NTNU – Trondheim
Norwegian University of
Science and Technology

Improving on the Number Field Sieve

Per Kristian Ørke

Master of Science in Mathematics
Submission date: May 2015
Supervisor: Kristian Gjøsteen, MATH

Norwegian University of Science and Technology
Department of Mathematical Sciences

Abstract

We look at efficient methods for computing logarithms in finite fields of any type. To achieve this, we first develop methods for factoring integers and computing discrete logarithms in fields of prime order using algebraic number theory. Then we show how this can be improved in the general case.

Sammendrag

Vi studerer effektive metoder for å regne ut diskrete logaritmer i vilkårlige, endelige kropper. For å oppnå dette, utvikler vi først metoder for å faktorise heltall og regne ut diskrete logaritmer i primtallskropper ved å benytte algebraisk tallteori. Deretter viser vi hvordan dette kan forbedres i det generelle tilfellet.

Preface

During my year of writing this thesis, I have had limited contact with my supervisor, Kristian Gjøsteen, due to his paternity leave. This has led to situations in which I have been working on a certain problem for quite a long time, only to realize the solution was completely trivial after talking to him for two minutes. He was always able to understand my more or less vague questions, and in most cases, he would immediately see the answer and guide me towards it. I am very grateful for having such a nice supervisor.

Also deserving my gratitude are the graduates whose previous work on the number field sieve I have built upon. Finally, I would like to thank the Norwegian University of Science and Technology for offering me the opportunity to study my favourite branch of science and and write this thesis.

Contents

Chapter 1

Introduction

Several cryptographic systems and schemes are based on the assumptions that integer factorization and discrete logarithm computation is far from trivial. A standard example is the RSA cryptosystem, in which the public key contains a product of large prime numbers. To break the system directly, one would have to know the factorization. Similarly, the public key in the ElGamal cryptosystem contains a group generator raised to a certain power, and one needs to know the exponent, i.e. find the discrete logarithm, in order to decrypt.

A central objective in cryptography is therefore to analyze how difficult these problems really are. If one can find polynomial time algorithms for factoring integers and/or computing discrete logarithms, one would have to adjust these cryptosystems or stop using them entirely. So trying to find the fastest such algorithms possible is a vital part of modern cryptography.

Integer factorization and dicrete logarithm computation turn out to be closely related, and some of the same algorithms can be used to attack both problems. In 1988, John Pollard introduced the *number field sieve* which exploits algebraic number theory to factor integers faster than ever before. Daniel M. Gordon adapted in 1992 the algorithm to the discrete logarithm problem for prime fields, where it also became the fastest known method.

In 2013, Antoine Joux proposed a method for computing discrete logarithms in fields of any order, which reduces the problem to computing certain discrete logarithms in small underlying fields, and can therefore be built on top of the number field sieve. The running time of this algorithm relative to the size of the field was a significant improval of the prime case. In fact, it was later shown that the algorithm could obtain so-called quasi-polynomial complexity in certain cases.

We will present and discuss all these algorithms in this thesis, along with their theoretical foundations. We will also provide analyses of their complexities.

Chapter 2

Algebraic theory

This chapter will deal with algebraic concepts and theoretical mathematics that will be necessary to understand the algorithms and proofs presented in later chapters. All definitions and related results will be stated here and then referred to whenever needed.

Prerequisites for understanding this thesis is set theory, elementary number theory (modular arithmetic), linear algebra, basic abstract algebra (groups, fields, rings, ideals, modules), some Galois theory and a certain amount of basic calculus. We we will also assume knowledge of Zorn's lemma.

2.1 Number fields and number rings

Let $f \in \mathbb{Q}[x]$ be a monic, irreducible polynomial of degree d, and assume $\alpha \in \mathbb{C}$ to be a root of f. Consider the field extension

$$\mathbb{Q}[\alpha] = \left\{ a_0 + a_1\alpha + \ldots + a_{d-1}\alpha^{d-1} \mid a_i \in \mathbb{Q} \ \forall i \right\}$$

of the rational numbers. We will refer to this as a *number field.* An element $\beta \in \mathbb{Q}[\alpha]$ in a number field is an *algebraic integer* if there is a monic polynomial $g \in \mathbb{Z}[x]$ such that β is a root of g.

Proposition 1. *Let $\frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$ and $\gcd(a,b) = 1$ be an algebraic integer. Then $\frac{a}{b} \in \mathbb{Z}$.*

Proof. Let

$$g(x) = x^{d'} + \sum_{i=0}^{d'-1} c_i x^i$$

be the minimal polynomial of $\frac{a}{b}$ over $\mathbb{Z}$. We then have

$$\begin{aligned} g\left(\frac{a}{b}\right) &= \left(\frac{a}{b}\right)^{d'} + \sum_{i=0}^{d'-1} c_i \left(\frac{a}{b}\right)^{i} = 0 \\ \implies \sum_{i=0}^{d'-1} c_i \frac{a^i}{b^i} &= -\frac{a^{d'}}{b^{d'}} \\ \implies \sum_{i=0}^{d'-1} c_i a^i b^{d'-1-i} &= -\frac{a^{d'}}{b} \end{aligned}$$

from multiplying each side by $b^{d'-1}$. The left hand side is now a $\mathbb{Z}$-linear combination of elements in $\mathbb{Z}$ and is hence in $\mathbb{Z}$, so the right hand side must also be an integer. Since $\gcd(a, b) = 1$, this implies $b = \pm 1$, which means that $\frac{a}{b} = \pm a \in \mathbb{Z}$. □

The collection of all algebraic integers in a number field $\mathbb{Q}[\alpha]$ is denoted $\mathcal{O}_{\mathbb{Q}[\alpha]}$. In other words, $\mathcal{O}_{\mathbb{Q}[\alpha]}$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\alpha]$. We will refer to $\mathcal{O}_{\mathbb{Q}[\alpha]}$ as a *number ring*, and it is in fact a subring of $\mathbb{Q}[\alpha]$. An important fact about $\mathcal{O}_{\mathbb{Q}[\alpha]}$ is that every non-zero proper ideal can be factored (uniquely) into a product of prime ideals. This follows from the fact that the ring is a Dedekind domain, a preperty we will now study in detail.

2.2 Dedekind domains

A *Dedekind domain* is an integral domain which is integrally closed, Noetherian and in which every non-zero prime ideal is maximal. To show the unique factorization property of Dedekind domains, we first need to establish a few lemmas. We say that an ideal is *pre-factorizable* if it contains a product of non-zero prime ideals and *factorizable* if it equals a product of prime ideals.

Lemma 2. *Let D be a Dedekind domain. Then every non-zero ideal in D is pre-factorizable.*

Proof. Let $M = \{J \text{ ideal in } D \mid J \text{ not pre-factorizable}\}$. It is then sufficient to show that this set is empty. We will assume that it is not and arrive at a contradiction.

Observe that M is a poset under set inclusion. Let $J_1 \subset J_2 \subset \ldots$ be a chain in M. Since D is Dedekind and hence Noetherian, there exists r such that $J_r = J_{r+1} = \ldots$, this makes J_r an upper bound for the chain. Since every chain then has an upper bound in M, Zorn's lemma tells ut that M has a maximal element A with respect to inclusion.

Clearly, A can not be a prime ideal, as it would then be trivially pre-factorizable and not lie in M. Because of this, there must exist $b_1, b_2 \in D$

such that $b_1b_2 \in A$, but $b_1 \notin A$ and $b_2 \notin A$. Otherwise, A would be prime by definition. Let $A_1 = \langle b_1 \rangle + A$ and $A_2 = \langle b_2 \rangle + A$. Clearly, we have $A \subset A_1$ and $A \subset A_2$, but there can not be equalities since $b_1 \in A_1$ and $b_2 \in A_2$, when none of them were in A. Hence we have $A \subsetneq A_1$ and $A \subsetneq A_2$. But A was the maximal element of M, so this must mean that A_1 and A_2 are not in M and are therefore pre-factorizable. Say that

$$\prod_{i=1}^{r} P_i \subset A_1$$
$$\prod_{j=1}^{s} Q_j \subset A_2$$

where P_i and Q_j are prime ideals for all i and j.

We now claim that $A_1A_2 \subset A$. Let $a_1 \in A_1$ and $a_2 \in A_2$, i.e. there exists $c_1, c_2 \in D$ and ${a_1}', {a_2}' \in A$ such that $a_1 = c_1b_1 + {a_1}'$ and $a_2 = c_2b_2 + {a_2}'$. Then

$$a_1a_2 = c_1c_2b_1b_2 + c_2b_2{a_1}' + c_1b_1{a_2}' + {a_1}'{a_2}' \in A$$

since $b_1b_2 \in A$. This shows that $A_1A_2 \subset A$. Hence we have

$$\prod_{i=1}^{r} P_i \prod_{j=1}^{s} Q_j \subset A_1A_2 \subset A$$

and A is pre-factorizable, a contradiction since it is in M. We conclude that $M = \emptyset$ and hence every ideal is pre-factorizable. □

Lemma 3. *Let D be a Dedekind domain and let P be a prime ideal in D. Let K be the field of fractions of D and $P' = \{k \in K \mid kP \subset D\}$. Let I be an ideal in D. Then $IP' \neq I$.*

Proof. It is clear that $D \subset P'$, but do we have equality? Let $0 \neq a \in P$. Lemma 2 tells us that $\langle a \rangle$ is pre-factorizable, so assume that $\prod_{i=1}^{r} P_i \subset \langle a \rangle$ where all the P_i are prime ideals and the r is as small as possible.

Assume that $P_i \not\subset P \ \forall i$. Then there exists $a_i \in P_i \setminus P$ for all i. But then

$$\prod_{i=1}^{r} a_i \in \prod_{i=1}^{r} P_i \subset \langle a \rangle \subset P,$$

and since P is prime, there must be a j such that $a_j \in P$. This is a contradiction, so we know that there is a j such that $P_j \subset P$. Now, P_j is a prime ideal and therefore maximal since D is a Dedekind domain. This means that P must either be equal to P_j or the whole ring D. Since P is prime, we can conclude that $P = P_j$.

Without loss of generality, we can assume that $j = 1$. Recall that r was chosen as small as possible, therefore $\prod_{i=2}^{r} P_i \not\subset \langle a\rangle$. So let $b \in (\prod_{i=2}^{r} P_i) \setminus \langle a\rangle$. Consider the element $\frac{b}{a}$ in K. This is not in D, since then we would have $a \cdot \frac{b}{a} = b \in \langle a\rangle$, a contradiction. But

$$bP \subset \left(\prod_{i=2}^{r} P_i\right) P = \prod_{i=1}^{r} P_i \subset \langle a\rangle,$$

so for all p in P, there is a c in D such that $bp = ca$. Hence

$$\frac{b}{a} \cdot p = c \in D \implies \frac{b}{a} P \subset D \implies \frac{b}{a} \in P'$$

The conclusion is that $D \neq P'$.

In a Noetherian ring, every ideal is finitely generated. So, since D is a Dedekind domain, we have that $I = \langle \alpha_1, \ldots, \alpha_n\rangle$ for some $\alpha_i \in I$. Now assume that $IP' = I$, the opposite of what we are trying to show. Let $k \in P'$. Then $k\alpha_i \in IP' = I\ \forall i$, so we can express these elements using the set of generators:

$$k\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j$$

where $a_{ij} \in D\ \forall i, j$. Define

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

and consider the matrix $A = \left(k\delta_{ij} - a_{ij}\right)_{ij}$ where i and j range from 1 to n. Then

$$\begin{aligned} A\left(\alpha_i\right)_i &= \left((k - a_{ii})\alpha_i - \textstyle\sum_{j\neq i} a_{ij}\alpha_j\right)_i \\ &= \left(k\alpha_i - \textstyle\sum_j a_{ij}\alpha_j\right)_i = \left(k\alpha_i - k\alpha_i\right)_i \\ &= \left(0\right) \end{aligned}$$

From [4], we have that $Bx = 0 \implies \det(B)x = 0$, so we have in our case that $\det(A)\alpha_i = 0\ \forall i$. Since the α_i are generators, they are non-zero, and since D is an integral domain, we then have that $\det(A) = 0$. Now consider the polynomial $g(X) = \det\left(X\delta_{ij} - a_{ij}\right)_{ij} \in D[X]$, which is monic since X only appears on the diagonal and never with any coefficient (other than 1) in front of it. We have just shown that k is a root of this polynomial. Since D is integrally closed, being a Dedekind domain, and k is the root of a monic polynomial over D, we have that $k \in D$.

This means that $P' \subset D$ and hence $P' = D$. But we have already seen that this is not true, so we conclude that our assumption $IP' = I$ was wrong.

□

We are ready for our main result concerning Dedekind domains.

Theorem 4. *Let D be a Dedekind domain. Then every non-zero, proper ideal in D is factorizable and its factorization into prime ideals is unique up to ordering.*

Proof. We first prove existence of the factorization. Mirroring the idea from the proof of Lemma 2, we consider the set $M = \{J \text{ ideal in } D \mid J \text{ not factorizable}\}$, which we assume is non-empty. The exact same argument gives us a maximal element A, which again can not be a prime ideal. All ideals are contained in a maximal ideal, so let P be a maximal (and therefore prime) ideal with $A \subset P$.

$1P = P \subset D$ and therefore $1 \in P'$, so $A \subset AP'$. Also, $PP' \subset D$ by definition of P'. In total, we have $A \subset AP' \subset PP' \subset D$. The second inclusion is clearly strict, and from Lemma 3, we also have that the first inclusion is. So we have $A \subsetneq AP' \subsetneq D$. Since A was the maximal element of M, this means that $AP' \notin M$. It is therefore factorizable, so assume

$$AP' = \prod_{i=1}^{r} P_i$$

Lemma 3 also tells us that $P \neq PP'$. But clearly $P \subset PP'$, so $P \subsetneq PP'$. Note that PP' is an ideal in D. Since P was a maximal ideal, this means that we must have $PP' = D$. But then

$$A = AD = APP' = P \prod_{i=1}^{r} P_i,$$

and hence A is factorizable, a contradiction. We conclude that $M = \emptyset$ and hence every ideal is factorizable.

To prove uniqueness, assume that an ideal I has two factorizations

$$I = \prod_{i=1}^{r} P_i = \prod_{j=1}^{s} Q_j,$$

where P_i and Q_j are prime ideals for all i and j. Assume without loss of generality that $r \leq s$. Using the properties of prime ideals, we get

$$\begin{aligned} \prod_{i=1}^{r} P_i = \prod_{j=1}^{s} Q_j \subset Q_1 &\implies P_1 \subset Q_1 \text{ or } \prod_{i=2}^{r} P_i \subset Q_1 \implies \dots \\ &\implies P_1 \subset Q_1 \text{ or } \dots \text{ or } P_r \subset Q_1 \end{aligned}$$

So assume without loss of generality that $P_1 \subset Q_1$. Every prime ideal in D is maximal, so P_1 is a maximal ideal. The inclusion then means that Q_1 is equal to either P_1 or D, but since Q_1 is prime, we must have $P_1 = Q_1$.

Now, mutiplying the two factorizations with P_1', we get

$$P_1'\prod_{i=1}^{r}P_i = P_1'\prod_{j=1}^{s}Q_j \implies P_1'P_1\prod_{i=2}^{r}P_i = P_1'P_1\prod_{j=2}^{s}Q_j \implies \prod_{i=2}^{r}P_i = \prod_{j=2}^{s}Q_j$$

since $P_1'P_1 = D$. We can continue eliminating prime ideals using the same argument until we are left with $P_r = \prod_{j=r}^{s} Q_j$ Assume that $r < s$. Then we can use the argument again and multiply by P_r' to obtain

$$P_r'P_r = P_r'P_r\prod_{j=r+1}^{s}Q_j \implies D = \prod_{j=r+1}^{s}Q_j,$$

an impossibility. Hence $r = s$. We have also shown that $P_i = Q_i$ for all i after reordering. Therefore, the factorization is unique. □

The important observation for us is that $\mathcal{O}_{\mathbb{Q}[\alpha]}$ is a Dedekind domain. For a proof of this, see [4]. This allows us to talk about factorization of ideals in $\mathcal{O}_{\mathbb{Q}[\alpha]}$ and also the concept *ramification*. Let p be a prime and

$$p\mathcal{O}_{\mathbb{Q}[\alpha]} = \prod_i P_i^{f_i}$$

be the factorization of the ideal generated by p into prime ideals P_i. We say that p is unramified if $f_i = 1$ for all i, i.e. the ideal is ”square-free”.

2.3 Finite fields

Before proceeding with our number rings, we need to mention some topics on finite fields. To perform computations in a finite field, we need to have a model for it. For prime fields F_p we will use $\mathbb{Z}_p$, the integers modulo p with addition and multiplication modulo p. For fields on the form F_{p^k}, we will use the model we already have for F_p together with an irreducible polynomial P over $\mathrm{F}_p[x]$ to form the model $\mathrm{F}_p/\langle P\rangle$. The context will decide whether we refer to the field or the model throughout this thesis.

Given a finite field F_n, define the projective line $\mathrm{P}^1(\mathrm{F}_n)$ to be the set

$$\mathrm{P}^1(\mathrm{F}_n) = \left(\mathrm{F}_n^2 \setminus \{(0,0)\}\right) / \sim\,,$$

where $(a,b) \sim (c,d) \iff \exists f \in \mathrm{F}_n^*$ such that $(a,b) = f(c,d)$. Note that $\{(f,1)\}_{f\in\mathrm{F}_n} \cup \{(1,0)\}$ is a set of representatives for $\mathrm{P}^1(\mathrm{F}_n)$. We will call this representation the *homogenous coordinates* of $\mathrm{P}^1(\mathrm{F}_n)$. Consequently, we have that $\left|\mathrm{P}^1(\mathrm{F}_n)\right| = n+1$.

Proposition 5. *Let q be a prime and let $\{(\alpha, \beta)\}$ be the homogenous coordinates of* $\mathrm{P}^1(\mathrm{F}_q)$*. Then the following equality holds in any field of cardinality q:*

$$XY^q - X^qY = \prod_{(\alpha,\beta)} (\beta X - \alpha Y) \tag{2.1}$$

Proof. Recall that

$$X^q - X = \prod_{f \in \mathrm{F}_q} (X - f)$$

Replacing X with $\frac{X}{Y}$, we obtain

$$\left(\frac{X}{Y}\right)^q - \frac{X}{Y} = \prod_{f \in \mathrm{F}_q} \left(\frac{X}{Y} - f\right)$$

Multiplying each side by $-Y^{q+1}$, we get

$$\begin{aligned} XY^q - X^qY &= -Y \prod_{f \in \mathrm{F}_q} (X - fY) \\ &= (0X - 1Y) \prod_{f \in \mathrm{F}_q} (1X - fY) \\ &= \prod_{(\alpha,\beta) \in \mathrm{P}^1(\mathrm{F}_q)} (\beta X - \alpha Y) \end{aligned}$$

□

2.4 The norm

A concept that will be of great importance in the discussion of our algorithms, is the *norm* of an element in a number field. We will first show that there are exactly d embeddings of $\mathbb{Q}[\alpha]$ in $\mathbb{C}$ that fix every element of $\mathbb{Q}$: Let $\alpha_1, \ldots, \alpha_d$ be the roots of f. Consider the d homomorphisms $\sigma_i : \mathbb{Q}[\alpha] \to \mathbb{C}$ defined by $\alpha \mapsto \alpha_i$. These are all embeddings, so there are at least d such. Now assume that we have another one, namely a σ_{d+1} that sends α to some β. If we write f as $\sum_{i=0}^{d} c_i x^i$, we have that

$$\begin{aligned} f(\beta) &= \sum_{i=0}^{d} c_i \beta^i = \sum_{i=0}^{d} c_i \sigma_{d+1}(\alpha)^i = \sum_{i=0}^{d} \sigma_{d+1}(c_i) \sigma_{d+1}\left(\alpha^i\right) \\ &= \sigma_{d+1}\left(\sum_{i=0}^{d} c_i \alpha^i\right) = \sigma_{d+1}(f(\alpha)) = \sigma_{d+1}(0) \\ &= 0 \end{aligned}$$

Here we used that the c_i are all in $\mathbb{Q}$ and hence will be fixed by σ_{d+1}. The conclusion is that β is a root of f and therefore equals one of the α_i, so σ_{d+1} is one of the d embeddings we already had. Hence there can be no more.

Now we are ready to give the definition. Let $\theta \in \mathbb{Q}[\alpha]$. The norm of θ is

$$N(\theta) = \prod_{i=1}^{d} \sigma_i(\theta)$$

First observe that the norm function maps elements in $\mathbb{Q}[\alpha]$ to $\mathbb{Q}$ and elements in $\mathcal{O}_{\mathbb{Q}[\alpha]}$ to $\mathbb{Z}$. Note that if $a + b\alpha$ is in $\mathbb{Z}[\alpha]$, then

$$\begin{aligned} N(a+b\alpha) &= \prod_{i=1}^{d} \sigma_i(a+b\alpha) = \prod_{i=1}^{d} (a+b\alpha_i) \\ &= \prod_{i=1}^{d} b\left(\frac{a}{b} + \alpha_i\right) = -b^d \prod_{i=1}^{d} \left(-\frac{a}{b} - \alpha_i\right) \\ &= -b^d f\left(-\frac{a}{b}\right) \end{aligned} \tag{2.2}$$

since $f(x) = \prod_{i=1}^{d} (x - \alpha_i)$.

The norm of an ideal in $\mathbb{Z}[\alpha]$ is a notion closely related to the norm of elements. We define the norm of an ideal I to be

$$N(I) = [\mathbb{Z}[\alpha] : I]$$

Ideals are then mapped to positive integers. We claim that for $\theta \in \mathbb{Z}[\alpha]$, we have $N(\langle\theta\rangle) = |N(\theta)|$. For a proof of this, see [2].

2.5 First degree prime ideals

Another important concept will be the set $R(p)$, defined as

$$R(p) = \{r \in \{0, 1, ..., p-1\} \mid f(r) \equiv 0 \pmod{p}\}$$

for a prime p. We first show that for the factors of $N(a + b\alpha)$, this set has a special property.

Proposition 6. *Let $a + b\alpha \in \mathbb{Z}[\alpha]$ and let p be a prime number. Assume that p does not divide b. Then p divides $N(a + b\alpha)$ if and only if there is an r in $R(p)$ such that $a \equiv -br \pmod{p}$.*

Proof. Let $r \in R(p)$ be such that $a \equiv -br \pmod{p}$. Then

$$N(a+b\alpha) \equiv -b^d f\left(-\frac{a}{b}\right) \equiv -b^d f\left(-\frac{-br}{b}\right) \equiv -b^d f(r) \equiv 0 \pmod{p}$$

from the definition of $R(p)$ and since f is a polynomial. Assume now that p divides $N(a + b\alpha)$, so, $-b^d f\left(-\frac{a}{b}\right) \equiv 0 \pmod{p}$. Since $p \nmid b$, we have that $f\left(-\frac{a}{b}\right) \equiv 0 \pmod{p}$. Let $r = -\frac{a}{b} \bmod p$. Then $a \equiv -br \pmod{p}$ and $f(r) \equiv 0 \pmod{p}$ since f is a polynomial. □

When we get to our algorithms, we will only consider elements $a + b\alpha$ of $\mathbb{Z}[\alpha]$ such that $\gcd(a, b) = 1$. Note that if p does indeed divide b, it cannot be a factor of any such $N(a + b\alpha)$. Proposition 6 states that if that was the case, we would have an $r \in R(p)$ such that $a \equiv -br \equiv 0 \pmod{p}$. Hence, we would have $\gcd(a, b) \geq p > 1$. Also note that we can only have one r such that $a \equiv -br \pmod{p}$. If $a \equiv -br_1 \equiv -br_2 \pmod{p}$, we must have $r_1 \equiv r_2 \pmod{p}$ since p does not divide b. This is clearly impossible when r_1 and r_2 are both between 0 and $p - 1$.

The set $R(p)$ is also connected to certain prime ideals in $\mathbb{Z}[\alpha]$. We first observe that if $N(P)$ is a prime number for an ideal P, then P is a prime ideal. To see this, we have the following chain of implications

$$\begin{aligned} N(P) = p &\implies [\mathbb{Z}[\alpha] : P] = p \implies \mathbb{Z}[\alpha]/P \cong \mathbb{Z}_p \\ &\implies \mathbb{Z}[\alpha]/P \text{ is a field} \implies P \text{ is a maximal ideal} \\ &\implies P \text{ is a prime ideal} \end{aligned}$$

Conversely, we have that if P is a prime ideal, its norm must be a prime power. If $N(P) = p^n$ for some prime p and some integer n, we say that P is an n'th degree prime ideal. We will be particularly interested in first degree prime ideals, i.e. P such that $N(P) = p$. As noted, this is equivalent to $\mathbb{Z}[\alpha]/P$ being isomorphic to the field with p elements.

The crucial observation is that first degree prime ideals are in one-to-one correspondence with pairs (p, r) such that $r \in R(p)$. To see that a first degree prime ideal admits such a pair, first note that, by definition, its norm is a prime p. Then consider the homomorphism $\phi : \mathbb{Z}[\alpha] \to \mathbb{Z}_p$ and let $r = \phi(\alpha)$. Since $\phi(1) = 1$, we have

$$\begin{aligned} \phi(f(\alpha)) &= \phi\left(\sum_{i=0}^{d} c_i \alpha^i\right) = \left(\sum_{i=0}^{d} c_i \phi(\alpha)^i\right) \bmod p = \left(\sum_{i=0}^{d} c_i r^i\right) \bmod p \\ &= f(r) \bmod p \end{aligned}$$

But $f(\alpha) = 0$, and $\phi(0) = 0$, so r must be a root of f modulo p. Hence $r \in R(p)$.

To go from a pair (p, r) to a first degree prime ideal is quite similar. We construct the homomorphism $\phi : \mathbb{Z}[\alpha] \to \mathbb{Z}_p$ sending α to r. Then we define P to be $\ker(\phi)$. Our map is clearly onto, so the first isomorphism theorem for rings tells us that $\mathbb{Z}[\alpha]/P$ is isomorphic to $\mathbb{Z}_p$. Hence $N(P) = [\mathbb{Z}[\alpha] : P] = |\mathbb{Z}_p| = p$ and P is a first degree prime ideal. We note that P is generated by p and $\alpha - r$: For all θ_1, θ_2 in $\mathbb{Z}[\alpha]$, we have

$$\begin{aligned} \phi(\theta_1 p + \theta_2(\alpha - r)) &= \phi(\theta_1)\phi(p) + \phi(\theta_2)\phi(\alpha) - \phi(\theta_2)\phi(r) \\ &= \phi(\theta_1) \cdot 0 + \phi(\theta_2) \cdot r - \phi(\theta_2) \cdot r \\ &= 0, \end{aligned}$$

so the ideal generated by p and $(\alpha - r)$ is contained in P. For the other inclusion, assume that $\theta = \sum_{i=0}^{d-1} a_i \alpha^i \in P$, i.e. $\phi(\theta) \equiv 0 \pmod{p}$. Then there is an integer k such that

$$\begin{aligned} kp = \phi(\theta) &= \phi\left(\sum_{i=0}^{d-1} a_i \alpha^i\right) = \sum_{i=0}^{d-1} a_i r^i \\ \implies kp + \theta &= \sum_{i=0}^{d-1} a_i r^i + \theta \\ \implies \theta &= kp + \sum_{i=0}^{d-1} a_i \alpha^i - \sum_{i=0}^{d-1} a_i r^i = kp + \sum_{i=0}^{d-1} a_i \left(\alpha^i - r^i\right) \end{aligned}$$

and $(\alpha - r)$ is clearly a factor in the sum. Therefore, $\theta = kp + \gamma(\alpha - r)$ for some $\gamma \in \mathbb{Z}[\alpha]$.

The next observation will be used as part of a proof in a later chapter, so we state is as a lemma:

Lemma 7. *Let P be a first degree prime ideal in $\mathbb{Z}[\alpha]$ corresponding to (p, r). Then $a + br \equiv 0 \pmod{p}$ if and only if $a + b\alpha \in P$.*

Proof. Assume there is a k in $\mathbb{Z}$ such that $a + br = kp$. Then

$$a + b\alpha = a + br + b\alpha - br = kp + b(\alpha - r),$$

which is in P, since P is generated by p and $(\alpha - r)$. Now assume that $a + b\alpha$ is in P. Let γ be the map $\mathbb{Z}[\alpha] \to \mathbb{Z}_p$ with kernel P. Since $a + b\alpha \in P$, we have that

$$\gamma(a + b\alpha) = a + br = 0$$

in $\mathbb{Z}_p$, which means that $a + br \equiv 0 \pmod{p}$. □

2.6 The discriminant

We will need more facts about the structure of $\mathcal{O}_{\mathbb{Q}[\alpha]}$, but then we first need more terminology. Let $\sigma_1, \ldots, \sigma_d$ be the d embeddings of $\mathbb{Q}[\alpha]$ in $\mathbb{C}$. Given elements $\theta_1, \ldots, \theta_d \in \mathbb{Q}[\alpha]$, we define the *discriminant* of the elements, $\operatorname{disc}(\theta_1, \ldots, \theta_d)$, to be the square of the determinant of the matrix with the element $\sigma_i(\theta_j)$ in position ij. We will denote this matrix $[\sigma_i(\theta_j)]$, so

$$\operatorname{disc}(\theta_1, \ldots, \theta_d) = |[\sigma_i(\theta_j)]|^2$$

We want to show that the discriminant maps into $\mathbb{Q}$. To do this, we first observe that

$$\begin{aligned}\operatorname{disc}(\theta_1,\dots,\theta_d) &= |[\sigma_i(\theta_j)]||[\sigma_i(\theta_j)]| = |[\sigma_i(\theta_j)]^T||[\sigma_i(\theta_j)]| = |[\sigma_j(\theta_i)][\sigma_i(\theta_j)]| \\ &= \left|\left[\sum_{k=1}^{d}\sigma_k(\theta_i\theta_j)\right]\right|\end{aligned}$$

Define the *trace* of an element $\theta \in \mathbb{Q}[\alpha]$ to be

$$T(\theta) = \sum_{k=1}^{d}\sigma_k(\theta)$$

Hence we can rewrite $\operatorname{disc}(\theta_1,\dots,\theta_d) = |[T(\theta_i\theta_j)]|$.

Now we claim that the trace maps into $\mathbb{Q}$. We study the number field $\mathbb{Q}[\theta]$, which is a subfield of $\mathbb{Q}[\alpha]$. Let $d' = [\mathbb{Q}[\theta] : \mathbb{Q}]$ and let $\sigma'_1,\dots,\sigma'_{d'}$ be the embeddings of $\mathbb{Q}[\theta]$ in $\mathbb{C}$. We use the notation $t(\theta) = \sum_{i=1}^{d'}\sigma'_i(\theta)$. Now, the minimal polynomial of θ over $\mathbb{Q}$ will look like $\prod_{i=1}^{d'}(x-\sigma_i(\theta))$. The coefficient in front of $x^{d'-1}$ will then be $t(\theta)$, so we conclude that $t(\theta)$ lies in $\mathbb{Q}$.

Lemma 8. *$T(\theta) = \frac{d}{d'}t(\theta)$.*

Proof. From Galois theory, we know that every embedding σ' of $\mathbb{Q}[\theta]$ in $\mathbb{C}$ extends to exactly $\frac{d}{d'}$ embeddings of $\mathbb{Q}[\alpha]$ in $\mathbb{C}$, i.e. embeddings σ such that $\sigma(\gamma) = \sigma'(\gamma)\ \forall\gamma \in \mathbb{Q}[\theta]$.. Let σ'_j be extended to $\sigma_{(j-1)\frac{d}{d'}+1}, \sigma_{(j-1)\frac{d}{d'}+2}, \dots, \sigma_{j\frac{d}{d'}}$ for $j \in \{1,\dots,d'\}$. Then we have

$$\begin{aligned}T(\theta) &= \sum_{i=1}^{d}\sigma_i(\theta) = \sum_{j=1}^{d'}\sum_{k=1}^{\frac{d}{d'}}\sigma_{(j-1)\frac{d}{d'}+k}(\theta) \\ &= \sum_{j=1}^{d'}\sum_{k=1}^{\frac{d}{d'}}\sigma'_j(\theta) = \sum_{j=1}^{d'}\frac{d}{d'}\sigma'_j(\theta) = \frac{d}{d'}\sum_{j=1}^{d'}\sigma'_j(\theta) \\ &= \frac{d}{d'}t(\theta)\end{aligned}$$

□

We conclude from the lemma that the trace is a product of rational numbers and hence itself lies in $\mathbb{Q}$. Since $\operatorname{disc}(\theta_1,\dots,\theta_d) = |[T(\theta_i\theta_j)]|$, and $[T(\theta_i\theta_j)]$ only consists of rational elements, we have shown that $\operatorname{disc}(\theta_1,\dots,\theta_d) \in \mathbb{Q}$. Furthermore, if θ_i is an algebraic integer for all i, we have that $\operatorname{disc}(\theta_1,\dots,\theta_d) \in \mathbb{Z}$, see [3]. We will use the discriminant and the properties we have proven about it, to show that $\mathcal{O}_{\mathbb{Q}[\alpha]}$ is in fact a free $\mathbb{Z}$-module.

2.7 Module structure of number rings

Lemma 9. *Let $\theta \in \mathbb{Q}[\alpha]$. Then there exists $m \in \mathbb{Z}$ such that $m\theta \in \mathcal{O}_{\mathbb{Q}[\alpha]}$.*

Proof. Let $g(x) = \sum_{i=0}^{d'} a_i x^i \in \mathbb{Z}[x]$ be such that $g(\theta) = 0$. Define $m = a_{d'}$ and $h(x) = x^{d'} + \sum_{i=0}^{d'-1} a_i m^{\left(d'-1-i\right)} x^i$. Then $h(x)$ is a monic polynomial in $\mathbb{Z}[x]$ and

$$\begin{aligned} h(m\theta) &= (m\theta)^{d'} + \sum_{i=0}^{d'-1} a_i m^{\left(d'-1-i\right)} (m\theta)^i = m^{d'} \theta^{d'} + \sum_{i=0}^{d'-1} a_i m^{\left(d'-1\right)} \theta^i \\ &= m^{\left(d'-1\right)} \left(m\theta^{d'} + \sum_{i=0}^{d'-1} a_i \theta^i \right) = m^{\left(d'-1\right)} \sum_{i=0}^{d'} a_i \theta^i = m^{\left(d'-1\right)} g(\theta) \\ &= 0 \end{aligned}$$

Hence, $m\theta$ is an algebraic integer. □

Lemma 10. *There exists a basis for $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$ where all basis elements are algebraic integers.*

Proof. Let $\{\theta_1, \ldots, \theta_d\}$ be a basis for $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$. For $i = 1, \ldots d$, let $m_i \in \mathbb{Z}$ be such that $m_i \theta_i \in \mathcal{O}_{\mathbb{Q}[\alpha]}$ using Lemma 9. Let $m = \prod_{i=1}^d m_i$. Since $\mathcal{O}_{\mathbb{Q}[\alpha]}$ is a ring, and all integers are algebraic integers, $m\theta_i$ is in $\mathcal{O}_{\mathbb{Q}[\alpha]}$ for all i. Hence, we have a basis $\{m\theta_1, \ldots, m\theta_d\}$ for $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$ where all basis elements are in $\mathcal{O}_{\mathbb{Q}[\alpha]}$. □

We will proceed to show that there are free $\mathbb{Z}$-modules M_1 and M_2, both of rank d, such that $M_1 \subset \mathcal{O}_{\mathbb{Q}[\alpha]} \subset M_2$. Since submodules of free $\mathbb{Z}$-modules are themselves free $\mathbb{Z}$-modules of smaller or equal rank, this will prove that $\mathcal{O}_{\mathbb{Q}[\alpha]}$ is a free $\mathbb{Z}$-module of rank d.

Using Lemma 10, let $\{\theta_i\}_{i=1}^d$ be a basis for $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$ such that $\theta_i \in \mathcal{O}_{\mathbb{Q}[\alpha]}$ $\forall i$. Define

$$M_1 = \bigoplus_{i=1}^d \mathbb{Z}\theta_i$$

We have $\mathbb{Z}\theta_i \cong \mathbb{Z}$ $\forall i$, so M_1 is a free $\mathbb{Z}$-module of rank d. Again, since $\mathcal{O}_{\mathbb{Q}[\alpha]}$ is a ring, we have $M_1 \subset \mathcal{O}_{\mathbb{Q}[\alpha]}$. We will construct M_2 using M_1, but we will need a result about the discriminant.

Proposition 11. *Let $\{\theta_i\}_{i=1}^d$ be a basis for $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$ consisting only of algebraic integers. Let $\theta \in \mathcal{O}_{\mathbb{Q}[\alpha]}$ and denote* $\operatorname{disc}(\theta_1, \ldots, \theta_d)$ *by* disc. *Then there exist $m_1, \ldots, m_d \in \mathbb{Z}$ such that*

$$\theta = m_1 \frac{\theta_1}{\operatorname{disc}} + \ldots + m_d \frac{\theta_d}{\operatorname{disc}}$$

Proof. We write θ as a linear combination of the basis elements: $\theta = \sum_{i=1}^{d} x_i\theta_i$, $x_i \in \mathbb{Q}\ \forall i$. Now we apply our embeddings σ_i to get d equations on the form

$$\sigma_i(\theta) = \sigma_i\left(\sum_{i=1}^{d} x_i\theta_i\right) = \sum_{i=1}^{d} \sigma_i(\theta_i)x_i$$

We write these equations as the linear system $Ax = b$ where $A = [\sigma_i(\theta_j)], x = (x_i)_{i=1}^{d}$ and $b = (\sigma_i(\theta))_{i=1}^{d}$. Denote by A_j the matrix where the j'th column of A is replaced by b. Cramer's Rule gives us the solution $x_j = \frac{|A_j|}{|A|}$. Observe that $|A|^2 = \text{disc}$, so

$$\text{disc}\, x_j = |A|^2 x_j = |A|^2\frac{|A_j|}{|A|} = |A||A_j|$$

Since σ maps any algebraic integer to another one, we have that $|A|$ and $|A_j|$ are both in $\mathcal{O}_{\mathbb{Q}[\alpha]}$, and hence $\text{disc}\, x_j \in \mathcal{O}_{\mathbb{Q}[\alpha]}$. But we know that both disc and x_j are rational, so their product is also in $\mathbb{Q}$. And since we have from Proposition 1 that the only rational numbers that are algebraic integers are the integers themselves, we must have $\text{disc}\, x_j \in \mathbb{Z}\ \forall i$. Define $m_j = \text{disc}\, x_j$ for $j = 1, \ldots, d$. Then

$$m_1\frac{\theta_1}{\text{disc}} + \ldots + m_d\frac{\theta_d}{\text{disc}} = x_1\theta_1 + \ldots\ x_d\theta_d = \theta$$

□

Since the θ_i are all algebraic integers, we have from Section 2.6 that disc $\in \mathbb{Z}$. Define $M_2 = \frac{1}{\text{disc}}A$, i.e.

$$M_2 = \bigoplus_{i=1}^{d} \mathbb{Z}\frac{\theta_i}{\text{disc}}$$

Proposition 11 tells us that $\mathcal{O}_{\mathbb{Q}[\alpha]} \subset M_2$. Again, M_2 is clearly a free $\mathbb{Z}$-module of rank d. Hence, we have achieved the "squeezing" $M_1 \subset \mathcal{O}_{\mathbb{Q}[\alpha]} \subset M_2$ and can conclude that $\mathcal{O}_{\mathbb{Q}[\alpha]}$ is a free $\mathbb{Z}$-module of rank d.

Chapter 3

Factoring integers

3.1 General idea

The number field sieve (NFS-fact) is an algorithm for factoring integers. Assume that $n \in \mathbb{Z}$ is not a power of a prime. (If it was, the prime would be relatively easy to find). We attempt to find $x, y \in \mathbb{Z}$ such that $x^2 \equiv y^2 \pmod{n}$. Then it is quite likely that $\gcd(x - y, n)$ is a non-trivial factor of n.

Let $f \in \mathbb{Z}[x]$ be monic and irreducible of degree d. Let $m \in \mathbb{Z}$ be such that $f(m) \equiv 0 \pmod{n}$. Let $\alpha \in \mathbb{C}$ be a root of f. Consider the projection map $\pi : \mathbb{Z} \to \mathbb{Z}_n$ and the homomorphism

$$\begin{aligned} \phi : \mathbb{Z}[\alpha] &\to \mathbb{Z}_n \\ \alpha &\mapsto m \bmod p \end{aligned}$$

The NFS-fact attempts to find a square in $\mathbb{Z}$ (say x^2) and a square in $\mathbb{Z}[\alpha]$ (say β^2) such that $\phi\left(\beta^2\right) = \pi\left(x^2\right)$. If we can find this connection, we have also found the congruence we wanted: Simply let $y \in \mathbb{Z}$ be such that $\pi(y) = \phi(\beta)$. Then

$$\pi\left(y^2\right) = \pi(y)^2 = \phi(\beta)^2 = \phi\left(\beta^2\right) = \pi\left(x^2\right),$$

which means that $x^2 \equiv y^2 \pmod{n}$.

So how do we search for such elements? Observe that if the square in $\mathbb{Z}$ is on the form $x^2 = \prod_{(a,b)\in S}(a + bm)$ and the square in $\mathbb{Z}[\alpha]$ is on the form

$\beta^2 = \prod_{(a,b)\in S}(a+b\alpha)$ for the same set $S \subset \mathbb{Z}\times\mathbb{Z}$, then

$$\begin{aligned}\phi\left(\beta^2\right) &= \phi\left(\prod_{(a,b)\in S}(a+b\alpha)\right) = \prod_{(a,b)\in S}\phi(a+b\alpha) = \prod_{(a,b)\in S}((a+bm) \bmod n) \\ &= \left(\prod_{(a,b)\in S}(a+bm)\right) \bmod n = \pi\left(\prod_{(a,b)\in S}(a+bm)\right) \\ &= \pi\left(x^2\right)\end{aligned}$$

So finding squares on this form will be sufficient.

Now we need to know how to find the set S. Assume that we have a set $T \subset \mathbb{Z}\times\mathbb{Z}$, with $\gcd(a,b) = 1\ \forall (a,b) \in T$, such that we know the factorization of both $a+bm$ and $N(a+b\alpha)$ for all (a,b) in T. We then proceed to find a subset $S \subset T$ that satisfies four criteria. Two of these together assure that $\prod_{(a,b)\in S}(a+bm)$ is a square in $\mathbb{Z}$, while the last two together make it very likely that $\prod_{(a,b)\in S}(a+b\alpha)$ is a square in $\mathbb{Z}[\alpha]$. Finding a subset that satisfies all these criteria can be formulated as finding a linearly dependent subset of certain vectors $e(a,b)$ defined for all (a,b) in T. In particular, the vectors are defined over $\mathbb{Z}_2$ in such a way that a subset $S \subset T$ satisfies a criterion if and only if $\sum_{(a,b)\in S} e(a,b)_i = 0$ for certain i's.

In addition to all the missing details here, it still remains to explain where we get the set T from. This is done through a couple of sieving procedures, from which the algorithm gets its name. Also, it is not obvious how we should choose or find the parameters f, d, m and α. We will elaborate on all this, present the algorithm and analyze its complexity.

3.2 Sieving for smooth values

As explained in Section 3.1, we need to start by finding a set $T \subset \mathbb{Z}\times\mathbb{Z}$ such that we know the factorization of $a+bm$ and $N(a+b\alpha)$ for all (a,b) in T. In fact, we want to require that the factorizations yield only small primes, since this will speed up the algorithm. So let y be an integer. We say that an integer is *y-smooth* if all of its prime factors p satisfy $p \leq y$. Thus we want T such that $a+bm$ and $N(a+b\alpha)$ are y-smooth for all (a,b) in T. We now need to decide which pairs of integers (a,b) we should search through. Let u be an integer whose optimal value will be discussed later. We require $|a| \leq u$ and $0 < b \leq u$. There is no need for checking negative b's, because then $-(a+bm)$ would already have been checked, and clearly this is y-smooth if and only if $a+bm$ is y-smooth. Furthermore, we should only search among pairs with $\gcd(a,b) = 1$. Again, if $k \in \{2,\ldots,y\}$ is a common factor, then $\frac{a+bm}{k}$ would already have been checked and is y-smooth if and only if $a+bm$ is.

We have to do two different searches, first for a set T_1 such that all $a + bm$ are y-smooth, then for a set T_2 such that all $N(a + b\alpha)$ are y-smooth. The set T will then quite simply be $T = T_1 \cap T_2$. The first search will be called the rational sieve and the second one the algebraic sieve.

Let us begin with the rational sieve. We call the set

$$\{p \text{ prime} \mid p \leq y\}$$

the *rational factor base*. For a possible b, we list the values $a+bm$ for all possible a. Now, a prime p divides $a+bm$ if and only if $a \equiv -bm \pmod{p}$ (by definition), so we start by calculating $-bm$. Then, for a prime p in the factor base, we find all a such that the congruence holds. For any such a, we find the corresponding entry in the list and divide it out with p as many times as possible. After we have done this for all p in the factor base, we locate the entries in the list that are equal to ± 1. (Since we have divided out by all our small primes, any entry that is not equal to ± 1 can not originally have been y-smooth.) We save the corresponding pairs (a, b). This procedure is repeated for all possible b, and we end up with the set T_1.

The algebraic sieve is similar, but we cannot use the same congruence. Recall from Section 2.5 the set $R(p)$. Define the *algebraic factor base* to be the set

$$\{(p, r) \mid p \text{ prime}, \ r \in R(p)\}$$

We use the same idea as in the rational sieve. Fix a b, list the values $N(a + b\alpha)$ for all possible a. For a pair (p, r) in the factor base, we find all a such that $a \equiv -br \pmod{p}$. Again, divide out the corresponding entries in the list with the highest possible power of p. When this is done for all possible (p, r), we locate the entries that are equal to ± 1 and save the corresponding pairs (a, b). After doing this for all possible b, we have found the set T_2. Notice that whenever we come across a prime p that divides b, we can just skip it, as there can be no possible a with $p \mid N(a + b\alpha)$ in this case. This is because if $b \equiv 0 \pmod{p}$, then

$$p \mid N(a + b\alpha) \iff a \equiv 0 \pmod{p} \iff p \mid \gcd(a, b)$$

and we don't consider such pairs (a, b).

As noted, we can now find the set T by calculating $T = T_1 \cap T_2$.

3.3 Finding a square in $\mathbb{Z}$

We have found a set T where both $a + bm$ and $N(a + b\alpha)$ are y-smooth for all (a, b) in T. Now we want a subset $S \subset T$ such that $\prod_{s \in S} (a + bm)$ is a square in $\mathbb{Z}$ and $\prod_{s \in S} (a + b\alpha)$ is a square in $\mathbb{Z}[\alpha]$. We will deal with these tasks separately, so let's first consider the rational side.

Denote by $\pi(y)$ the number of primes in the rational factor base. Assume that we have $|T| > \pi(y)+1$. (Whether this is true will be affected by how u and y are chosen, which will be discussed later.) Now, from the rational sieve, we have the factorization of every $a+bm$ in T in terms of our primes $p_1, \ldots, p_{\pi(y)}$. Define maps

$$\begin{aligned} e_p &: T \to \mathbb{Z} \\ (a,b) &\mapsto \mathrm{ord}_p(a+bm) \end{aligned}$$

Also define

$$e_{p_0} : (a,b) \mapsto \begin{cases} 1 & \text{if } a+bm > 0 \\ -1 & \text{otherwise} \end{cases}$$

Now, for all (a,b) in T, consider the vector

$$e_1(a+bm) = (e_{p_0}(a+bm) \bmod 2, \ldots, e_{p_{\pi(y)}}(a+bm) \bmod 2)$$

in $\mathbb{Z}_2^{\pi(y)+1}$. (The significance of the subscript 1 will be made clear in a later chapter.) Define $B = \pi(y)+1$. We now have $|T| > B$ vectors in $\mathbb{Z}_2^B$, and hence we are guaranteed to have dependent vectors. So let S_1 be a subset of T such that $\sum_{(a,b)\in S_1} e_1(a+bm) = 0$. We have

$$\sum_{(a,b)\in S_1} \mathrm{ord}_{p_j}(a+bm) \bmod 2 = 0 \ \forall j,$$

which means that for all j, we can find an integer s_j such that

$$\sum_{(a,b)\in S_1} \mathrm{ord}_{p_j}(a+bm) = 2s_j$$

Now we can actually conclude that $\prod_{(a,b)\in S_1}(a+bm)$ is a square in $\mathbb{Z}$! Because

$$\begin{aligned} \prod_{(a,b)\in S_1}(a+bm) &= \prod_{(a,b)\in S_1}\left(\prod_{j=0}^{k} p_j^{\mathrm{ord}_{p_j}(a+bm)}\right) = \prod_{j=0}^{k}\left(\prod_{(a,b)\in S_1} p_j^{\mathrm{ord}_{p_j}(a+bm)}\right) \\ &= \prod_{j=0}^{k} p_j^{\sum_{(a,b)\in S_1}\mathrm{ord}_{p_j}(a+bm)} = \prod_{j=0}^{k} p_j^{2s_j} = \prod_{j=0}^{k}(p_j^{s_j})^2 \\ &= \left(\prod_{j=0}^{k} p_j^{s_j}\right)^2 \end{aligned}$$

We have thus used the set of y-smooth values to produce a square on the form we presented in Section 3.1.

3.4 Finding a square in $\mathbb{Z}[\alpha]$

3.4.1 Exponent maps

On the rational side, we were ”lucky”: Having enough smooth values was sufficient for finding a square. Now that we start working in $\mathbb{Z}[\alpha]$, we find that things are not so simple. In fact, it turns out that the best we can hope for are necessary conditions. As explained in Section 3.1, we will develop two such criteria and convince ourselves that they together will almost guarantee the existence of a square on the form we want.

The first criterion is reminiscent of what we did on the rational side, we attempt to find certain ”exponents” that sum up to 0. If we try the exact same idea, and use our factorizations of the $N(a + b\alpha)$, we will end up with a set S_2^* such that $\prod_{(a,b)\in S_2^*} N(a + b\alpha)$ is a square in $\mathbb{Z}$, but that's not what we're after since it turns out not to be sufficient to conclude that $\prod_{(a,b)\in S_2^*} (a + b\alpha)$ is a square in $\mathbb{Z}[\alpha]$.

We will still use the exponent of a prime p in the factorization of $N(a+b\alpha)$, but in order to utilize it, we need to associate it not only with p, but with a certain element of $R(p)$. Recall from Proposition 6 that p divides $N(a + b\alpha)$ if and only if there is an r in $R(p)$ such that $a \equiv -br \pmod p$. This r will then clearly be unique. Define $e_{p,r} : \mathbb{Z}[\alpha] \to \mathbb{Z}$ by

$$e_{p,r} : (a + b\alpha) \mapsto \begin{cases} \operatorname{ord}_p\left(N(a + b\alpha)\right) & \text{if } a \equiv -br \pmod p \\ 0 & \text{otherwise.} \end{cases}$$

We trivially observe that

$$|N(a + b\alpha)| = \prod_{(p,r)} p^{e_{p,r}(a+b\alpha)}$$

The idea behind this is that if $e_{p,r}$ turned out to be a group homomorphism, we could prove a necessary condition for the squareness property, stated below as Theorem 15. Unfortunately, this is not the case. However, we can still obtain the result by finding a group homomorphism that ”imitates” $e_{p,r}$ in a sense that will become clear. Recall the notion of first degree prime ideals in $\mathbb{Z}[\alpha]$ from Chapter 2, specifically that they correspond to pairs (p, r). We want to use this correspondence when finding the mentioned group homomorphism.

Proposition 12. *Let $P \subset \mathbb{Z}[\alpha]$ be a prime ideal. Then there exists a group homomorphism $l_P : \mathbb{Q}[\alpha]^* \to \mathbb{Z}$ such that:*

1. *If $0 \neq \beta \in \mathbb{Z}[\alpha]$, then $l_P(\beta) \geq 0$.*
2. *If $0 \neq \beta \in \mathbb{Z}[\alpha]$, then $l_P(\beta) > 0$ if and only if $\beta \in P$.*

3. If $\beta \in \mathbb{Q}[\alpha]^*$, then $\{P$ prime ideal $\mid l_P(\beta) \neq 0\}$ is a finite set and

$$\prod_{\substack{P \text{ prime ideal} \\ \text{in } \mathbb{Z}[\alpha]}} N(P)^{l_P(\beta)} = |N(\beta)|$$

For a proof of Proposition 12, see [2]. These l_p's have some interesting properties regarding first degree prime ideals that we will exploit.

Lemma 13. *Let $a, b \in \mathbb{Z}$ be such that $\gcd(a, b) = 1$. Let $P \subset \mathbb{Z}[\alpha]$ be a prime ideal that is not of first degree. Then $l_P(a + b\alpha) = 0$.*

Proof. Assume $l_P(a + b\alpha) \neq 0$. Then, by Proposition 12, part 1, we have that $l_P(a+b\alpha) > 0$. Proposition 12, part 2, now gives us that $a+b\alpha \in P$. Consider the projection map

$$\begin{aligned} \pi : \mathbb{Z}[\alpha] &\to \mathbb{Z}[\alpha]/P \\ \theta &\mapsto \theta + P =: \bar{\theta} \end{aligned}$$

Since $a + b\alpha \in P$, we have $\pi(a + b\alpha) = \bar{0}$. $\mathbb{Z}[\alpha]/P$ is a finite field, so assume $\mathbb{Z}[\alpha]/P \cong \mathrm{F}_{p^k}$. We claim that $p \nmid b$. Assume that $p \mid b$. Then $p \mid b\alpha$, so $b\alpha \in P$ and $\pi(b\alpha) = \bar{0}$. Now,

$$\pi(a) = \pi(a + b\alpha - b\alpha) = \pi(a + b\alpha) - \pi(b\alpha) = \bar{0} - \bar{0} = \bar{0}$$

Hence, $a \in P$ and $p \mid a$. But then $\gcd(a, b) \geq p > 1$, a contradiction. We conclude that $p \nmid b$ and thus $b \notin P$, which means $\pi(b) \neq \bar{0}$. Then $\pi(b)$ has an inverse in $\mathbb{Z}[\alpha]/P$, we define it to be $\hat{b}$. This gives us

$$\pi(\alpha) = \pi(b\alpha)\pi(b)^{-1} = (\pi(a + b\alpha) - \pi(a))\pi(b)^{-1} = \left(\bar{0} - \bar{a}\right)\hat{b} = -\bar{a}\hat{b},$$

which is an element in F_p. Hence, all linear combinations of powers of α, i.e. all elements in $\mathbb{Z}[\alpha]$, are also mapped to F_p by π. π is surjective, so we conclude that

$$\mathrm{F}_p \cong \pi\left(\mathbb{Z}[\alpha]\right) = \mathbb{Z}[\alpha]/P \cong \mathrm{F}_{p^k}$$

Hence, $k = 1$ and P is a first degree prime. □

This is then used to show that l_p ”imitates” $e_{p,r}$:

Proposition 14. *Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$. Let $P \subset \mathbb{Z}[\alpha]$ be a first degree prime ideal corresponding to (p, r). Then $l_P(a + b\alpha) = e_{p,r}(a + b\alpha)$.*

Proof. Let us start by showing that $l_P(a+b\alpha) = 0$ if and only if $e_{p,r}(a+b\alpha) = 0$. By Proposition 12, part 2, $l_P(a + b\alpha) \neq 0 \iff a + b\alpha \in P$. By Lemma 7, $a + b\alpha \in P \iff a + br \equiv 0 \pmod{p}$. By definition, $a + br \equiv 0 \pmod{p} \iff e_{p,r}(a + b\alpha) \neq 0$.

We now let $a + b\alpha$ be any element of $\mathbb{Z}[\alpha]$. Proposition 12, part 3, states that

$$\prod_{P \text{ prime ideal}} N(P)^{l_P(a+b\alpha)} = |N(a+b\alpha)|$$

Lemma 13 tells us that the exponent on the left hand side is non-zero only for first degree ideals. We also use our factorization of $N(a + b\alpha)$ and obtain

$$\prod_{P \text{ fdpi}} N(P)^{l_P(a+b\alpha)} = \prod_{(p,r)} p^{e_{p,r}(a+b\alpha)}$$

Let p be fixed. Then we are left with

$$\prod_{\substack{P \text{ with} \\ N(P)=p}} p^{l_P(a+b\alpha)} = \prod_{r} p^{e_{p,r}(a+b\alpha)}$$

Hence, by comparing powers,

$$\sum_{\substack{P \text{ with} \\ N(P)=p}} l_P(a+b\alpha) = \sum_{r} e_{p,r}(a+b\alpha)$$

Now, we know that we can have at most one r such that $a + br \equiv 0 \pmod p$ and therefore $e_{p,r}(a + b\alpha) \neq 0$ by definition. So there is an r such that

$$\sum_{\substack{P \text{ with} \\ N(P)=p}} l_P(a+b\alpha) = e_{p,r}(a+b\alpha)$$

We utilize the first part of this proof, that the maps have exactly the same zeroes, and find that $l_P(a + b\alpha) = e_{p,r}(a + b\alpha)$ where P corresponds to (p, r). This equality, together with $l_{P^*}(a + b\alpha) = 0 = e_{p,r^*}(a + b\alpha)$ for all other first degree prime ideals with $N(P^*) = p$, gives us what we wanted to show. □

Now we are ready to prove the first necessary condition for squareness in $\mathbb{Z}[\alpha]$:

Theorem 15. *Let S be a subset of $\mathbb{Z} \times \mathbb{Z}$ such that $\prod_{(a,b)\in S} (a + b\alpha)$ is a square in $\mathbb{Q}[\alpha]$. Let p be a prime number and $r \in R(p)$. Then*

$$\sum_{(a,b)\in S} e_{p,r}(a+b\alpha) \equiv 0 \pmod 2$$

Proof. Let γ in $\mathbb{Q}[\alpha]$ be such that $\prod_{(a,b)\in S} (a + b\alpha) = \gamma^2$. Note that the group operation in $\mathbb{Z}$ is written additively, while in $\mathbb{Q}[\alpha]^*$ it is written multiplicatively. Since l_P is a homomorphism, and using Proposition 14, we obtain

$$\begin{aligned} \sum_{(a,b)\in S} e_{p,r}(a+b\alpha) &= \sum_{(a,b)\in S} l_P(a+b\alpha) = l_P\left(\prod_{(a,b)\in S}(a+b\alpha)\right) \\ &= l_P\left(\gamma^2\right) = l_p(\gamma) + l_p(\gamma) = 2l_P(\gamma) \\ &\equiv 0 \pmod 2 \end{aligned}$$

□

So one method for testing the squareness of our product is the following: For a bunch of primes p and corresponding integers r, check that $\left(\sum_{(a,b)\in S} e_{p,r}(a+b\alpha)\right)$ mod 2 always equals 0. Still, this can only gives us a square in $\mathbb{Q}[\alpha]$, and we want a square in $\mathbb{Z}[\alpha]$. But if γ^2 is a square in $\mathbb{Q}[\alpha]$, then $f'(\alpha)^2\gamma^2$ is a square in $\mathbb{Z}[\alpha]$, see [2]. For the rest of the text, we will ignore this factor for simplicity.

3.4.2 Quadratic characters

The next property that a square in $\mathbb{Z}[\alpha]$ has, is related to the Legendre symbol. In $\mathbb{Z}$, we observe that if there is a prime p such that $\left(\frac{l}{p}\right) = -1$, the integer l cannot be a square. If it was, say $l = r^2$, we would trivially have $l \equiv r^2 \pmod{p}$ and so $\left(\frac{l}{p}\right) = 1$. Hence, the more primes p we test without the corresponding Legendre symbol being equal to -1, the more convinced we should be that l actually is a square in $\mathbb{Z}$. This is the basic idea we want to generalize.

Theorem 16. *Let S be a subset of $\mathbb{Z}\times\mathbb{Z}$ such that $\prod_{(a,b)\in S}(a+b\alpha)$ is a square in $Z[\alpha]$. Let q be an odd prime and s an element of $R(p)$ such that $a+bs \not\equiv 0 \pmod{q}$ for all (a,b) in S. Then*

$$\prod_{(a,b)\in S}\left(\frac{a+bs}{q}\right) = 1$$

Proof. Let γ in $\mathbb{Z}[\alpha]$ be such that $\prod_{(a,b)\in S}(a+b\alpha) = \gamma^2$. Define the ring homomorphism

$$\begin{aligned} \omega : \mathbb{Z}[\alpha] &\to \mathbb{Z}_q \\ \alpha &\mapsto s \bmod q \end{aligned}$$

Let $Q = \ker(\omega)$. By definition, we have that Q is the first degree prime ideal corresponding to (q, s). We now observe that

$$\omega\left(\prod_{(a,b)\in S}(a+b\alpha)\right) = \prod_{(a,b)\in S}(\omega(a+b\alpha)) = \prod_{(a,b)\in S}(a+bs) \not\equiv 0 \pmod{q}$$

since our assumption was that none of the $(a+bs)$ were congruent to 0 modulo q. Hence, by definition of Q, $\prod_{(a,b)\in S}(a+b\alpha) = \gamma^2$ is not in Q. So γ is not in Q either. This means that we can use γ^2 and γ as arguments in the map

$$\begin{aligned} \chi_Q : \mathbb{Z}[\alpha]\backslash Q &\to \{\pm 1\} \\ \theta &\mapsto \left(\frac{\omega(\theta)}{q}\right) \end{aligned}$$

We have that

$$\begin{aligned}\chi_Q\left(\prod_{(a,b)\in S}(a+b\alpha)\right) &= \left(\frac{\omega\left(\prod_{(a,b)\in S}(a+b\alpha)\right)}{q}\right)\\ &= \left(\frac{\prod_{(a,b)\in S}(a+bs)}{q}\right)\\ &= \prod_{(a,b)\in S}\left(\frac{a+bs}{q}\right)\end{aligned}$$

But also,

$$\chi_Q\left(\gamma^2\right) = \left(\frac{\omega\left(\gamma^2\right)}{q}\right) = \left(\frac{\omega(\gamma)^2}{q}\right) = 1$$

The proposition follows. □

So we now have another method of convincing ourselves that a given product is a square. Namely, we choose a lot of primes q outside the factor base, with corresponding integers s, and check that we never end up with $\prod_{(a,b)\in S}\left(\frac{a+bs}{q}\right) = -1$. It it possible to show that $\lceil\frac{3\ln n}{\ln 2}\rceil$ primes is a good estimate for how many such primes we need, see [2]. Note that when we include $f'(\alpha)^2$ as a factor, we need to assume that $f'(s) \not\equiv 0 \pmod q$ for Theorem 16 to hold.

3.5 The linear system

We now feel, for all practical purposes, that we have developed sufficient criteria for squareness both in $\mathbb{Z}$ and in $\mathbb{Z}[\alpha]$. What we want now is a method that given the set T we found in Section 3.2, produces a subset $S \subset T$ that satisfies all these criteria at once. We would also like the method to be fast and easy to use.

Recall the mapping e_1 from Section 3.3. We used this to define vectors in $\mathbb{Z}_2$, one for each pair (a,b) in T, such that we could search through them for a linear depency. Such a depency would provide us with a product $\prod_{(a,b)\in S_1}(a+bm)$ satisfying our criterion. We want to transform the other criteria into linear problems over $\mathbb{Z}_2$, so that we can solve them all simultaneously. Let's start with the exponent map criterion, which is quite similar. Let C be the size of the algebraic factor base and define

$$\begin{aligned}&e_2 : T \to \mathbb{Z}_2^C\\ &(a,b) \mapsto (e_{p_1,r_1}(a+b\alpha) \bmod 2, \ldots, e_{p_C,r_C}(a+b\alpha) \bmod 2)\end{aligned}$$

Now the criterion stated at the end of Subsection 3.4.1 can be satisfied by considering the set $\{e_2(a,b)\}_{(a,b)\in T}$ and finding a linearly dependent subset.

The quadratic character criterion concerns finding a product that equals 1, but we will transform that problem into finding a sum that equals 0, so that we can use the same method as above. Given a prime q outside the algebraic factor base and an integer s in $R(q)$, define $e_3^{(q,s)} : T \to \mathbb{Z}_2$ by

$$e_3^{(q,s)} : (a,b) \mapsto \begin{cases} 0 & \text{if } \left(\frac{a+bs}{q}\right) = 1 \\ 1 & \text{if } \left(\frac{a+bs}{q}\right) = -1 \end{cases}$$

We extend this to $D = \left\lceil \frac{3 \ln n}{\ln 2} \right\rceil$ primes and define

$$\begin{aligned} &e_3 : T \to \mathbb{Z}_2^D \\ &(a,b) \mapsto \left(e_3^{(q_1,s_1)}(a,b), \ldots, e_3^{(q_D,s_D)}(a,b) \right) \end{aligned}$$

The crucial observation is that

$$\prod_{(a,b)} \left(\frac{a+bs}{q} \right) = 1 \ \forall (q,s) \iff \sum_{(a,b)} e_3(a,b) = 0,$$

so we have achieved what we wanted and can solve this criterion together with the two others.

What we want is a subset S of T such that $\sum_{(a,b)\in S} e_i(a,b) = 0$ for i being both 1, 2 and 3. Clearly, we can solve these in a common matrix. Define

$$\begin{aligned} &e : T \to \mathbb{Z}_2^{B+C+D} \\ &(a,b) \mapsto (e_1(a,b), e_2(a,b), e_3(a,b)) \end{aligned}$$

Considering all the vectors $e(a,b)$ for (a,b) in T will reduce the problem of finding a subset that satisfies all three criteria to finding a linearly dependent subset of these vectors. We are guaranteed to find this if $|T| > B + C + D$. Whether this is true, depends on our parameter choices, and will be elaborated on in Section 3.7.

Such a subset S will thus guarantee that $\prod_{(a,b)\in S}(a + bm)$ is a square in $\mathbb{Z}$ and make it highly likely that $\prod_{(a,b)\in S}(a + b\alpha)$ is a square in $\mathbb{Z}[\alpha]$. Note that in order to use the method presented in Section 3.1, we need a way of calculating the square roots of these products. In $\mathbb{Z}$, this is straightforward, as we already know the factorization of all the $a + bm$. However, in $\mathbb{Z}[\alpha]$, we only know the factorization of the ideal generated by the product. For an explanation on how to then find the square root, see [2].

3.6 The algorithm

To summarize everything we've done in this chapter, we present the step-by-step algorithm for finding a non-trivial factor of an integer n with the number field sieve.

Let $d, u, y \in \mathbb{N}$ be such that $n > d^{2d^2}$.

1. Find an integer m and a polynomial $f \in \mathbb{Z}[x]$ such that $f(m) \equiv 0 \pmod{n}$. Decide on a root $\alpha \in \mathbb{C}$ of f.
2. Using the sieving procedures described, find a set $T \subset \mathbb{Z} \times \mathbb{Z}$ such that for all (a, b) in T, we have that $\gcd(a, b) = 1$, $|a| \leq u$, $0 < b \leq u$, $a + bm$ is y-smooth and $N(a + b\alpha)$ is y-smooth.
3. Solving the linear system described, find a subset S of T such that $\sum_{(a,b)\in S} e(a, b) = 0$.
4. Try to find a square root β of $f'(\alpha)^2 \prod_{(a,b)\in S} (a + b\alpha)$ in $\mathbb{Z}[\alpha]$. If no such β is found, return to step 3 and find a new dependency.
5. Find a square root x of $f'(m)^2 \prod_{(a,b)\in S} (a + bm)$ in $\mathbb{Z}$.
6. Calculate $a = \gcd(x - \phi(\beta), n)$. If $a \neq 1$ and $a \neq n$, return a. If not, return to step 3 and remove one element of S from T.

3.7 Complexity analysis

Let's first discuss how we should choose f, m and α. To optimize the running time, we want f to have small coefficients. Given d, we define $m = \lfloor \sqrt[d]{n} \rfloor$. Then we express n in base m, i.e. $n = \sum_{i=0}^{d} c_i m^i$ such that $c_i < m \ \forall i$. Define

$$f = \sum_{i=0}^{d} c_i x^i$$

Then we have $f(m) = n \equiv 0 \pmod{n}$, as we wanted.

It is clear that steps 2, 3 and 4 in the NFS-fact are the most time-consuming. We will estimate the running time of step 2, and then argue that this step dominates steps 3 and 4. Hence we will conclude that the running time of the entire algorithm can be estimated by the running time of step 2.

We will introduce some special notation to ease matters a bit. Expressions on the form

$$L_n(v; c) := e^{c(\ln n)^v (\ln \ln n)^{1-v}}$$

will appear with different parameters c and v throughout the analysis. The special case $L_n\left(\frac{1}{2}; 1\right)$ will be written as just L_n.

First, we will establish a general result about finding smooth numbers. Suppose that we are checking random numbers smaller than or equal to x for y-smoothness. Denote by $\psi(x, y)$ the number of such smooth integers. The probability that a random integer between 1 and x is y-smooth is then $\frac{\psi(x,y)}{x}$. So, if we want to find t y-smooth integers, we expect to check about $\frac{tx}{\psi(x,y)}$ integers. We investigate the special case $t = y$.

Proposition 17.

$$\frac{yx}{\psi(x,y)} \geq L_x^{\sqrt{2}}$$

For a proof, see [2]. If we assume that we will always have to check at least the expected number of integers, this proposition provides a lower bound for the running time of such a selection. Note that the choice for y that achieves equality in the proposition is $y = L_x^{\frac{1}{\sqrt{2}}}$.

We will now use Proposition 17 result to prove a lemma that seems rather technical, but which turns out to be both applicable and understandable in the context of our algorithm.

Lemma 18. *Assume* $n > d^{2d^2}$. *Assume* $u(n, d) \geq 2$ *and* $y(n, d) \geq 2$. *Let* $x = 2(d + 1)\sqrt[d]{n^2}u^{d+1}$ *and assume* $\frac{u^2\psi(x,y)}{x} \geq y$. *Then*

$$2 \ln u \geq d \ln d + \sqrt{(d \ln d)^2 + 4 \ln\left(\sqrt[d]{n}\right) \ln \ln\left(\sqrt[d]{n}\right)}$$

Proof. The last assumption implies that $u^2 \geq \frac{yx}{\psi(x,y)}$. which we know from Proposition 17 is greater than or equal to $L_x^{\sqrt{2}}$. We therefore obtain

$$\begin{aligned} \ln\left(u^2\right) \geq \ln\left(L_x^{\sqrt{2}}\right) &\implies 2 \ln u \geq \sqrt{2 \ln x \ln \ln x} \\ &\implies \sqrt{2} \ln u \geq \sqrt{\ln x \ln \ln x} \\ &\implies 2(\ln u)^2 \geq \ln x \ln \ln x \end{aligned}$$

Just like $\ln t$, $\frac{t}{\ln t}$ is an increasing function (when $t \geq e$), so we can divide each side of the inequality by its own logarithm. We calculate $\ln\left(2(\ln u)^2\right) = \ln 2 + 2 \ln \ln u$ and $\ln(\ln x \ln \ln x) = \ln \ln x + \ln \ln \ln x$ to obtain

$$\frac{2(\ln u)^2}{\ln 2 + 2 \ln \ln u} \geq \frac{\ln x \ln \ln x}{\ln \ln x + \ln \ln \ln x}$$

Now, since $\ln \ln \ln x \geq \ln 2$, we get

$$\begin{aligned} &\frac{2(\ln u)^2}{2 \ln \ln u} \geq \frac{\ln x \ln \ln x}{\ln \ln x} \\ \implies &\frac{(\ln u)^2}{\ln \ln u} \geq \ln x = \ln\left(2(d+1)\sqrt[d]{n^2}u^{d+1}\right) \\ &\qquad = \ln 2 + \ln(d+1) + \frac{2}{d} \ln n + (d+1) \ln u \\ &\qquad \geq \frac{2}{d} \ln n + (d+1) \ln u \end{aligned}$$

Finally, we apply Lemma 10.9 in [2] with $k \geq d+1$ and $l \geq 2\ln\left(\sqrt[d]{n}\right)$ to obtain what we wanted. □

We are now ready to start the analysis of step 2 in the NFS-fact algorithm. We start by finding a lower bound for the time taken by this step using the lemma we just proved. To be guaranteed the existence of a linearly dependent set in step 3, we need the number of rows in the matrix to exceed the number of columns. We will use this assumption in our argument. So what is the number of rows? We have one row for each pair (a, b) in T, so we need to estimate the cardinality of T, namely, how many smooth integers we find. Recall that the probability of a random integer smaller than or equal to x being y-smooth was $\frac{\psi(x,y)}{x}$. We check approximately u^2 such integers in step 2. Hence, we can expect to find $\frac{u^2\psi(x,y)}{x}$ y-smooth integers. We will make the heuristic assumption that this is in fact the number of integers that we find, and hence also the number of rows. Since the numbers B, C and D are all bounded by y, we can say that the number of columns is approximately y. So having at least as many rows as columns is the same as having

$$\frac{u^2\psi(x,y)}{x} \geq y$$

We note that this looks similar to one of the assumptions in Lemma 18.

But in order to apply Lemma 18, we need x to be expressed in a certain way using n, d and u. Let us try to estimate this number. First observe that checking both $a+bm$ and $N(a+b\alpha)$ for y-smoothness is the same as checking $(a+bm)N(a+b\alpha)$. What is the largest value of $(a+bm)N(a+b\alpha)$ that we check? Recall that the coefficients of f are bounded by m and that $m < \sqrt[d]{n}$. Also, recall from Section 3.2 that we only check pairs (a, b) where both integers are smaller than or equal to u. Finally, recall (2.2), that told us we can express $N(a+b\alpha)$ as

$$\begin{aligned} N(a+b\alpha) &= (-b)^d f\left(-\frac{a}{b}\right) \\ &= a^d - c_{d-1}a^{d-1}b + c_{d-2}a^{d-2}b^2 - \ldots + (-1)^{d-1}c_1ab^{d-1} + (-1)^d c_0 b^d \end{aligned}$$

So we can deduce that

$$\begin{aligned} N(a+b\alpha) &\leq u^d + \underbrace{mu^d + \ldots + mu^d}_{d} = u^d(1+dm) \leq u^d(m+dm) \\ &= u^d m(d+1) \end{aligned}$$

and hence

$$\begin{aligned} (a+bm)N(a+b\alpha) &\leq (u+um)u^d m(d+1) = u^{d+1}(m+1)m(d+1) \\ &\leq u^{d+1}(2m)m(d+1) = 2(d+1)m^2u^{d+1} \\ &\leq 2(d+1)\sqrt[d]{n^2}u^{d+1} \end{aligned}$$

So all numbers we check are lower than or equal to this number. Hence, we can use

$$x = 2(d+1)\sqrt[d]{n^2}u^{d+1}$$

This is exactly what we required, so we can use Lemma 18 and conclude that, with our parameters,

$$2\ln u \geq d\ln d + \sqrt{(d\ln d)^2 + 4\ln\left(\sqrt[d]{n}\right)\ln\ln\left(\sqrt[d]{n}\right)}$$

Since e^t is an increasing function, we can raise e to each side and keep the inequality. We get

$$u^2 \geq \exp\left(d\ln d + \sqrt{(d\ln d)^2 + 4\ln\left(\sqrt[d]{n}\right)\ln\ln\left(\sqrt[d]{n}\right)}\right)$$

We know that the running time of step 2 is u^2, since this is approximately the number of integers we check for smoothness, and now we have calculated a lower bound for this number expressed by n and d. We have therefore established our first result regarding the complexity of the NFS-fact. Now we want to show that this lower bound is in fact achievable with the right choices of u and y, and that the algorithm is likely to succeed with these parameters. Then we can conclude that this is the optimal running time for step 2.

Once again our argument will be based on the number of rows and columns in the matrix in step 3, but this time we will show and use that with our special choice of u and y, the number of rows will be larger than or equal to the number of columns plus the maximal number of times we perform step 3. If we can show this, we will be able to conclude that we are guaranteed to find a linear dependency every single time, even though we remove one row every time step 6 does not produce a non-trivial factor of n. This will convince us that we are likely to find a non-trivial factor eventually.

Let us start with the choices of u and y. It is clear that if we choose u to be the square root of the optimal running time, we will obtain this running time. So let

$$u_0 = \exp\left(\frac{1}{2}\left(d\ln d + \sqrt{(d\ln d)^2 + 4\ln\left(\sqrt[d]{n}\right)\ln\ln\left(\sqrt[d]{n}\right)}\right)\right)$$

In fact, this will also be our choice for y_0. Let $x_0 = 2n\sqrt[d]{n^2}{u_0}^{d+1}$. We will need u and y to be a bit larger in order to apply our argument, because with these choices, we have

$$\frac{{u_0}^2\psi(x_0, y_0)}{x_0} = y_0^{1+o(1)},$$

and we will see later that we need some sort of inequality. Therefore, let $\epsilon > 0$, let

$$u = y = \exp\left(\frac{1+\epsilon}{2}\left(d\ln d + \sqrt{(d\ln d)^2 + 4\ln\left(\sqrt[d]{n}\right)\ln\ln\left(\sqrt[d]{n}\right)}\right)\right),$$

and let $x = 2n\sqrt[d]{n^2}u^{d+1}$. Note that $y_0^{1+\epsilon} = y_0$ (and hence also $u_0^{1+\epsilon} = u_0$) and $x_0^{1+\epsilon} \geq x$. This means that $\ln(y) = \ln\left(y_0^{1+\epsilon}\right) = (1+\epsilon)\ln(y_0)$ and $\ln(x) \leq \ln\left(x_0^{1+\epsilon}\right) = (1+\epsilon)\ln(x_0)$. We thus have

$$\frac{\ln(x)}{\ln(y)} \leq \frac{(1+\epsilon)\ln(x_0)}{(1+\epsilon)\ln(y_0)} = \frac{\ln(x_0)}{\ln(y_0)}$$

This now leads to

$$\frac{\psi(x,y)}{x} \geq \left(\frac{\psi(x_0,y_0)}{x_0}\right)^{1+o(1)}$$

From this we get

$$\begin{aligned}
\frac{u^2\psi(x,y)}{x} &\geq \left(\frac{u^2\psi(x_0,y_0)}{x_0}\right)^{1+o(1)} = \left(\frac{u_0^{2(1+\epsilon)}\psi(x_0,y_0)}{x_0}\right)^{1+o(1)} \\
&= \left(\left(u_0^{2\epsilon}\right)\frac{u_0^2\psi(x_0,y_0)}{x_0}\right)^{1+o(1)} = \left(\left(u_0^{2\epsilon}\right)y_0^{1+o(1)}\right)^{1+o(1)} \\
&= \left(\left(u_0^{2\epsilon}\right)y_0\right)^{1+o(1)} = \left(y_0^{1+2\epsilon}\right)^{1+o(1)} \\
&= \left(\left(y^{\frac{1}{1+\epsilon}}\right)^{1+2\epsilon}\right)^{1+o(1)} = \left(y^{\frac{1+2\epsilon}{1+\epsilon}}\right)^{1+o(1)} \\
&> y^{1+o(1)}
\end{aligned}$$

Recall that we used $\frac{u^2\psi(x,y)}{x}$ as an estimate for the number of rows in the matrix in step 3, and now we have an inequality involving that number. What is the number of columns? Recall from Section 3.5 that this is $B+C+D$. We first note that $B = \pi(y) + 1 \leq y$. Since we can find at most d roots of f given any modulus,

$$C \leq d\pi(y) \leq dy \leq y\ln n = y^{1+o(1)}$$

Furthermore, $D \leq 3\ln n = y^{o(1)}$. In total,

$$B + C + D = y^{1+o(1)}$$

Now it only remains to calculate how many times we perform step 3. We go back to this step every time step 6 fails to find a non-trivial factor of n. An upper bound for the number of times this happens is $(\ln n)^{O(1)} = y^{o(1)}$ [2]. Hence, the number of columns plus the number of times we perform step 3 is $y^{1+o(1)}$, which is the right hand side of last inequality in the previous paragraph. The left hand side was the number of rows. We have therefore shown exactly what we wanted. As mentioned above, we can now conclude that there are enough rows in the matrix to be guaranteed a linear dependency every time we perform step 3. We then feel convinced that one of these will lead to a non-trivial factorization in step 6. So the algorithm works with these optimal choices for u and y. We let ϵ tend to 0 when n goes to ∞ and write

$$u = y = \exp\left(\left(\frac{1}{2} + o(1)\right)\left(d\ln d + \sqrt{(d\ln d)^2 + 4\ln\left(\sqrt[d]{n}\right)\ln\ln\left(\sqrt[d]{n}\right)}\right)\right)$$

Up to this point, we have worked with a fixed d. Now we want to optimize this parameter as well and gain the optimal running time for any given n. The best we could do with a given d was

$$\exp\left(d\ln d + \sqrt{(d\ln d)^2 + 4\ln\left(\sqrt[d]{n}\right)\ln\ln\left(\sqrt[d]{n}\right)}\right)$$

To minimize the radicand, we would like the two summands to be of approximately the same size. We conjecture that if $d \approx \sqrt[3]{\frac{\ln n}{\ln\ln n}}$, we will obtain what we want. In the following calculations, we ignore small, constant factors. With our choice of d, we obtain

$$\ln d \approx \frac{1}{3}\ln\left(\frac{\ln n}{\ln\ln n}\right) = \ln\ln n - \ln\ln\ln n \approx \ln\ln n$$

Also, $d^2 \approx \sqrt[3]{\frac{(\ln n)^2}{(\ln\ln n)^2}}$. This means that

$$(d\ln d)^2 \approx \sqrt[3]{\frac{(\ln n)^2}{(\ln\ln n)^2}}(\ln\ln n)^2 = \sqrt[3]{\left(\ln n\,(\ln\ln n)^2\right)^2}$$

On the other side, we have

$$\ln\left(\sqrt[d]{n}\right) = \frac{1}{d}\ln n \approx \frac{\ln n\sqrt[3]{\ln\ln n}}{\sqrt[3]{\ln n}} = \sqrt[3]{(\ln n)^2\ln\ln n}$$

and so we get

$$\ln\ln\left(\sqrt[d]{n}\right) \approx \frac{1}{3}\ln\left((\ln n)^2\ln\ln n\right) \approx 2\ln\ln n + \ln\ln\ln n \approx \ln\ln n$$

Finally,

$$4\ln\left(\sqrt[d]{n}\right)\ln\ln\left(\sqrt[d]{n}\right) \approx \sqrt[3]{(\ln n)^2\ln\ln n}\,\ln\ln n = \sqrt[3]{\left(\ln n(\ln\ln n)^2\right)^2},$$

and we have justified our conjecture. By considering the expression for the optimal running time given n and d, we can make the approximation more precise:

$$d = \left(\sqrt[3]{3} + o(1)\right)\sqrt[3]{\frac{\ln n}{\ln\ln n}}$$

will minimize the running time. With this choice, the expressions for u and y simplify to

$$u = y = L_n\left(\frac{1}{3}; \sqrt[3]{\frac{8}{9}}\right)$$

So, given n, we can choose d, u, and y such that the running time of step 2 becomes

$$u^2 = \left(L_n\left(\frac{1}{3}; \sqrt[3]{\frac{8}{9}}\right)\right)^2 = L_n\left(\frac{1}{3}; \frac{4}{\sqrt[3]{9}}\right)$$

It only remains to show that this is the dominating step in the algorithm. It can be shown that the running time of step 3 and step 4 are y^2, see [2]. Hence, no step increases the complexity of the algorithm significantly. We conclude that the optimal running time for the NFS-fact is, heuristically,

$$L_n\left(\frac{1}{3}; \frac{4}{\sqrt[3]{9}}\right) = e^{4\sqrt[3]{\frac{\ln n(\ln\ln n)^2}{9}}} \tag{3.1}$$

A similar, but easier algorithm, the quadratic sieve, has complexity $L_n = e^{\sqrt{\ln n \ln\ln n}}$. If we compare these two, we find that

$$\begin{aligned} 4\sqrt[3]{\frac{\ln n(\ln\ln n)^2}{9}} \leq \sqrt{\ln n\ln\ln n} &\iff \frac{4}{\sqrt[3]{9}}(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}} \leq (\ln n)^{\frac{1}{2}}(\ln\ln n)^{\frac{1}{2}} \\ &\iff (\ln n)^{\frac{1}{6}}(\ln\ln n)^{-\frac{1}{6}} \geq \frac{4}{\sqrt[3]{9}} \\ &\iff \frac{\ln n}{\ln\ln n} \geq \left(\frac{4}{\sqrt[3]{9}}\right)^6 = \frac{4096}{81} \end{aligned}$$

So when n is sufficiently large, the number field sieve is superior.

Chapter 4

Finding d-logs in fields of prime order

4.1 General idea

As mentioned in the introduction, the main concepts of the NFS-fact can also be applied to discrete logarithm problems. This number field sieve (NFS-dlog) is similar in both setup, execution and analysis, and will therefore be more briefly discussed than the NFS-fact. However, there are some complicating issues, for instance that we need to find higher powers than only squares. This will also require some new concepts.

Let p be a prime number and consider the finite field F_p. Let t be an element of F_p^*, considered as an integer modulo p, and let g be an element of the subgroup generated by t. In other words, there is an integer z such that $t^z \equiv g \pmod{p}$. We want to find the smallest such integer, and we denote it by $\log_t g$. In other words,

$$z \equiv \log_t g \pmod{p-1}$$

Due to certain complications, we instead try to find congruences on the form $z \equiv \log_t g \pmod{l}$, where l is a prime divisor of $p-1$ and then solve the original problem through application of the Chinese Remainder Theorem.

As before, we need $f \in \mathbb{Z}[x]$ to be monic and irreducible of degree d, $m \in \mathbb{Z}$ to be such that $f(m) \equiv 0 \pmod{p}$ and $\alpha \in \mathbb{C}$ to be a root of f. This time, we try to find an l'th power in $\mathbb{Z}$ (say x^l) and an l'th power in $\mathbb{Z}[\alpha]$ (say β^l) that are connected in a certain way. Again, consider the projection map $\pi : \mathbb{Z} \to \mathbb{Z}_p$ and the homomorphism

$$\begin{aligned} \phi : \mathbb{Z}[\alpha] &\to \mathbb{Z}_p \\ \alpha &\mapsto (m \bmod p) \end{aligned}$$

The relation we are looking for this time is $\pi\left(x^l\right) = t^{x_t} g\phi\left(\beta^l\right)$ for some x_t.

When we have found our l'th powers, it is clear that $\pi\left(x^l\right) = \pi(x)^l$ and $\phi\left(\beta^l\right) = \phi(\beta)^l$ are themselves l'th powers in $\mathbb{Z}_p$, say k_1^l and k_2^l. The equation $\pi\left(x^l\right) = t^{x_t} g\phi\left(\beta^l\right)$ then tells us that $t^{x_t} g = \left(k_1 k_2^{-1}\right)^l$ and hence $t^{x_t} g$ is also an l'th power. Specifically, we have that there is an s in $\mathbb{Z}$ such that

$$t^{x_t} g \equiv s^l \pmod{p-1}$$

But since $t^{x_t} g$ is in $\langle t \rangle$, we must also have $s \in \langle t \rangle$. In other words, there is an r such that $s \equiv t^r \pmod{p-1}$. If we write g as $t^{\log_t g}$, we thus have $t^{x_t} t^{\log_t g} \equiv t^{rl} \pmod{p-1}$. Considering the exponents, we obtain

$$x_t + \log_t g \equiv rl \pmod{p-1}$$

Any congruence that holds modulo $p-1$ will trivially hold for any divisor of $p-1$, so $x_t + \log_t g \equiv rl \pmod{l}$. But $rl \equiv 0 \pmod{l}$, so

$$x_t \equiv -\log_t g \pmod{l}$$

We will then have found the logarithm modulo l. If we can do this for all prime divisors of $p-1$, we end up with a system of linear congruences on the form

$$x \equiv \log_t g \pmod{l}$$

where the product of the moduli is $p-1$. Therefore, we can easily apply the Chinese Remainder Theorem and find an integer z such that

$$z \equiv \log_t g \pmod{p-1},$$

which is the discrete logarithm we were trying to find.

This time, we observe that if our l'th powers are on the form

$$\begin{aligned} x^l &= t^{x_t} g \prod_{(a,b)\in T} (a+bm)^{x_{a,b}}, \\ \beta^l &= \prod_{(a,b)\in T} (a+b\alpha)^{x_{a,b}} \end{aligned}$$

in $\mathbb{Z}$ and $\mathbb{Z}[\alpha]$ respectively, we will have

$$\begin{aligned}\pi\left(x^l\right) &= \pi\left(t^{x_t} g \prod_{(a,b)\in T} (a+bm)^{x_{a,b}}\right) \\ &= \pi\left(t^{x_t} g\right) \pi\left(\prod_{(a,b)\in T} (a+bm)^{x_{a,b}}\right) \\ &= t^{x_t} g \phi\left(\prod_{(a,b)\in T} (a+b\alpha)^{x_{a,b}}\right) \\ &= t^{x_t} g \phi(\beta^l)\end{aligned}$$

since $\phi(\alpha) = \pi(m)$ and $t, g \in \mathrm{F}_q$. So we will search for such a set $T \subset \mathbb{Z} \times \mathbb{Z}$. What remains to explain is how to find the integers x_t and $x_{a,b}$.

4.2 Character maps

We find T in exactly the same way as in the NFS-fact, using sieving techniques. As we will see in Section 4.3, finding l'th powers in $\mathbb{Z}$ is simple. Unfortunately, using the norm we can only directly find an element in $\mathcal{O}_{\mathbb{Q}[\alpha]}$ such that the ideal generated by it is an l'th power. This is not sufficient, but we will find another necessary condition which will mirror the quadratic characters from the NFS-fact.

For the remainder of this chapter, let l be a divisor of $p-1$. Let

$$\Gamma = \left\{\gamma \in \mathcal{O}_{\mathbb{Q}[\alpha]} \mid N(\gamma) \not\equiv 0 \pmod{l}\right\}$$

We want to find an integer ϵ such that $\gamma^\epsilon \equiv 1 \pmod{l}$ $\forall \gamma \in \Gamma$. This turns out to be possible if l has a certain property we discussed in Section 2.3, namely being unramified. Assume that l is unramified and let $\epsilon = \operatorname{lcm}\left\{\left|(\mathcal{O}_{\mathbb{Q}[\alpha]}/L_i)^*\right|\right\}$, where the L_i are the prime ideals in the factorization of the ideal generated by l. Since any $\left|(\mathcal{O}_{\mathbb{Q}[\alpha]}/L_i)^*\right|$ divides this ϵ by construction, we have r_i such that $\epsilon = r_i \left|(\mathcal{O}_{\mathbb{Q}[\alpha]}/L_i)^*\right|$. Then for all γ in Γ, we have

$$\begin{aligned}\gamma^\epsilon + L_i &= (\gamma + L_i)^\epsilon = (\gamma + L_i)^{r_i\left|(\mathcal{O}_{\mathbb{Q}[\alpha]}/L_i)^*\right|} \\ &= ((\gamma + L_i)^{\left|(\mathcal{O}_{\mathbb{Q}[\alpha]}/L_i)^*\right|})^{r_i} = (1 + L_i)^{r_i} \\ &= 1 + L_i\end{aligned}$$

Hence $\gamma^\epsilon - 1 \in L_i$ for all i, which means that $\gamma^\epsilon - 1 \in \bigcap_i L_i$. But

$$\bigcap_i L_i = \prod_i L_i = l\mathcal{O}_{\mathbb{Q}[\alpha]}$$

since l is unramified. Hence $\gamma^\epsilon - 1 \in l\mathcal{O}_{\mathbb{Q}[\alpha]}$ and therefore $\gamma^\epsilon \equiv 1 \pmod{l}$.

Define

$$\begin{aligned} \lambda : \Gamma &\to l\mathcal{O}_{\mathbb{Q}[\alpha]}/l^2\mathcal{O}_{\mathbb{Q}[\alpha]} \\ \gamma &\mapsto [\gamma^\epsilon - 1] \end{aligned}$$

We proceed to show that λ is a homomorphism.

$$\begin{aligned} \lambda(\gamma\hat{\gamma}) &= [(\gamma\hat{\gamma})^\epsilon - 1] = [(\gamma^\epsilon\hat{\gamma}^\epsilon - 1) + (1 - 1) + (\gamma^\epsilon - \gamma^\epsilon) + (\hat{\gamma}^\epsilon - \hat{\gamma}^\epsilon)] \\ &= [(\gamma^\epsilon\hat{\gamma}^\epsilon - \gamma^\epsilon - \hat{\gamma}^\epsilon + 1) + (\gamma^\epsilon - 1) + (\hat{\gamma}^\epsilon - 1)] \\ &= [(\gamma^\epsilon - 1)(\hat{\gamma}^\epsilon - 1) + (\gamma^\epsilon - 1) + (\hat{\gamma}^\epsilon - 1)] \\ &= [(\gamma^\epsilon - 1)(\hat{\gamma}^\epsilon - 1)] + [(\gamma^\epsilon - 1)] + [(\hat{\gamma}^\epsilon - 1)] \end{aligned}$$

We claim that the first summand equals 0. Since $(\gamma^\epsilon - 1)$ and $(\hat{\gamma}^\epsilon - 1)$ are both in $l\mathcal{O}_{\mathbb{Q}[\alpha]}$, there are ω and $\hat{\omega}$ in $\mathcal{O}_{\mathbb{Q}[\alpha]}$ such that $\gamma^\epsilon - 1 = l\omega$ and $\hat{\gamma}^\epsilon - 1 = l\hat{\omega}$. Then $(\gamma^\epsilon - 1)(\hat{\gamma}^\epsilon - 1) = l^2\omega\hat{\omega}$, which lies in $l^2\mathcal{O}_{\mathbb{Q}[\alpha]}$. Hence

$$\lambda(\gamma\hat{\gamma}) = [(\gamma^\epsilon - 1)] + [(\hat{\gamma}^\epsilon - 1)] = \lambda(\gamma) + \lambda(\hat{\gamma})$$

and λ is a homomorphism.

The interesting thing about of λ is that it maps l'th powers in $\mathcal{O}_{\mathbb{Q}[\alpha]}$ to 0. Because of the homomorphism property, we have $\lambda\left(\gamma^l\right) = l\lambda(\gamma) = 0$ since $\lambda(\gamma) \in l\mathcal{O}_{\mathbb{Q}[\alpha]}/l^2\mathcal{O}_{\mathbb{Q}[\alpha]}$.

We will now split λ into d maps by showing that $l\mathcal{O}_{\mathbb{Q}[\alpha]}/l^2\mathcal{O}_{\mathbb{Q}[\alpha]}$ has a free module structure. We start by observing that it has a natural $\mathbb{Z}$-module structure, given by $k[l\theta] := [(kl)\theta]$. This can be extended into a $\mathbb{Z}_l$-module structure by trying to define $(k \bmod l)[l\theta] := [(kl)\theta]$. But is this well-defined? Assume $k_1 \bmod l = k_2 \bmod l$, i.e. $k1 - k2 = rl$ for some r in $\mathbb{Z}$. Then

$$(k_1 l)\theta - (k_2 l)\theta = (k_1 - k_2)l\theta = rl^2\theta = l^2(r\theta) \in l^2\mathcal{O}_{\mathbb{Q}[\alpha]}$$

Hence $[(k_1 l)\theta] = [(k_2 l)\theta]$, and the module structure is well-defined.

Recall from Section 2.7 that $\mathcal{O}_{\mathbb{Q}[\alpha]}$ is a free Z-module. Hence

$$\begin{aligned} \mathcal{O}_{\mathbb{Q}[\alpha]} &\cong \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{d} \\ \implies l\mathcal{O}_{\mathbb{Q}[\alpha]} &\cong \underbrace{l\mathbb{Z} \oplus \ldots \oplus l\mathbb{Z}}_{d} \\ \implies l^2\mathcal{O}_{\mathbb{Q}[\alpha]} &\cong \underbrace{l^2\mathbb{Z} \oplus \ldots \oplus l^2\mathbb{Z}}_{d} \end{aligned}$$

From module theory, we then know that

$$l\mathcal{O}_{\mathbb{Q}[\alpha]}/l^2\mathcal{O}_{\mathbb{Q}[\alpha]} \cong \underbrace{l\mathbb{Z}/l^2\mathbb{Z} \oplus \ldots \oplus l\mathbb{Z}/l^2\mathbb{Z}}_{d} \cong \underbrace{\mathbb{Z}_l \oplus \ldots \oplus \mathbb{Z}_l}_{d}$$

In other words, $l\mathcal{O}_{\mathbb{Q}[\alpha]}/l^2\mathcal{O}_{\mathbb{Q}[\alpha]}$ is a free $\mathbb{Z}_l$-module of rank d. It therefore has a basis $\{[l\theta_i]\}_{i=1}^{d}$, where $\theta_i \in \mathcal{O}_{\mathbb{Q}[\alpha]}$ $\forall i$, as a $\mathbb{Z}_l$-module.

Let

$$\mu : l\mathcal{O}_{\mathbb{Q}[\alpha]}/l^2\mathcal{O}_{\mathbb{Q}[\alpha]} \to \underbrace{\mathbb{Z}_l \oplus \ldots \oplus \mathbb{Z}_l}_{d}$$
$$[l\theta] \mapsto (k_1 \bmod l, \ldots, k_d \bmod l)$$

where the $k_i \bmod l$ are the coefficients of $l\theta$ relative to its basis, i.e.

$$[l\theta] = \sum_{i=1}^{d} (k_i \bmod l)[l\theta_i]$$

Let p_i denote the projections

$$p_i : \underbrace{\mathbb{Z}_l \oplus \ldots \oplus \mathbb{Z}_l}_{d} \to \mathbb{Z}_l$$
$$(r_1 \bmod l, \ldots, r_d \bmod l) \mapsto r_i \bmod l$$

We now consider the compositions $\lambda_i = p_i \circ \mu \circ \lambda$. We then have

$$[\gamma^\epsilon - 1] = \lambda(\gamma) = \sum_{i=1}^{d} p_i(\mu(\lambda(\gamma)))[l\theta_i] = \sum_{i=1}^{d} \lambda_i(\gamma)[l\theta_i]$$

for all γ in Γ. This can be rewritten as

$$\gamma^\epsilon - 1 \equiv \sum_{i=1}^{d} \lambda_i(\gamma) l\theta_i \pmod{l^2}$$

λ, μ and p_i are all homomorphisms, so the λ_i are also homomorphisms.

For an l'th power in $\mathcal{O}_{\mathbb{Q}[\alpha]}$, we then have that $\lambda_i\left(\gamma^l\right) = p_i\left(\mu\left(\lambda\left(\gamma^l\right)\right)\right) = p_i(\mu(0)) = p_i((0, \ldots, 0)) = 0$ for all i. We thus have a new necessary requirement for an element in $\mathcal{O}_{\mathbb{Q}[\alpha]}$ being an l'th power, one that we can check in $\mathbb{Z}_l$. This we will utilize in our linear system.

4.3 The linear system

In a similar fashion to what we did in the NFS-fact, we now construct vectors associated to each element in T using three different maps. Define

$$v_1 : T \to \mathbb{Z}_l^B$$
$$(a, b) \mapsto (e_{p_0}(a + bm) \bmod l, \ldots, e_{p_{\pi(y)}}(a + bm) \bmod l),$$

then

$$\begin{aligned}&v_2 : T \to \mathbb{Z}_l^C\\&(a,b) \mapsto (e_{p_1,r_1}(a+b\alpha) \bmod l, \dots, e_{p_C,r_C}(a+b\alpha) \bmod l)\end{aligned}$$

and finally

$$\begin{aligned}&v_3 : T \to \mathbb{Z}_l^d\\&(a,b) \mapsto (\lambda_1(a+b\alpha), \dots, \lambda_d(a+b\alpha))\end{aligned}$$

We put all this together in the map

$$\begin{aligned}&v : T \to \mathbb{Z}_l^{B+C+d}\\&(a,b) \mapsto (v_1(a,b), v_2(a,b), v_3(a,b))\end{aligned}$$

Furthermore, we let

$$\begin{aligned}v(t) &= (\mathrm{ord}_{p_0}(t), \dots, \mathrm{ord}_{p_{\pi(y)}}(t), 0, \dots, 0),\\v(g) &= (\mathrm{ord}_{p_0}(g), \dots, \mathrm{ord}_{p_{\pi(y)}}(g), 0, \dots, 0)\end{aligned}$$

be vectors of length $B+C+d$.

Now define $A = \begin{pmatrix} v(t) & v(a,b)_1 & \dots & v(a,b)_{|T|}\end{pmatrix}$ and solve

$$Ax \equiv -v(g) \pmod{l}$$

We end up with a solution with $|T|+1$ coordinates that we will write as $x \equiv \Big(x_t, x_{(a,b)_1}, \dots, x_{(a,b)_{|T|}}\Big)$. The properties of the solution are the following:

$$v_{q_j}(t)x_t + \sum_{(a,b)\in T} v_{q_j}(a+bm)x_{a,b} + v_{q_j}(g) \equiv 0 \pmod{l}$$

for all q_j in the rational factor base,

$$\sum_{(a,b)\in T} v_{Q_j}(a+b\alpha)x_{a,b} \equiv 0 \pmod{l}$$

for all Q_j in the algebraic factor base and

$$\sum_{(a,b)\in T} \lambda_i(a+b\alpha)x_{a,b} \equiv 0 \pmod{l}$$

for all character maps λ_i.

We now define

$$\begin{aligned}\delta &= t^{x_t} g \prod_{(a,b)\in T} (a+bm)^{x_{a,b}}\\\gamma &= \prod_{(a,b)\in T} (a+b\alpha)^{x_{a,b}}\end{aligned}$$

Because of the abovementioned properties, we have

$$\begin{aligned}\delta &= \left(\prod_j q_j^{v_{q_j}(t)}\right)^{x_t} \prod_j q_j^{v_{q_j}(g)} \prod_{(a,b)\in T} \left(\prod_j q_j^{v_{q_j}(a+bm)}\right)^{x_{a,b}} \\ &= \prod_j q_j^{v_{q_j}(t)x_t + v_{q_j}(g) + \sum_{(a,b)\in T} v_{q_j}(a+bm)x_{a,b}}\end{aligned}$$

We recognize the exponent(s) as the expression(s) above that were congruent to 0 modulo l, hence there is an r_j for each j such that the exponent equals $r_j l$. We get

$$\delta = \prod_j q_j^{r_j l} = \left(\prod_j q_j^{r_j}\right)^l$$

The conclusion is that δ is an l'th power in $\mathbb{Z}$. Similarly, we have

$$\begin{aligned}\langle\gamma\rangle &= \prod_{(a,b)\in T} \left(\prod_j Q_j^{v_{Q_j}(a+b\alpha)}\right)^{x_{a,b}} \\ &= \prod_j Q_j^{\sum_{(a,b)\in T} v_{Q_j}(a+b\alpha)x_{a,b}} \\ &= \prod_j Q_j^{s_j l} = \left(\prod_j Q_j^{s_j}\right)^l\end{aligned}$$

and thus the ideal generated by γ is an l'th power in $\mathcal{O}_{\mathbb{Q}[\alpha]}$. This is necessary for γ being an l'th power in $\mathcal{O}_{\mathbb{Q}[\alpha]}$, which is what we want.

Using the homomorphism property of the character maps, we get

$$\begin{aligned}\lambda_i(\gamma) &= \lambda_i\left(\prod_{(a,b\in T)} (a+b\alpha)^{x_{a,b}}\right) = \sum_{(a,b\in T)} \lambda_i\left((a+b\alpha)^{x_{a,b}}\right) \\ &= \sum_{(a,b\in T)} x_{a,b}\lambda_i(a+b\alpha),\end{aligned}$$

which, as previously shown, is congruent to 0 modulo l for all λ_i. It turns out that this is not likely to happen if γ is not an l'th power in $\mathcal{O}_{\mathbb{Q}[\alpha]}$, so together with the observations made in the previous paragraph, we consider this sufficient to conclude that this is in fact the case. As was the case with the NFS-fact, we need to multiply all l'th powers with $f'(\alpha)^l$ to be guaranteed that they are l'th powers in $\mathbb{Z}[\alpha]$.

4.4 The algorithm

We summarize our work with this algorithm describing how to find the discrete logarithm of g with base t in a field with p elements.

Let $d, u, y \in \mathbb{N}$ be such that $p > 2^d$.

1. Find an integer m and a polynomial $f \in \mathbb{Z}[x]$ such that $f(m) \equiv 0 \pmod{p}$. Decide on a root $\alpha \in \mathbb{C}$ of f.
2. Using the sieving procedures described, find a set $T \subset \mathbb{Z} \times \mathbb{Z}$ such that for all (a, b) in T, we have that $\gcd(a, b) = 1$, $|a| \leq u$, $0 < b \leq u$, $a + bm$ is y-smooth and $N(a + b\alpha)$ is y-smooth.
3. Find a prime divisor l of $p - 1$.
4. Solving the linear system described, find x such that $f'(m)t^{x_t}g \prod (a + bm)^{x_{a,b}}$ and $f'(\alpha) \prod (a + b\alpha)^{x_{a,b}}$ are l'th powers in $\mathbb{Z}$ and $\mathbb{Z}[\alpha]$ respectively.
5. Repeat steps 3 and 4 until all prime divisors of $p - 1$ have been used.
6. Use the Chinese Remainder Theorem to solve the system of congruences $x_t \equiv -\log_t g \pmod{l}$, return the solution.

4.5 Some remarks

It would seem from our description that we can only find the discrete logarithm when both t and g are smooth, since we need to know their factorizations. But in fact, it will suffice that they have smooth preimages under ϕ, see [6].

The complexity analysis of the NFS-dlog is quite similar to the NFS-fact. The dominating step in the previous analysis is exactly the same as step 2 in this algorithm. Elsewhere, n is just replaced by p. We should point out that the linear system in the NFS-dlog will require a bit more work, as it is solved over $\mathbb{Z}_l$ and not $\mathbb{Z}_2$. Still, it should not dominate the other steps in the algorithm. See [6] for clarification on this.

Chapter 5

Finding d-logs in more general finite fields

5.1 General idea

Similar to the way the idea of the NFS-fact was extended to a new problem, it is possible to extend the idea of the NFS-dlog to finding discrete logarithms in other finite fields than the prime ones. Recall from Section 2.3 that if n is not a prime, we can not use $\mathbb{Z}_n$ as a model for F_n as we have done so far. We would therefore need some new ideas. One such algorithm is described in [5]. The linear system and the properties of the solution are quite similar to the NFS-dlog, but the details are a lot more complicated. Furthermore, this turns out not to be the most efficient algorithm for the general discrete logarithm problem. In this chapter, we will present an algorithm running in quasi-polynomial time.

We want to find discrete logarithms in a field $\mathrm{F}_{q^{2k}}$. Elements in this field will be represented by polynomials over F_{q^2} of degree less than k. So let

$$P = \sum_{i=0}^{D} a_i X^i$$

(of degree D) and Q be elements in $\mathrm{F}^*_{q^{2k}}$ such that P is in the subgroup generated by Q, i.e. there is an integer s such that $Q^s = P$ in the field. We denote by $\log_Q(P)$ the smallest such integer.

The idea is to express $\log_Q(P)$ as a linear combination of logarithms of lower degree polynomials. Then we repeat the process on the new polynomials until we have written $\log_Q(P)$ as a linear combination of only linear polynomials. If we can then show that we can compute the logarithms of linear polynomials, we have succeeded in finding the logarithm we wanted.

For this algorithm to work, we need to consider fields on the form $\mathrm{F}_{q^{2k}}$. In addition, we require that there exist polynomials h_0 and h_1 over F_{q^2} of small degree such that $h_1X^q - h_0$ has an irreducible factor of degree k. This means that $h_1X^q - h_0 \equiv 0$, and so

$$X^q \equiv \frac{h_0}{h_1} \tag{5.1}$$

5.2 Reducing the problem

Recall from Proposition 5 that

$$X^qY - XY^q = \prod_{(\alpha,\beta)\in \mathrm{P}^1(\mathrm{F}_q)} (\beta X - \alpha Y)$$

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix defined over F_q. Letting $X = aP + b$ and $Y = cP + d$ in the equality, we obtain

$$\begin{aligned}(aP+b)^q(cP+d) - (aP+b)(cP+d)^q &= \prod_{(\alpha,\beta)} (\beta(aP+b) - \alpha(cP+d)) \\ &= \prod_{(\alpha,\beta)} ((-c\alpha + a\beta)P - (d\alpha - b\beta))\end{aligned} \tag{5.2}$$

Notice that:

$$A^{-1}\begin{pmatrix}\alpha \\ \beta\end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a\end{pmatrix}\begin{pmatrix}\alpha \\ \beta\end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} d\alpha - b\beta \\ -c\alpha + a\beta\end{pmatrix}$$

Hence, which factors appear in the right hand side of (5.2) depends on the set $\{A^{-1}(\mathrm{P}^1(\mathrm{F}_q))\} \subset \mathrm{P}^1(\mathrm{F}_{q^2})$.

Let's study the right hand side of (5.2) some more. We want to take the terms in front of P out of the product. To do this, we obviously divide out by $(-c\alpha + b\beta)$ in every factor. We have to be careful, though, because one of those terms may be 0. If there is such a factor, it will look like $(-c\alpha + a\beta)P - (d\alpha - b\beta) = 0P - (d\alpha - b\beta) = -(d\alpha - b\beta)$, so we divide out by this constant instead. We then end up with a product on the form $\lambda \prod_i (P - f_i)$, where $\lambda \in \mathrm{F}_{q^2}$, $f_i \in \mathrm{F}_{q^2}$ for all i and there are either q or $q+1$ terms in the last product. So the equations now look like:

$$(aP+b)^q(cP+d) - (aP+b)(cP+d)^q = \lambda \prod_i (P - f_i), \tag{5.3}$$

Now, let's focus on the left hand side of (5.3). To ease notation, we make the following definitions:

$$\tilde{a} := a^q$$

$$\tilde{P}(X) := \sum_{i=0}^{D} \tilde{a}_i X^i$$

Then the left hand side of (5.3) becomes

$$\begin{aligned}
&(aP+b)^q(cP+d)-(aP+b)(cP+d)^q\\
&=(a^qP^q+b^q)(cP+d)-(aP+b)(c^qP^q+d^q)\\
&=\left(\tilde{a}\tilde{P}(X^q)+\tilde{b}\right)(cP+d)-(aP+b)\left(\tilde{c}\tilde{P}(X^q)+\tilde{d}\right)
\end{aligned}$$

Now we use (5.1). We get

$$\begin{aligned}
&\left(\tilde{a}\tilde{P}(X^q)+\tilde{b}\right)(cP+d)-(aP+b)\left(\tilde{c}\tilde{P}(X^q)+\tilde{d}\right)\\
&=\left(\tilde{a}\tilde{P}\left(\frac{h_0}{h_1}\right)+\tilde{b}\right)(cP+d)-(aP+b)\left(\tilde{c}\tilde{P}\left(\frac{h_0}{h_1}\right)+\tilde{d}\right)
\end{aligned}$$

If we write this out as a fraction, we can clearly obtain h_1^D as the denominator by multiplying terms in the numerator by powers of h_1. Then the numerator will be a polynomial where the highest degree term will be either h_0^D (which has degree $(1+\deg(h_0))D$) or h_1^D (which has degree $(1+\deg(h_1))D$), so its degree is $(1+\max\{\deg(h_0),\deg(h_1)\})D$.

We say that a polynomial is *n-smooth* if it can be factored into polynomials that are all of degree n or lower. Since h_0 and h_1 are of low degrees, the degree of the numerator on the left hand side of (5.3) is a low multiple of D. It is then not too unlikely that it is $\lceil \frac{D}{2} \rceil$-smooth. If the numerator is in fact $\lceil \frac{D}{2} \rceil$-smooth, we can write the left hand side of (5.3) as $\frac{\prod_j P_j}{h_1^D}$, where the P_j are polynomials of degree $\lceil \frac{D}{2} \rceil$ or lower. Taking the logarithm, we obtain

$$\log_Q\left(\frac{\prod_j P_j}{h_1^D}\right)=\log_Q\left(\prod_j P_j\right)-\log_Q\left(h_1^D\right)=\sum_j \log_Q(P_j)-D\log_Q(h_1)$$

Taking the logarithm on the other side of (5.3) yields

$$\log_Q\left(\lambda\prod_i (P-f_i)\right)=\log_Q(\lambda)+\sum_i \log_Q(P-f_i)$$

In total, we have the following equation:

$$\sum_j \log_Q(P_j)-D\log_Q(h_1)-\log_Q(\lambda)=\sum_i \log_Q(P-f_i) \tag{5.4}$$

We are getting closer to expressing the logarithm of P in terms of logarithms of ”smaller” polynomials. The idea now is to find several equalities (5.4) such that a certain linear combination of them would leave only $\log_Q(P)$ on the right hand side. To do this, we first go through all matrices (we will make clear which matrices to choose from in Section 5.5) and form the corresponding equalities (5.3). We check which left hand sides are $\lceil \frac{D}{2} \rceil$-smooth and keep the matrices that correspond to those equalities. Let's call the matrices $A_1, \ldots, A_r$ and the left hand sides of the corresponding equalities (5.4) $LS_1, \ldots, LS_r$.

To find the desired linear combination, we solve a linear system. Given A_i, we define a vector $v(A_i)$ indexed by the elements of $\mathrm{P}^1(\mathrm{F}_{q^2})$ in the following way:

$$v(A)_{(f,1)} = \begin{cases} 1 & \text{if } \log_Q(P-f) \text{ appears on the right hand side of (3)} \\ 0 & \text{otherwise} \end{cases}$$

$$v(A)_{(1,0)} = \begin{cases} 1 & \text{if there are only } q \text{ terms on the right hand side of (3)} \\ 0 & \text{otherwise} \end{cases}$$

We proceed to form the matrix H whose columns are the vectors $v(A_i)$. The important assumption is now that this matrix has full rank q^2+1 over $\mathbb{Z}$. This will allow us to always find a linear combination of the columns that equals a certain vector, namely v defined by:

$$v_{\gamma,\delta} = \begin{cases} 1 & \text{if } (\gamma,\delta) = (0,1) \\ 0 & \text{otherwise} \end{cases}$$

In other words, we solve the system $Hx = v$. So let $x = (x_1, \ldots, x_r)$ be a solution to this system. This means that:

$$\sum_{i=1}^{r} x_i v(A_i)_{(0,1)} = 1$$
$$\sum_{i=1}^{r} x_i v(A_i)_{(f,1)} = 0 \ \forall f \neq 0 \in \mathrm{F}_{q^2}$$
$$\sum_{i=1}^{r} x_i v(A_i)_{(1,0)} = 0$$

Before we apply the solution, let's rewrite the right hand sides of the equalities (5.4) using the vectors $v(A_i)$. We have

$$\sum_{i} \log_Q(P - f_i) = \sum_{f \in \mathrm{F}_{q^2}} v(A)_{(f,1)} \log_Q(P-f) + v(A)_{(1,0)}$$

Now we multiply equation i with x_i and add them all together:

$$\begin{aligned}
\sum_{i=1}^{r} x_i(LS_i) &= \sum_{i=1}^{r} x_i \left(\sum_{f\in \mathrm{F}_{q^2}} v(A)_{(f,1)} \log_Q(P-f) + v(A)_{(1,0)} \right) \\
&= \left(\sum_{i=1}^{r} x_i v(A_i)_{(0,1)} \right) \log_Q(P-0) \\
&+ \sum_{f\neq 0} \left(\sum_{i=1}^{r} x_i v(A_i)_{(f,1)} \right) \log_Q(P-f) + \sum_{i=1}^{r} x_i v(A_i)_{(1,0)} \\
&= \log_Q(P) + \sum_{f\neq 0} 0 + 0 \\
&= \log_Q(P)
\end{aligned}$$

As expected, only the logarithm of P remains on the right hand side.

We have thus expressed $\log_Q(P)$ as a linear combination of the left hand sides. The left hand sides themselves are linear combinations of the logarithms of polynomials of smaller degree, $\log_Q(h_1)$ and the logarithms of elements in F_{q^2}. As stated in Section 5.1, we now repeat this process until we have a linear combination of only logarithms of linear polynomials and $\log_Q(h_1)$. The next problem we will discuss is therefore how to find those logarithms explicitly.

5.3 Logarithms of linear polynomials

We now want to calculate $\log_Q(X-f)$ for all $f \in \mathrm{F}_{q^2}$ and also $\log_Q(h_1)$. We use a similar strategy as above to begin with. Using X instead of P, equation (5.3) becomes:

$$(aX+b)^q(cX+d) - (aX+b)(cX+d)^q = \lambda \prod_i (X-f_i)$$

Again, we only use equations where the numerator on the left hand side is smooth. The smoothness limit this time is $\left\lceil \frac{\deg(X)}{2} \right\rceil = \left\lceil \frac{1}{2} \right\rceil = 1$, which means that the numerator can be factored into linear polynomials. Hence, we obtain a system of equations on the following form:

$$\sum_j \log_Q(X-f_j) - D\log_Q(h_1) - \log_Q(\lambda) = \sum_i \log_Q(X-f_i) \tag{5.5}$$

Now, we have the logarithms of linear polynomials (and h_1) on both sides of these equations. This means that we don't need to form a new system like we did above, but we can find the logarithms by solving this system directly. Note that this is the part of the algorithm where we actally use the basis for the logarithm, namely Q. The λ's (and possibly some of the linear polynomials) lie in F_{q^2}, and there we can compute logarithms much more efficiently. Let

$$l := \frac{\left|\mathrm{F}^*_{q^{2k}}\right|}{\left|\mathrm{F}^*_{q^2}\right|},$$

then we know that $Q^l \in \mathrm{F}^*_{q^2}$. Computing $\log_{Q^l}(\lambda)$ in this smaller field yields

$$\lambda = \left(Q^l\right)^{\log_{Q^l}(\lambda)} = Q^{l \log_{Q^l}(\lambda)}$$

and hence we have found the logarithm of λ in $\mathrm{F}_{q^{2k}}$. Using these values, we solve the system defined by the equations (5.5) to find the logarithms of all the linear polynomials and h_1. Again, this step relies on a heuristic stating that the corresponding matrix has maximal rank over $\mathbb{Z}$.

As already mentioned, we now have the tools to compute the logarithm of P. By applying the algorithms several times, we obtain

$$\begin{aligned}\log_Q(P) &= \sum_j a_j \log_Q(P_j) + b \log_Q(h_1) + \sum_k \log_Q(\lambda_k) \\ &= \sum_j a_j \left(\sum_l a_l \log_Q(P_l) + c \log_Q(h_1) + \sum_m \log_Q(\lambda_m) \right) \\ &+ a \log_Q(h_1) + \sum_k \log_Q(\lambda_k) = \dots \\ &= \sum_i a_i \log_Q(X - f_i) + a \log_Q(h_1) + \sum_n \lambda_n\end{aligned}$$

where f_i and λ_n are in F_{q^2}. Inserting the computed values for $\log_Q(X - f_i)$ and $\log_Q(h_1)$, we obtain the solution explicitly.

5.4 The algorithm

The algorithm for computing the discrete logarithm of P with base Q in a field with q^{2k} elements is as follows.

Let h_0 and h_1 such that $X^q \equiv \frac{h_0}{h_1}$.

1. Solving the linear system described, express $\log_Q(P)$ as a linear combination of logarithms of polynomials of at most half the degree of P.

2. Repeat step 1 with the new polynomials used instead of P.

3. Repeat step 2 until all remaining polynomials are linear.

4. Solving the linear system described, compute the discrete logarithms of the linear polynomials obtained in step 3.

5. Compute $\log_Q(P)$ as a linear combination of the discrete logarithms produced in step 4.

5.5 Complexity analysis

Let's first consider how many matrices we have to check. When calculating equation (5.3), we want to require that all factors on the right hand side are different. How can make sure that this is the case? Well, if a matrix A has full rank, the set $\left\{A^{-1}(\mathrm{P}^1(\mathrm{F}_q))\right\}$ will consist of $q+1$ different elements. However, if A does not have full rank, some of them might be equal. So we require that our matrices must have full rank, i.e. $\det(A) \neq 0$. Hence, we choose matrices in the set

$$GL\left(2, q^2\right) = \left\{A \in M_{2\times 2}(\mathrm{F}_{q^2}) \mid \det(A) \neq 0\right\}$$

If we have already found a matrix that gives us a smooth numerator on the left hand side, we want to avoid checking matrices that yield the same factors on the right hans side, as these will not contribute to the linear system. Can we in any way characterize some such classes of matrices? Assume that a matrix is a scalar multiple of another one, i.e. there is an m in F_{q^2} such that:

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = m \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

The right hand side of equation (5.2) corresponding to the first matrix is

$$\begin{aligned}\prod_{(\alpha,\beta)} \left((-c'\alpha + a'\beta)\,P - (d'\alpha - b'\beta)\right) &= \prod_{(\alpha,\beta)} ((-mc\alpha + ma\beta)P - (md\alpha - mb\beta)) \\ &= m \prod_{(\alpha,\beta)} ((-c\alpha + a\beta)P - (d\alpha - b\beta)),\end{aligned}$$

which is a scalar multiple of the right hand side of equation (5.2) corresponding to the second matrix. In other words, the two matrices yield exactly the same factors in equation (5.3). So we want to treat matrices that are scalar multiples of each other as "the same" and just check one of them. Observe that

$$A = mA' \iff A = (mI)A' \iff A(A')^{-1} = mI \iff A(A')^{-1} \in Z(2, q^2)$$

where $Z(2, q^2) = \{A \in GL(2, q^2) \mid \exists m \in \mathrm{F}_{q^2} \text{ such that } A = mI\}$. Therefore, we choose matrices from the set $PGL(2, q^2) = GL(2, q^2)/Z\left(2, q^2\right)$ and we avoid checking a bunch of matrices that won't give us anything new.

So multiplying matrices by scalars (diagonal matrices) does not change the corresponding factors. What if we multiply by a matrix over F_q? Assume that there are f_1, f_2, f_3, f_4 in F_q such that:

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Denote the matrices A', B and A, respectively. We must have $\det(B) \neq 0$, otherwise we would have $\det(A') = \det(B)\det(A) = 0$, and we only consider invertible matrices now. Since B has full rank and is defined over F_q, we have that

$$\left\{B^{-1}(\mathrm{P}^1(\mathrm{F}_q))\right\} = \left\{\begin{pmatrix} f_4\alpha - f_2\beta \\ -f_3\alpha + f_1\beta \end{pmatrix}\right\}_{(\alpha,\beta \in P^1(\mathrm{F}_q))} = \mathrm{P}^1(\mathrm{F}_q)$$

Now, we evaluate the right hand side of equation (5.2) corresponding to A'. We have

$$\begin{aligned}
&\prod_{(\alpha,\beta)} \left(\left(-c'\alpha + a'\beta\right) P - \left(d'\alpha - b'\beta\right) \right) \\
&= \prod_{(\alpha,\beta)} \left((-(f_3a + f_4c)\alpha + (f_1a + f_2c)\beta)P - ((f_3b + f_4d)\alpha - (f_1b + f_2d)\beta) \right) \\
&= \prod_{(\alpha,\beta)} (-f_3a\alpha - f_4c\alpha + f_1a\beta + f_2c\beta)P - (f_3b\alpha + f_4d\alpha - f_1b\beta - f_2d\beta)) \\
&= \prod_{(\alpha,\beta)} ((-c(f_4\alpha - f_2\beta) + a(-f_3\alpha + f_1\beta))P - (d(f_4\alpha - f_2\beta) - b(-f_3\alpha + f_1\beta)))
\end{aligned}$$

Using the set equality above, we know that as (α, β) ranges over $\mathrm{P}^1(\mathrm{F}_q)$, so does $(f_4\alpha - f_2\beta, -f_3\alpha + f_1\beta)$. Hence, by reordering the factors in some way, we obtain

$$\prod_{(\alpha,\beta)} \left(\left(-c'\alpha + a'\beta\right) P - \left(d'\alpha - b'\beta\right) \right) = \prod_{((\alpha,\beta)} ((-c\alpha + a\beta)P - (d\alpha - b\beta)),$$

which is the right hand side of equation (5.2) corresponding to A. So the two matrices yield the same factors in equation (5.3).

Once again, we would then like to avoid checking both A and A'. In order to identify them, we observe that

$$A = FA' \iff A\left(A'\right)^{-1} = F \iff A\left(A'\right)^{-1} \in PGL(2, q),$$

so we can now restrict us to picking matrices from $\mathcal{P}_q = PGL\left(2, q^2\right)/PGL(2, q)$ without losing anything.

We need to know how many matrices there are in $\mathcal{P}_q$. It is known that $\left|PGL\left(2, q^i\right)\right| = q^{3i} - q^i$, so we get

$$|\mathcal{P}_q| = \frac{\left|PGL\left(2, q^2\right)\right|}{|PGL(2, q)|} = \frac{q^6 - q^2}{q^3 - q} = q^3 + q$$

This fact is used as the basis of the heuristic argument presented in [1], which attempts to show that the matrix H indeed has full rank. The argument is quite unrigorous and the conclusion is not very close to what we really want, so it will we skipped here. Still, the assumption that H has full rank seems to be true experimentally. Because it is vital to the algorithm, we point out that producing a more rigorous argument is important for the development of this method.

How much time does step 1 take? Well, we need to go through all matrices in $\mathcal{P}_q$ and check their corresponding equations for smoothness. This can be done in polynomial time in q and $D \leq k$. It is known that the linear system can be solved with $O\left(q^5\right)$ operations, see [1]. In total, we have that the cost of one iteration of the algorithm is polynomial in q and k.

Since steps 2 and 3 only involve repeating step 1, the big question is how many times this first step is performed. We first need to find out how many terms there are in the sum on the left hand side of equation (5.4). Recall that the product of the polynomials P_i is a polynomial of degree at most $(1 + \max\{\deg(h_0), \deg(h_1)\})D$. There are therefore at most

$$(1 + \max\{\deg(h_0), \deg(h_1)\})D = O(D)$$

polynomials in the sum. Note that in this "worst" case, we would actually end up with only linear polynomials and hence be done. Still, we will assume that we can have this many polynomials in every iteration and that we only halve the degree of the polynomials every time. The quasi-polynomial result will still be obtainable.

So each equation has $O(D)$ polynomials on the left hand side, but how many equations do we need? Since H has rank q^2+1, we need at most $q^2+1 = O\left(q^2\right)$ columns to form a linear combination that equals v. Each column corresponds to an equation that we will use, so there are $O\left(q^2\right)$ such equations. Each of those contains $O(D)$ polynomials, as shown above, so we express a logarithm as a linear combination of

$$O\left(q^2 D\right) = O\left(q^2 k\right)$$

polynomials every time we perform step 1. Hence, every iteration of this step generates $O\left(q^2 k\right)$ new iterations.

But when does this stop? If we halve the degree every time, we reach step 3 at most $\log_2(D) = O(\log_2(k))$ times. The total number of iterations of step 1 is then less than $\left(q^2 k\right)^{O(\log_2(k))}$. The running time of every iteration was polynomial in q and k, so the total running time for finding a discrete logarithm in $\mathrm{F}_{q^{2k}}$ becomes

$$\max\{q, k\}^{O(\log_2(k))}, \tag{5.6}$$

which is quasi-polynomial in q and k.

Chapter 6

Concluding remarks

The recent developments in integer factorization and dicrete logarithm computation are quite impressive. In just the last 25 years, methods for solving these problems have achieved significantly lower running time than one could previously hope for. Still, no one is able to produce a polynomial time algorithm for either of these problems that can finally put an end to the search. So maybe it's just not possible? And even if it is, as long as the world's finest mathematicians are unable to do it, who can then break the cryptosystems?

Readers of this thesis might notice that as the algorithms we study get faster and seemingly more applicable, the level of rigorousness decreases and heuristics take over. There are also still a lot of situations in which our algorithms are inapplicable and/or inefficient, and several of the ”good” results only hold under special assumptions. There is therefore significant work yet to be done, both in analyzing, implementing and improving these algorithms.

Bibliography

[1] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *Advances in Cryptology — EUROCRYPT 2014*, Lecture Notes in Computer Science. Springer, 2014.

[2] J.P. Buhler, Jr. H.W. Lenstra, and Carl Pomerance. Factoring integers with the number field sieve. In *The Development of the Number Field Sieve*. Springer, 1993.

[3] Daniel A. Marcus. *Number Fields*. Universitext. Springer, 1977.

[4] Jürgen Neukirch. *Algebraic number theory*. Grundlehren der mathematischen Wissenschaften. Springer, 1999.

[5] Oliver Schirokauer. Using number fields to compute logarithms in finite fields. *Mathematics of Computation*, 69(231), 2000.

[6] Oliver Schirokauer. The impact of the number field sieve on the discrete logarithm problem in finite fields. In *Algorithmic Number Theory*, volume 44 of *Mathematical Sciences Research Institute Publications*. MSRI, 2008.