trivial as an antonym of f is non-empty.

Let f be an integer-valued finite sequence. Let us observe that f is multiplicative-trivial if and only if:

(Def. 1) There exists a natural number i such that $i \in \operatorname{dom} f$ and $f_i = 0$.

One can verify the following observations:

- ∗ there exists an integer-valued finite sequence which is multiplicative-trivial,
- ∗ there exists an integer-valued finite sequence which is non multiplicative-trivial, and
- ∗ there exists an integer-valued finite sequence which is non empty and positive yielding.

The following proposition is true

(23) For every multiplicative-trivial integer-valued finite sequence m holds $\prod m = 0$.

Let f be an integer-valued finite sequence. We say that f is Chinese remainder if and only if:

(Def. 2) For all natural numbers i, j such that i, $j \in \operatorname{dom} f$ and $i \neq j$ holds f_i and f_j are relative prime.

One can verify that there exists an integer-valued finite sequence which is non empty, positive yielding, and Chinese remainder.

A CR-sequence is a non empty positive yielding Chinese remainder integer-valued finite sequence.

Let us note that every CR-sequence is non multiplicative-trivial.

One can verify that every integer-valued finite sequence which is multiplicative-trivial is also non empty.

We now state the proposition

(24) For every CR-sequence f and for every natural number m such that $0 < m \leq \operatorname{len} f$ holds $f{\restriction}m$ is a CR-sequence.

Let m be a CR-sequence. Observe that $\prod m$ is positive and natural.

Next we state the proposition

(25) Let m be a CR-sequence and i be a natural number. If $i \in \operatorname{dom} m$, then for every integer m_3 such that $m_3 = \frac{\prod m}{m_i}$ holds

4. Integer Arithmetic based on CRT

let u be an integer and let m be an integer-valued finite sequence. The functor $\operatorname{mod}(u, m)$ yields a finite sequence and is defined as follows:

(Def. 3) $\operatorname{len} \operatorname{mod}(u, m) = \operatorname{len} m$ and for every natural number i such that $i \in \operatorname{dom} \operatorname{mod}(u, m)$ holds $(\operatorname{mod}(u, m))_i = u \bmod m_i$.

Let u be an integer and let m be an integer-valued finite sequence. Observe that $\operatorname{mod}(u, m)$ is integer-valued.

Let m be a CR-sequence. A finite sequence is called a CR-coefficient sequence for m if it satisfies the conditions (Def. 4).

(Def. 4)(i) $\operatorname{len} \mathrm{it} = \operatorname{len} m$, and

(ii) for every natural number i such that $i \in \operatorname{dom} \mathrm{it}$ there exists an integer s and there exists an integer m_3 such that $m_3 = \frac{\prod m}{m_i}$ and $s \cdot m_3 \equiv 1 \pmod{m_i}$ and $\mathrm{it}_i = s \cdot \frac{\prod m}{m_i}$.

Let m be a CR-sequence. Note that every CR-coefficient sequence for m is integer-valued.

Next we state several propositions:

(26) Let m be a CR-sequence, c be a CR-coefficient sequence for m, and i be a natural number. If $i \in \operatorname{dom} c$, then $c_i \equiv 1 \pmod{m_i}$.

(27) Let m be a CR-sequence, c be a CR-coefficient sequence for m, and i, j be natural numbers. If i, $j \in \operatorname{dom} c$ and $i \neq j$, then $c_i \equiv 0 \pmod{m_j}$.

(28) Let m be a CR-sequence, c_1, c_2 be CR-coefficient sequences for m, and i be a natural number. If $i \in \operatorname{dom} c_1$, then $(c_1)_i \equiv (c_2)_i \pmod{m_i}$.

(29) Let u be an integer-valued finite sequence and m be a CR-sequence. Suppose $\operatorname{len} m = \operatorname{len} u$. Let c be a CR-coefficient sequence for m and i be a natural number. If $i \in \operatorname{dom} m$, then $\sum u\, c \equiv u_i \pmod{m_i}$.

(30) Let u be an integer-valued finite sequence and m be a CR-sequence. Suppose $\operatorname{len} m = \operatorname{len} u$. Let c_1, c_2 be CR-coefficient sequences for m. Then $\sum u\, c_1 \equiv \sum u\, c_2 \pmod{\prod m}$.

Let u be an integer-valued finite sequence and let m be a CR-sequence. Let us assume that $\operatorname{len} m = \operatorname{len} u$. The functor $\mathbb{Z}(u, m)$ yields an integer and is defined as follows:

(Def. 5) For every CR-coefficient sequence c for m holds $\mathbb{Z}(u,m) = (\sum u\,c) \bmod \prod m$.

We now state a number of propositions:

(31) For every integer-valued finite sequence u and for every CR-sequence m such that $\operatorname{len} m = \operatorname{len} u$ holds $0 \leq \mathbb{Z}(u,m) < \prod m$.

(32) For every integer u and for every CR-sequence m and for every natural number i such that $i \in \operatorname{dom} m$ holds $u \equiv (\operatorname{mod}(u,m))_i \pmod{m_i}$.

(33) Let u, v be integers, m be a CR-sequence, and i be a natural number. If $i \in \operatorname{dom} m$, then $(\operatorname{mod}(u,m) + \operatorname{mod}(v,m))_i \equiv u + v \pmod{m_i}$.

(34) Let u, v be integers, m be a CR-sequence, and i be a natural number. If $i \in \operatorname{dom} m$, then $(\operatorname{mod}(u,m)\ \operatorname{mod}(v,m))_i \equiv u \cdot v \pmod{m_i}$.

(35) Let u, v be integers, m be a CR-sequence, and i be a natural number. If $i \in \operatorname{dom} m$, then $\mathbb{Z}(\operatorname{mod}(u,m) + \operatorname{mod}(v,m), m) \equiv u + v \pmod{m_i}$.

(36) Let u, v be integers, m be a CR-sequence, and i be a natural number. If $i \in \operatorname{dom} m$, then $\mathbb{Z}(\operatorname{mod}(u,m) - \operatorname{mod}(v,m), m) \equiv u - v \pmod{m_i}$.

(37) Let u, v be integers, m be a CR-sequence, and i be a natural number. If $i \in \operatorname{dom} m$, then $\mathbb{Z}(\operatorname{mod}(u,m)\ \operatorname{mod}(v,m), m) \equiv u \cdot v \pmod{m_i}$.

(38) For all integers u, v and for every CR-sequence m such that $0 \leq u+v < \prod m$ holds $\mathbb{Z}(\operatorname{mod}(u,m) + \operatorname{mod}(v,m), m) = u + v$.

(39) For all integers u, v and for every CR-sequence m such that $0 \leq u-v < \prod m$ holds $\mathbb{Z}(\operatorname{mod}(u,m) - \operatorname{mod}(v,m), m) = u - v$.

(40) For all integers u, v and for every CR-sequence m such that $0 \leq u \cdot v < \prod m$ holds $\mathbb{Z}(\operatorname{mod}(u,m)\ \operatorname{mod}(v,m), m) = u \cdot v$.

5. Chinese Remainder Theorem Revisited

We now state two propositions:

(41) Let u be an integer-valued finite sequence and m be a CR-sequence. Suppose $\operatorname{len} u = \operatorname{len} m$. Then there exists an integer z such that $0 \leq z < \prod m$ and for every natural number i such that $i \in \operatorname{dom} u$ holds $z \equiv u_i \pmod{m_i}$.

(42) Let u be an integer-valued finite sequence, m be a CR-sequence, and z_1, z_2 be integers. Suppose that

(i) $0 \leq z_1$,

(ii) $z_1 < \prod m$,

(iii) for every natural number i such that $i \in \operatorname{dom} m$ holds $z_1 \equiv u_i \pmod{m_i}$,

(iv) $0 \leq z_2$,

(v) $z_2 < \prod m$, and

(vi) for every natural number i such that $i \in \operatorname{dom} m$ holds $z_2 \equiv u_i \pmod{m_i}$.

Then $z_1 = z_2$.

References

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

[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

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

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

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

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

[7] Artur Korniłowicz. On the real valued functions. *Formalized Mathematics*, 13(**1**):181–187, 2005.

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

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

[10] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[11] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.

Received May 13, 2008