Extended Euclidean Algorithm and CRT Algorithm

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 \( \text{gcd} \), Extended Euclidean Algorithm can calculate a pair of two integers \((x, y)\) that holds \(ax + by = \text{gcd}(a, b)\). 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].

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 \(x \mod p = x \mod p\).

Let \(a, b\) be elements of \(\mathbb{Z}\). The functor \(\text{ALGO}GCD(a, b)\) 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) \(B(0) = |b|\).
(iii) for every element \( i \) of \( \mathbb{N} \) holds \( A(i + 1) = B(i) \) and \( B(i + 1) = A(i) \mod B(i) \), and

(iv) \( \text{ALGO}_{\text{GCD}}(a, b) = A(\min\{i \in \mathbb{N} : B(i) = 0\}) \).

Next we state the proposition

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

2. Extended Euclidean Algorithm

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

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

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

Let \( x, y \) be elements of \( \mathbb{Z} \). The functor \( \text{ALGO}_{\text{EXGCD}}(x, y) \) 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

\[
\begin{align*}
\qquad a(0) &= 1 \quad \text{and} \quad b(0) = 0 \quad \text{and} \quad g(0) = x \quad \text{and} \quad q(0) = 0 \quad \text{and} \quad u(0) = 0 \\
\qquad v(0) &= 1 \quad \text{and} \quad w(0) = y \quad \text{and} \quad t(0) = 0 \quad \text{and} \quad \text{for every element} \quad i \quad \text{of} \quad \mathbb{N} \quad \text{holds} \\
\qquad q(i + 1) &= g(i) \div w(i) \quad \text{and} \quad t(i + 1) = g(i) \mod w(i) \quad \text{and} \quad a(i + 1) = u(i) \quad \text{and} \\
\qquad b(i + 1) &= v(i) \quad \text{and} \quad g(i + 1) = w(i) \quad \text{and} \quad u(i + 1) = a(i) - q(i + 1) \cdot u(i) \quad \text{and} \\
\qquad v(i + 1) &= b(i) - q(i + 1) \cdot v(i) \quad \text{and} \quad w(i + 1) = t(i + 1) \quad \text{and} \quad i_1 = \min\{i \in \mathbb{N} : w(i) = 0\} \quad \text{and} \quad \text{if} \quad 0 \leq g(i_1) \quad \text{then} \quad \text{ALGO}_{\text{EXGCD}}(x, y) = \langle a(i_1), b(i_1), g(i_1) \rangle \\
\end{align*}
\]

One can prove the following propositions:

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

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

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

(6) For all elements \( x, y \) of \( \mathbb{Z} \) holds \( \text{ALGO}_{\text{EXGCD}}(x, y))_{3,3} = x \gcd y \) and \( \text{ALGO}_{\text{EXGCD}}(x, y))_{1,3} \cdot x + (\text{ALGO}_{\text{EXGCD}}(x, y))_{2,3} \cdot y = x \gcd y \).
Let \( x, p \) be elements of \( \mathbb{Z} \). The functor \( \text{ALGO}_{\text{INVERSE}}(x, p) \) 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 \( y = x \mod p \). Then

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

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

Next we state the proposition

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

3. CRT Algorithm

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

(Def. 4)(i) If \( \text{len} n_1 = 1 \), then \( \text{ALGO}_{\text{CRT}} n_1 = n_1(1)_1 \), and

(ii) if \( \text{len} n_1 \neq 1 \), 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 \( \text{len} m = \text{len} n_1 \) and \( \text{len} n = \text{len} n_1 \) and \( \text{len} p_1 = \text{len} n_1 - 1 \) and \( \text{len} p_2 = \text{len} n_1 - 1 \) and \( m(1) = 1 \) and for every natural number \( i \) such that \( 1 \leq i \leq \text{len} m - 1 \) there exist elements \( d, x, y \) of \( \mathbb{Z} \) such that \( x = n_1(i) \cdot 2 \) and \( m(i + 1) = m(i) \cdot x \) and \( y = m(i + 1) \) and \( d = n_1(i + 1) \cdot 2 \) and \( p_2(i) = \text{ALGO}_{\text{INVERSE}}(y, d) \) and \( p_1(i) = y \) and \( M_0 = n_1(\text{len} m) \cdot 2 \) and \( M = p_1(\text{len} m - 1) \cdot M_0 \) and \( n(1) = n_1(1)_1 \) and for every natural number \( i \) such that \( 1 \leq i \leq \text{len} m - 1 \) there exist elements \( u, u_0, u_1 \) of \( \mathbb{Z} \) such that \( u_0 = n_1(i + 1) \) and \( u_1 = n_1(i + 1)_2 \) and \( u = (u_0 - n(i)) \cdot p_2(i) \mod u_1 \) and \( n(i + 1) = n(i) + u \cdot p_1(i) \) and \( \text{ALGO}_{\text{CRT}} n_1 = n(\text{len} m) \mod M \).

One can prove the following propositions:

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

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

(10) Let \( a, b, c \) be elements of \( \mathbb{Z} \). Suppose \( c \neq 0 \) and \( a = b \mod c \) 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) \( \text{len} a = \text{len} b \),

(ii) \( \text{len} a = \text{len} n_1 \),

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

(iv) for every natural number \( i \) such that \( i \in \text{Seg} \text{len} n_1 \) holds \( n_1(i) \cdot 1 = a(i) \) and \( n_1(i)_2 = b(i) \), and
(v) for all natural numbers $i, j$ such that $i, j \in \text{Seg len } n_1$ and $i \neq j$ holds $b(i)$ and $b(j)$ are relative prime.
Let $i$ be a natural number. If $i \in \text{Seg len } n_1$, then $\text{ALGO}_{\text{CRT}} n_1 \mod b(i) = a(i) \mod b(i)$.

(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) $2 \leq \text{len } b$,
(ii) for all natural numbers $i, j$ such that $i, j \in \text{Seg len } b$ and $i \neq j$ holds $b(i)$ and $b(j)$ are relative prime,
(iii) for every natural number $i$ such that $i \in \text{Seg len } b$ holds $x \mod b(i) = y \mod b(i)$, and
(iv) $m(1) = 1$.
Let $k$ be an element of $\mathbb{N}$. Suppose $1 \leq k \leq \text{len } b$ and for every natural number $i$ such that $1 \leq i \leq k$ holds $m(i+1) = m(i) \cdot b(i)$. Then $x \mod m(k+1) = y \mod m(k+1)$.

(13) For every finite sequence $b$ of elements of $\mathbb{Z}$ such that $\text{len } b = 1$ 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 $\text{len } m = \text{len } b + 1$ and $m(1) = 1$ and for every natural number $i$ such that $1 \leq i \leq \text{len } b$ holds $m(i+1) = m(i) \cdot b(i)$ and $\prod b = m(\text{len } b + 1)$.

(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 $\text{len } a = \text{len } b$ and $\text{len } a = \text{len } n_1$ and for every natural number $i$ such that $i \in \text{Seg len } n_1$ holds $b(i) \neq 0$ and for every natural number $i$ such that $i \in \text{Seg len } n_1$ holds $n_1(i)_1 = a(i)$ and $n_1(i)_2 = b(i)$ and for all natural numbers $i, j$ such that $i, j \in \text{Seg len } n_1$ and $i \neq j$ holds $b(i)$ and $b(j)$ are relative prime and for every natural number $i$ such that $i \in \text{Seg len } n_1$ holds $x \mod b(i) = a(i) \mod b(i)$ and $y = \prod b$. Then $\text{ALGO}_{\text{CRT}} n_1 \mod y = x \mod y$.

References
Received February 8, 2012