Number Theory Algorithms

Ervin Gegprifti

gegprifti.ervin@gmail.com

Abstract

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

Linear Congruence In Two Variables

The Linear Congruence In Two Variable $ax + by \equiv c \pmod{m}$ is equivalent to the Linear Diophantine Equation In Three Variables $ax + by + mz = c$. If $GCD(a, b, m) \nmid c$ there is no solution modulo m and if $GCD(a, b, m) \mid c$ there are solutions modulo m.

Algorithm 1: Linear Congruence In Two Variablea

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

Let $g = GCD(a, b, m)$
if $g \nmid c$ **then** there is no solution modulo m. Stop.
if $g \mid c$ **then** there are solutions modulo m. Continue...
The Congruence $ax + by \equiv c \pmod{m} \iff x + by = mz + c \iff x + by + mz = c$
Let $h = GCD(a, b)$, $d = a/h$, $e = b/h$
Factoring out $ax + by$ we get $h(dx + ey) + mz = c$
Note that $GCD(d, e)$ is always 1, since $d = a/h$ and $e = b/h$
Let $dx + ey = w$
Rewriting we must solve $hw + mz = c$
Simplify $hw + mz = c$ by dividing both sides with $i = GCD(h, m, c)$ to get $jw + nz = f$
Let $k = GCD(j, n)$
if $k \nmid f$ **then** there is no integer solution. Stop.
if $k \mid f$ **then** there are infinitely many integer solutions. Continue...
Use EEA to find w_{ee} and z_{ee} from $|j|w + |n|z = GCD(|j|, |n|) = k$
A particular first initial solution is $w_0 = w_{ee}(f/k)$ and $z_0 = z_{ee}(f/k)$
For $r \in \mathbb{Z}$, the general solution to $jw + nz = f$ is $w = w_0 + (n/k)r$ and $z = z_0 - (j/k)r$
Let $p = (n/k)$ and $q = (j/k)$, hence the general solution is $w = w_0 + pr$ and $z = z_0 - qr$
Substituting for w, then we have $dx + ey = w_0 + pr$
Since $GCD(d, e)$ is always 1, then we find x_0 and y_0 by solving $dx + ey = 1$
Use EEA to find x_{ee} and y_{ee} from $|d|x + |e|y = GCD(|d|, |e|) = 1$, hence $dx_{ee} + ey_{ee} = 1$
Multiplying both sides with $w_0 + pr = w$ we have $dx_{ee}(w_0 + pr) + ey_{ee}(w_0 + pr) = w$
Hence $x_0 = x_{ee}(w_0 + pr) = x_{ee}w_0 + x_{ee}pr$ and $y_0 = y_{ee}(w_0 + pr) = y_{ee}w_0 + y_{ee}pr$
The general x, y solution is $x = x_{ee}w_0 + x_{ee}pr + et$ and $y = y_{ee}w_0 + y_{ee}pr - dt$
The congruence $ax + by \equiv c \pmod{m}$ can be written as
$a(x_{ee}w_0 + x_{ee}pr + et) + b(y_{ee}w_0 + y_{ee}pr - dt) \equiv c \pmod{m}$
return x, y *general solution*