# Rotations and Translations of Number Field Sieve Polynomials

Jason E. Gower
CERIAS & Dept. of Mathematics
Purdue University
jgower@math.purdue.edu

December 2003

## Congruent Squares

Let $N$ be an odd positive integer that we wish to factor.

Some of the most successful integer factorization algorithms (CFRAC, quadratic sieve, number field sieve) are based on the following idea:

**Proposition:** If $x, y \in \mathbb{Z}$ with $x \not\equiv \pm y \bmod N$ and $x^2 \equiv y^2 \bmod N$, then $\gcd(x \pm y, N)$ are non-trivial factors of $N$.

If $N$ is a product of $k$ distinct odd primes, then a randomly generated pair $(x, y)$ with only $x^2 \equiv y^2 \bmod N$ will produce a non-trivial factorization of $N$ with probability $2^{1-k}$.

## Basic Idea of NFS

Let $f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ be irreducible in $\mathbb{Z}[X]$, $d > 1$.
Let $\alpha \in \mathbb{C}$ be a root of $f$ and $m \in \mathbb{Z}$ be a root of $f$ modulo $N$.

A ring homomorphism $\phi : \mathbb{Z}[\alpha] \to \mathbb{Z}/N\mathbb{Z}$ is given by

$$\phi(\alpha) = m \bmod N.$$

## Basic Idea of NFS (2)

Now suppose we can find a set $\mathcal{S}$ consisting of $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ with $\gcd(a, b) = 1$ such that:

$$\prod_{(a,b)\in\mathcal{S}} (a - bm) = x^2 \text{ for some } x \in \mathbb{Z} \tag{1}$$

$$\prod_{(a,b)\in\mathcal{S}} (a - b\alpha) = \beta^2 \text{ for some } \beta \in \mathbb{Z}[\alpha]. \tag{2}$$

If $y \in \mathbb{Z}$ satisfies $\phi(\beta) \equiv y \bmod N$, then we will have the desired $x^2 \equiv y^2 \bmod N$.

## Squares from Smooth Integers

**Smooth Integers:** We say that a positive integer $x$ is $B$-smooth if no prime factor of $x$ is greater than $B$.

Suppose $B > 1$, $\{p_1, \ldots, p_l\}$ are the primes no greater than $B$, and we have a way of generating many $B$-smooth integers.

Then for each $B$-smooth $s$, write:

$$s = (-1)^{v_0(s)} \prod_{j=1}^{l} p_j^{v_j(s)}.$$

Note that $\prod_{i \in \mathcal{I}} s_i$ is a square if and only if $\sum_{i \in \mathcal{I}} v_j(s_i)$ is even for $j = 0, 1, \ldots, l$.

## Squares from Smooth Integers (2)

Define the exponent vector of $s$ by:

$$v(s) = (v_0(s), v_1(s), \ldots, v_l(s))$$

If we take

$$\overline{v}(s) = (\overline{v_0}(s), \overline{v_1}(s), \ldots, \overline{v_l}(s)),$$

where $\overline{v_i}(s) = v_i(s) \bmod 2$, then we have reduced the problem of finding a square in $\mathbb{Z}$ to finding a linear dependency in $\mathbb{F}_2^{l+1}$.

As soon as we have $l+2$ distinct elements, we can find a dependency.

## Squares from Smooth Integers (3)

Let $\alpha_1, \ldots, \alpha_d$ be the roots of $f(X)$. The norm map from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}$ is given by $N(g(\alpha)) = \prod_{i=1}^{d} g(\alpha_i)$.

When $g(\alpha) = a - b\alpha$, we have:

$$N(a - b\alpha) = F(a, b),$$

where

$$F(X, Y) = Y^d f(X/Y) = \sum_{i=0}^{d} a_i X^i Y^{d-i}$$

is the homogenization of $f(X) = \sum_{i=0}^{d} a_i X^i$.

## Squares from Smooth Integers (4)

**Smooth Algebraic Numbers:** An algebraic number is $B$-smooth if its norm is $B$-smooth.

**Proposition:** $\beta$ is a square in $\mathbb{Z}[\alpha] \Rightarrow N(\beta)$ is a square in $\mathbb{Z}$.

Unfortunately the converse is false.

However, by modifying our definition of exponent vector, we can build squares in $\mathbb{Z}[\alpha]$ using the ideas that we used to build squares in $\mathbb{Z}$.

## Polynomial Selection for NFS

**Question:** How can we construct an irreducible $f \in \mathbb{Z}[X]$ of fixed degree $d$ and $m \in \mathbb{Z}$ such that $f(m) \equiv 0 \bmod N$?

**Base-$m$ Method:** Choose an integer $m$ such that

$$\lfloor N^{\frac{1}{d+1}} \rfloor < m \leq \lfloor N^{\frac{1}{d}} \rfloor$$

and write the base-$m$ expansion of $N$

$$N = a_d m^d + \cdots + a_1 m + a_0$$

where $0 \leq a_i < m$.

## Polynomial Selection for NFS (2)

Take $f$ to be:

$$f(X) = a_d X^d + \cdots + a_1 X + a_0$$

By construction: $\deg(f) = d$ and $f(m) \equiv 0 \bmod N$.

**Brillhart, Filaseta, Odlyzko:** If $f$ is reducible, $f(X) = g(X)h(X)$, then $N = g(m)h(m)$ is a non-trivial factorization. This is *good*.

## Good NFS Polynomials

**Question:** What makes for a good NFS polynomial?

**Size:** For a fixed set of inputs, a polynomial is said to have small size, if the magnitude of the outputs are small.

Clearly, the smaller the size, the more likely that the outputs will be smooth.

**Root Properties:** A polynomial is said to have good root properties if it has many roots modulo many small primes.

The outputs of a polynomial with good root properties are more likely to be smooth than otherwise.

## Roots

Roots come in two types. To distinguish these, let $f(X) \in \mathbb{Z}[X]$ and let $F(X,Y) \in \mathbb{Z}[X,Y]$ be the homogenization of $f(X)$. Fix a prime $p$.

**Projective Roots:** A co-prime pair $(a,b)$ in $\mathbb{Z} \times \mathbb{Z}$ is a projective root if $F(a,b) \equiv 0 \bmod p$ and $p$ divides $b$.

Note that $F(X,Y)$ will have projective roots when $p$ divides the leading coefficient of $f(X)$.

But we can easily choose the leading coefficient of a base-$m$ polynomial.

First choose a suitable leading coefficient $L$.

## **Roots** (2)

Now choose $m$ such that

$$\lfloor (N/(L+1))^{\frac{1}{d}} \rfloor < m \leq \lfloor (N/L)^{\frac{1}{d}} \rfloor.$$

The resulting base-$m$ polynomial will have leading coefficient $L$.

Previously we required that $f(X)$ be monic.

However, we can modify NFS to allow for non-monic polynomials, and it can be advantageous to do so.

**Regular Roots:** A co-prime pair $(a, b)$ in $\mathbb{Z} \times \mathbb{Z}$ is a regular root if $F(a, b) \equiv 0 \bmod p$ and $p$ does not divide $b$.

Note that regular roots correspond to roots of $f(X)$ modulo $p$.

## Rotations and Translations

**Murphy:** We can use translations and rotations to construct NFS polynomials with good root properties and small size.

**Rotations:** Let $f(X), g(X) \in \mathbb{Z}[X]$ with the degree of $g$ less than the degree of $f$. Then

$$f(X) + (X - m)\, g(X)$$

is the rotation of $f(X)$ by $g(X)$.

Note that if $h(X)$ is a rotation of $f(X)$, then $\deg(h(X)) = d$ and $h(m) \equiv 0 \bmod N$.

We hope to choose $g(X)$ so that the resulting rotation has good root properties and small size.

## Rotations and Translations (2)

**Translations:** Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $d > 1$, and $t \in \mathbb{Z}$. Then

$$f(X - t)$$

is the translation of $f(X)$ by $t$.

If $h(X)$ is the translation of $f(X)$ by $t$, then $h(m + t) \equiv 0 \bmod N$ and $\deg(h(X)) = d$.

Although we cannot change root properties by translation, we can hope to choose $t$ so that the resulting translation has small size.

## CRT Rotations

**Murphy:** The function

$$\alpha_B(F) = \sum_{p \le B} \left(1 - q_p \frac{p}{p+1}\right) \frac{\log p}{p-1},$$

quantifies the root properties of $F$, where $q_p$ is the number of roots (regular and projective) of $f(X)$ modulo $p$.

We can think of $F(a,b)$ as behaving like a random integer of size $F(a,b)e^{\alpha_B(F)}$.

The more negative $\alpha_B(F)$ is, the more likely $F$-values will be $B$-smooth.

So we want $q_p$ to be large for many small primes $p$.

## **CRT Rotations** (2)

This motivates the following idea:

For a suitable prime $p$, we can choose a set of roots and construct a rotation that will have all of these roots modulo $p$.

Then we can use the Chinese Remaider Theorem to find a single rotation that has all the roots modulo each of the primes.

## CRT Rotations (3)

Let $1 \leq r < d-1$ and $\mathcal{P} = \{p_1 < p_2 < \cdots < p_s\}$ be a set of primes with $r+1 < p_1$.

Fix a prime $p_i$,let $g_i(X) = a_{ir}X^r + \cdots + a_{i0}$, and take $h_i(X) = f(X) + (X-m)\,g_i(X)$.

Choose distinct $k_{i0}, \ldots, k_{ir}$ from $\{0, \ldots, p_i - 1\}$ s. t. $m \not\equiv k_{ij} \bmod p_i$ for all $j$.

Finally, let $z_{ij} \equiv (m - k_{ij})^{-1} f(k_{ij}) \bmod p_i$.

## **CRT Rotations** (4)

Then $h_i(k_{ij}) \equiv 0 \bmod p_i$ for all $j$ leads to the system:

$$\begin{pmatrix} 1 & k_{i0} & \cdots & k_{i0}^r \\ \vdots & \vdots & & \vdots \\ 1 & k_{ir} & \cdots & k_{ir}^r \end{pmatrix} \begin{pmatrix} a_{i0} \\ \vdots \\ a_{ir} \end{pmatrix} \equiv \begin{pmatrix} z_{i0} \\ \vdots \\ z_{ir} \end{pmatrix} \bmod p_i$$

For each $p_i$, this system can be solved modulo $p_i$.

## **CRT Rotations** (5)

We now have $s$ polynomials $g_1, \ldots, g_s$, each corresponding to a rotation with roots $k_{i0}, \ldots, k_{ir}$ modulo $p_i$.

We obtain a single rotation with roots $k_{ij}$ modulo $p_i$ for all $i, j$ by solving the system:

$$a_j \equiv a_{ij} \bmod p_i$$

for $i = 1, 2, \ldots, s$, using the Chinese Remainder Theorem.

Note: We may replace $p_i$ with $p_i^{e_i}$.

## Weighted Translations

The CRT rotation step may produce a polynomial with large coefficients. While we can choose the coefficients of the rotation modulo $\prod_{i=1}^{s} p_i^{e_i}$ to help control size, we may need to translate to further reduce size.

By changing the shape of the sieving region, we can allow the low order coefficients to be somewhat larger than the high order coefficients.

## Weighted Translations (2)

Fix $\omega = (\omega_0, \ldots, \omega_d) \in (\mathbb{R}^\times)^{d+1}$, depending on the sieving region, and define:

$$\|a_d X^d + \cdots + a_0\|_{\omega,\infty} = \max_{0 \le i \le d} |\omega_i a_i|$$

$$\|a_d X^d + \cdots + a_0\|_{\omega,k} = \left( \sum_{i=0}^{d} |\omega_i a_i|^k \right)^{\frac{1}{k}}$$

## **Weighted Translations** (3)

We seek $t \in \mathbb{Z}$ such that $\|f(X-t)\|_{\omega,\infty}$ is minimal, for a fixed $f(X) \in \mathbb{Z}[X]$.

For example, we could choose $\omega$ so that the coefficients grow no worse than geometrically, from high to low order.

It is difficult to work with $\|\cdot\|_{\omega,\infty}$.

However, for a fixed even $k$, finding $f(X-t)$ minimal with respect to $\|\cdot\|_{\omega,k}$ is a simple calculus exercise.

## Weighted Translations (4)

**Proposition:** If $g_k(X)$ and $h(X)$ are minimal with respect to $\|\cdot\|_{\omega,k}$ and $\|\cdot\|_{\omega,\infty}$, respectively, then we have:

$$\|g_k(X)\|_{\omega,\infty} \leq \sqrt[k]{d+1} \cdot \|h(X)\|_{\omega,\infty}.$$

**Corollary:** For large enough $k$, we will have $g_k(X)$ minimal with respect to $\|\cdot\|_{\omega,\infty}$.

It may not be practical to work with large $k$. However, even for small $k$, the proposition guarantees that $g_k(X)$ is still "close" to being minimal with respect to $\|\cdot\|_{\omega,\infty}$ when $d$ is small.

## Choosing Good Polynomials for NFS

**Strategy:** Generate many base-$m$ polynomials with desirable leading coefficients, i.e. many projective roots...

Using a suitable set of primes, find a CRT rotation for each polynomial to produce a set of polynomials with good regular *and* projective root properties...

Using a suitable $\omega \in (\mathbb{R}^\times)^{d+1}$, find a translation for each polynomial to produce a set of polynomials with good root properties *and* small size...

Finally, calculate $\alpha_B(F)$ for each polynomial. Keep those with $\alpha_B(F)$ below some threshold.

Perform sieving experiments to identify the best polynomial.

## Future Work

1. These ideas must be implemented, tested and compared with existing methods for choosing NFS polynomials.

2. Perhaps the best strategy would be a combination of some/all of the existing methods.

   For example, perhaps a good strategy would be a CRT rotation followed by a numerical minimization of $\int\int_S F^2(x,y)\,dxdy$ with respect to the translation parameter and sieving region, à la Murphy.

3. Factoring numbers such as RSA-140 and RSA-155 would provide a good first test.