Number Theory Algorithms

Ervin Gegprifti

gegprifti.ervin@gmail.com

Abstract

This paper is the documentation for the Linear Diophantine Equation In Two Variables module in Number Theory Algorithms mobile application.

Linear Diophantine Equation In Two Variables

The equation $ax + by = c$ where $a, b, x, y \in \mathbb{Z}$ with $a, b \neq 0$ has no integer solution if $GCD(a, b) \nmid c$ and many integer solutions if $GCD(a, b) \mid c$. The implementation of this algorithm is based on ([1] pg. 137, [2] pg. 183).

Algorithm 1: Linear Diophantine Equation In Two Variables

Input: $a, b, c, x, y \in \mathbb{Z}$ with $a, b \neq 0$
Output: x, y solutions if any

```
Set g = GCD(a, b)
if g ∤ c then there is no integer solution. Stop.
if g | b then there are infinitely many integer solutions. Continue..
Use Extended Euclidean Algorithm to find x_ee and y_ee from
    |a|x + |b|y = GCD(|a|, |b|) = g
Set x_ee = sign(a)x_ee and y_ee = sign(b)y_ee
A particular first initial solution is x_0 = x_ee(c/g) and y_0 = y_ee(c/g)
For r ∈ ℤ, any integer x = x_0 + (b/g)r and y = y_0 − (a/g)r is a solution
return solutions
```

References

[1] Rosen, Kenneth H. *Elementary Number Theory and Its Applications. - 6th ed.* Pearson Education London, 2011.

[2] Tattersall, James J. *Elementary number theory in nine chapters. - 2nd ed.* Cambridge University Press, 1999.