Number Theory Algorithms

Ervin Gegprifti

gegprifti.ervin@gmail.com

Abstract

This paper is the documentation for the Mod Factors module in Number Theory Algorithms mobile application.

Mod Factors

Any number n can be written as $(ax+c)(ay+b) = n$. Distributing we have $a(axy+bx+cy)+bc = n$. Given any a we can find b, c such as $n \equiv bc \pmod{a}$.

Algorithm 1: Mod Factors

Input: $n, a \in \mathbb{N}$
Output: b, c such as $n \equiv bc \pmod{a}$

1 Let $n \pmod{a} = r$
2 For every b, c combination where $b, c \in \{0, \ldots, a-1\}$
3 **if** $bc \pmod{a} = r$ **then** Display and count.
4 **return** b, c *such as* $n \equiv bc \pmod{a}$