GTBAC, Télécom ParisTech — February 26, 2015

Comments on Schirokauer's tower number field sieve

Razvan Barbulescu[1] Pierrick Gaudry Thorsten Kleinjung
CNRS and IMJ-PRG

Motivation

A bit of history

1. In 2000 Joux proposed to use pairings-based crypto-systems. Their security depends on the difficulty of computing discrete logarithms (DLP)
   - on elliptic curves (given P and $[x]P$, find x);
   - in finite fields other than prime fields (given g and g^x, find x).
2. In 2013, Joux, Franklin and Boneh received the Gödel prize for their works on pairings.
3. The most popular pairings were those which rely on the difficulty of DLP in $\mathbb{F}_{q^k}$ where $k \leq 12$ and q is
   - prime
   - or a power of 2 or 3.
4. in 2013 and 2014, the case where q is a power of 2 or 3 was abandoned.

Motivation

A bit of history

1. In 2000 Joux proposed to use pairings-based crypto-systems. Their security depends on the difficulty of computing discrete logarithms (DLP)
   - on elliptic curves (given P and $[x]P$, find x);
   - in finite fields <u>other than prime fields</u> (given g and g^x, find x).
2. In 2013, Joux, Franklin and Boneh received the Gödel prize for their works on pairings.
3. The most popular pairings were those which rely on the difficulty of DLP in $\mathbb{F}_{q^k}$ where $k \leq 12$ and q is
   - prime
   - or a power of 2 or 3.
4. in 2013 and 2014, the case where q is a power of 2 or 3 was abandoned.

$\boxed{\text{One needs to evaluate the difficulty of DLP in } \mathbb{F}_{p^k} \text{ with small } k > 1.}$

The number field sieve(NFS)

Factoring

First NFS variant published in 1989. NFS is the fastest algorithm

- asymptotically;
- in practice for integers $N \geq 10^{100}$ (record at 232 digits).

DLP in $\mathbb{F}_p$

First NFS variant published in 1993. NFS is the fastest algorithm

- asymptotically (same complexity as factoring);
- in practice for primes $p \geq 10^{100}$ (record at 180 digits).

DLP in $\mathbb{F}_{p^k}$

We have two NFS variants

- Schirokauer 2000 (same complexity as factoring when it applies)
- Joux, Lercier, Smart, Vercauteren 2006 (same complexity C as factoring for some fields (large characteristic) and $C^{\sqrt[3]{2}}$ in all the other cases.

Outline of the talk

- Number field sieve
- Tower number field sieve
- Applications
- Practical details

Smoothness

Definition

An integer is B-smooth if all its prime factors are less than B.

Computation

The choice algorithm is ECM, which, given x finds the factors less than B in time

$$T(B)\log(x)^{O(1)},$$

where $T(B) \approx e^{\sqrt{\log B}}$ and $O(1) = 4$ in theory and 2 in practice.

Smoothness probability

Canfield-Erdös-Pomerance proved that the probability of an integer less than x to be $x^{1/u}$-smooth is

$$\text{Prob} = 1/u^u,$$

up to a $(1 + o(1))$ exponent, uniformly on x and u.

The number field sieve (NFS): diagram

NFS for DLP in $\mathbb{F}_p$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

$$\begin{tikzcd}
 & a - bx \in \mathbb{Z}[x] \arrow[dl] \arrow[dr] & \\
\mathbb{Z}[x]/\langle f(x) \rangle \arrow[dr] & & \mathbb{Z}[x]/\langle g(x) \rangle \arrow[dl] \\
 & \mathbb{Z}/p\mathbb{Z} &
\end{tikzcd}$$

The number field sieve (NFS): diagram

NFS for DLP in $\mathbb{F}_p$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

$$\begin{tikzcd}
& a - bx \in \mathbb{Z}[x] \arrow[dl, "x \mapsto \alpha_f"'] \arrow[dr, "x \mapsto \alpha_g"] & \\
\mathbb{Z}[\alpha_f] \arrow[dr, "\alpha_f \mapsto m"'] & & \mathbb{Z}[\alpha_g] \arrow[dl, "\alpha_g \mapsto m"] \\
& \mathbb{Z}/p\mathbb{Z} &
\end{tikzcd}$$

The NFS algorithm for DLP

$F(a,b) = \sum_{i=0}^{d} f_i a^i b^{d-i}$ where $d = \deg f$ and $G(a,b) = g_1 a + g_0 b$.

Input a finite field $\mathbb{F}_p$, two elements t (generator) and s
Output $\log_t s$

1: (Polynomial selection) Choose two polynomials f and g in $\mathbb{Z}[x]$ which have a common root modulo p;

2: (Sieve) Collect coprime pairs (a,b) such that $F(a,b)$ and $G(a,b)$ are B-smooth (for a parameter B);

3: Write a linear equation for each pair (a,b) found in the Sieve stage.

4: (Linear algebra) Solve the linear system to find (virtual) logarithms of the prime ideals of norm less than B;

5: (Individual logarithm) Write $\log_t s$ in terms of the previously computed logs.

Polynomial selection: Base-m method

Put $m = \lfloor p^{1/d} \rfloor$ and write $p = m^d + N_{d-1}m^{d-1} + \cdots N_1 m + N_0$ in base m and put

- $f = x^d + \cdots + N_1 x + N_0$;
- $g = x - m$.

Algorithm for sieving

Algorithm

One dimensional sieve

Input a polynomial $Q(x)$ in $\mathbb{Z}[x]$ and parameters **fbb**, B, E_1, E_2, **thrs**;
Output $\approx$all the integers $u \in [E_1, E_2]$ for which $Q(u)$ is B-smooth.

1: (makefb) Make a list (p^k, r) of prime powers $p^k \leq \max\{|Q(u)|, u \in [E_1, E_2]\}$, with $p <$ **fbb**, and integers $0 \leq r < p^k$ such that $Q(r) \equiv 0 \bmod p^k$
2: (norm initialization) Define an array indexed by $u \in [E_1, E_2]$ and initialize it with $\log_2 |Q(u)|$
3: **for** all (p^k, r) considered above **do**
4:     **for** u in $[E_1, E_2]$ and $u \equiv r \bmod p^k$ **do**
5:         Subtract $\log_2 p$ from the entry of index u; $\triangleright$ actual sieve
6:     **end for**
7: **end for**
8: (co-factorization) Collect the indices u where the array is less than **thrs** and test B-smoothness with ECM.

Comments

1. In the theoretical presentation of the algorithm we take **fbb** $= B$ and **thrs** $= 0$, but in practice **fbb** $< B$.
2. Polynomials of n-variables are sieved similarly: enumerate on the first $n-1$ variables and sieve on the last one.

Working with ideals

Factor base

We call factor base of f the set

$$\mathcal{F}_f = \left\{ \begin{array}{c} \text{prime ideals } \mathfrak{q} \text{ in } \mathcal{O}_f \text{ of degree one, of norm less than } B \\ \text{or above prime factors of } l(f) \end{array} \right\},$$

Similarly, we define $\mathcal{F}_g$ and set $\mathcal{F} = \mathcal{F}_f \bigcup \mathcal{F}_g$.

Theorem (Dedekind)

For all primes q, not dividing $[\mathcal{O}_f : \mathbb{Z}[\alpha_f]]$, the prime ideals above q of degree one are

$$\{\langle q, \alpha_f - r\rangle \mid f(r) \equiv 0 \mod q\}.$$

Moreover, if a and b are two coprime integers, and $F(a,b) = \pm l(f)\,\mathrm{N}_{K/\mathbb{Q}}(a - b\alpha_f)$ is B-smooth, then $(a - b\alpha_f)$ factors into elements of the factor base and, if $q \nmid \mathrm{Disc}(f) l(f)$,

$$\mathrm{val}_q \mathrm{N}(a - b\alpha_f) = \mathrm{val}_{\langle q, \alpha_f - (a \cdot b^{-1} \bmod q)\rangle}(a - b\alpha_f).$$

Linear algebra and individual log

Virtual logarithms

Let ℓ be a large prime factor of $p-1$. Let h be the class number of K_f. For each prime ideal $\mathfrak{q}$ in the factor base, we put

$$\log \mathfrak{q} = \frac{1}{h} \log \gamma_{\mathfrak{q}} \bmod \ell,$$

where γ_h is a generator of $\mathfrak{q}^h$ chosen using the Schirokauer maps.

Linear algebra

- We solve a linear system $Ax = 0$ where x are the virtual logarithms of the prime ideals $\mathfrak{q} \in \mathcal{F}$.
- The matrix A is very similar in different DLP variants of NFS.

Individual logarithms

- If $\mathfrak{q}$ is a prime ideal, we search equations of type $\log \mathfrak{q} = \sum_i \log \mathfrak{q}_i$, where $\mathfrak{q}_i$ are prime ideals of degree one and smaller norm.
- In various DLP variants of NFS it take a time smaller than or equal to than of the main stages (sieve and linear algebra).

Outline of the talk

- Number field sieve
- Tower number field sieve
- Applications
- Practical details

Algorithms for DLP in $\mathbb{F}_{p^k}$

JLSV's variant of the number field sieve

- In 2006, JLSV proposed a variant of NFS which is identical to the classical NFS for prime fields, except for the selection of polynomials.
- Methods of polynomial selection:
  - two methods of JLSV
  - generalized Joux-Lercier (Matyukhin 2006);
  - conjugation method (B, Gaudry, Guillevic, Morain 2014).
- Records:
  - $\mathbb{F}_{p^3}$, 120 decimal digits, JLSV 2006, with a method of JLSV;
  - $\mathbb{F}_{p^2}$, 180 decimal digits, BGGM 2014, with the conjugation method.

Schirokauer's tower number field sieve

In 2000, Schirokauer proposed the first variant of the number field sieve for non-prime fields.

- it uses towers of number fields (new implementation);
- has the same complexity as factoring when k is fixed and $p^k \to \infty$;
- has not been implemented (only top level presentation).

Schirokauer's TNFS diagram

NFS for DLP in $\mathbb{F}_p$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

$$\begin{tikzcd}
 & a - bx \in \mathbb{Z}[x] \arrow[dl] \arrow[dr] & \\
\mathbb{Z}[x]/\langle f(x) \rangle = \mathbb{Z}[\alpha_f] \arrow[dr] & & \mathbb{Z}[x]/\langle g(x) \rangle = \mathbb{Z}[\alpha_g] \arrow[dl] \\
 & \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p &
\end{tikzcd}$$

Schirokauer's TNFS diagram

NFS for DLP in $\cancel{\mathbb{F}_p}$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

Let $h \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree k such that p is inert in its number field $\mathbb{Q}(\iota)$; we have $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k}$.

$$
\begin{tikzcd}
 & a - bx \in \cancel{\mathbb{Z}}[x] \arrow[dl, "x \mapsto \alpha_f"'] \arrow[dr, "x \mapsto \alpha_g"] & \\
\cancel{\mathbb{Z}}[x]/\langle f(x) \rangle = \cancel{\mathbb{Z}}[\alpha_f] \arrow[dr, "\alpha_f \mapsto m"'] & & \cancel{\mathbb{Z}}[x]/\langle g(x) \rangle = \cancel{\mathbb{Z}}[\alpha_g] \arrow[dl, "\alpha_g \mapsto m"] \\
 & \cancel{\mathbb{Z}}/p\cancel{\mathbb{Z}} \simeq \cancel{\mathbb{F}_p} &
\end{tikzcd}
$$

Schirokauer's TNFS diagram

NFS for DLP in $\mathbb{F}_{p^k}$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

Let $h \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree k such that p is inert in its number field $\mathbb{Q}(\iota)$; we have $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k}$.

$$\begin{tikzcd}
 & a - bx \in \mathbb{Z}[\iota][x] \arrow[dl, "x \mapsto \alpha_f"'] \arrow[dr, "x \mapsto \alpha_g"] & \\
\mathbb{Z}[\iota][x]/\langle f(x) \rangle = \mathbb{Z}[\iota][\alpha_f] \arrow[dr, "\alpha_f \mapsto m"'] & & \mathbb{Z}[\iota][x]/\langle g(x) \rangle = \mathbb{Z}[\iota][\alpha_g] \arrow[dl, "\alpha_g \mapsto m"] \\
 & \mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k} &
\end{tikzcd}$$

Polynomial selection

In practice

We try polynomials h with small coefficients until we find one which is irreducible modulo p.
We can take h in a family which ensures that h has $\deg h$ automorphisms.

Theorem (Adleman and Lenstra 1986)

Let m and p be two primes and k a divisor of $m-1$. If $x^k - p$ is irreducible modulo m, then p is inert in the unique subfield of $\mathbb{Q}(\zeta_m)$ of degree k.

Corollary

Under ERH, there exists a constant $c > 0$ such that, for any integer k and any prime $p > k$, there exists an effectively constructible polynomial $h \in \mathbb{Z}[x]$ such that:

- h is irreducible modulo p;
- $\|h\|_\infty < (2ck^4 \log(kp)^2)^k$.

Factor base

Factor base

We define the factor base associated to f the set

$$\mathcal{F}_f = \left\{ \begin{array}{c} \text{prime ideals } \mathfrak{q} \text{ in } \mathcal{O}_f \text{ of degree one } \underline{\text{over } \mathbb{Q}(\iota)}\text{, of norm less than } B \\ \text{or above prime factors of } l(f) \end{array} \right\},$$

Representation

All primes of $\mathcal{O}_f$ of degree one, except for a small finite set (dividing $\operatorname{disc}(f)\operatorname{disc}(h)$) are of the form

$$\mathfrak{Q} = \langle \mathfrak{q}, \alpha_f - r(\iota) \rangle,$$

where $r(x) \in \mathbb{Z}[x]$ is such that $f(r(\iota)) \equiv 0 \bmod \mathfrak{q}$.

Cardinality

- Landau's prime ideal theorem states that the number of prime ideals $\mathfrak{q}$ of norm at most B is $B/\log B$.
- Chebotarev's density theorem states that, the average number of degree one ideals above each $\mathfrak{q}$ is one.
- Hence, the factor base has approximatively the same cardinality as for NFS, so the linear algebra has the same cost.

Sieve (1/2)

Naive method

- One can collect n-tuples in S where a polynomial $f(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ is smooth in time $(\#S)^{1+o(1)}$ if $\#S = B^c$ for a constant $c > 0$.
- $\mathrm{N}_{K/\mathbb{Q}}(a - b\alpha) = \mathrm{N}_{\mathbb{Q}(\iota)/\mathbb{Q}}(F(a, b))$ is a multivariate polynomial in the coordinates of $a = a(\iota)$ and $b = b(\iota)$.

Sieving space

$$S = \{(a = a_0 + ta_1 + \cdots + a_{k-1}t^{k-1}, b = b_0 + tb_1 + \cdots + b_{k-1}t^{k-1}) \in \mathbb{Z}[t]^2 \mid |a_i|, |b_j| \leq A\},$$

for a parameter A.
If E^2 corresponds to the prime case, we take

$$A = E^{1/k}.$$

Sieve (2/2)

For each prime ideal $\mathfrak{Q}$ of the factor base, we update the pairs (a, b) in the lattice:

$$
M_{\mathfrak{Q}} = \left(\begin{array}{ccc|ccccc}
q & & & 0 & \cdots & & \cdots & 0 \\
 & \ddots & & \vdots & & & & \vdots \\
 & & q & & & & & \\
\boxed{\text{vector}(\varphi_{\mathfrak{q}})} & & & & & & & \\
 & \ddots & & \vdots & & & & \vdots \\
 & & \boxed{\text{vector}(\varphi_{\mathfrak{q}})} & 0 & \cdots & & \cdots & 0 \\
\hline
 & \text{vector}(\rho) & & 1 & & & & \\
 & \text{vector}(\rho\iota) & & & \ddots & & & \\
 & \vdots & & & & \ddots & & \\
 & \text{vector}(\rho\iota^j) & & & & & \ddots & \\
 & \vdots & & & & & & \ddots \\
 & \text{vector}(\rho\iota^{k-1}) & & & & & & 1
\end{array}\right)
$$

where $\mathfrak{Q} = \langle \mathfrak{q}, \alpha_f - \rho \rangle$ and $\mathfrak{q} = \langle q, \varphi_{\mathfrak{q}}(\iota) \rangle$.

From relations to equations

Absolute polynomial

Let θ be a complex number in K_f such that $\mathbb{Q}(\iota, \alpha_f) = \mathbb{Q}(\theta)$ and f_h the minimal polynomial of θ over $\mathbb{Q}$ (an absolute polynomial of the tower).

Virtual logarithm

The definition of virtual logarithms doesn't depend on the manner in which the relations are collected. Hence, we can consider that we are working doing NFS for f_h.

Why not using f_h directly

- Seen as elements of $\mathbb{Q}(\theta)$, the numbers $a - b\alpha_f$ have no easy structure.
- The estimations of $\mathrm{N}_{K/\mathbb{Q}}(a - b\alpha_f)$ are wrong if we see them as random elements of θ with coordinates of the same size.

Outline of the talk

- Number field sieve
- Tower number field sieve
- Applications
- Practical details

Application 1: an alternative for general fields

Advantage

Same polynomials f and g are used as those used for computations in $\mathbb{F}_p$.
Several methods are optimized:

- Kleinjung's methods for factoring NFS (2006 and 2008) can be used for discrete logs;
- Joux-Lercier's method for discrete log (2003) is very competitive when p is small.

Obsolete advantage

- In 2014 Pierrick Gaudry gave a talk on TNFS and pointed out that it was the state of art when $p = L_{p^k}(2/3, c)$ for some values of c.
- The generalized Joux-Lercier method (GJL), presented in 2014 by BGGM, improved the complexity of JLSV, so TNFS is not any more the state-of-art.

Application 2: sporadic families of pairing-friendly curves

Example (ex 6.9 of Freeman, Scott, Teske 2010)

One has to solve DLP in $\mathbb{F}_{p^k}$ for

$$\begin{aligned} k &= 4 \\ t(x) &= -4x^3 \\ r(x) &= 4x^4 + 4x^3 + 2x^2 + 2x + 1 \\ p &= \tfrac{1}{3}(16x^6 + 8x^4 + 4x^3 + 4x^2 + 4x + 1). \end{aligned}$$

$\boxed{\text{Can we use the special form of } p\text{?}}$

Special form

SNFS numbers

An integer is SNFS for a parameter d if

$$p = P(u)$$

for an integer u and $P \in \mathbb{Z}[x]$ with $\deg P = d$ and $\|P\|_\infty = O(1)$.

Context

- SNFS variants of NFS for factoring and DLP have complexity $C^{1/\sqrt[3]{2}}$ where C is the complexity of NFS;
- SNFS moduli are not used for RSA although they have a better arithmetic.

Joux-Pierrot's SNFS (2013)

Asymptotic results

- large characteristic: same as SNFS factoring, i.e. $C = L_{p^k}(1/3, \sqrt[3]{\frac{32}{9}})$;
- medium characteristic: same as classical NFS, i.e. $C^{\sqrt[3]{2}} = L_{p^k}(1/3, \sqrt[3]{\frac{64}{9}})$.

Properties of the polynomials, $Q = p^k$

	deg	$\|\cdot\|_\infty$
f	dk	$O(1)$
g	k	$Q^{1/kd}$.

Note that n is given and d is fixed by the shape of the prime p.

Norm's size

Joux-Pierrot

- We introduce a parameter t, so that we sieve on t-term polynomials ϕ. To keep the same cardinality of the sieving space we impose $\|\phi\|_\infty \leq E^{2/t}$ where E is the parameter used when $t = 2$.
- $\|\varphi\|_\infty^{\deg f + \deg g} \|f\|_\infty^t \|g\|_\infty^t$ or

$$\boxed{\text{bound on norms} = E^{2k(d+1)/t} Q^{t/(kd)}}$$

TNFS on SNFS primes

- If A is the bound on coefficients of a and b,

$$|\,\mathrm{N}_{K/\mathbb{Q}}\left(a(\iota) - b(\iota)\alpha_f\right)| < A^{dk} \|f\|_\infty^k \|h\|_\infty^{d(k-1)} C(k,d),$$

  where $d = \deg f$ and $C(k,d) = (k+1)^{(3d+1)k/2}(d+1)^{3k/2}$.
- In order to have the same size of sieving space we take $A = E^{1/k}$.
- If we take $\|h\|_\infty = 1$ and we neglect the combinatorial overhead:

$$\boxed{\text{bound on norms} = E^{d+1} Q^{1/d}.}$$

Precise comparison

General condition

- Q is given and E is measured by practical experiments so $\log Q / \log E$ is fixed.
- TNFS is better if and only if

$$\boxed{\left(\frac{t-1}{k}-1\right)\frac{\log Q}{\log E} > d(d+1)\left(1-\frac{2k}{t}\right)}$$

Copying parameters from a record

- The SNFS record of factoring, a 1039-bit number, is due to Aoki et al. We have
  - $d = 6$;
  - $\log_2 E \approx 31$ and $\log_2 Q \approx 1039$;
  - $\frac{\log Q}{\log E} \approx 34.2$.

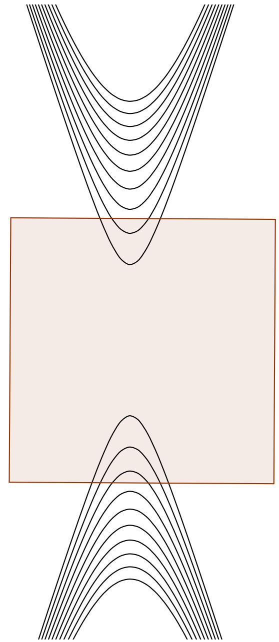
Comparison on our example

- In our example $k = 4$. We take p to be a 256-bit prime in our family.
- The condition is true for any t, the best value is $t = 9$.
- The bound on the norms for the best parameters are

Joux-Pierrot	TNFS
768	386

Explanation

- The absolute degree of the field of f in TNFS and the degree of the field of f in Joux-Pierrot's algorithm is the same: kd.
- While JLSV and Joux-Pierrot sieve in a box, the elements considered by Schirokauer follow the geometry of the problem.
- The elements sieved by Schirokauer in the drawing below would be close to the vertical sides of the square.



Outline of the talk

- Number field sieve
- Tower number field sieve
- Applications
- Practical details

Franke-Kleinjung

Algorithm

Franke-Kleinjung (2009)

Input parameters I, J, a prime q and an integer s;

Output the intersection of the lattice $L_{q,s} = \{(a,b) \in \mathbb{Z}^2 \mid a \equiv bs \mod q\}$ with the rectangle $[-I/2, I/2] \times [0, J]$.

1: Prepare a basis $\{(\alpha,\beta),(\gamma,\delta)\}$ of $L_{q,s}$ so that
- $\beta, \delta > 0$;
- $-I < \alpha \le 0 \le \gamma < I$ and $\gamma - \alpha \ge I$.

2: The next point to enumerate after (i,j) is obtained by adding:
- (γ,δ) if $i < I/2 - \gamma$;
- $(\alpha+\gamma, \beta+\delta)$ if $I/2 - \gamma \le i < -I/2 - \alpha$;
- (α,β) if $i \ge -I/2 - \alpha$.

TNFS special-Q

The lattice $L_{q,s}$ is replaced by the lattice below, more precisely q is replaced by $\mathfrak{p} = \langle p, \varphi_{\mathfrak{p}}(\iota)\rangle$, a prime ideal of $\mathbb{Z}[\iota]$, and s by some integer coordinates i_*^*.

$$M_{\mathfrak{Q},\mathfrak{L}} = \left(\begin{array}{cccc|ccccc}
p & & & & 0 & \cdots & & \cdots & 0 \\
 & \ddots & & & \vdots & & & & \vdots \\
 & & p & & & & & & \\
\multicolumn{3}{|c|}{\text{vector}(\varphi_{\mathfrak{p}})} & & & & & & \\
 & & & \ddots & \vdots & & & & \vdots \\
 & & \multicolumn{2}{|c|}{\text{vector}(\varphi_{\mathfrak{p}})} & 0 & \cdots & & \cdots & 0 \\
\hline
i_0^{(0)} & \cdots & \cdots & i_{n-1}^{(0)} & 1 & & & & \\
\vdots & & & \vdots & & \ddots & & & \\
 & & & & & & \ddots & & \\
 & & & & & & & \ddots & \\
\vdots & & & \vdots & & & & & \ddots \\
i_0^{(n-1)} & \cdots & \cdots & i_{n-1}^{(n-1)} & & & & & 1
\end{array}\right),$$

Problem

The Franke-Kleinjung algorithm only works in dimension two.

Roots of unity

Classical variant

In order to avoid duplicates, we sieve only one of the pairs (a, b) and $(-a, -b)$. For this we restrict to the pairs when $a > 0$.

TNFS

- When $\iota = \sqrt{-1}$, the roots of unity are $1, -1, \iota, -\iota$. We restrict to pairs (a, b) where $a = a_0 + \iota a_1$ with $a_0, a_1 > 0$.
- In the general case, e.g. $\iota^4 = -1$, we have a similar situation.

Consequences

We have less pairs to sieve with a given norm size. It is as if we lost one or two bits in the norm size.

Automorphisms of $\mathbb{Q}(\iota)$

Polynomial selection

We restrict the search of h to families with k automorphisms over $\mathbb{Q}$.

Theorem

If $\mathbb{Q}(\iota)$ is Galois and σ is an automorphism, then any ideal $\mathfrak{Q} = \langle \mathfrak{q}, \alpha_f - r(\iota) \rangle$ in the factor base has conjugates

$$\mathfrak{Q}^\sigma = \langle \mathfrak{q}^\sigma, \alpha_f - r(\sigma(\iota)) \rangle.$$

Relation collection

- The sieve is organized in tasks which collect pairs (a, b) such that $(a - b\alpha_f)$ is divisible by $\mathfrak{Q}$.
- As BGGM (2014) we use only one ideal in each conjugacy class. The speed-up is
  - k in the sieve;
  - k^2 in the linear algebra.
- When $k \not\in \{2, 3, 4, 6, 8\}$, TNFS is the only variant of NFS which can take advantage of automorphisms.

Conclusion and open questions

1. Some parings-based crypto-systems rely on the difficulty of DLP in $\mathbb{F}_{p^k}$ when p is SNFS.
2. Schirokauer's TNFS offers a good candidate for computation records.
3. It is an interesting generalization of NFS from a mathematical point of view.
4. It puts new algorithmic problem, the most important being to extend the Franke-Kleinjung method to dimension > 2.