FORMALIZED MATHEMATICS
Vol. 20, No. 2, Pages 175–179, 2012
DOI: 10.2478/v10037-012-0020-2

VERSITA
versita.com/fm/

Extended Euclidean Algorithm and CRT Algorithm[1]

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yosiki Aoki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article we formalize some number theoretical algorithms, Euclidean Algorithm and Extended Euclidean Algorithm [9]. Besides the a gcd b, Extended Euclidean Algorithm can calculate a pair of two integers (x, y) that holds $ax + by = a$ gcd b. In addition, we formalize an algorithm that can compute a solution of the Chinese remainder theorem by using Extended Euclidean Algorithm. Our aim is to support the implementation of number theoretic tools. Our formalization of those algorithms is based on the source code of the NZMATH, a number theory oriented calculation system developed by Tokyo Metropolitan University [8].

MML identifier: `NTALGO_1`, version: `7.12.02 4.181.1147`

The terminology and notation used in this paper have been introduced in the following papers: [3], [4], [5], [12], [10], [11], [1], [2], [7], [13], and [6].

1. Euclidean Algorithm

One can prove the following proposition

(1) For all integers x, p holds $x \bmod p \bmod p = x \bmod p$.

Let a, b be elements of $\mathbb{Z}$. The functor $\mathrm{ALGO}_{\mathrm{GCD}}(a, b)$ yielding an element of $\mathbb{N}$ is defined by the condition (Def. 1).

(Def. 1) There exist sequences A, B of $\mathbb{N}$ such that

(i) $A(0) = |a|$,

(ii) $B(0) = |b|$,

[1]This work was supported by JSPS KAKENHI 21240001 and 22300285.

ISSN 1426–2630(p), 1898-9934(e)

(iii) for every element i of $\mathbb{N}$ holds $A(i+1) = B(i)$ and $B(i+1) = A(i) \bmod B(i)$, and

(iv) $\mathrm{ALGO}_{\mathrm{GCD}}(a, b) = A(\min^*\{i \in \mathbb{N}\colon B(i) = 0\})$.

Next we state the proposition

(2) For all elements a, b of $\mathbb{Z}$ holds $\mathrm{ALGO}_{\mathrm{GCD}}(a, b) = a \gcd b$.

2. Extended Euclidean Algorithm

The scheme *QuadChoiceRec* deals with non empty sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$, an element $\mathcal{E}$ of $\mathcal{A}$, an element $\mathcal{F}$ of $\mathcal{B}$, an element $\mathcal{G}$ of $\mathcal{C}$, an element $\mathcal{H}$ of $\mathcal{D}$, and a 9-ary predicate $\mathcal{P}$, and states that:

> There exists a function f from $\mathbb{N}$ into $\mathcal{A}$ and there exists a function g from $\mathbb{N}$ into $\mathcal{B}$ and there exists a function h from $\mathbb{N}$ into $\mathcal{C}$ and there exists a function i from $\mathbb{N}$ into $\mathcal{D}$ such that $f(0) = \mathcal{E}$ and $g(0) = \mathcal{F}$ and $h(0) = \mathcal{G}$ and $i(0) = \mathcal{H}$ and for every element n of $\mathbb{N}$ holds $\mathcal{P}[n, f(n), g(n), h(n), i(n), f(n+1), g(n+1), h(n+1), i(n+1)]$

provided the parameters satisfy the following condition:

- Let n be an element of $\mathbb{N}$, x be an element of $\mathcal{A}$, y be an element of $\mathcal{B}$, z be an element of $\mathcal{C}$, and w be an element of $\mathcal{D}$. Then there exists an element x_1 of $\mathcal{A}$ and there exists an element y_1 of $\mathcal{B}$ and there exists an element z_1 of $\mathcal{C}$ and there exists an element w_1 of $\mathcal{D}$ such that $\mathcal{P}[n, x, y, z, w, x_1, y_1, z_1, w_1]$.

Let x, y be elements of $\mathbb{Z}$. The functor $\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y)$ yielding an element of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is defined by the condition (Def. 2).

(Def. 2) There exist sequences g, w, q, t of $\mathbb{Z}$ and there exist sequences a, b, v, u of $\mathbb{Z}$ and there exists an element i_1 of $\mathbb{N}$ such that $a(0) = 1$ and $b(0) = 0$ and $g(0) = x$ and $q(0) = 0$ and $u(0) = 0$ and $v(0) = 1$ and $w(0) = y$ and $t(0) = 0$ and for every element i of $\mathbb{N}$ holds $q(i+1) = g(i) \operatorname{div} w(i)$ and $t(i+1) = g(i) \bmod w(i)$ and $a(i+1) = u(i)$ and $b(i+1) = v(i)$ and $g(i+1) = w(i)$ and $u(i+1) = a(i) - q(i+1) \cdot u(i)$ and $v(i+1) = b(i) - q(i+1) \cdot v(i)$ and $w(i+1) = t(i+1)$ and $i_1 = \min^*\{i \in \mathbb{N}\colon w(i) = 0\}$ and if $0 \leq g(i_1)$, then $\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y) = \langle a(i_1), b(i_1), g(i_1) \rangle$ and if $g(i_1) < 0$, then $\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y) = \langle -a(i_1), -b(i_1), -g(i_1) \rangle$.

One can prove the following propositions:

(3) For all integers i_3, i_2 such that $i_3 \leq 0$ holds $i_2 \bmod i_3 \leq 0$.

(4) For all integers i_3, i_2 such that $i_3 < 0$ holds $-(i_2 \bmod i_3) < -i_3$.

(5) For all elements x, y of $\mathbb{Z}$ such that $|y| \neq 0$ holds $|x \bmod y| < |y|$.

(6) For all elements x, y of $\mathbb{Z}$ holds $(\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y))_{\mathbf{3},3} = x \gcd y$ and $(\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y))_{\mathbf{1},3} \cdot x + (\mathrm{ALGO}_{\mathrm{EXGCD}}(x, y))_{\mathbf{2},3} \cdot y = x \gcd y$.

Let x, p be elements of $\mathbb{Z}$. The functor $\mathrm{ALGO}_{\mathrm{INVERSE}}(x, p)$ yielding an element of $\mathbb{Z}$ is defined by the condition (Def. 3).

(Def. 3) Let y be an element of $\mathbb{Z}$ such that $y = x \bmod p$. Then

(i) if $(\mathrm{ALGO}_{\mathrm{EXGCD}}(p, y))_{\mathbf{3},3} = 1$, then if $(\mathrm{ALGO}_{\mathrm{EXGCD}}(p, y))_{\mathbf{2},3} < 0$, then there exists an element z of $\mathbb{Z}$ such that $z = (\mathrm{ALGO}_{\mathrm{EXGCD}}(p, y))_{\mathbf{2},3}$ and $\mathrm{ALGO}_{\mathrm{INVERSE}}(x, p) = p + z$ and if $0 \leq (\mathrm{ALGO}_{\mathrm{EXGCD}}(p, y))_{\mathbf{2},3}$, then $\mathrm{ALGO}_{\mathrm{INVERSE}}(x, p) = (\mathrm{ALGO}_{\mathrm{EXGCD}}(p, y))_{\mathbf{2},3}$, and

(ii) if $(\mathrm{ALGO}_{\mathrm{EXGCD}}(p, y))_{\mathbf{3},3} \neq 1$, then $\mathrm{ALGO}_{\mathrm{INVERSE}}(x, p) = \emptyset$.

Next we state the proposition

(7) For all elements x, p, y of $\mathbb{Z}$ such that $y = x \bmod p$ and $(\mathrm{ALGO}_{\mathrm{EXGCD}}(p, y))_{\mathbf{3},3} = 1$ holds $\mathrm{ALGO}_{\mathrm{INVERSE}}(x, p) \cdot x \bmod p = 1 \bmod p$.

3. CRT ALGORITHM

Let n_1 be a non empty finite sequence of elements of $\mathbb{Z} \times \mathbb{Z}$. The functor $\mathrm{ALGO}_{\mathrm{CRT}}\, n_1$ yielding an element of $\mathbb{Z}$ is defined by the conditions (Def. 4).

(Def. 4)(i) If $\operatorname{len} n_1 = 1$, then $\mathrm{ALGO}_{\mathrm{CRT}}\, n_1 = n_1(1)_{\mathbf{1}}$, and

(ii) if $\operatorname{len} n_1 \neq 1$, then there exist finite sequences m, n, p_1, p_2 of elements of $\mathbb{Z}$ and there exist elements M_0, M of $\mathbb{Z}$ such that $\operatorname{len} m = \operatorname{len} n_1$ and $\operatorname{len} n = \operatorname{len} n_1$ and $\operatorname{len} p_1 = \operatorname{len} n_1 - 1$ and $\operatorname{len} p_2 = \operatorname{len} n_1 - 1$ and $m(1) = 1$ and for every natural number i such that $1 \leq i \leq \operatorname{len} m - 1$ there exist elements d, x, y of $\mathbb{Z}$ such that $x = n_1(i)_{\mathbf{2}}$ and $m(i+1) = m(i) \cdot x$ and $y = m(i+1)$ and $d = n_1(i+1)_{\mathbf{2}}$ and $p_2(i) = \mathrm{ALGO}_{\mathrm{INVERSE}}(y, d)$ and $p_1(i) = y$ and $M_0 = n_1(\operatorname{len} m)_{\mathbf{2}}$ and $M = p_1(\operatorname{len} m - 1) \cdot M_0$ and $n(1) = n_1(1)_{\mathbf{1}}$ and for every natural number i such that $1 \leq i \leq \operatorname{len} m - 1$ there exist elements u, u_0, u_1 of $\mathbb{Z}$ such that $u_0 = n_1(i+1)_{\mathbf{1}}$ and $u_1 = n_1(i+1)_{\mathbf{2}}$ and $u = (u_0 - n(i)) \cdot p_2(i) \bmod u_1$ and $n(i+1) = n(i) + u \cdot p_1(i)$ and $\mathrm{ALGO}_{\mathrm{CRT}}\, n_1 = n(\operatorname{len} m) \bmod M$.

One can prove the following propositions:

(8) For all elements a, b of $\mathbb{Z}$ such that $b \neq 0$ holds $a \bmod b \equiv a \pmod{b}$.

(9) For all elements a, b of $\mathbb{Z}$ such that $b \neq 0$ holds $a \bmod b \gcd b = a \gcd b$.

(10) Let a, b, c be elements of $\mathbb{Z}$. Suppose $c \neq 0$ and $a = b \bmod c$ and b and c are relative prime. Then a and c are relative prime.

(11) Let n_1 be a non empty finite sequence of elements of $\mathbb{Z} \times \mathbb{Z}$ and a, b be finite sequences of elements of $\mathbb{Z}$. Suppose that

(i) $\operatorname{len} a = \operatorname{len} b$,

(ii) $\operatorname{len} a = \operatorname{len} n_1$,

(iii) for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} n_1$ holds $b(i) \neq 0$,

(iv) for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} n_1$ holds $n_1(i)_{\mathbf{1}} = a(i)$ and $n_1(i)_{\mathbf{2}} = b(i)$, and

(v) for all natural numbers i, j such that i, $j \in \operatorname{Seg} \operatorname{len} n_1$ and $i \neq j$ holds $b(i)$ and $b(j)$ are relative prime.

Let i be a natural number. If $i \in \operatorname{Seg} \operatorname{len} n_1$, then $\mathrm{ALGO}_{\mathrm{CRT}}\, n_1 \bmod b(i) = a(i) \bmod b(i)$.

(12) Let x, y be elements of $\mathbb{Z}$ and b, m be non empty finite sequences of elements of $\mathbb{Z}$. Suppose that

(i) $2 \leq \operatorname{len} b$,

(ii) for all natural numbers i, j such that i, $j \in \operatorname{Seg} \operatorname{len} b$ and $i \neq j$ holds $b(i)$ and $b(j)$ are relative prime,

(iii) for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} b$ holds $x \bmod b(i) = y \bmod b(i)$, and

(iv) $m(1) = 1$.

Let k be an element of $\mathbb{N}$. Suppose $1 \leq k \leq \operatorname{len} b$ and for every natural number i such that $1 \leq i \leq k$ holds $m(i+1) = m(i) \cdot b(i)$. Then $x \bmod m(k+1) = y \bmod m(k+1)$.

(13) For every finite sequence b of elements of $\mathbb{Z}$ such that $\operatorname{len} b = 1$ holds $\prod b = b(1)$.

(14) Let b be a finite sequence of elements of $\mathbb{Z}$. Then there exists a non empty finite sequence m of elements of $\mathbb{Z}$ such that $\operatorname{len} m = \operatorname{len} b + 1$ and $m(1) = 1$ and for every natural number i such that $1 \leq i \leq \operatorname{len} b$ holds $m(i+1) = m(i) \cdot b(i)$ and $\prod b = m(\operatorname{len} b + 1)$.

(15) Let n_1 be a non empty finite sequence of elements of $\mathbb{Z} \times \mathbb{Z}$, a, b be non empty finite sequences of elements of $\mathbb{Z}$, and x, y be elements of $\mathbb{Z}$. Suppose that $\operatorname{len} a = \operatorname{len} b$ and $\operatorname{len} a = \operatorname{len} n_1$ and for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} n_1$ holds $b(i) \neq 0$ and for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} n_1$ holds $n_1(i)_{\mathbf{1}} = a(i)$ and $n_1(i)_{\mathbf{2}} = b(i)$ and for all natural numbers i, j such that i, $j \in \operatorname{Seg} \operatorname{len} n_1$ and $i \neq j$ holds $b(i)$ and $b(j)$ are relative prime and for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} n_1$ holds $x \bmod b(i) = a(i) \bmod b(i)$ and $y = \prod b$. Then $\mathrm{ALGO}_{\mathrm{CRT}}\, n_1 \bmod y = x \bmod y$.

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. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

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

[6] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

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

[8] NZMATH development Group. `http://tnt.math.se.tmu.ac.jp/nzmath/`.
[9] Donald E. Knuth. *Art of Computer Programming*. Volume 2: Seminumerical Algorithms, 3rd Edition, Addison-Wesley Professional, 1997.
[10] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[11] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[12] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[13] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received February 8, 2012