Number Theory Algorithms

Ervin Gegprifti

gegprifti.ervin@gmail.com

Abstract

This paper is the documentation for the Linear Congruence In One Variable module in Number Theory Algorithms mobile application.

Linear Congruence In One Variable

The Linear Congruence In One Variable $ax \equiv b \pmod{m}$ is equivalent to the Linear Diophantine Equation In Two Variables $ax - my = b$. If $GCD(a, m) \nmid c$ there is no solution modulo m and if $GCD(a, m) \mid c$ there are g incongruent solutions modulo m. The implementation of this algorithm is based on ([1] pg. 123, [2] pg. 157).

Algorithm 1: Linear Congruence In One Variable

Input: $a, b, x \in \mathbb{Z}$, $m \in \mathbb{N}$
Output: x general solution if any

Check solubility
Let $g = GCD(a, m)$
if $g \nmid b$ **then** there is no solution modulo m. Stop.
if $g \mid b$ **then** there are g incongruent solutions modulo m. Continue...
Use Extended Euclidean Algorithm to find x_{ee} from $|a|x + |m|y = GCD(|a|, |m|) = g$
Set $x_{ee} = sign(a)x_{ee}$
A particular first initial solution is $x_0 = x_{ee}(b/g) \pmod{m}$
All initial solutions for $n = \{0, ..., g-1\}$ are $x_n = n(m/g) + x_0 \pmod{m}$
For $r \in \mathbb{Z}$, any integer $x = mr + x_n$ is a solution
return x *general solution*

References

[1] Yan, Song Y. *Number Theory for Computing. - 2nd ed.* Springer Science & Business Media, 2002.

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