Number Theory Algorithms

Ervin Gegprifti

gegprifti.ervin@gmail.com

Abstract

Nothing to claim here. This paper is the documentation for the Euclidean Algorithm module in Number Theory Algorithms mobile application.

Extended Euclidean Algorithm

The Extended Euclidean Algorithm is used to compute integers x, y for $ax + by = GCD(a, b)$ where $a, b \in \mathbb{Z}_{>0}$. The implementation of this algorithm is based on ([1] pg. 16).

Algorithm 1: Extended Euclidean Algorithm

Input: $a, b \in \mathbb{Z}_{>0}$

Output: Integers x, y for $ax + by = GCD(a, b)$

$r_{n-2} := a$
$r_{n-1} := b$
$q_{n-1} :=$ quotient of r_{n-2}/r_{n-1}
$r_n :=$ remainder of r_{n-2}/r_{n-1}
$x_{n-2} := 1$, $x_{n-1} := 0$, $x_{temp} := x_{n-1}$, $x_{n-1} := x_{n-2} - x_{n-1} \cdot q_{n-1}$, $x_{n-2} := x_{temp}$
$y_{n-2} := 0$, $y_{n-1} := 1$, $y_{temp} := y_{n-1}$, $y_{n-1} := y_{n-2} - y_{n-1} \cdot q_{n-1}$, $y_{n-2} := y_{temp}$

while $r_n > 0$ **do**

$r_{n-2} := r_{n-1}$
$r_{n-1} := r_n$
$q_{n-1} :=$ quotient of r_{n-2}/r_{n-1}
$r_n :=$ remainder of r_{n-2}/r_{n-1}
$x_{temp} := x_{n-1}$
$x_{n-1} := x_{n-2} - x_{n-1} \cdot q_{n-1}$
$x_{n-2} := x_{temp}$
$y_{temp} := y_{n-1}$
$y_{n-1} := y_{n-2} - y_{n-1} \cdot q_{n-1}$
$y_{n-2} := y_{temp}$

end

return $x = x_{n-2}$, $y = y_{n-2}$

References

[1] Cohen, Henri. *A course in computational algebraic number theory.* Springer-Verlag, 1996.