

# Notes on the General Number Field Sieve

Simon Pohmann

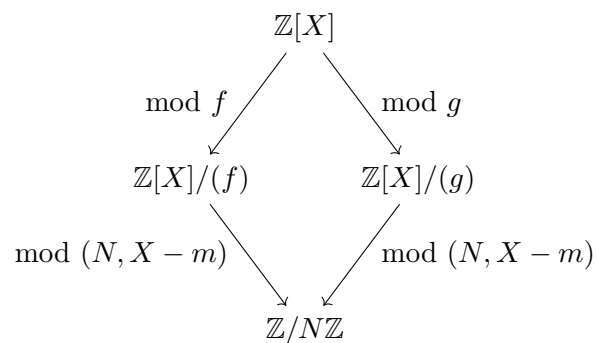
July 19, 2023

## Contents

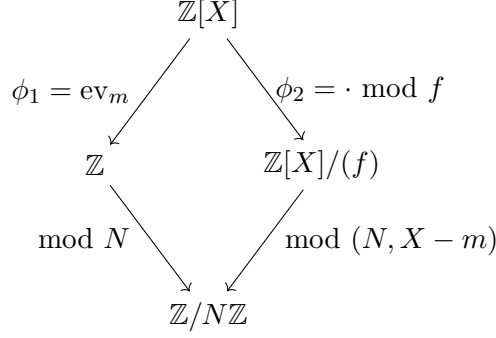
<b>1 Setup</b>	<b>1</b>
<b>2 A special case</b>	<b>2</b>
<b>3 The general case</b>	<b>2</b>
<b>4 Choice of parameters</b>	<b>3</b>
4.1 Details . . . . .	4

## 1 Setup

The basic situation is given by the diagram



where  $f, g$  are coprime, irreducible polynomials with  $f(m) = g(m) = 0 \pmod{N}$ . It is common to choose  $g = X - m$ . We will work with this simplified situation, so have



## 2 A special case

For now assume that  $\mathbb{Z}[X]/(f)$  is the ring of integers  $\mathcal{O}_K$  in the number field  $K = \mathbb{Q}[X]/(f)$ , and additionally that it has class number 1 and trivial unit group  $\mathcal{O}_K^* = \{\pm 1\}$ .

We choose a smoothness bound  $B$ , and have the factor bases  $\{p \in \mathbb{Z} \mid p \leq B \text{ prime}\}$  in  $\mathbb{Z}$  and  $\{\mathfrak{p} \leq \mathcal{O}_K \mid \mathfrak{p} \text{ prime ideal over prime } p \leq B\}$  in  $K$ . Now we search a wide range of values  $aX + b \in \mathbb{Z}[X]$  for elements such that both  $\phi_1(aX + b) = am + b$  and  $\phi_2(aX + b)$  factor over the factor base.

Having found enough, we can multiply a suitable subset and find  $aX + b$  such that both

$$\phi_1(aX + b) = am + b = x^2 \quad \text{and} \quad \phi_2(aX + b) = y^2$$

are squares. With some luck now,

$$x \bmod N \neq \pm y \bmod (N, X - N)$$

and we have found a congruent square.

## 3 The general case

If we use the same approach in the general case, we will end up with  $aX + b$  such that

$$(\phi_2(aX + b)) = \mathfrak{a}^2$$

for an ideal  $\mathfrak{a} \leq \mathcal{O}_K$ . However,  $\mathfrak{a}$  might not be principal, and even if  $\mathfrak{a} = (y)$ , we might have that  $y \notin \mathbb{Z}[X]/(f)$ , or that only  $y^2 = \epsilon \phi_2(aX + b)$  with  $\epsilon \in \mathcal{O}_K^*$  but  $\epsilon \neq 1$ .

We fix this by introducing a quadratic character base of characters

$$\chi : \mathbb{Z}[X]/(f) \rightarrow \{-1, 0, 1\}$$

and find  $aX + b$  such that not only  $(\phi_2(aX + b)) = \mathfrak{a}^2$  but also  $\chi(\phi_2(aX + b)) = 1$  for all  $\chi$  in the character base. After that, we just hope that these “problems” do not occur.

More concretely, we choose another bound  $B'$  and take the characters

$$\chi : \mathbb{Z}[X]/(f) \rightarrow \{-1, 0, 1\}, \quad x \mapsto \begin{cases} 1 & \text{if } x \bmod \mathfrak{p} \text{ is a square in } \mathbb{F}_{p^f} \\ 0 & \text{if } x \in \mathfrak{p} \\ -1 & \text{if } x \bmod \mathfrak{p} \text{ not a square in } \mathbb{F}_{p^f} \end{cases}$$

where  $\mathfrak{p}$  is a prime ideal of  $\mathcal{O}_K$  over the prime number  $B < p \leq B'$  and has degree of inertia  $f$ . Note that if  $p > B$  and  $\phi_2(aX + b)$  is  $B$ -smooth, then this implies that  $\chi(\phi_2(aX + b)) \neq 0$ .

## 4 Choice of parameters

First of all, we use the following theorem.

**Theorem 4.1** (Canfield-Erdos-Pomerance). *Let  $n$  be a uniformly random integer  $\leq x$ . Then the probability that  $n$  is  $B$ -smooth is at least*

$$\exp(-u \log(u)) = u^{-u}$$

for sufficiently large  $x$ , where

$$u = \frac{\log(x)}{\log(B)}$$

We ignore the quadratic characters in the following. Note that for  $a, b$  and  $\theta := \phi_2(X)$ , we know that  $\phi_2(aX + b) = a\theta + b$  factors over the algebraic factor base iff  $N(a\theta + b)$  is  $B$ -smooth. Furthermore

$$N(a\theta + b) = a^d \text{MiPo}(\theta)(-b/a) \leq \|\text{MiPo}(\theta)\|_1 \max(|a|^d, |b|^d)$$

In particular, if  $|a|, |b| \leq C$  then  $N(a\theta + b)$  is of size approximately  $mC^d$ .

Now we have that both  $N(a\theta + b)$  and  $am + b$  are  $B$ -smooth iff  $(am + b)N(a\theta + b)$  is. We assume that this value is uniformly distributed, and of size approximately  $m^2 C^{d+1}$ . In other words, for a random  $aX + b$  with  $|a|, |b| \leq C$ , we find a relation with probability

$$\exp\left(-\frac{\log(m^2 C^{d+1})}{\log(B)}(\log \log(m^2 C^{d+1}) - \log \log(B))\right)$$

As we need  $B$  such relation to find a solution to the linear equations, we need to search

$$\exp\left(\log(B) + \frac{\log(m^2 C^{d+1})}{\log(B)}(\log \log(m^2 C^{d+1}) - \log \log(B))\right)$$

tuples  $(a, b)$ . We insert that  $\log(m) = \log(N)/d$  and expand, to get

$$\exp\left(\log(B) + \frac{\frac{2}{d} \log(N) + (d+1) \log(C)}{\log(B)} \left(\log(d) + \log \log(C) - \log \log(B) + O\left(\frac{2 \log(N)}{d^2 \log(C)}\right)\right)\right)$$

To optimize this, we first consider an approximation of this expression, namely

$$\exp\left(\log(B) + \frac{\log(N) + d^2 \log(C)}{d \log(B)}\right)$$

We want to optimize this, subject to

$$\exp\left(\log(B) + \frac{\log(N) + d^2 \log(C)}{d \log(B)}\right) \leq \exp(\log(C)) \leq \exp(2 \log(C))$$

which just means that there are enough tuples  $(a, b)$  with  $|a|, |b| \leq C$  to yield the desired amount of relations.

Taking logarithms, we arrive at

$$\text{minimize } \underbrace{b + \frac{n + d^2 c}{db}}_{=:R} \quad \text{subject to } b + \frac{n + d^2 c}{db} \leq c$$

We find

$$\nabla R = \left(1 - \frac{n + d^2 c}{db^2}, \frac{d}{b}, \frac{2d^2 c - (n + d^2 c)}{d^2 b}\right)^T$$

This clearly has no optima, so we consider the border of the region, i.e. assume

$$c = b + \frac{n + d^2 c}{db} \quad \text{hence} \quad \left(1 - \frac{d}{b}\right) c = b + \frac{n}{db}$$

and we arrive at

$$\text{minimize } b + \frac{n(1 - \frac{d}{b}) + d^2(b + \frac{n}{db})}{(1 - \frac{d}{b})db} = b + \frac{ndb - nd^2 + d^3 b^2 + nd^2}{d^2 b^2 - d^3 b} = b + \frac{n + d^2 b}{db - d^2}$$

Now we have

$$\nabla \left(b + \frac{n + d^2 b}{db - d^2}\right) = \left(\frac{b(b - 2d)d - n}{(b - d)^2 d}, \frac{n(2d - b) + b^2 d^2}{(b - d)^2 d^2}\right)$$

Setting this to 0, and ignoring small constants, we find

$$d \log(B)^2 \approx \log(N), \quad d^2 \log(B)^2 \approx \log(N)(2d - \log(B))$$

and so  $\log(B) \approx \log(N)^{1/3}$  and  $d \approx \log(N)^{1/3}$ .

## 4.1 Details

To get a more precise estimate without exploding all the expressions, we now use the Landau symbol

$$L_N(\alpha, a) = \exp((a + o(1)) \log(N)^\alpha \log \log(N)^{1-\alpha})$$

We set  $B = L_N(1/3, b)$  and  $C = L_N(\gamma, c)$  and  $d = (1 + o(1)) \log(N)^{1/3}$ . Then the probability that some tuple gives us a relation (i.e. the images under  $\phi_1, \phi_2$  are smooth) can now be written as

$$\begin{aligned}
& \exp \left( - \frac{\log(m^2 C^{d+1})}{\log(B)} (\log \log(m^2 C^{d+1}) - \log \log(B)) \right) \\
&= \exp \left( - \frac{(2 + o(1)) \log(N)^{2/3} + (d + 1)(c + o(1)) \log(N)^\gamma \log \log(N)^{1-\gamma}}{(b + o(1)) \log(N)^{1/3} \log \log(N)^{2/3}} \right. \\
&\quad \left( \log \left( (2 + o(1)) \log(N)^{2/3} + (1 + o(1)) \log(N)^{\gamma+1/3} \log \log(N)^{1-\gamma} \right) \right. \\
&\quad \left. \left. - \log((b + o(1)) \log(N)^{1/3} \log \log(N)^{2/3}) \right) \right)
\end{aligned}$$