Number Theory Algorithms

Ervin Gegprifti

gegprifti.ervin@gmail.com

Abstract

This paper is the documentation for the Simple Quadratic Form module in Number Theory Algorithms mobile application.

Simple Quadratic Form

$$bxy + dx + ey = f \tag{1}$$

The equation (1) is a simpler case of the more generic Quadratic Form $ax^2+bxy+cy^2+dx+ey = f$ where $a = c = 0$. The algorithm make use of the factoring technique known as (Simon's Favorite Factoring Trick SFFT) in order to find solutions to (1) if any. The implementation of this algorithm is based on ([1] pg. 56).

```
Algorithm 1: Simple Quadratic Form Algorithm
  Input: $b, d, e, f, x, y \in \mathbb{Z}$ and $b \neq 0$
  Output: $x, y$ solutions if any
  Multiply both sides with $b$ then $b^2xy + bdx + bey = bf$
  Add $de$ to both sides then $b^2xy + bdx + bey + de = bf + de$
  The LHS can be written as $(bx + e)(by + d)$
  Let $n = bf + de$ then we must solve $(bx + e)(by + d) = n$
  Factor $n$ into $pq$ pairs
  if there are no $pq$ factors of $n$ then return there is no solution other than the trivial
  solutions ← empty
  for each $pq$ pair factor of $n$ do
      if $b \mid (p - e)$ and $b \mid (q - d)$ then
          $x = (p - e)/b$
          $y = (q - d)/b$
          solutions ← x,y
      else
          // there is no integer solution for this pair
      end
  end
  return solutions
```

References

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