Number Theory Algorithms

Ervin Gegprifti

gegprifti.ervin@gmail.com

Abstract

This paper is the documentation for the Euclidean Algorithm module in Number Theory Algorithms mobile application.

Euclidean Algorithm

The Euclidean Algorithm is used to compute the greatest common divisor (GCD) of two numbers a and b. The (GCD) is the largest number that divides both a and b without leaving a remainder. The implementation of this algorithm is based on ([1] pg. 40).

Algorithm 1: Euclidean Algorithm

```
Input: $a, b \in \mathbb{Z}$
Output: The greatest common divisor (GCD) of $a$ and $b$

if $a < 0$ then $a = |a|$
if $b < 0$ then $b = |b|$
if $a = b$ then return $a$, since $a|a$ and $a|b$
if $a \neq 0$ and $b = 0$ then return $a$
if $a = 0$ and $b \neq 0$ then return $b$
if $a = 0$ and $b = 0$ then return $0$
if $b|a$ then return $b$

$r_{n-2} := a$
$r_{n-1} := b$
$q_{n-1} :=$ quotient of $r_{n-2}/r_{n-1}$
$r_n :=$ remainder of $r_{n-2}/r_{n-1}$

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 $r_{n-2}/r_{n-1}$
end

return $r_{n-1}$
```

References

[1] Yan, Song Y. *Number theory for computing.* Springer Science & Business Media, 2002.