The Number Field Sieve and its Applications in Factorization

Emmanouil Doulgerakis

Supervisor

Jannis A. Antoniadis

Master Thesis

Department of Mathematics and Applied Mathematics
University of Crete

To my parents !

Acknowledgments

The present master thesis was presented at the Department of Mathematics and Applied Mathematics in 2 May 2017. My master thesis examination committee consisted of Jannis A. Antoniadis, Theodoulos Garefalakis and Nikolaos G. Tzanakis.

I would like to thank them for being members of this committee. More particularly I would like to thank my supervisor, prof. Jannis A. Antoniadis, who helped me all the way to the completion of this master thesis, and my master studies in general. Also I have to thank my colleagues Alexandros Galanakis and Anthi Zervou, for their patience to attend the lectures I gave in order to present in detail the content of my master thesis.

Master's thesis examination committee:

- Jannis A. Antoniadis (supervisor),
- Theodoulos Garefalakis and
- Nikolaos G. Tzanakis

Contents

Introduction

By the time public key cryptography was introduced many cryptosystems of this kind have been developed. For the most of these cryptosystems their security is based on the difficulty of either of the following two problems, integer factorization and the discrete logarithm problem. One of the first public key cryptosystems developed was RSA which was introduced in 1977 by Ron Rivest , Adi Shamir and Leonard Adleman and then widely used. This cryptosystem bases its security on the difficulty of integer factorization. Therefore in order to test the security of ciphers like that the problems of integer factorization and the discrete logarithm problem have been extensively studied by researchers the last 40 years. One algorithm that was developed through those studies was the Number Field Sieve. As the NFS is the algorithm that holds the current world records for integer factorization we choose to study this algorithm.

The goal of this master thesis is to present the Number Field Sieve algorithm and the mathematical background which was used for its development. The algorithm was first introduced as a factoring algorithm. More particularly, the first version of the algorithm could factor only integers n of the form $n = r^e - s$ with $r, |s|$ small positive integers. This algorithm presented in [16, pp. 11-42] will be studied in the first chapter of this master thesis. To indicate the strength of the algorithm we mention two factorizations that were done using it. Its first success was the complete factorization of the ninth Fermat number in 1993 [15]. Apart from that, it also holds a record for factoring the 320-digit number $n = 2^{1061} - 1$ in 2012 [7]. As later versions of the NFS were based on this one we try to explain each step in as much detail as possible. The main goal of the algorithm is to construct a congruence of squares such that $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y \pmod{n}$. In order to achieve that the NFS attempts to find a sufficient number of smooth elements over some factor base and then tries to find a combination of them which will lead to a congruence of squares. For the development of the algorithm we need many results from algebraic number theory, linear algebra and even graph theory. In the first chapter we mention all the theory that we need and prove many results. Finally we give a small example of a factorization so that the ideas described in the previous sections to be illustrated.

The second chapter is devoted to the General Number Field Sieve [16, pp. 50-92]. This is a version of the algorithm described in chapter 1 which can factor arbitrary inte-

gers. Although slower than the one described in chapter 1 it is still faster than any other factoring algorithm for integers with more than about 110 decimal digits. It actually holds a record for factoring the 232−digit number RSA-768.

$$\begin{aligned} RSA-768 =& 123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 \end{aligned}$$

The factorization of RSA-768 reported in [13] finished in the end of 2009 and took about three years.

$$\begin{aligned} RSA-768 =& 33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489 \\ &\times 36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917 \end{aligned}$$

In this chapter we explain all the modifications included in this version and prove the mathematical background needed. Finally we give again a small example of a factorization.

Heraklion 2/5/2017

Chapter 1

The Special Number Field Sieve

Building upon modern ideas about factoring integers in 1990 A.K. Lenstra, H.W. Lenstra Jr., M.S. Manasse and J.M. Pollard published the paper "The number field sieve" [16, pp. 11-42]. This paper describes the algorithm which we are going to study in this chapter (we will call it special number field sieve). The SNFS is one of the most powerful algorithms available at the moment for factoring integers. Its first success was the complete factorization of the ninth Fermat number in 1993 [15]. Apart from that, it also holds a record for factoring the 320-digit number $n = 2^{1061} - 1$ in 2012 [7]. However, it is not a general purpose factoring algorithm as it factors only integers of the form $n = r^e - s$ for small positive r and $|s|$. Additionally, it gets faster than other methods if the number we are trying to factor has more than about 100 decimal digits. In case we are trying to factor a number with less than 100 decimal digits, the quadratic sieve or the elliptic curve method will probably be faster.
The basic idea originating back to Fermat is that of constructing congruences of squares modulo the number we want to factor. Let n be an integer that we want to factor and assume that we have found $x,\ y \in \mathbb{Z}$ such that $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y \pmod{n}$. It then follows that $gcd(x - y, n)$ is a non-trivial factor of n. So our goal is to construct congruences like the above. In order to achieve that the SNFS associates a number field to n and then using sieving techniques it attempts to find a sufficient number of smooth elements. Finally using linear algebra it combines these smooth elements in order to construct congruences of squares.

1.1 Preliminaries on algebraic number theory

In this section we are going to take some results of algebraic number theory for granted without proving them. These results are included in almost any book concerning algebraic number theory as [19], we used [2].
A key concept for the number field sieve is the concept of a smooth number.

Definition 1.1.1. *Let $n \in \mathbb{Z}$ and $B \in \mathbb{N}$. The number n is called $B - smooth$ if all its prime factors are less than B.*

Definition 1.1.2. *A field K will be called a number field if it is a subfield of $\mathbb{C}$ and it is a finite extension of $\mathbb{Q}$.*

For every number field K we define the ring of algebraic integers R_K to be as follows.

Definition 1.1.3. *Let $a \in K$, then $a \in R_K$ if and only if $Irr(a, \mathbb{Q}) \in \mathbb{Z}[X]$*

For the needs of our algorithm we wish to extend the concept of a smooth number to the ring R_K so we are going to study some of its properties.
First of all, it is an easy result of algebraic number theory that there is a $\theta \in R_K$ such that $K = \mathbb{Q}(\theta)$. Let $[K : \mathbb{Q}] = n$ and

$$f(X) = Irr(\theta, \mathbb{Q}) = (X - \theta^{(1)}) \cdot (X - \theta^{(2)}) \cdot ... \cdot (X - \theta^{(n)}) \quad \text{where} \quad \theta := \theta^{(1)}$$

.

Having this in mind it is easy to show that there are exactly n embeddings of K in $\mathbb{C}$, defined as

$$\begin{aligned} \sigma_j : K &\to \mathbb{C} \\ \sum_{i=0}^{n-1} a_i \theta^i &\mapsto \sum_{i=0}^{n-1} a_i {\theta^{(j)}}^i \end{aligned}$$

We now use this embeddings in order to define the norm map of the field K.

Definition 1.1.4. *Let $K = \mathbb{Q}(\theta)$ be a number field ,$a \in K$ and $\sigma_1, \sigma_2, ..., \sigma_n$ be the embeddings of K in $\mathbb{C}$. We define the norm of the element a to be*

$$N(a) = \prod_{i=1}^{n} \sigma_i(a)$$

The following result about the norm map will allow us to extend the concept of a smooth element to the ring R_K.

Proposition 1.1.5. *Let K be a number field, then the norm map defined above is a multiplicative function that maps the elements of K to $\mathbb{Q}$ and the elements of R_K to $\mathbb{Z}$.*

Definition 1.1.6. *Let $a \in R_K$ and $B \in \mathbb{N}$ then the element a is called B-smooth if its norm is B-smooth.*

In the case of the ring $\mathbb{Z}$ the definition of a smooth element is depended on its prime factorization. As we will see next for the needs of SNFS we need to have something similar for the ring R_K. So at this point we need to make some comments about the property of factorization in the ring R_K. Initially we define what is a unit of the ring R_K.

Definition 1.1.7. *Let $a \in R_K$, then a is called a unit of R_K if $N(a) = \pm 1$.*

The units of the ring R_K form a group which we denote by $E(R_K)$.

Definition 1.1.8. *Let R be an integral domain, then R is called a unique factorization domain (UFD) if every non-zero and non-unit element can be written as a product of prime elements, uniquely up to order and units.*

Definition 1.1.9. *Let R be an integral domain, then R is called a principal ideal domain (PID) if every ideal of R is principal.*

In general every principal ideal domain is a unique factorization domain but the opposite does not hold. However for the ring of algebraic integers R_K of a number field K the two properties are equivalent. That means that R_K either has both of the above properties or none of them. In the next paragraphs we are going to study the SNFS making the simplifying assumption that R_K possesses both of the properties (i.e. the class number of K , $h_K = 1$). In the end of the chapter we are going to mention how it can be adjusted in order to apply in the case that R_K does not possess none of them (i.e. $h_K > 1$). Even though in both cases the algorithm works fine there is one property of R_K that we need in both cases. That is the property of a Dedekind domain.

Definition 1.1.10. *Let R be an integral domain, then R is called a Dedekind domain if and only if the following three properties hold:*
i) The ring R is noetherian.
ii) Every prime ideal of R is maximal.
iii) R is integrally closed.

The following theorem holds for every Dedekind domain.

Theorem 1.1.11. *Let R be a Dedekind domain, then every non-zero ideal of R has a unique factorization in prime ideals of R.*

The above theorem makes clear why we want R_K to be a Dedekind domain. The reason is that in both cases we need unique factorization of ideals.

Theorem 1.1.12. *Let K be a number field and R_K be its ring of algebraic integers. Then R_K is a Dedekind domain.*

We will also need to define the norm of an ideal.

Definition 1.1.13. *Let I be an ideal of R_K, then we define the norm of I to be $N(I) = \#(R_K/I)$.*

Remark 1.1.14. *It is well known that this number is finite.*

Definition 1.1.15. *Let $\mathfrak{p}$ be a prime ideal of R_K, we define the inertia degree $f(\mathfrak{p}/p\mathbb{Z})$ to be the degree $[R_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$ of the field extension.*

The ring $\mathbb{Z}[\theta]$ is a subring of R_K. In the case that $R_K = \mathbb{Z}[\theta]$ that simplifies a little bit the algorithm as we will see later. However, there are cases in which that does not hold so, $\mathbb{Z}[\theta] \subsetneq R_K$. In these cases we cannot substitute the ring R_K with $\mathbb{Z}[\theta]$ and work with it. The reason is that $\mathbb{Z}[\theta]$ is not integrally closed and so not a Dedekind domain, which follows that we do not have unique factorization of ideals. That justifies our choice to work with the ring R_K instead of $\mathbb{Z}[\theta]$. As we will see in the next chapter this is a difference between the special and the general number field sieve, as in the later we will work in the ring $\mathbb{Z}[\theta]$.

Comment 1.1.16. *For the rest of the chapter we are going to take the ring R_K for granted without mentioning how it was found. For more information on how to compute the ring of algebraic integers of a number field we refer to [8].*

1.2 Description of the algorithm

In the following description we consider the large prime variation of SNFS as in practice it is proved to be more efficient. That means that in the sieving step, where we are looking for smooth elements we allow one prime factor to exceed the smoothness bound. For the rest of this chapter n will denote the number that we are trying to factor. Our goal is to construct a congruence of squares $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y \pmod{n}$. The SNFS tries to achieve that through the following four main steps.

Step 1) We first choose the degree d of the extension in which we are going to work and then associate a number field $K = \mathbb{Q}(\theta)$ to the number n. This is done through the irreducible polynomial $f(x)$ of θ. We choose $f(x)$ in a specific way as we wish it to have the following property.

$$\text{There is an integer m (of size } n^{1/d}\text{) such that} \quad f(m) \equiv 0 \pmod{n}$$

Step 2) As we have chosen the number field K in which we are going to work, the next step is to choose our smoothness bounds B_1, B_2, B_3, B_4 such that $B_1 \leq B_3$ and

$B_2 \leq B_4$. Then we construct the factor base. Our factor base consists of three sets **P**, **U** and **G**.

$$\mathbf{P} = \{p \in \mathbb{P},\ p \leq B_1\}$$
$$\mathbf{U} = \{\text{a generating set of the group of units of } R_K\}$$
$$\mathbf{G} = \{\pi \in R_K : < \pi >= \mathfrak{p} \quad \forall\, \mathfrak{p} \in \mathbb{P}(K) \text{ such that } f(\mathfrak{p}/p\mathbb{Z}) = 1 \text{ and } N(\mathfrak{p}) \leq B_2\}$$
$$\cup \{\pi \in R_K : < \pi >= \mathfrak{p} \quad \forall\, \mathfrak{p} \mid fR_K\}$$

where $f = [R_K : \mathbb{Z}[\theta]]$ and $f(\mathfrak{p}/p\mathbb{Z})$ is the inertia degree.

Step 3) We choose two sieving bounds U_1, U_2 and we try to find a sufficient number of relations. More specifically we are looking for pairs $(a,\ b)$ where $a,\ b$ are integers with $|a| \leq U_1$ and $0 < b \leq U_2$ such that :
i) $\gcd(a,\ b) = 1$
ii) $|a+bm|$ is B_1-smooth except for at most one prime factor p_1 such that $B_1 < p_1 < B_3$
iii) $a + b\theta$ is B_2-smooth except for at most one prime ideal $\mathfrak{p}_2$ in the factorization of $< a + b\theta >$ with $N(\mathfrak{p}_2) = p_2$ and $B_2 < p_2 < B_4$
When we find a pair $(a,\ b)$ that satisfies the above three conditions we say that we have found a relation.

Step 4) Once we have enough relations we form a matrix depending on the factorization of the elements $a + bm$ and $a + b\theta$ that each relation corresponds to. Let S be the set of all relations that we found in step 3. Then using linear algebra techniques we attempt to find a subset T of S such that :

$$\prod_{(a,\ b)\in T} (a + bm) = \quad \text{square in } \mathbb{Z} \tag{1.1}$$
$$\prod_{(a,\ b)\in T} (a + b\theta) = \quad \text{square in } R_K \tag{1.2}$$

We are now going to make some comments on some points of the above steps that may not have been clear.
In step 2 the choice of the smoothness bounds is done better empirically, however later in this chapter we will mention some suggested choices depending on the running time analysis of this algorithm. Also, in step 2 when we construct the set **G** we take the elements π to be pairwise not associates so, for each prime ideal we take only one generator. At this point our assumption that the ring R_K is a PID is necessary. If R_K was not a PID then we could not construct the set **G**. The reason for this is that some ideals may not be principal so we cannot find a generator π. Finally as we will see later the set **U** is finite so we just have to determine it.

Step 3 is the sieving step. The prime p_1 if it exists is called the large prime and the prime ideal $\mathfrak{p}_2$ the large prime ideal. We distinguish between the following cases.
In a relation if there is not a large prime or a large prime ideal then we set $p_1 = 1$, $\mathfrak{p}_2 = \langle 1 \rangle = R_K$ and we call the relation a full relation. Otherwise we call it a partial relation. So in a full relation we have

$$a + bm = \prod_{p \in \mathbf{P}} p^{e(p)} \quad \text{and} \quad a + b\theta = \prod_{u \in \mathbf{U}} u^{e(u)} \prod_{g \in \mathbf{G}} g^{e(g)}$$

where $e(p), e(g) \in \mathbb{N}$ and $e(u) \in \mathbb{Z}$.

Definition 1.2.1. *Let C be a set of partial relations, then C will be called a cycle if for each $(a,\, b) \in C$ there is a sign $s(a,b) \in \{\pm 1\}$ such that*

$$\prod_{(a,\, b) \in C} (a + bm)^{s(a,b)} = \prod_{p \in \boldsymbol{P}} p^{e(p)} \quad \textit{and} \quad \prod_{(a,\, b) \in C} (a + b\theta)^{s(a,b)} = \prod_{u \in \boldsymbol{U}} u^{e(u)} \prod_{g \in \boldsymbol{G}} g^{e(g)}$$

So in order to take advantage of partial relations our target will be to construct a maximal set of independent cycles.

There is also a kind of relations called free relations. This kind actually corresponds to the case where $b = 0$ and $a \in \mathbb{P}$. As we will see later for each prime $p \leq \min\{B_1,\, B_2\}$ for which $f(x)$ factors completely in linear factors in $\mathbb{F}_p[X]$ there is such a relation. When the number of full relations plus the number of free relations plus the number of independent cycles exceeds $|\mathbf{P}| + |\mathbf{U}| + |\mathbf{G}|$ we stop sieving.

Each full relation, each free relation and each cycle that we have from step 3 gives rise to two elements, one in $\mathbb{Z}$ and one in R_K. If we consider a relation (a, b) these two corresponding elements are $a + bm$ and $a + b\theta$ respectively. If we consider a cycle C then these two elements are

$$\prod_{(a,\, b) \in C} (a + bm)^{s(a,b)} \quad \text{and} \quad \prod_{(a,\, b) \in C} (a + b\theta)^{s(a,b)}.$$

In both cases these elements factor completely over our factor base. So, for every such element we compute its factorization. For example, let $(a,\, b)$ be a full relation and

$$a + bm = \prod_{p \in \mathbf{P}} p^{e(p)} \quad \text{and} \quad a + b\theta = \prod_{u \in \mathbf{U}} u^{e(u)} \prod_{g \in \mathbf{G}} g^{e(g)}$$

then we form a vector $v_{(a,\, b)}$ over $\mathbb{F}_2$ like this

$$v_{(a,\, b)} = \left((e(p) \bmod 2)_{p \in \mathbf{P}}, (e(g) \bmod 2)_{g \in \mathbf{G}}, (e(u) \bmod 2)_{u \in \mathbf{U}}\right)$$

In step 4 we form a matrix A using all these vectors as columns of A. Then using linear algebra we attempt to find vectors of the nullspace of A. Each such vector gives rise to a subset T of S (where S is the set of all full relations, free relations and cycles) such that :

$$\prod_{(a,\,b)\in T}(a+bm) = \quad \text{square in } \mathbb{Z}$$
$$\prod_{(a,\,b)\in T}(a+b\theta) = \quad \text{square in } R_K$$

Remark 1.2.2. *The nullspace of A contains non-zero vectors as we have $\#S > |\boldsymbol{P}| + |\boldsymbol{U}| + |\boldsymbol{G}|$*

Finally, once step 4 is completed we have constructed two squares, one in $\mathbb{Z}$ and one in R_K respectively. Then we will use a ring homomorphism $\varphi : R_K \to \mathbb{Z}/n\mathbb{Z}$ for which the images of the two squares are equal in order to construct a congruence of squares $\pmod n$.

The next sections of this chapter are devoted to the study of the above four steps.

1.3 Polynomial selection and definition of φ

In this section we will see how we construct the number field in which we are going to work and how we define the ring homomorphism φ mentioned above. The number field is constructed with the help of an irreducible polynomial which depends on the special form of n as we will see. We have already mentioned on the previous section that the first parameter which we choose is the degree of the extension in which we are going to work. Let d be the degree of the extension and k the least positive integer such that $kd \geq e$ where $n = r^e - s$. We set

$$t = sr^{kd-e} \quad , \quad f(x) = x^d - t \quad \text{and} \quad m = r^k$$

We have that

$$f(m) = r^{kd} - sr^{kd-e} = r^{kd-e}(r^e - s) \equiv 0 \pmod n$$

so the polynomial $f(x)$ has the property that step 1 of the algorithm requires. At this point we make the assumption that $f(x)$ is irreducible. This condition is likely to be satisfied since in realistic cases a non-trivial factor of $f(x)$ gives rise to a non-trivial factor of n. As we have an irreducible polynomial, let θ be one of its roots. We set $K = \mathbb{Q}(\theta)$ to be the number field in which we are going to work. Moreover as $f(x)$ is irreducible it follows that $[K : \mathbb{Q}] = d$.

Comment 1.3.1. *In practice the degree of the extension used for the SNFS is less than 7.*

Remark 1.3.2. *At this point before proceeding to the next steps there are two things that have to be done. The first one is to find the ring R_K and the second is to compute the class number h_K of the field in which we are working. However the study of these computational problems is beyond the scope of this master thesis.*

The next step is to define the ring homomorphism φ. We are going to define φ initially in $\mathbb{Z}[\theta]$ and then extend it to R_K in case $\mathbb{Z}[\theta] \subsetneq R_K$. We define

$$\begin{aligned} \varphi : \mathbb{Z}[\theta] &\to \mathbb{Z}/n\mathbb{Z} \\ \sum_{i=0}^{d-1} a_i\theta^i &\mapsto \sum_{i=0}^{d-1} a_i m^i \pmod{n} \end{aligned}$$

where $f(m) \equiv 0 \pmod{n}$. We are going to keep this notation for φ for the rest of this chapter. In order to extend φ to R_K we must first define the discriminant of an element.

Definition 1.3.3. *Let K be a number field with $[K : \mathbb{Q}] = d$, we define the discriminant of d elements of K, $\{a_1, a_2, \dots, a_d\}$ to be $D_K(\{a_1, a_2, \dots, a_d\}) = (det[\sigma_i(a_j)])^2$. We define the discriminant of an element $a \in K$ to be $D_K(a) = (det[\sigma_i(a^j)])^2$*

It can be proved that $D_K(\theta) = \prod_{1 \le i < j \le d} (\sigma_i(\theta) - \sigma_j(\theta))^2 = (-1)^{\frac{d(d-1)}{2}} N(f'(\theta))$.

Proposition 1.3.4. *Let $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = d$ then $R_K \subseteq \frac{1}{D_K(\theta)}\mathbb{Z}[\theta]$*

Proof. Let $a \in R_K$ hence a can be written as $a = \sum_{k=0}^{d-1} a_k\theta^k$, $a_k \in \mathbb{Q}$. Let $a^{(i)} = \sigma_i(a)$ for $i = 1, \dots, d$. Then $a^{(i)} = \sum_{k=0}^{d-1} a_k {\theta^{(i)}}^k$ for $i = 1, \dots, d$ so we have,

$$\begin{pmatrix} 1 & \theta & \dots & \theta^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \theta^{(d)} & \dots & {\theta^{(d)}}^{d-1} \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \end{pmatrix} \begin{pmatrix} a \\ a^{(2)} \\ \vdots \\ a^{(d)} \end{pmatrix}$$

Therefore that $a_k = \frac{A_k}{D}$ for $k = 1, \dots, d-1$ where $D = \prod_{1 \le i < j \le d} (\sigma_i(\theta) - \sigma_j(\theta))$ $D \neq 0$ and

$$A_k = det \begin{bmatrix} 1 & \theta & \dots & a & \dots & \theta^{d-1} \\ 1 & \theta^{(2)} & \dots & a^{(2)} & \dots & {\theta^{(2)}}^{d-1} \\ \vdots & \vdots & & \vdots & & \vdots \\ 1 & \theta^{(d)} & \dots & a^{(d)} & \dots & {\theta^{(d)}}^{d-1} \end{bmatrix}$$

Also, $A_k \in \widetilde{\mathbb{Z}},\ D \in \widetilde{\mathbb{Z}}$. But now we have that $a_k = \frac{A_k D}{D^2} \Rightarrow A_k D = a_k D^2$ which follows that $A_k D \in \mathbb{Q}$ as $D^2 = D_K(\theta) \in \mathbb{Q}$ and $a_k \in \mathbb{Q}$. So, finally we get that $A_k D \in \mathbb{Q} \cap \widetilde{\mathbb{Z}} = \mathbb{Z}$. Now $D^2 a = \sum_{k=0}^{d-1} D^2 a_k \theta^k = \sum_{k=0}^{d-1} A_k D \theta^k \in \mathbb{Z}[\theta] \Rightarrow a \in \frac{1}{D_K(\theta)} \mathbb{Z}[\theta]$ so $R_K \subseteq \frac{1}{D_K(\theta)} \mathbb{Z}[\theta]$. □

We are now going to compute the discriminant of θ.

$$\begin{aligned} D_K(\theta) &= (-1)^{\frac{d(d-1)}{2}} N(f'(\theta)) \\ &= (-1)^{\frac{d(d-1)}{2}} N(d\theta^{d-1}) \\ &= (-1)^{\frac{d(d-1)}{2}} d^d N(\theta)^{d-1} \\ &= (-1)^{\frac{d(d-1)}{2}} d^d \left((-1)^{d+1} t\right)^{d-1} \\ &= (-1)^{\frac{(d-1)(3d+2)}{2}} d^d t^{d-1} \quad \text{where} \quad t = sr^{kd-e} \end{aligned}$$

Consequently as we showed that $R_K \subseteq \frac{1}{D_K(\theta)} \mathbb{Z}[\theta]$ then for all $\gamma \in R_K$ there exists a $\beta \in \mathbb{Z}[\theta]$ and an $l \mid D_K(\theta)$ such that $\gamma = \frac{\beta}{l}$. As we have made the assumption that s, r, d are small we can also assume that $\gcd(drs,\, n) = 1$ and so we can extend φ in R_K as follows,

$$\varphi(\gamma) = \varphi(\beta)(\varphi(l))^{-1}$$

Next we define the discriminant of a number field.

Theorem 1.3.5. *The ring R_K is a finitely generated free abelian group with $rank = d$ and hence $R_K = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \oplus ... \oplus \mathbb{Z}\omega_d$ where $\omega_i \in R_K$.*

Definition 1.3.6. *Every such $\mathbb{Z}$-basis of R_K is called an integral basis of $K/\mathbb{Q}$.*

The discriminant of two different integral bases are equal, so we give the following definition.

Definition 1.3.7. *We define the discriminant of a number field K to be the discriminant of any integral basis. We use the notation $D_{K/\mathbb{Q}}$*

The following theorem about the discriminant of a number field gives us an interesting connection.

Theorem 1.3.8. *Let $K = \mathbb{Q}(\theta)$ be a number field. Then $D_K(\theta) = [R_K : \mathbb{Z}[\theta]]^2 D_{K/\mathbb{Q}}$.*

Comment 1.3.9. *In this step we used essentially the special form of n in order to construct K and φ. This special form of n enabled us to associate to it a number field of special form with "small" discriminant. These special properties enable us to solve in a reasonable amount of time computational problems like the construction of the factor base. As we will see in the next chapter in the case where n is not of this special form then constructing the factor base is out of the question.*

1.4 Factor base construction

In this section we are going to study how we construct some necessary sets for the sieving step. This implies that we have to compute the sets **P** , **U** , **G** and something extra as we will see.

The easiest set is $\mathbf{P} = \{p \in \mathbb{P},\ p \leq B_1\}$ as we can just get it from a database of prime numbers.

The next set we are going to examine is

$$\mathbf{G} = \{\pi \in R_K : < \pi >= \mathfrak{p} \quad \forall\, \mathfrak{p} \in \mathbb{P}(K) \text{ such that } f(\mathfrak{p}/p\mathbb{Z}) = 1 \text{ and } N(\mathfrak{p}) \leq B_2\}$$
$$\cup \{\pi \in R_K : < \pi >= \mathfrak{p} \quad \forall\, \mathfrak{p} \mid fR_K\}$$

Initially we consider the construction of the subset

$$\mathbf{G}_1 = \{\pi \in R_K : < \pi >= \mathfrak{p} \quad \forall\, \mathfrak{p} \in \mathbb{P}(K) \text{ such that } f(\mathfrak{p}/p\mathbb{Z}) = 1 \text{ and } N(\mathfrak{p}) \leq B_2\}$$

of **G**. In order to do that we first need to have a convenient representation of the prime ideals $\mathfrak{p} \in \mathbb{P}(K)$ such that $f(\mathfrak{p}/p\mathbb{Z}) = 1$. The following theorem will give us exactly what we need.

Theorem 1.4.1. *Let $K = \mathbb{Q}(\theta)$ be a number field, where θ is an algebraic integer, whose (monic) minimal polynomial is denoted $T(X)$. Let $f = [R_K : \mathbb{Z}[\theta]]$. Then for any prime number p not dividing f one can obtain the prime decomposition of pR_K as follows. Let,*

$$T(X) \equiv \prod_{i=1}^{g} T_i(X)^{e_i} \pmod{p}$$

be the decomposition of T into irreducible factors in $\mathbb{F}_p[X]$, where the T_i are taken to be monic. then,

$$pR_K = \prod_{i=1}^{g} \mathfrak{p}_i{}^{e_i}$$

where $\mathfrak{p}_i = < p, T_i(\theta) >$. Furthermore, the inertia degree f_i is equal to the degree of T_i.

For a proof of the above theorem we refer to [8].

Corollary 1.4.2. *Let $K = \mathbb{Q}(\theta)$ be a number field and $f(x) = Irr(\theta, \mathbb{Q})$. Then, prime ideals $\mathfrak{p}$ of degree $f(\mathfrak{p}/p\mathbb{Z}) = 1$ not dividing the index $[R_K : \mathbb{Z}[\theta]]$ are in bijective correspondence with the pairs $(p, c \bmod p)$ where $f(c) \equiv 0 \pmod{p}$.*

Proof. Let $\mathfrak{p}$ be a prime ideal of degree $f(\mathfrak{p}/p\mathbb{Z}) = 1$. Then Theorem 1.4.1 implies that $\mathfrak{p} = < p, f_i(\theta) >$ where $\deg f_i = f(\mathfrak{p}/p\mathbb{Z}) = 1$ and f_i is monic. That follows $\mathfrak{p} = < p, \theta - c >$ where $f(c) \equiv 0 \pmod{p}$. So, we map $\mathfrak{p}$ to the pair $(p, c \bmod p)$ where $f(c) \equiv 0 \pmod{p}$.
Conversely, let $(p, c \bmod p)$ be a pair with $f(c) \equiv 0 \pmod{p}$. As $f(c) \equiv 0 \pmod{p}$ we get that $f(x) \equiv (x-c)g(x) \pmod{p}$ for some monic $g(x)$. Then Theorem 1.4.1 implies that the factor $x-c$ corresponds to the prime ideal $< p, \theta-c >$ in the factorization of pR_K. That finishes the proof. □

The next step is to compute all these pairs $(p, c \bmod p)$ for $p < B_2$ as $f(\mathfrak{p}/p\mathbb{Z}) = 1$ i.e. $N(\mathfrak{p}) = p$. We have already mentioned that we can assume we know all primes less than B_2 so we just have to find the roots of $f(x) \bmod p$ for all primes less than B_2. In order to do that we use the following algorithm.

Step 1) We set $g(x) = \gcd(f(x), x^p - x)$. If $g(0) \equiv 0 \pmod{p}$ we conclude that 0 is a root and we set $g(x) \leftarrow \dfrac{g(x)}{x}$.
If $\deg g = 0$ we terminate the algorithm.

Step 2) If $\deg g = 1$ and $g(x) = a_1 x + a_0$ then $-a_0 {a_1}^{-1} \pmod{p}$ is a root ,terminate.
If $\deg g = 2$ and $g(x) = a_2 x^2 + a_1 x + a_0$ we set $d = {a_1}^2 - 4a_0 a_2$ and we find an e such that $e^2 \equiv d \pmod{p}$. Then $(-a_1 \pm e)(2a_2)^{-1} \pmod{p}$ are roots, terminate.

Step 3) If $\deg g > 2$ we choose a random $a \in \mathbb{F}_p$ and if $g(a) \not\equiv 0 \pmod{p}$, we set $h_1(x) = \gcd(x^{\frac{p-1}{2}} - 1, g(x-a))$ and $h_2(x) = \dfrac{g(x-a)}{h_1(x)}$.
If $\deg h_1 = 0$ or $\deg h_1 = \deg g$ we choose another value for a and repeat step 3.

Step 4) We use recursively the above algorithm in order to factor $h_1(x)$, $h_2(x)$. If r is a root of $h_1(x)$ then $r - a$ is a root of $g(x)$.

As $x^p - x = \prod_{i=0}^{p-1} (x-i)$ in step 1 we actually isolate in $g(x)$ all linear factors of $f(x)$. Step 2 considers two special cases in which we have a formula for the roots and so we deal with them faster. In step 2 in the case where $\deg g = 2$ we took for granted that there will exist an e such that $e^2 \equiv d \pmod{p}$. That will actually be true, as $g(x) \mid x^p - x$ so it factors in linear factors. In step 3 we split the factors of $g(x)$ (in the first iteration) between h_1 and h_2 as,

$$g(x-a) \mid x^p - x = x(x^{p-1} - 1) = x(x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1).$$

Also in order step 3 to fail, so $\deg h_1 = 0$ or $\deg h_1 = \deg g$ all factors of $g(x-a)$ must divide $(x^{\frac{p-1}{2}} - 1)$ or $(x^{\frac{p-1}{2}} + 1)$ respectively. That means that there is only a chance of $\frac{1}{2^{\deg g - 1}}$ to fail. Furthermore as in each iteration step 3 will produce polynomials $h_1(x)$ and $h_2(x)$ with degree strictly less than the previous step the algorithm will terminate after a finite number of steps.

Now we are ready to compute,

$$\mathbf{G}_1 = \{\pi \in R_K : < \pi >= \mathfrak{p} \quad \forall\, \mathfrak{p} \in \mathbb{P}(K) \text{ such that } f(\mathfrak{p}/p\mathbb{Z}) = 1 \text{ and } N(\mathfrak{p}) \leq B_2\}$$

Let ω_d be the volume of the unit ball in $\mathbb{R}^d$. We set,

$$v_d = \left(\frac{4}{d}\right)^{d/2} \frac{1}{\omega_d} \quad , \quad C = \left(v_d \sqrt{|D_K|} B_2\right)^{2/d} \text{ and } M = [v_d \sqrt{|D_K|}]$$

The following algorithm attempts to find a generator for all prime ideals $\mathfrak{p}$ for which $f(\mathfrak{p}/p\mathbb{Z}) = 1$ and $M < N(\mathfrak{p}) \leq B_2$.

Step 1) Set $m(\mathfrak{p}) = M + 1$ for all $\mathfrak{p}$ we are interested in.
Step 2) For all $\gamma \in R_K$, $\gamma = \sum_{i=0}^{d-1} s_i \theta^i$ for which $\sum_{i=0}^{d-1} {s_i}^2 |\theta|^{2i} \leq C$ we do the following :
Step 3) Compute the norm $N(\gamma)$.
Step 4) If $N(\gamma) = kp$ for some p in the list of pairs $(p,\, c)$ and $|k| \leq M$ then :
1) Identify the prime ideal $\mathfrak{p}$ that corresponds to this p and $\mathfrak{p} \mid < \gamma >$. Equivalently we find the pair $(p,\, c)$ for which $\sum_{i=0}^{d-1} s_i c^i \equiv 0 \pmod{p}$ (see Lemma 1.5.3).
2) If $k < m(\mathfrak{p})$ then we set $m(\mathfrak{p}) \leftarrow |k|$ and $\pi_{\mathfrak{p}} \leftarrow \gamma$.

Remark 1.4.3. *At the end of the algorithm $m(\mathfrak{p}) < M$ $\forall \mathfrak{p}$ for which $f(\mathfrak{p}/p\mathbb{Z}) = 1$ and $M < N(\mathfrak{p}) \leq B_2$.*

Remark 1.4.4. *If $m(\mathfrak{p}) = 1$ then the above algorithm guarantees that $\mathfrak{p} \mid < \pi_{\mathfrak{p}} >$ and $< \pi_{\mathfrak{p}} >$ is a prime ideal so, $\mathfrak{p} = < \pi_{\mathfrak{p}} >$. Otherwise if $m(\mathfrak{p}) > 1$ then as $M < N(\mathfrak{p})$ it follows that $\mathfrak{p}$ appears only once in the factorization of $< \pi_{\mathfrak{p}} >$. So, we can deduce that $< \pi_{\mathfrak{p}} > = I\mathfrak{p}$ for some ideal I with $N(I) = m(\mathfrak{p}) \leq M$.*

Hence, the only thing left in order to finish the construction of $\mathbf{G}_1$ is computing generators for ideals I with norm $N(I) \leq M$. In practice these generators is very likely to be encountered during the above search, so when we find them we store them. Then for the ideals $\mathfrak{p}$ for which $m(\mathfrak{p}) > 1$ if for example we have $< \pi_{\mathfrak{p}} > = I\mathfrak{p}$ and $I =< \beta >$

we can deduce that $\mathfrak{p} =< \pi_{\mathfrak{p}}\beta^{-1} >$.
The next thing we have to compute is the set

$$\mathbf{G}_2 = \{\pi \in R_K :< \pi >= \mathfrak{p} \quad \forall\, \mathfrak{p} \mid fR_K\}$$

As we will see in the next section the primes dividing the index $f = [R_K : \mathbb{Z}[\theta]]$ and essentially causing some problems are smaller than the degree of the extension $K/\mathbb{Q}$ and so smaller than M. Consequently, we expect the above argument to apply in this case as well, which means that we expect to find the generators while the above algorithm is searching for the $\pi_{\mathfrak{p}}$.

Remark 1.4.5. *In case* $[R_K : \mathbb{Z}[\theta]] = 1$ *the set* $\boldsymbol{G}_2$ *is empty.*

The last set left to compute is

$$\mathbf{U} = \{\text{a generating set of the group of units of } R_K\}$$

The following theorem guarantees that the above set is finite.

Theorem 1.4.6 (Dirichlet Unit Theorem)**.** *The group* $E(R_K)$ *is the product of a finite cyclic group of roots of unity with a free abelian group of rank* $r + s - 1$*, where r is the number of real embeddings of K and s is the number of complex conjugate pairs of embeddings.*

Definition 1.4.7. *The units that generate the* $r + s - 1$ *copies of* $\mathbb{Z}$ *in* $E(R_K)$ *are called fundamental units.*

In general the task of finding a system of generators for $E(R_K)$ is considered to be very hard. For the needs of our algorithm we are going to make again the assumption that we will encounter these generators during the search of the prime elements $\pi_{\mathfrak{p}}$ as described above. However, we must be careful, by making this assumption we do not claim that in general the fundamental units will have "small" coefficients. In many cases advanced algorithms for computing such a system may exist in number theory applications like SAGE or PARI and can be used but their study is beyond the scope of this master thesis.

1.5 Sieving

In this section we are going to examine how the SNFS attempts to find pairs $(a,\, b)$ such that :
i) $\gcd(a,\, b) = 1$
ii) $|a+bm|$ is B_1-smooth except for at most one prime factor p_1 such that $B_1 < p_1 < B_3$
iii) $a + b\theta$ is B_2-smooth except for at most one prime p_2 such that $B_2 < p_2 < B_4$.

This prime will correspond to a prime ideal $\mathfrak{p}_2$ in the factorization of $< a + b\theta >$ with $N(\mathfrak{p}_2) = p_2$.

In order to do that, we first find pairs $(a,\ b)$ such that (ii) and (iii) hold. Finally from the remaining pairs we will choose those that satisfy (i) as well.

In both cases (ii) and (iii) we have two free variables $a,\ b$ so we will use two nested loops in order to check all combinations. That leads us to the following algorithm :

For each b with $1 \leq b < U_2$ we initialize two "sieve arrays" A_1 and A_2 as follows. For each a with $-U_1 \leq a \leq U_1$ we set the a^{th} position of A_1 to contain the number $a + bm$ and the a^{th} position of A_2 to contain the number $N(a + b\theta)$. Then we examine the smoothness of the elements of the two arrays separately. For the array A_1 we have to check if each of the $a + bm$ is B_1-smooth. In order to do that, for each prime $p \in \mathbf{P}$ we do the following. For each position a that satisfies $a \equiv -bm \pmod{p}$ we divide the prime p out of the element stored in that position as many times as possible. After this is done for all primes $p \in \mathbf{P}$ the elements of the array that are equal to ± 1 represent values of a such that $a + bm$ is B_1-smooth so, they could lead to full relations (if additionally $N(a + b\theta)$ is B_2-smooth). The elements of the array that are less than B_3 represent potential partial relations. So in order to decide which are the pairs we are going to keep we have to check the smoothness of the elements of A_2. For this we are going to use a technique similar to the one used for A_1.

Remark 1.5.1. *Let $p \in \mathbf{P}$, then while we are sieving we divide elements of the array A_1 by p only when it is guaranteed that the corresponding element is divisible by p. This greatly improves the algorithm as no unnecessary divisions are performed.*

Proposition 1.5.2. *If $a,\ b \in \mathbb{Z}$ with $\gcd(a,\ b) = 1$ then every prime ideal $\mathfrak{p}$ that divides $< a + b\theta >$ either divides the index $f = [R_K : \mathbb{Z}[\theta]]$, or $f(\mathfrak{p}/p\mathbb{Z}) = 1$.*

Proof. With p we denote the prime number below $\mathfrak{p}$. Then $p \nmid b$ as if $p \mid b$ then $b\theta \in \mathfrak{p}$. But we also have that $a + b\theta \in \mathfrak{p}$ so $a \in \mathfrak{p}$ which then follows that $a \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z} \Rightarrow p \mid a \Rightarrow p \mid \gcd(a,\ b) = 1$, contradiction. Let, $p \nmid f$ so $\mathfrak{p} \nmid < f >$. Hence, at this point we have that

$$\gcd(p,\ b) = 1 \Rightarrow \exists c \in \mathbb{Z} \text{ such that } bc \equiv 1 \pmod{p}$$
$$\gcd(p,\ f) = 1 \Rightarrow \exists u \in \mathbb{Z} \text{ such that } fu \equiv 1 \pmod{p}$$

As $\mathfrak{p} \mid < a + b\theta > \Rightarrow a + b\theta \equiv 0 \pmod{\mathfrak{p}} \Rightarrow \theta \equiv -ac \pmod{\mathfrak{p}}$
because $bc = 1 + kp \Rightarrow bc \in 1 + \mathfrak{p} \Rightarrow bc \equiv 1 \pmod{\mathfrak{p}}$
Let $x \in R_K$ then $fx \in \mathbb{Z}[\theta]$ as $|R_K/\mathbb{Z}[\theta]| = f$ which gives us that $f(x + \mathbb{Z}[\theta]) = \mathbb{Z}[\theta] \Rightarrow fx + \mathbb{Z}[\theta] = \mathbb{Z}[\theta] \Rightarrow fx \in \mathbb{Z}[\theta]$. Hence there exists a polynomial $g(X) \in \mathbb{Z}[X]$ such that $fx = g(\theta)$. This leads to the following,

$$fx \equiv g(-ac) \pmod{\mathfrak{p}} \Rightarrow x \equiv ug(-ac) \pmod{\mathfrak{p}}.$$

So, we can conclude that every $x \in R_K$ is equivalent to an integer $(\mathrm{mod}\ \mathfrak{p})$. This follows that the ring homomorphism

$$\begin{aligned} \psi : \mathbb{Z} &\to R_K/\mathfrak{p} \\ a &\mapsto a \pmod{\mathfrak{p}} \end{aligned}$$

is surjective. Moreover $\ker(\psi) = \{a \in \mathbb{Z} : a \in \mathfrak{p}\} = \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Hence by the first isomorphism theorem we get that $\mathbb{Z}/p\mathbb{Z} \cong R_K/\mathfrak{p} \quad \Rightarrow f(\mathfrak{p}/p\mathbb{Z}) = 1$. □

The above proposition justifies our choice for the set **G** in the factor base. The reason is the following, as we work in a Dedekind domain by Theorem 1.1.11 we get unique factorization of ideals so, for every pair $(a,\ b)$ we will have that

$$< a + b\theta >= \mathfrak{p}_1{}^{e_1}\mathfrak{p}_2{}^{e_2} \cdots \mathfrak{p}_k{}^{e_k}$$

and for each $\mathfrak{p}_i$ it will hold that either $\mathfrak{p}_i \mid< f >$, or $f(\mathfrak{p}_i/p\mathbb{Z}) = 1$ as we just saw. But when we sieve we want $N(a+b\theta)$ to be B_2-smooth (except to at most one prime factor). We are now going to make the connection between the factorization of $N(a + b\theta)$, $< a + b\theta >$ and $a + b\theta$. Let $\gamma, \delta \in R_K$ the connection follows by,

$$\begin{aligned} &|N(\gamma)| = N(< \gamma >) \quad \text{and} \\ &< \gamma > \ = < \delta > \quad \Rightarrow \ \gamma = \varepsilon\delta \quad \text{where } \varepsilon \text{ is a unit.} \end{aligned}$$

By the first relation we get that,

$$\begin{aligned} |N(a + b\theta)| &= N(< a + b\theta >) \\ &= N(\mathfrak{p}_1{}^{e_1}\mathfrak{p}_2{}^{e_2} \ldots \mathfrak{p}_k{}^{e_k}) \\ &= N(\mathfrak{p}_1)^{e_1} N(\mathfrak{p}_2)^{e_2} \ldots N(\mathfrak{p}_k{}^{e_k}) \\ &= (p_1{}^{f_1})^{e_1} (p_2{}^{f_2})^{e_2} \ldots (p_k{}^{f_k})^{e_k} \end{aligned} \tag{1.3}$$

where $f_i = 1$ if $\mathfrak{p}_i \nmid< f >$.
This leads us to the following conclusion. The prime factors of $N(a + b\theta)$ correspond to prime ideals in the factorization of $< a + b\theta >$. Hence if the norm $N(a + b\theta)$ is B_2-smooth it then follows that $< a + b\theta >$ is a product of prime principal ideals generated by elements of **G**.
Finally, if we have computed the factorization of $< a + b\theta >$ as

$$< a + b\theta >= \prod_{\pi \in \mathbf{G}} < \pi >^{e(\pi)}$$

we then get that

$$\begin{aligned} a + b\theta &= \varepsilon \prod_{\pi \in \mathbf{G}} \pi^{e(\pi)} \\ &= \prod_{u \in \mathbf{U}} u^{e(u)} \prod_{\pi \in \mathbf{G}} \pi^{e(\pi)} \end{aligned}$$

In the case of $a + bm$ we saw how we could accomplish the sieving in the array A_1 and by the same way find the factorization of these elements. In the rest of this section we study how we do the sieving in the array A_1 and how we get the factorization of the elements $a + b\theta$.

Lemma 1.5.3. *Let $\mathfrak{p}$ be a prime ideal with degree $f(\mathfrak{p}/p\mathbb{Z}) = 1$ not dividing the index $[R_K : \mathbb{Z}[\theta]]$ that corresponds to the pair (p, c) and $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$. Then $\mathfrak{p} \mid < a + b\theta >$ if and only if $a + bc \equiv 0 \pmod{p}$.*

Proof. By the proof of Proposition 1.5.2 we get that if $y \in R_K$ and $f = [R_K : \mathbb{Z}[\theta]]$ then there is a polynomial $g(x)$ such that $y = \frac{1}{f}g(\theta)$. As $f(\mathfrak{p}/p\mathbb{Z}) = 1$ and $\gcd(p, f) = 1$ we can see that

$$\begin{aligned} \phi &: R_K/\mathfrak{p} \to \mathbb{Z}/p\mathbb{Z} \\ \frac{1}{f}\sum_{i=0}^{d-1} a_i\theta^i + \mathfrak{p} &\mapsto f^{-1}\sum_{i=0}^{d-1} a_i c^i + p\mathbb{Z} \end{aligned}$$

is a ring isomorphism. Therefore $a + b\theta \in \mathfrak{p}$ if and only if $a + bc \equiv 0 \pmod{p}$ which implies that $\mathfrak{p} \mid < a + b\theta >$ if and only if $a + bc \equiv 0 \pmod{p}$. □

Remark 1.5.4. *If we forget the contribution of the ideals that divide the index we can see why we chose to work with elements of the form $a + b\theta$. The first reason is that in the factorization of $< a + b\theta >$ appear prime ideals of special form which are easily stored in the computer by their representation as pairs (p, c). The second reason is that by the above lemma we get a very easy condition of when such a prime ideal divides $< a + b\theta >$.*

Remark 1.5.5. *Each prime p dividing the $N(a + b\theta)$ and not dividing the index $[R_K : \mathbb{Z}[\theta]]$ corresponds to exactly one prime ideal $\mathfrak{p}$ that divides $< a + b\theta >$. Assume that there were two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ dividing $< a + b\theta >$ that corresponded to the pairs (p, c_1) and (p, c_2) respectively. Then we would have,*

$$\begin{aligned} a + bc_1 &\equiv 0 \pmod{p} \quad \textit{and} \\ a + bc_2 &\equiv 0 \pmod{p} \end{aligned}$$

Additionally $p \nmid b$ as if $p \mid b$ then $a \equiv 0 \pmod{p}$ and therefore $p \mid \gcd(a, b) = 1$, contradiction. Hence from the above two congruences follows then $c_1 \equiv c_2 \pmod{p}$. But the prime ideals of degree 1 are in bijective correspondence with the pairs (p, c) and so $\mathfrak{p}_1 = \mathfrak{p}_2$.

We now return to the array A_2. Initially in each position of A_2 we store $N(a+b\theta)$

$$\begin{aligned} N(a+b\theta) &= \sigma_1(a+b\theta)\sigma_2(a+b\theta)\dots\sigma_d(a+b\theta) \\ &= (a+b\theta^{(1)})(a+b\theta^{(2)})\dots(a+b\theta^{(d)}) \\ &= b^d(\frac{a}{b}+\theta^{(1)})(\frac{a}{b}+\theta^{(2)})\dots(\frac{a}{b}+\theta^{(d)}) \\ &= (-b)^d(-\frac{a}{b}-\theta^{(1)})(-\frac{a}{b}-\theta^{(2)})\dots(-\frac{a}{b}-\theta^{(d)}) \\ &= (-b)^d f(-\frac{a}{b}) \\ &= (-b)^d\left[\left(-\frac{a}{b}\right)^d - t\right] = a^d - t(-b)^d \end{aligned}$$

so given $a,\ b$ we can easily compute the $N(a+b\theta)$. As we saw prime factors of $N(a+b\theta)$ correspond to prime ideals that divide $< a+b\theta >$. We will separate the sieving in two steps. The first step concerns the prime ideals that do not divide the index. For those ideals we proceed as follows. For each pair $(p,\ c)$ we retrieve the elements of A_2 that are in positions a such that $a \equiv -bc \pmod{p}$. We then divide them by the highest power of p that they are divisible and store in the array the quotient.
In case the index $[R_K : \mathbb{Z}[\theta]] = 1$ then we are done. Otherwise we have one more step. In this case as we have assumed that we found R_K, an integral basis is known. Then using the relation $D_K(\theta) = [R_K : \mathbb{Z}[\theta]]^2 D_{K/\mathbb{Q}}$ we can find $[R_K : \mathbb{Z}[\theta]]$. As we will see later we do not expect its prime divisors to be very large so we can factor it. Then for all the elements of A_2 we check whether they are divisible by any of these primes. If any element is divisible by any such prime we divide it out and keep the quotient.

Even though at this point we are done with the sieving, we also wish to know the factorization of the smooth elements $a+bm$ and $a+b\theta$ that we found. For the $a+bm$ the sieving technique used previously can give us the factorization as well. However for the $a+b\theta$ the situation is different. Initially we will try to find the factorization of $< a+b\theta >$. Let

$$< a+b\theta > = \mathfrak{p}_1{}^{e_1}\mathfrak{p}_2{}^{e_2}\dots\mathfrak{p}_k{}^{e_k}$$

so we wish to find the ramification index e_i. Let $\mathfrak{p}$ be a prime ideal with $f(\mathfrak{p}/p\mathbb{Z}) = 1$ that corresponds to the pair $(p,\ c)$ and $p \mid N(a+b\theta)$. Then the exponent of $\mathfrak{p}$ in the factorization of $< a+b\theta >$ will be equal to the exponent of p in the factorization of $N(a+b\theta)$ by equation 1.3 and remark 1.5.5. Therefore, if we exclude the one ideal (if it exists) that exceeds our smoothness bound, it is only the exponents of the prime ideals that divide the index left to be computed.

First of all, for these primes we would like to have a theorem like 1.4.1. Let $K = \mathbb{Q}(\theta)$. One idea would be to try to find another $\theta' \in R_K$ such that $K = \mathbb{Q}(\theta')$ and hope

that $p \nmid [R_K : \mathbb{Z}[\theta']]$. If that is the case, then we can apply Theorem 1.4.1. However there are cases of primes p where for every $\theta \in R_K$ it holds that $p \mid [R_K : \mathbb{Z}[\theta]]$. Let $D(\theta) = m(\theta)^2 D_{K/\mathbb{Q}}$, where $m(\theta) = [R_K : \mathbb{Z}[\theta]]$. We set $m_K = \gcd\{m(\theta) \mid \theta \in R_K, K = \mathbb{Q}(\theta)\}$.

Definition 1.5.6. *If $m_K > 1$ then every prime $p \mid m_K$ is called an essential discriminant divisor.*

Hensel's criterion.
i) If $p \mid m_K$, then $p < d$ where $d = [K : \mathbb{Q}]$
ii) If pR_K factors completely in K, then $p \mid m_K \Leftrightarrow p < d$

The decomposition law of these primes is very hard and we are not going to study it here. In order to find the exponent of these ideals in the factorization of an ideal $I =< a + b\theta >$ we will compute the $\mathfrak{p}-$adic valuation of I.

By [8, p. 188] for a $\mathfrak{p} \mid< f >$ we can get a basis of the form

$$\mathfrak{p} = < p, -c + y\theta, \gamma_2, \dots, \gamma_{d-1} >$$

where $c, y \in \mathbb{Z}$, $y \mid p$ and $y \mid c$ and γ_i polynomials of degree i in θ (not necessarily with integer coefficients).
Having this in mind

$$\begin{aligned} a + b\theta \in \mathfrak{p} &\Leftrightarrow a + b\theta = kp + l(-c + y\theta) \\ &\Leftrightarrow a = kp - lc \quad \text{and} \quad b = yl \\ &\Leftrightarrow y \mid b \quad \text{and} \quad a \equiv -\frac{b}{y}c \pmod{p} \end{aligned}$$

We have that $y \mid p$ but, if $y = p$ then $p \mid b$ and $p \mid c$ so $p \mid a$, contradiction. Hence, y=1 so finally $a + b\theta \in \mathfrak{p} \Leftrightarrow a + bc \equiv 0 \pmod{p}$. Also, $\theta - c \in \mathfrak{p} \Rightarrow c \equiv \theta \pmod{\mathfrak{p}} \Rightarrow f(c) \equiv f(\theta) \pmod{\mathfrak{p}} \Rightarrow f(c) \equiv 0 \pmod{\mathfrak{p}}$. Therefore the condition is the same as in the case where $\mathfrak{p} \nmid< f >$. However in this case the pairs (p, c) are not in bijective correspondence with the ideals $\mathfrak{p} \mid< f >$. In order to deal with these ideals we will use a different approach.

Definition 1.5.7. *Let K be a number field and $R \subseteq K$. The set R is called an order of K when the following two conditions hold :*
i) $R = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z} \oplus \dots \oplus \omega_d\mathbb{Z}$ where $d = [K : \mathbb{Q}]$ and $\omega_i \in R_K$.
ii) R is a subring of K with $1 \in K$.

An order $R \subset R_K$ fails to be a Dedekind domain only because it is not integrally closed. So it is noetherian and every prime ideal of R is maximal.

Proposition 1.5.8. *Let R be an order of K. Then every non-zero integral ideal I of R contains a finite product of prime ideals.*

Proof. Let $\mathcal{A} = \{I \text{ ideal of } R,\ I \neq < 0 >, R \text{ for which the proposition does not hold}\}$ and assume that $\mathcal{A} \neq \emptyset$. As R is noetherian, $\mathcal{A}$ has a maximal elements. Let, M_0 be a maximal element of $\mathcal{A}$. Then M_0 is not a prime ideal of R, because if it was then we would have $P = M_0$ and therefore $P \subseteq M_0$. Hence, there are $a,\ b \notin M_0$ such that $ab \in M_0$ and we set $A = M_0 + aR$ and $B = M_0 + bR$. As $ab \in M_0$ it then follows that $AB \subset M_0$ and $A \neq R$, $B \neq R$. This is true as if $A = R$ for example, then by $AB \subset M_0$ we would get that $B \subset M_0$. The last relation would then imply that $b \in M_0$, contradiction. Additionally, we have that $M_0 \subsetneqq A$ and $M_0 \subsetneqq B$ as $a \notin M_0$ and $b \notin M_0$. But, M_0 is a maximal element of $\mathcal{A}$ which then implies that for A and B the proposition holds. If we combine this with $AB \subset M_0$ it then follows that the proposition holds for M_0 as well, contradiction. So $\mathcal{A} = \emptyset$. □

Proposition 1.5.9. *Let R be an order of K and $\mathfrak{p}$ a prime ideal of R. Then there exists an $a \in K \backslash R$ such that $a\mathfrak{p} \subset R$. Furthermore $\mathfrak{p}$ is invertible in R if and only if $a\mathfrak{p} \not\subset \mathfrak{p}$ and $\mathfrak{p}^{-1} = R + aR$.*

Proof. Let $x \in \mathfrak{p}$, $x \neq 0$ so $xR \neq < 0 >$ so by the previous proposition there are prime ideals $\mathfrak{q}_i$ such that $\prod_{i \in E} \mathfrak{q}_i \subset xR$ for some finite set E. We choose E to be minimal in the sense that there is not a proper subset E' of E such that $\prod_{i \in E'} \mathfrak{q}_i \subset xR$. Furthermore, we have that $\prod_{i \in E} \mathfrak{q}_i \subset xR \subset \mathfrak{p}$ so $\exists j \in E$ such that $\mathfrak{q}_j \subset \mathfrak{p}$. Let $\mathfrak{q} = \prod_{i \in E i \neq j} \mathfrak{q}_i$ and so $\mathfrak{p}\mathfrak{q} \subset xR$ and $\mathfrak{q} \nsubseteq xR$ as we have chosen E to be minimal. We choose a $y \in \mathfrak{q}$ such that $y \notin xR$. Hence, $y \notin xR$ and $y\mathfrak{p} \subset \prod_{i \in E} \mathfrak{q}_i \subset xR$, so we set $a = \dfrac{y}{x}$.

$y \notin xR \Rightarrow \dfrac{y}{x} \notin R \Rightarrow a \notin R$ and

$a\mathfrak{p} = x^{-1}y\mathfrak{p} \subset x^{-1}xR = R$

Let $P = \mathfrak{p} + a\mathfrak{p}$, then $\mathfrak{p} \subseteq P \subseteq R$ but $\mathfrak{p}$ is prime so it is also maximal, which leaves two options.

i) If $P = R$ then $a\mathfrak{p} \not\subset \mathfrak{p}$ and $(R + aR)\mathfrak{p} = \mathfrak{p} + a\mathfrak{p} = R \ \Rightarrow\ \mathfrak{p}^{-1} = R + aR$.

ii) If $P = \mathfrak{p}$ then $a\mathfrak{p} \subset \mathfrak{p}$ and $(R + aR)\mathfrak{p} = \mathfrak{p}R$. If $\mathfrak{p}$ was invertible then $R + aR = R \ \Rightarrow a \in R$, contradiction. □

Lemma 1.5.10. *Let I be an integral ideal of R_K and $\mathfrak{p}$ be a prime ideal. Then $\mathfrak{p} \mid I$ if and only if $aI \subset R_K$ where a is the one given by the previous proposition for $\mathfrak{p}$. Moreover, the $\mathfrak{p}-$adic valuation of I $v_{\mathfrak{p}}(I)$, is equal to greatest integer v such that $a^v I \subset R_K$*

Proof. Let $\mathfrak{p} \mid I \ \Rightarrow\ I \subset \mathfrak{p} \Rightarrow aI \subset a\mathfrak{p} \subset R_K$.

Conversely, let $aI \subset R_K$, this implies that $a\mathfrak{p}I \subset \mathfrak{p} \ \Rightarrow\ \mathfrak{p} \mid a\mathfrak{p}I \ \Rightarrow \mathfrak{p} \mid a\mathfrak{p}$ or

$\mathfrak{p} \mid I$. But in R_K all ideals are invertible, hence by the previous proposition we get that $a\mathfrak{p} \not\subset \mathfrak{p} \Rightarrow \mathfrak{p} \nmid a\mathfrak{p}$ and so $\mathfrak{p} \mid I$. Let $I = \mathfrak{p}^k J$ where $\mathfrak{p} \nmid J$.
If $\upsilon \leq k : a^\upsilon I = a^\upsilon \mathfrak{p}^k J = (a\mathfrak{p})^\upsilon \mathfrak{p}^{k-\upsilon} J \subset R_K$
If $\upsilon = k+1$: Let $a^{k+1} I \subset R_K \Rightarrow a^{k+1}\mathfrak{p}^{k+1} I \subset \mathfrak{p}^{k+1}$. This implies that either $\mathfrak{p} \mid (a\mathfrak{p})^{k+1}$ or $\mathfrak{p} \mid I$. If $\mathfrak{p} \mid (a\mathfrak{p})^{k+1}$ then $\mathfrak{p} \mid a\mathfrak{p}$, contradiction so $\mathfrak{p} \nmid (a\mathfrak{p})^{k+1}$. Therefore $\mathfrak{p}$ must divide I. So, at this point we have that $\mathfrak{p} \mid I$ and $\mathfrak{p} \nmid (a\mathfrak{p})^{k+1}$. If we combine these with the fact that $\mathfrak{p}^{k+1} \mid (a\mathfrak{p})^{k+1} I$ we get that $\mathfrak{p}^{k+1} \mid I$, contradiction. Therefore $a^{k+1} I \not\subset R_K$. That finishes the proof □

As the previous lemma suggests, our next goal is to compute the $a \in K \backslash R_K$ of Proposition 1.5.9 for every prime ideal $\mathfrak{p}$ we are interested in computing $\upsilon_\mathfrak{p}(I)$. For a we have that $a\mathfrak{p} \subset R_K$ so $ap \in R_K$ which follows that there exists a $\beta \in R_K$ such that $a = \dfrac{\beta}{p}$ where p is the prime below $\mathfrak{p}$. For a it holds that $a \in K \backslash R_K$ and $a\mathfrak{p} \subset R_K$ so for β the following should hold :

$$\beta \in R_K \backslash pR_K \quad \text{and} \quad \beta\mathfrak{p} \subset pR_K$$

Let $\omega_1, \omega_2, \dots, \omega_d$ be an integral basis of R_K and $\mathfrak{p} = <\gamma>$. Let $\beta = \sum_{i=1}^{d} x_i\omega_i$, $x_i \in \mathbb{Z}$. So it is sufficient to find $x_i \in \mathbb{Z}$ such that they are not all divisible by p and $\beta\gamma \in pR_K$.
$\beta\gamma \in pR_K \Rightarrow \sum_{i=1}^{d} x_i\omega_i\gamma \in pR_K$. Let $\omega_i\gamma = \sum_{k=1}^{d} a_{ik}\omega_k$, then we will have

$$\sum_{i=1}^{d} x_i \sum_{k=1}^{d} a_{ik}\omega_k \in pR_K \Rightarrow \sum_{i=1}^{d}\sum_{k=1}^{d} x_i a_{ik}\omega_k \in pR_K \Rightarrow \sum_{k=1}^{d}\Big(\sum_{i=1}^{d} x_i a_{ik}\Big)\omega_k \in pR_K \Rightarrow$$

$$\sum_{i=1}^{d} x_i a_{ik} \equiv 0 \pmod{p} \quad \text{for} \quad k = 1, \dots, d$$

We solve the $d \times d$ linear system and we find the x_i and therefore β and finally a. Let's assume that we have $I = <\gamma_1>$, $\mathfrak{p} = <\gamma_2>$ with $\mathfrak{p} \mid < f >$ and $I = \mathfrak{p}^k J$ and $\mathfrak{p} \nmid J$. Then k will be the greatest integer such that such that $a^k I \subset R_K \Leftrightarrow a^k < \gamma_1 > \subset R_K \Leftrightarrow < a^k\gamma_1 > \subset R_K \Leftrightarrow a^k\gamma_1 \in R_K$.

Even though the irreducible polynomial of the following example is not of the form we examine in this chapter it will illustrate how we are going to use in practise the above method.

Example 1.5.11. *Let $f(x) = x^3 - x^2 - 2x - 8$ and θ be a root of $f(x)$. We set $K = \mathbb{Q}(\theta)$ for which it holds that $h_K = 1$, $[R_K : \mathbb{Z}[\theta]] = 2$ and in particular $R_K = \mathbb{Z} \oplus \theta\mathbb{Z} \oplus \frac{\theta+\theta^2}{2}\mathbb{Z}$. Find the decomposition in prime ideals of the ideal $I = < 2 + \theta >$.*

The first step is to compute the norm of I. $N(I) = |N(2+\theta)| = 16 = 2^4$ *so in the decomposition of* I *we will have only prime ideals* $\mathfrak{p}$ *such that* $\mathfrak{p} \mid < 2 >$ *and as* $f = 2$ *we have that* $\mathfrak{p} \mid < f >$. *At this point we need the decomposition in prime ideals of* $2R_K$. *In this case* 2 *is an essential discriminant divisor. As we have already mentioned the decomposition of primes dividing the index is very hard and we are not going to study it in this master thesis. However, in [8, p. 351] we can find some results that will lead us to the the following conclusion,*

$$2R_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$$

and $\mathfrak{p}_1 = < \gamma_1 >$, $\mathfrak{p}_2 = < \gamma_2 >$, $\mathfrak{p}_3 = < \gamma_3 >$ *where* $\gamma_1 = \frac{1}{2}\theta^2 + \frac{1}{2}\theta + 1$, $\gamma_2 = \theta^2 + 2\theta + 3$, $\gamma_3 = \frac{3}{2}\theta^2 + \frac{5}{2}\theta + 4$. *The next step is to compute the values* a_i *that corresponds to each* $\mathfrak{p}_i$.
For $\mathfrak{p}_1$ *we have :*
$1\cdot\gamma_1 = 1 + 1\cdot\frac{\theta+\theta^2}{2}$, $\theta\cdot\gamma_1 = 4 + 1\cdot\theta + 2\cdot\frac{\theta+\theta^2}{2}$, $\frac{\theta+\theta^2}{2}\cdot\gamma_1 = 6 + 2\theta + 4\cdot\frac{\theta+\theta^2}{2}$
So, we have to solve the following system in $\mathbb{F}_2$ *:*

$$\begin{pmatrix} 1 & 4 & 6 \\ 0 & 1 & 2 \\ 1 & 2 & 4 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

a solution is $x_1 = x_2 = 0$ *and* $x_3 = 1$ *hence* $a_1 = \frac{1}{2}\frac{\theta+\theta^2}{2} = \frac{\theta+\theta^2}{4}$.
For $\mathfrak{p}_2$ *we have :*
$1\cdot\gamma_2 = 3 + 1\cdot\theta + 2\cdot\frac{\theta+\theta^2}{2}$, $\theta\cdot\gamma_2 = 8 + 2\cdot\theta + 6\cdot\frac{\theta+\theta^2}{2}$, $\frac{\theta+\theta^2}{2}\cdot\gamma_2 = 16 + 4\theta + 11\cdot\frac{\theta+\theta^2}{2}$
So, we have to solve the following system in $\mathbb{F}_2$ *:*

$$\begin{pmatrix} 3 & 8 & 16 \\ 1 & 2 & 4 \\ 2 & 6 & 11 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

a solution is $x_1 = x_3 = 0$ *and* $x_2 = 1$ *hence* $a_2 = \frac{1}{2}\theta$.
For $\mathfrak{p}_3$ *we have :*
$1\cdot\gamma_3 = 4 + 1\cdot\theta + 3\cdot\frac{\theta+\theta^2}{2}$, $\theta\cdot\gamma_3 = 12 + 3\cdot\theta + 8\cdot\frac{\theta+\theta^2}{2}$, $\frac{\theta+\theta^2}{2}\cdot\gamma_3 = 22 + 6\theta + 15\cdot\frac{\theta+\theta^2}{2}$
So, we have to solve the following system in $\mathbb{F}_2$ *:*

$$\begin{pmatrix} 4 & 12 & 22 \\ 1 & 3 & 6 \\ 3 & 8 & 15 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

a solution is $x_1 = x_2 = x_3 = 1$ *hence* $a_3 = \frac{1}{2}(1 + \theta + \frac{\theta+\theta^2}{2}) = \frac{2+3\theta+\theta^2}{4}$.
So in order to compute the factorization of I *we need to compute* $\upsilon_{\mathfrak{p}_i}(I)$. *But as we saw*

this is equivalent to computing the greatest integer k_i such that ${a_i}^{k_i}(2+\theta) \in R_K$.
For $\mathfrak{p}_1$:
$a_1(2+\theta) = 2 + 2\frac{\theta+\theta^2}{2} \in R_K$
$a_1^2(2+\theta) = 6 + 2\theta + 4\frac{\theta+\theta^2}{2} \in R_K$
$a_1^3(2+\theta) = 16 + 4\theta + 11\frac{\theta+\theta^2}{2} \in R_K$
$a_1^4(2+\theta) = 41 + \frac{101}{4}\theta + \frac{57}{4}\theta^2 \notin R_K \Rightarrow \mathfrak{p}_1^3 \| I$
For $\mathfrak{p}_2$:
$a_2(2+\theta) = \theta + \frac{\theta^2}{2} \notin R_K \Rightarrow \mathfrak{p}_2 \nmid I$
For $\mathfrak{p}_3$:
$a_3(2+\theta) = 3 + \theta + 3\frac{\theta+\theta^2}{2} \in R_K$
$a_3^2(2+\theta) = \frac{37}{2} + \frac{43}{4}\theta + \frac{25}{4}\frac{\theta+\theta^2}{2} \notin R_K \Rightarrow \mathfrak{p}_3 \| I$
Therefore, $I = \mathfrak{p}_1^3\mathfrak{p}_3$

Remark 1.5.12. *Even though $I = \mathfrak{p}_1^3\mathfrak{p}_3$ we have that $2+\theta \neq (\frac{1}{2}\theta^2 + \frac{1}{2}\theta + 1)^3(\frac{3}{2}\theta^2 + \frac{5}{2}\theta + 4)$. The reason is that we have not taken into account the contribution of units in the factorization of $2+\theta$.*

Finding the unit contribution will be our next step. At this point, we need to make clear for which elements we are going to find the unit contribution. We are going to do this for full relations (i.e. $a + b\theta$ is B_2-smooth), free relations and cycles but not for partial relations. In the cycles construction step, where we try to construct cycles by combining partial relations only the factorization of the corresponding ideals is necessary, not the factorization of the elements.
We are going to study the problem for the case of a full relation, the other two cases are treated in the same way.

Let $I = < a + b\theta >$ be an ideal with $\gcd(a, b) = 1$ and $a + b\theta$ to be B_2-smooth. Then we know that $I = \prod \mathfrak{p}^{e(\mathfrak{p})}$ with $N(\mathfrak{p}) < B_2$ and $f(\mathfrak{p}/p\mathbb{Z}) = 1$ or $\mathfrak{p} \mid < f >$ and we have seen how to compute such a decomposition. Additionally for every such $\mathfrak{p}$ we have found an element $\pi \in R_K$ such that $\mathfrak{p} = < \pi >$. Hence, we can obtain a factorization like the following :

$$a + b\theta = \prod_{u \in \mathbf{U}} u^{e(u)} \prod_{\pi \in \mathbf{G}} \pi^{e(\pi)}$$

where we already know the $e(\pi)$ and we are left to find the $e(u)$. We have that U is a generating set of $E(R_K)$. By Theorem 1.4.6 we have that $U = \{u_0, u_1, \dots, u_r\}$ where $r = s + t - 1$ and u_0 is a root of unity and $u_1, \dots, u_r$ are fundamental units. We choose r embeddings $\sigma_1, \dots, \sigma_r$ of K in $\mathbb{C}$ such that there are no two conjugate complex embeddings. We then define the map :

$$\begin{aligned} l \; : \; K^* &\to \mathbb{R}^r \\ x &\mapsto (log|\sigma_1(x)|, \dots, log|\sigma_s(x)|, log|\sigma_{s+1}(x)|^2, \dots, log|\sigma_r(x)|^2) \end{aligned}$$

where $\sigma_1, \dots, \sigma_s$ are real embeddings and $\sigma_{s+1}, \dots, \sigma_r$ are complex embeddings. By the Dirichlet unit theorem we know that the image of $E(R_K)$ under l is a lattice of dimension r in $\mathbb{R}^r$. We define W to be the $r \times r$ matrix whose columns are the $l(u_i)$ for $i = 1, \dots, r$. The columns of W form a base of the previous lattice. Indeed, let $\varepsilon \in E(R_K)$ then $\varepsilon = {u_0}^{e_0} {u_1}^{e_1} \dots {u_r}^{e_r} \Rightarrow$

$$
\begin{aligned}
l(\varepsilon) &= l({u_0}^{e_0} {u_1}^{e_1} \dots {u_r}^{e_r}) \\
&= (log|\sigma_1({u_0}^{e_0} {u_1}^{e_1} \dots {u_r}^{e_r})|, \dots, log|\sigma_r({u_0}^{e_0} {u_1}^{e_1} \dots {u_r}^{e_r})|^2) \\
&= (log|\prod_{j=0}^{r} \sigma_1({u_j}^{e_j})|, \dots, log|\prod_{j=0}^{r} \sigma_r({u_j}^{e_j})|^{\,2}) \\
&= (\sum_{j=0}^{r} log|\sigma_1({u_j}^{e_j})|, \dots, \sum_{j=0}^{r} log|\sigma_r({u_j}^{e_j})|^2) \\
&= (\sum_{j=0}^{r} e_j log|\sigma_1(u_j)|, \dots, \sum_{j=0}^{r} e_j log|\sigma_r(u_j)|^2) \\
&= (\sum_{j=1}^{r} e_j log|\sigma_1(u_j)|, \dots, \sum_{j=1}^{r} e_j log|\sigma_r(u_j)|^2) \\
&= W \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix}
\end{aligned}
$$

as $log|\sigma_i(u_0)| = 0$ for $i = 1, \dots, r$ ($u_0 \in \ker l$). So the $l(u_i)$ span the lattice and they actually form a basis as they are as many as the dimension of the lattice. Therefore, let $a + b\theta = \prod_{i=0}^{r} {u_i}^{e(u_i)} \prod_{\pi \in \mathbf{G}} \pi^{e(\pi)}$ and we want to find the $e(u_i)$. We set $\upsilon = (a + b\theta) \prod_{\pi \in \mathbf{G}} \pi^{-e(\pi)}$ which is a unit so $l(\upsilon)$ is in the lattice spanned by the $l(u_i)$ and particularly

$$
l(\upsilon) = W \begin{pmatrix} e(u_1) \\ \vdots \\ e(u_r) \end{pmatrix}
$$

so

$$
\begin{pmatrix} e(u_1) \\ \vdots \\ e(u_r) \end{pmatrix} = W^{-1} l(\upsilon)
$$

We know W so we have to find $l(v)$ in order to be able to compute the $e(u_i)$. But

$$\begin{aligned} l(v) &= l((a+b\theta)\prod_{\pi\in\mathbf{G}}\pi^{-e(\pi)}) \\ &= l(a+b\theta)+l(\prod_{\pi\in\mathbf{G}}\pi^{-e(\pi)}) \\ &= l(a+b\theta)-\sum_{\pi\in\mathbf{G}}e(\pi)l(\pi) \end{aligned}$$

Therefore we have found the $e(u_i)$ for $i=1,\dots,r$ and $e(u_0)$ is left. But u_0 is a root of unity and in practice we use extensions $K/\mathbb{Q}$ with $[K:\mathbb{Q}]\leq 6$. This implies that if u_0 is an $n-$root of unity then $\phi(n)\leq 6$ where ϕ is the Euler function. But $\phi(n)\leq 6$ implies that $n\in\{1,2,3,4,5,6,7,8,9,10,12,14,18\}$ so after at most 18 attempts we will find $e(u_0)$.

We are finally going to make two remarks.

Remark 1.5.13. *In the sieving step we used two arrays A_1 and A_2 in which we stored $a+bm$ and $N(a+b\theta)$ respectively. In practice, when we implement the sieving step we can make some improvements. In the description of the sieving step in [16] it is mentioned an implementation in which we store $ln(|a+bm|)$ and $ln(|N(a+b\theta)|)$ instead of $a+bm$ and $N(a+b\theta)$ respectively. This can improve the performance of the algorithm at some minor cost.*

Remark 1.5.14. *We have mentioned that for each prime $p\leq\min\{B_1,B_2\}$ for which $f(x)$ factors completely in linear factors in $\mathbb{F}_p[X]$ there is a free relation. Obviously for these p, p factors over the set $\boldsymbol{P}$ and by Theorem 1.4.1 we get that pR_K will factor completely in first degree prime ideals. As we have that $p\leq B_2$ it then follows that $pR_K=\prod_{\pi\in\boldsymbol{G}}<\pi>$. These relations are considered as free, as we do not have to use the sieving step in order to conclude the smoothness of the corresponding elements.*

1.6 Cycles construction

As we have already mentioned in section 1.2 in order to take advantage of partial relations we try to combine them in cycles. In this section we present a solution of this problem as described in [17]. But first we remind the definition of a cycle.

Definition 1.6.1. *Let C be a set of partial relations, then C will be called a cycle if for each $(a,\,b)\in C$ there is a sign $s(a,b)\in\{\pm 1\}$ such that*

$$\prod_{(a,\,b)\in C}(a+bm)^{s(a,b)}=\prod_{p\in\boldsymbol{P}}p^{e(p)}\quad\text{and}\quad\prod_{(a,\,b)\in C}(a+b\theta)^{s(a,b)}=\prod_{u\in\boldsymbol{U}}u^{e(u)}\prod_{g\in\boldsymbol{G}}g^{e(g)}$$

Let R be the set of all the partial relations we found while sieving. Our goal is to find subsets $C \subset R$ such that they satisfy the above definition. In order to do that we are going to use graphs. In the rest of this section we are going to take for granted some results of graph theory without proving them. For more details and proofs we refer to [4], we used [14].

Definition 1.6.2. *A simple graph $G = (V, E)$ consists of a set vertices V and a set of edges E which is a set of pairs of elements of V.*

We are going to create a graph that will represent the connections among big primes and big prime ideals. In our case the set of vertices V will be such that $V \subseteq \{1\} \cup P_1 \cup P_2$ where $P_1 = \{\text{all the big primes}\}$ and $P_2 = \{\text{all the big prime ideals}\}$. We have that $V \subseteq \{1\} \cup P_1 \cup P_2$ and not $V = \{1\} \cup P_1 \cup P_2$ as some big primes or big prime ideals may not appear in any partial relation.
An edge will connect two vertices in the graph if there is a partial relation in which the corresponding elements of the two vertices appear as "big".

Definition 1.6.3. *A path in the graph G will be called a sequence of vertices*

$$u_1 \xrightarrow{e_1} u_2 \xrightarrow{e_2} \dots \xrightarrow{e_{n-1}} u_n$$

where the edge e_j connects the vertices u_j and u_{j+1} for $j = 1, 2, \dots, n-1$. The number of edges that appear in a path is defined to be the length of a path. A path in which the last and the first vertex is the same is called a cycle.

As we can easily imagine, a cycle in the graph implies a cycle of partial relations.

Definition 1.6.4. *A graph $G = (V, E)$ will be called bipartite if there is a partition of the set V such that $V = A \cup B$, $A \cap B = \emptyset$ and there is no edge connecting two elements of A or two elements of B respectively.*

The graph which we are going to construct will be the union of a bipartite graph with the vertex $\{1\}$ and all edges connected to it. Hence, a cycle of odd length will include the vertex $\{1\}$ as if it did not, that would imply the existence of an edge connecting two elements of P_1 or P_2, contradiction. So, for the cycles of the graph with even length we can assign the signs ± 1 to the edges alternately without bothering for where to start. As edges correspond to partial relations this will give us a cycle among partial relations. For cycles of odd length we must be more careful as they include the vertex $\{1\}$. For these cycles we have to start with an edge connected to $\{1\}$.

Our goal is to find the cycles of the graph which we constructed. However we do not have to find all cycles of the graph. If the symmetric difference of two cycles C_1 and C_2 is the cycle C_3 then C_3 will not give us any new information as we can get it by C_1 and C_2. Therefore, we want to find a maximal set of independent cycles of G. The first step will be to calculate how many independent cycles exist in the graph.

Definition 1.6.5. *A connected graph G which does not include any cycles is called a tree. A graph (connected or not) which does not include any cycles is called a forest.*

Definition 1.6.6. *A tree T, subgraph of G which contains all the vertices of G is called a spanning tree of G.*

Theorem 1.6.7. *Every connected graph G includes a spanning tree.*

Theorem 1.6.8. *Every tree with v vertices has $v-1$ edges.*

Theorem 1.6.9. *Let $G=(V,E)$ be a connected graph with $|V|=v$ and $|E|=e$. Then, G has $e-v+1$ independent cycles.*

Corollary 1.6.10. *Let $G=(V,E)$ be a graph with c connected components, $|V|=v$ and $|E|=e$. Then, G has $e-v+c$ independent cycles.*

Therefore, in order to be able to calculate how many cycles exist in the graph we have to determine e , v and c. The easiest of all is e as it is equal to the number of partial relations we have found. We are going to compute v and c using the following algorithm.

We construct an array T of two elements per row $T(d_i, a_i)$ where d_i will store vertices and a_i the position in T where is the root of the connected component of G that contains a_i.
Initially we set $v=0$, $c=0$ and $d_i=-1$. For each partial relation which we will consider, let p_1 be the big prime and $\mathfrak{p}_2$ be the big prime ideal (maybe $p_1=1$ or $\mathfrak{p}_2=1$). The first step is to insert p_1 and $\mathfrak{p}_2$ in the graph. For example in order to insert p_1 we are searching for the smallest j such that $d_j=p_1$ or $d_j=-1$. If $d_j=p_1$ then we do not add anything. If $d_j=-1$ then,

$$d_j \leftarrow p_1\,, \quad a_j \leftarrow j\,, \quad v \leftarrow v+1\,, \quad c \leftarrow c+1$$

We deal with $\mathfrak{p}_2$ in the same way. The next step is to find the roots of the connected components of G in which p_1 and $\mathfrak{p}_2$ belong. We illustrate how this can be done for p_1 and we use the same method for $\mathfrak{p}_2$. Let $d_j=p_1$, we set $r \leftarrow j$ and then $r \leftarrow a_r$ as long as $a_r \neq r$. In this way when we are done r will be the position in T of the root of the connected component of G in which p_1 belongs. In this way we get an r_1 and an r_2 corresponding to p_1 and $\mathfrak{p}_2$ respectively.
If $r_1 \neq r_2$ then $c \leftarrow c-1$
If $d_{r_1} < d_{r_2}$ then $a_{r_2} \leftarrow r_1$
If $d_{r_2} < d_{r_1}$ then $a_{r_1} \leftarrow r_2$
If $r_1 = r_2$ then p_1 and $\mathfrak{p}_2$ belong to same connected component of G.
After all partial relations in R have been processed, v will be the number of vertices in G and c the number of connected components.

The next step is to construct a set of independent cycles. The above algorithm has already found the connected components of G. The roots of these components will be our starting point. Our goal is to construct a spanning forest for G so then any edge not in the forest will imply a cycle. We are going again to construct an array that will store this forest and all the necessary information in order to build it and then conclude a cycle of partial relations. We built an array T with four elements per row, i.e. $T(d_i, a_i, a, b, depth \pmod 2)$. As before d_i stores vertices, a_i stores the immediate preceding vertex, (a, b) is the pair that gave us the partial relation and finally in the last field we store the depth $\pmod 2$ in the graph of the corresponding vertex. In depth 0 we place the roots found by the previous algorithm. Then we repeatedly scan the partial relations, considering only those that are not already used. For each partial relation that correspond to an edge we check if any of the two vertices is already included at the previous depth in the graph. If both vertices are not in the graph then we leave this relation for later use. If one vertex is in the graph at the previous depth, but the other vertex is neither present at the current nor the previous depth, we add that edge in the graph by updating the array T. Finally if one vertex is in the graph at the previous depth and the other in the current or the previous depth we have found a cycle. In order to actually get the cycle we follow the path from the one vertex corresponding to the new edge until the root and then back to the other.

Remark 1.6.11. *The above cycles will be independent as in each one of them we used one "new" edge to construct them and we used each such edge only once.*

1.7 Linear algebra

The last step of the SNFS is the linear algebra step. In this step we attempt to solve a large sparse system of linear equations over $\mathbb{F}_2$. In order to solve such a problem one choice would be Gaussian elimination. However the matrices encountered for record-breaking factorizations are really large and therefore we would like to have a more efficient method. Indeed, for this step there are two alternatives. These are the Block Lanczos algorithm [18] and the Block Wiedemann algorithm [9]. In this section we are going to describe how the Block Lanczos algorithm works according to [18]. Initially we are going to describe the Lanczos algorithm over the field $\mathbb{R}$ in order to understand the basic ideas behind the algorithm. Afterwards we will see how it can be adjusted in order to apply over the field $\mathbb{F}_2$.

Let A be a matrix such that $A \in M_n(\mathbb{R})$ and $y \in \mathbb{R}^n$. Our goal is to find a $x \in \mathbb{R}^n$ such that $Ax = y$. In case A is symmetric, positive-definite and sparse then we can apply the Lanczos algorithm in order to find a solution.
Let $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be the linear operator induced by the matrix A.

Definition 1.7.1. *Let $T : V \longrightarrow V$ be a linear operator. Then $S : V \longrightarrow V$ will be called the adjoint linear operator of T iff $< T(u), v >=< u, S(v) > \ \forall\, u, v \in V$.*

Remark 1.7.2. *If T is induced by A for which we have that $A^T = A$ then $S = T$. Indeed*

$$< T(u), v >= (Au)^T v = u^T A^T v = u^T Av =< u, T(v) >$$

In this case T is called self-adjoint.

The following subspace is of great importance for the Lanczos algorithm.

Definition 1.7.3. *Let T be a linear operator as above and $y \in \mathbb{R}^n$. The subspace $W = span(\{y, T(y), T^2(y), ...\})$ is called the $T-$cyclic subspace generated by y (or Krylov subspace generated by y).*

Proposition 1.7.4. *Let $B = \{w_0, w_1, ..., w_{m-1}\}$ be a basis of the $T-$cyclic subspace generated by y such that $< w_i, T(w_j) >= 0$ for $i \neq j$ and $< w_i, T(w_i) >\neq 0$ for $i = 0, 1, ..., m-1$. Then,*

$$x = \sum_{i=0}^{m-1} \frac{< w_i, y >}{< w_i, T(w_i) >} w_i$$

satisfies $T(x) = y$.

Proof. Let $w_j \in B$ then

$$\begin{aligned} < w_j, T(x) > &=< w_j, T\left(\sum_{i=0}^{m-1} \frac{< w_i, y >}{< w_i, T(w_i) >} w_i\right) > \\ &= \sum_{i=0}^{m-1} \frac{< w_i, y >}{< w_i, T(w_i) >} < w_j, T(w_i) > \\ &=< w_i, y > \end{aligned}$$

and therefore we can conclude that $< w_j, T(x) - y >= 0\ \forall w_j \in B$. But, B is a basis for W which implies that $< w, T(x) - y >= 0\ \forall w \in W$. Additionally T is self-adjoint and hence if $w_i \in B$ then $< w_i, T(T(x) - y) >=< T(w_i), T(x) - y >$. Moreover as $w_i \in B \Rightarrow w_i \in W \Rightarrow T(w_i) \in W$ and therefore $< T(w_i), T(x) - y >= 0$ as we have already shown. That follows $< w_i, T(T(x) - y) >= 0$. By the definition of W we have that $y \in W$ and by definition of x we get that $x \in W$ which imply that $T(x) - y \in W$ so, $T(x) - y = \sum_{i=0}^{m-1} c_i w_i$. Let $w_j \in B$ then,

$$\begin{aligned} 0 =< w_j, T(T(x) - y) >=< w_j, T\left(\sum_{i=0}^{m-1} c_i w_i\right) > \\ = \sum_{i=0}^{m-1} c_i < w_j, T(w_i) >= c_j < w_j, T(w_j) > \end{aligned}$$

□

and as $< w_j, T(w_j) > \neq 0$ we get that $c_j = 0$. But j was chosen randomly and hence $T(x) - y = 0 \Rightarrow T(x) = y$.

Our next step will be to find a way to compute a basis for W as in the previous proposition.

Proposition 1.7.5. *Let* $W = span(\{y, T(y), T^2(y), ..., T^{m-1}(y)\})$. *We set* $B = \{w_0, w_1, ..., w_{m-1}\}$ *with* $w_0 = y$ *and* $w_i = T(w_{i-1}) - \sum_{j=0}^{i-1} \frac{< T(w_j), T(w_{i-1}) >}{< T(w_j), w_j >} w_j$. *Then* B *is a basis for* W *such that* $< w_i, T(w_j) >= 0$ *for* $i \neq j$ *and* $< w_i, T(w_i) > \neq 0$.

Proof. Let $B_l = \{w_0, w_1, ..., w_{l-1}\}$ and assume that $< w_i, T(w_j) >= 0$ for $i \neq j$. Let $a_0 w_0 + ... + a_{l-1} w_{l-1} = 0$ with $a_i \in \mathbb{R}$. Therefore $T(a_0 w_0 + ... + a_{l-1} w_{l-1}) = 0$ and hence for $0 \leq j \leq l-1$ we have

$$\begin{aligned} 0 = < w_j, 0 > &= < w_j, T(a_0 w_0 + ... + a_{l-1} w_{l-1}) > \\ &= < w_j, a_0 T(w_0) + ... + a_{l-1} T(w_{l-1}) > \\ &= a_0 < w_j, T(w_0) > + ... + a_j < w_j, T(w_j) > + ... + a_{l-1} < w_j, T(w_{l-1}) > \\ &= a_j < w_j, T(w_j) > \end{aligned}$$

and hence $a_j = 0$ as $< w_j, T(w_j) > \neq 0$. We chose j randomly so $a_j = 0$ for $j = 0, ..., l-1 \Rightarrow$ the elements of B_l are linearly independent. Let $W_l = \{y, T(y), ..., T^{l-1}(y)\}$. We are going to to prove the proposition inductively. For $l = 0$ the proposition is trivially true. We assume it is true for some l with $l < m$ and we will show it for $l+1$. Let $w_j \in B_l$, then

$$\begin{aligned} < w_l, T(w_j) > &= < T(w_{l-1}) - \sum_{i=0}^{l-1} \frac{< T(w_i), T(w_{l-1}) >}{< T(w_i), w_i >} w_i, T(w_j) > \\ &= < T(w_{l-1}, T(w_j) > - \sum_{i=0}^{i-1} \frac{< T(w_i), T(w_{l-1}) >}{< T(w_i), w_i >} < w_i, T(w_j) > \\ &= < T(w_{l-1}), T(w_j) > - < T(w_j), T(w_{l-1}) > \\ &= 0 \end{aligned}$$

So, $< w_i, T(w_j) >= 0$ if $i \neq j$ in B_{l+1}. The next step is to show that B_{l+1} and W_{l+1} span the same space. Let $w_i \in B$ then $w_{i+1} = T(w_i) - \sum_{j=0}^{i} \frac{< T(w_j), T(w_i) >}{< T(w_j), w_j >} w_j$ which follows that $T(w_i) \in span(B_{i+2})$. We will show that $w_k = T^k(y) + \sum_{i=0}^{k-1} a_i w_i$.

For $k = 1 : w_1 = T(y) - \frac{< T(w_0), T(w_0) >}{< T(w_0), w_0 >} w_0$
We assume that it holds for k then,

$$w_{k+1} = T(w_k) - \sum_{j=0}^{k} b_j w_j = T(T^k(y) + \sum_{j=0}^{k-1} a_j w_j) - \sum_{j=0}^{k} b_j w_j$$
$$= T^{k+1}(y) + \sum_{j=0}^{k-1} a_j w_j - \sum_{j=0}^{k} b_j w_j$$

But we have that $T(w_i) \in span(B_{i+2}) \Rightarrow T(w_j) \in span(B_{k+1})$ for $j = 0, \dots, k-1$ and hence $w_{k+1} = T^{k+1}(y) + \sum_{j=0}^{k} c_j w_j$. So, $w_l = T^l(y) + \sum_{j=0}^{l-1} a_j w_j$ but $T^l(y) \in W_{l+1}$ and $w_i \in span(W_{l+1})$ for $i = 0, \dots, l-1$ as $w_i \in span(B_l) = span(W_l) \subseteq span(W_{l+1})$ by inductive hypothesis. Therefore $w_l \in span(W_{l+1})$ and so $span(B_{l+1}) \subseteq span(W_{l+1})$. The elements of B_{l+1} are linearly independent hence $dim(span(B_{l+1})) = l + 1$ and $dim(span(W_{l+1})) = l + 1$ so we get that $span(B_{l+1}) = span(W_{l+1})$ □

Proposition 1.7.6. *The basis B or the previous proposition can be computed recursively by the following formula*

$$w_i = T(w_{i-1}) - \frac{< T(w_{i-1}), T(w_{i-1}) >}{< T(w_{i-1}), w_{i-1} >} w_{i-1} - \frac{< T(w_{i-2}), T(w_{i-1}) >}{< T(w_{i-2}), w_{i-2} >} w_{i-2}$$

for $i \geq 2$.

Proof. Let $j < i - 2$ it is sufficient to show that $< T(w_j), T(w_{i-1}) >= 0$. By the definition of w_{j+1} we have that $T(w_j) = w_{j+1} + \sum_{k=0}^{j} \frac{< T(w_k), T(w_j) >}{< T(w_k), w_k >} w_k$.

$$< T(w_j), T(w_{i-1}) > = < \sum_{k=0}^{j} \frac{< T(w_k), T(w_j) >}{< T(w_k), w_k >} w_k, T(w_{i-1}) >$$
$$= < w_{j+1}, T(w_{i-1}) > + \sum_{k=0}^{j} \frac{< T(w_k), T(w_j) >}{< T(w_k), w_k >} < w_k, T(w_{i-1}) >$$
$$= 0$$

as $j + 1 < i - 1 \Rightarrow j + 1 \neq i - 1$ and $k \leq j < i - 2 < i - 1 \Rightarrow k \neq i - 1$ □

The above method will fail to find a vector x such that $Ax = y$ in our case mainly because of the following three reasons.
1) A is not symmetric.

2) $y = 0$ and therefore $W = \{0\}$.
3) As we work in the field $\mathbb{F}_2$ then $< w_i, T(w_i) > \neq 0$ may fail.

For these reasons the method will be adapted in a block version in order to meet the needs of the NFS. In this version the vectors w_i which we used above as a basis for the vector space W will be replaced by matrices W_i whose columns will span the subspaces $\mathcal{W}_i$. We are going to briefly describe how the method works, for more details and proofs we refer to [18].

Let A be a symmetric $n \times n$ matrix over a field K.

Definition 1.7.7. *Let $\mathcal{W}$ be a subspace of K^n, then $\mathcal{W}$ is called $A-$invertible if it has a basis W of column vectors such that $W^T AW$ is invertible.*

Assume we have found subspaces $\mathcal{W}_i$ such that:
1) $\mathcal{W}_i$ is $A-$invertible.
2) $\mathcal{W}_j^T A\mathcal{W}_i = \{0\}$ for $i \neq j$.
3) $A\mathcal{W} \subseteq \mathcal{W}$ where $\mathcal{W} = \mathcal{W}_0 + \mathcal{W}_1 + ... + \mathcal{W}_{m-1}$.

Proposition 1.7.8. *Let $b \in \mathcal{W}$ and W_i basis of $\mathcal{W}_i$ which satisfy the above three conditions. Then the*

$$x = \sum_{j=0}^{m-1} W_j (\mathcal{W}_j^T A \mathcal{W}_j)^{-1} \mathcal{W}_j^T b$$

satisfies $Ax = b$.

Like the previous case the next step is to construct such a set of subspaces $\mathcal{W}_i$. This will be done by choosing the bases W_i of each $\mathcal{W}_i$. Let $N > 0$ ($N = 32$ or 64) according to [18] we construct matrices $V_i : n \times N$, $S_i : N \times N_i$ where $N_i < N$ such that $\mathcal{W}_j^T A\mathcal{V}_i = 0$ for $j < i$ and $\mathcal{W}_i^T A\mathcal{W}_i$ to be invertible.

Proposition 1.7.9. *Let $W_i = V_i S_i$, $V_{i+1} = AW_i S_i^T + V_i - \sum_{j=0}^{i} W_j C_{i+1,j}$ for $i \geq 0$, $\mathcal{W}_i =< W_i >$, $C_{i+1,j} = (W_j^T AW_j)^{-1} W_j^T A(AW_i S_i^T + V_i)$ and $V_m = 0$. Then $\mathcal{W}_i$ is $A-$invertible , $\mathcal{W}_j^T A\mathcal{W}_i = \{0\}$ for $i \neq j$, $A\mathcal{W} \subseteq \mathcal{W}$ and $W_j^T AV_i = 0$ for $0 \leq j < i \leq m$.*

Remark 1.7.10. *The recurrence formula used to find the V_{i+1} can be simplified as in the case of vectors.*

We are now going to use the above results in order to find vectors in the null space of the matrix B deduced by the sieving step. Let B be $n_1 \times n_2$, we set $A = B^T B$ and $n_2 = n$ then A is an $n \times n$ symmetric matrix over $\mathbb{F}_2$. We will attempt to solve $Ax = 0$ and then conclude solutions for $Bx = 0$. Initially we choose a random $n \times N$ matrix

Y and compute AY. Our goal is to find a matrix X such that $AX = AY$. Then the columns of $X - Y$ will be vectors in the null space of A. In order to find X we use the Lanczos algorithm. We initialize $V_0 = AY$ and construct matrices W_i as described previously. Then

$$X = \sum_{i=0}^{m-1} W_i (W_i^T A W_i)^{-1} W_i^T V_0$$

will satisfy $AX = AY$ under some assumptions made in [18]. If not, then the method can be modified in order to work in that case as well. We set $Z = X - Y$, if $BZ = 0$ then the columns of Z are vectors in the null space of B. If $BZ \neq 0$ then we compute BZ and find a matrix U (at most $N \times N$) whose columns span the null space of BZ. Then a basis of subspace spanned by the columns of ZU will give us the desired vectors in the null space of B.

Comment 1.7.11. *According to [18, p.114] the algorithm described in this section is estimated to take about $O(n^2)$ time in contrast to the Gaussian elimination which takes $O(n^3)$.*

1.8 Runtime analysis

In this section we are going to present some heuristic runtime analysis for the SNFS as given in [16]. The running time of the SNFS can be given by the function $L_n[\nu, \lambda]$ where,

$$L_n[\nu, \lambda] = e^{\lambda(\log n)^{\nu}(\log\log n)^{1-\nu}}$$

Using this notation and the assumption that r and $|s|$ are below a fixed upper bound, the estimated running time of the SNFS is $L_n[\frac{1}{3}, c]$ where $c = \sqrt[3]{\frac{32}{9}} \approx 1.5263$. At this point we have to mention that the SNFS and GNFS (with $L_n[\frac{1}{3}, c]$, $c = \sqrt[3]{\frac{64}{9}} \approx 1.9229$) are the only known factoring algorithms which are conjectured to have a value $\nu < \frac{1}{2}$.
According to the analysis given in [16] we are now going to give the suggested choices for the smoothness bounds and sieving bounds as well as for the degree of the extension $K/\mathbb{Q}$ which we are going to use. The optimal choice for the sieving bounds U_1, U_2 and the smoothness bounds B_1, B_2 is

$$e^{(\frac{1}{2}+o(1))d\log d+\sqrt{(d\log d)^2+2\log(n^{1/d})\log\log(n^{1/d})}}$$

For the large prime and large prime ideal bounds B_3 and B_4 respectively we have to take $B_3 < B_1^2$ and $B_4 < B_2^2$. In this way it is guaranteed that the remaining factor of $a + bm$ and $N(a + b\theta)$ after sieving will be prime so we do not have to factor it. At this point a choice close to B_1^2 and B_2^2 respectively may seem appealing but as primes get larger they appear less often in partial relations. Therefore it is more difficult to be matched

in a cycle. A good choice for B_3 would be between $B_1^{1.2}$ and $B_1^{1.4}$ and similarly for B_4. Finally the optimal degree d of the extension is $d = (\frac{(3+o(1))\log n}{2\log\log n})^{1/3}$ for $e \longrightarrow \infty$ where e is the one in $n = r^e - s$.

1.9 The SNFS in the case $h_K > 1$

In this section we are going to briefly describe how the SNFS is adjusted in order to work in the case $h_K > 1$. In this case R_K is neither a PID nor a UFD. Therefore in this case we cannot search for generators for the prime ideals $\mathfrak{p}$ which implies that we cannot construct the set **G** like the case $h_K = 1$. Also the elements of R_K do not have a unique factorization. However, our goal will be again to find some algebraic integers for which both them and their images under φ will be smooth. Like the case $h_K = 1$ we will be searching for algebraic integers with small coefficients with respect to an integral basis. In this case we do not necessarily search for elements of the form $a + b\theta$. Let $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_s$ be the prime ideals with $N(\mathfrak{p}_i) \leq B$ and $N(\mathfrak{p}_i) \leq N(\mathfrak{p}_{i+1})$. Our goal is to generalize the set **G** for the case $h_K > 1$. In this case we construct the set **G** as follows. Initially we search for a $a_1 \in R_K$ such that $a_1 R_K = \mathfrak{p}_1^{k_{1,1}}$ and $k_{1,1}$ is the minimal power of $\mathfrak{p}_1$ such that $\mathfrak{p}_1^{k_{1,1}}$ is principal. Therefore $k_{1,1}$ is equal to the order of $[\mathfrak{p}_1]$ in the class group $Cl(K)$. Afterwards, we search for a $a_2 \in R_K$ such that $a_2 R_K = \mathfrak{p}_1^{k_{1,2}}\mathfrak{p}_2^{k_{2,2}}$ where $k_{1,2} < k_{1,1}$ and $k_{2,2}$ minimal, hence equal to the order of the coset $[\mathfrak{p}_2] < [\mathfrak{p}_1] >$ in $Cl(K)/ < [\mathfrak{p}_1] >$. We proceed in the same way for the rest of the $\mathfrak{p}_i$. In this way we construct an upper triangular matrix M with elements the $k_{i,j}$. Now we set **G** to be the set of all these a_i.

Remark 1.9.1. *The new set **G** is actually a generalization of the one in the case $h_K = 1$. Indeed, if $h_K = 1$ then we would have $k_{i,i} = 1$ and $k_{i,j} = 0$ for $i < j$ and hence the a_i would be generators of the respective $\mathfrak{p}_i$.*

Let $x \in R_K$ that is $B-$smooth then $xR_K = \prod_{i=1}^{s} \mathfrak{p}_i^{v_i}$ as R_K is a Dedekind domain. We will show that x has a unique factorization as a product of elements $a_i \in \mathbf{G}$ and a

unit. We search for μ_i for $i = 1, \dots, s$ such that $\prod_{j=1}^{s} {a_j}^{\mu_j} R_K = xR_K$. But,

$$\begin{aligned}\prod_{j=1}^{s} {a_j}^{\mu_j} R_K &= \prod_{j=1}^{s} \left(\prod_{\nu=1}^{j} \mathfrak{p}_\nu^{k_{\nu,j}} \right)^{\mu_j} \\ &= \prod_{j=1}^{s} \prod_{\nu=1}^{j} \mathfrak{p}_\nu^{k_{\nu,j}\mu_j} \\ &= \prod_{j=1}^{s} \mathfrak{p}_j^{\sum_{\nu=j}^{s} k_{j,\nu}\mu_\nu}\end{aligned}$$

Hence, $xR_K = \prod_{j=1}^{s} \mathfrak{p}_j^{\sum_{\nu=j}^{s} k_{j,\nu}\mu_\nu}$ and $xR_K = \prod_{j=1}^{s} \mathfrak{p}_j^{\upsilon_j}$ and we have unique factorization of ideals so, $\upsilon_j = \sum_{\nu=j}^{s} k_{j,\nu}\mu_\nu$. This implies that

$$M \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_s \end{pmatrix} = \begin{pmatrix} \upsilon_1 \\ \upsilon_2 \\ \vdots \\ \upsilon_s \end{pmatrix}$$

So in order to find the μ_i we need to solve the above system, where

$$M = \begin{pmatrix} k_{1,1} & k_{1,2} & k_{1,3} & \cdots & k_{1,s} \\ & k_{2,2} & k_{2,3} & \cdots & k_{2,s} \\ & & k_{3,3} & & k_{3,s} \\ & \mathbf{0} & & \ddots & \vdots \\ & & & & k_{s,s} \end{pmatrix}$$

Finally we get that $x = u \prod_{j=1}^{s} {a_j}^{\mu_j}$ where $u \in E(R_K)$. Then, we can proceed as in the case $h_K = 1$.

Remark 1.9.2. *The μ_i which we will get by solving the above system will be integers. Indeed, if we take μ_s for example, we want $k_{s,s}\mu_s = \upsilon_s$ so $k_{s,s}$ must divide υ_s. But $xR_K = \prod_{j=1}^{s} \mathfrak{p}_j^{\upsilon_j}$ and $k_{s,s}$ is the order of $[\mathfrak{p}_s]$ in $Cl(K)/ < \prod_{j=1}^{s-1} \mathfrak{p}_j >$ which implies that $k_{s,s} \mid \upsilon_s$. If we want to check that μ_{s-1} will be an integer we apply the above argument but this time for the ideal $x{a_s}^{-\mu_s} R_K$ and we continue in the same way.*

Comment 1.9.3. *The above remark justifies why we chose the* a_i *to satisfy* $a_i R_K = \prod_{j=1}^{i} \mathfrak{p}_j^{k_{j,i}}$ *and not just* $a_i R_K = \mathfrak{p}_i^{k_i}$.

Given these modifications new computational demands arise. The first is computing the structure of $Cl(K)$. Then, we have to find all ideals $\mathfrak{p}_i$ with $N(\mathfrak{p}_i) \leq B$. Afterwards, given the $Cl(K)$ and this set of prime ideals we have to compute the $k_{i,j}$ and a_i for each $\mathfrak{p}_i$ as described above. Moreover, in order to be able to compute the μ_i we must be able to compute the v_i in the factorization of xR_K. In this case we do not necessarily have $f(\mathfrak{p}_i/p\mathbb{Z}) = 1$. Hence, we will have to use the method used for the case $h_K = 1$ and $\mathfrak{p} \mid \langle f \rangle$ in order to compute the v_i (actually with a small modification as the $\mathfrak{p}_i$ are not principal in general).

1.10 A working example

In order to get a better understanding of what we have done so far we are going to give an example of a factorization using the SNFS. The number which we are going to factor is $n = 60698453$. Obviously, for factoring a number of this magnitude nowadays we do not have to use such a powerful algorithm as the SNFS, but here it will help us illustrate the procedure.

First of all in order to use the SNFS we need to write n in the form $r^e - s$. By trying some values for s we observe that $n + 4 = 393^3$ and so we have that $n = 393^3 - 4$. Hence in our example we have $r = 393$, $s = 4$ and $e = 3$. The next step is to choose the degree d of the extension $K/\mathbb{Q}$ in which we are going to work. We choose $d = 3$ so the least integer k such that $kd \geq e$ is $k = 1$. Therefore, as described in the first step of the algorithm we get

$$f(x) = x^d - sr^{kd-e} = x^3 - 4 \quad \text{and} \quad m = r^k = 393$$

and $f(x)$ is irreducible so the number field in which we are going to work is $K = \mathbb{Q}(\theta)$ where, $\theta = \sqrt[3]{4}$ Then using SAGE we find h_K and an integral basis for R_K. This can be done by giving the following commands :

```
R.<x> = QQ []
K.<a> = NumberField (x^3 -4)
h=K.class_number() ; h
RK = K.maximal_order()
RK.basis()
```

and we get that $h_K = 1$ and $R_K = \mathbb{Z} \oplus \sqrt[3]{4}\mathbb{Z} \oplus \frac{1}{2}\sqrt[3]{4}^2\mathbb{Z}$. As we can see in this case

$\mathbb{Z}[\sqrt[3]{4}] \subsetneq R_K$ so we define φ as follows :

$$\varphi : R_K \to \mathbb{Z}/60698453\mathbb{Z}$$
$$\frac{1}{2}(2x + 2y\sqrt[3]{4} + z(\sqrt[3]{4})^2) \mapsto ((2x + 2y393 + z393^2)2^{-1} \bmod 60698453)$$

Our next step is to choose the smoothness bounds B_1, B_2, B_3, B_4. We make the choices $B_1 = 43$, $B_2 = 43$ and $B_3 = 50$, $B_4 = 50$. This will give us that
$\mathbf{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43\}$
Afterwards we compute the pairs $(p,\ c)$ that correspond to the prime ideals $\mathfrak{p}$ with $f(\mathfrak{p}/p\mathbb{Z}) = 1$ and $N(\mathfrak{p}) \leq B_2$. Using the algorithm described in section 4 we conclude that these pairs are :

$$(3,\ 1),\ (5,\ -1),\ (11,\ 5),\ (17,\ -4),\ (23,\ 3),\ (29,\ 9)$$
$$(31,\ -3),\ (31,\ -13),\ (31,\ -15),\ (41,\ -16),\ (43,\ -5),\ (43,\ -8),\ (43,\ 13)$$

Comment 1.10.1. *We did not take into account the prime* 2 *because it divides the index as we can see below.*

We can compute the discriminant of the number field by computing the discriminant of the integral base. In SAGE this can be done by the following command :
d=K.absolute_discriminant() ;d

and we get that $D_{K/\mathbb{Q}} = -108 = -2^2 3^3$. Also, $D_K(\sqrt[3]{4}) = -3^3 2^4$ and as $D_K(\sqrt[3]{4}) = [R_K : \mathbb{Z}[\sqrt[3]{4}]]^2 D_{K/\mathbb{Q}}$ we get that $[R_K : \mathbb{Z}[\sqrt[3]{4}]] = 2$.

So now we can determine,

$$\mathbf{G}_1 = \{\pi \in R_K : <\pi> = \mathfrak{p} \quad \forall\, \mathfrak{p} \in \mathbb{P}(K) \text{ such that } f(\mathfrak{p}/p\mathbb{Z}) = 1 \text{ and } N(\mathfrak{p}) \leq B_2\}$$

In order to do that we must first compute the parameters of our search,

$$v_d = \left(\frac{4}{d}\right)^{d/2} \frac{1}{\omega_d} \simeq 0.367$$
$$C = (v_d\sqrt{|D_K|}B_2)^{2/d} \simeq 30$$
$$M = [v_d\sqrt{|D_K|}] = 3$$

These parameters imply a search for the generators among 344 elements of R_K. After this search is done we get a result as shown in table 1.1.

Also, while searching for the above elements we encounter the elements $1 + \frac{1}{2}\sqrt[3]{4}^2$, $\frac{1}{2}\sqrt[3]{4}^2$ and $-1 + \frac{1}{2}\sqrt[3]{4}^2$ of norm 3 , 2 and 1 respectively. The only ideal $\mathfrak{p}$ not dividing the

$(p,\ c)$	$m(\mathfrak{p})$	$\pi_{\mathfrak{p}}$
(5, -1)	1	$1+\sqrt[3]{4}$
(11, 5)	1	$-1+\sqrt[3]{4}+\frac{1}{2}\sqrt[3]{4}^2$
(17, -4)	1	$1+\sqrt[3]{4}^2$
(23, 3)	1	$-1-2\sqrt[3]{4}-\frac{1}{2}\sqrt[3]{4}^2$
(29, 9)	1	$3+\frac{1}{2}\sqrt[3]{4}^2$
(31, -3)	1	$3+\sqrt[3]{4}$
(31, -13)	1	$-1+\sqrt[3]{4}+\sqrt[3]{4}^2$
(31, -15)	1	$1-2\sqrt[3]{4}$
(41, -16)	1	$1+\sqrt[3]{4}+\frac{3}{2}\sqrt[3]{4}^2$
(43, -5)	1	$-1-2\sqrt[3]{4}+\frac{1}{2}\sqrt[3]{4}^2$
(43, -8)	1	$-3+\sqrt[3]{4}-\frac{1}{2}\sqrt[3]{4}^2$
(43, 13)	1	$3+\sqrt[3]{4}^2$

Table 1.1: Ideal generators

index with $N(\mathfrak{p}) \leq 3$ is the one corresponding to the pair $(3,\ 1)$ so if we add $1+\frac{1}{2}\sqrt[3]{4}^2$ in the above list we get,

$$\begin{aligned}\mathbf{G}_1 =\{&1+\frac{1}{2}\sqrt[3]{4}^2,\ 1+\sqrt[3]{4},\ -1+\sqrt[3]{4}+\frac{1}{2}\sqrt[3]{4}^2,\ 1+\sqrt[3]{4}^2,\ -1-2\sqrt[3]{4}-\frac{1}{2}\sqrt[3]{4}^2,\\ &3+\frac{1}{2}\sqrt[3]{4}^2,\ 3+\sqrt[3]{4},\ -1+\sqrt[3]{4}+\sqrt[3]{4}^2,\ 1-2\sqrt[3]{4},\ 1+\sqrt[3]{4}+\frac{3}{2}\sqrt[3]{4}^2,\\ &-1-2\sqrt[3]{4}+\frac{1}{2}\sqrt[3]{4}^2,\ -3+\sqrt[3]{4}-\frac{1}{2}\sqrt[3]{4}^2,\ 3+\sqrt[3]{4}^2\}\end{aligned}$$

Now it is the turn of $\mathbf{G}_2 = \{\pi \in R_K :< \pi >= \mathfrak{p} \quad \forall\, \mathfrak{p} \mid 2R_K\}$. In our case, 2 is not an essential discriminant divisor so we can apply the following trick. We have that $K = \mathbb{Q}(\sqrt[3]{4})$ but it is also true that $K = \mathbb{Q}(\sqrt[3]{2})$. Changing the generating element of K gives us the following advantage, $R_K = \mathbb{Z}[\sqrt[3]{2}]$ so now we can use Theorem 1.4.1. Using this theorem we conclude that there is only one prime ideal above 2 and it is of degree 1. Therefore this ideal will correspond to the pair $(2,\ 0)$ and will be generated by $\frac{1}{2}\sqrt[3]{4}^2$. Hence, we can deal with this ideal like the rest ideals of degree 1.

$\mathbf{G}_2 = \{\frac{1}{2}\sqrt[3]{4}^2\}$

The only thing left for finishing the construction of the factor base is to find a generating system for $E(R_K)$. Our number field K has one real embedding and two complex embeddings. Therefore using Theorem 1.4.6 we conclude that we are looking for a root of unity and for one fundamental unit. Our number field contains only real numbers so

the only roots of unity in it are ± 1. By the algorithm that searches for generators of ideals we have already found an element of norm 1, but is it a fundamental unit? The following proposition mentioned in [10] will give us the answer.

Proposition 1.10.2. *Let K be a pure cubic number field and R_K its ring of algebraic integers. If $\varepsilon \in R_K$ such that $\varepsilon > 1$ and $4\varepsilon^{3/2} + 24 < |D_K|$ then ε is a fundamental unit.*

We try to apply the above proposition for $-1 + \frac{1}{2}\sqrt[3]{4}^2$. But $-1 + \frac{1}{2}\sqrt[3]{4}^2 \simeq 0.259$ so $-1 + \frac{1}{2}\sqrt[3]{4}^2 < 1$. Let ε to be the inverse of $-1 + \frac{1}{2}\sqrt[3]{4}^2$, then $\varepsilon = 1 + \sqrt[3]{4} + \frac{1}{2}\sqrt[3]{4}^2$. But now $\varepsilon \simeq 3.846 > 1$ and $4\varepsilon^{3/2} + 24 \simeq 54.185 < |D_K| = 108$ so by the previous proposition we get that ε is a fundamental unit. Therefore $-1 + \frac{1}{2}\sqrt[3]{4}^2$ has infinite order as well and hence we can take,

$$\mathbf{U} = \{-1, -1 + \frac{1}{2}\sqrt[3]{4}^2\}$$

As we have constructed the factor base, the next step is sieving. We choose the sieving bounds to be $U_1 = 250$ and $U_2 = 100$ for example and we start sieving. As a result we get

Full relations			
b	a	$A_1(a)$	$A_2(a)$
1	-49	1	-1
1	-16	1	-1
1	-13	1	-1
1	-9	1	-1
1	-3	1	-1
1	-2	1	-1
1	-1	1	1
1	3	1	1
1	6	1	1
1	66	1	1
2	-9	1	-1
2	-3	1	1
3	4	1	1
5	3	1	1
5	13	1	1
7	-13	1	-1
7	207	1	1
8	15	1	1
11	12	1	1
13	8	1	1
17	7	1	1
17	179	1	1
31	-47	1	1
39	-32	1	1
41	37	1	1
53	-42	1	1
56	3	1	1
61	176	1	1

Partial relations			
b	a	$A_1(a)$	$A_2(a)$
3	-4	47	1
64	-101	47	1
5	- 43	1	-47
63	41	1	47

Free relations	
b	a
0	2
0	3
0	31
0	43

For the relations we have found we compute the factorization of $a+b393$ and $a+b\sqrt[3]{4}$ respectively and form the following vectors.

b	a	exponents vector $v_{(a,b)}$
1	-49	(3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)
1	-16	(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 2, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)
1	-13	(2, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)
1	-9	(7, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)
1	-3	(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)
1	-2	(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)
1	-1	(3, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)
1	3	(2, 2, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)
1	6	(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 2, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
1	66	(0, 3, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 2, 0, 5, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 2)
2	-9	(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)
2	-3	(0, 3, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2)
3	4	(0, 0, 0, 1, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)
5	3	(4, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)
5	13	(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)
7	-13	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 1, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 2)
7	207	(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 3, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)
8	15	(0, 5, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)
11	12	(0, 1, 1, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)
13	8	(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 2, 1, 2, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)
17	7	(5, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)
17	179	(2, 0, 1, 3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 3, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)
31	-47	(3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0, 3)
39	-32	(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)
41	37	(1, 0, 2, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 2, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)
53	-42	(0, 1, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 1, 0, 2, 0, 1, 0, 0, 0, 2, 0, 0, 1, 0, 0, 0, 0, 1, 1)
56	3	(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 2, 0, 0, 0, 1, 0, 0)
61	176	(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 2, 1, 2, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)

b	a	exponents vector $v_{(a,b)}$
3	-4	(0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 1)
64	-101	(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 2, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 4)
5	-43	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 1)
63	41	(5, 0, 2, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)

b	a	exponents vector $v_{(a,b)}$
0	2	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
0	3	(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)
0	31	(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)
0	43	(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)

In the partial relations' vectors we do not mention the large prime or the large prime ideal. We illustrate how we found the above vectors. For example, if we take $(a,\ b) = (-13,\ 1)$ then,
$a + b393 = -13 + 1 \cdot 393 = 380 = 2^2 \cdot 5 \cdot 19$ and
$\langle -13 + \sqrt[3]{4} \rangle = \langle 1 + \frac{1}{2}\sqrt[3]{4}^2 \rangle \langle 1 + \sqrt[3]{4}^2 \rangle \langle 3 + \sqrt[3]{4}^2 \rangle$ as
$-13 + 1 \cdot 1 \equiv 0 \pmod 3$,
$-13 + 1 \cdot (-4) \equiv 0 \pmod{17}$ and
$-13 + 1 \cdot 13 \equiv 0 \pmod{43}$. Therefore we get that

$$-13 + \sqrt[3]{4} = (-1)^{e_0}(-1 + \frac{1}{2}\sqrt[3]{4}^2)^{e_1}(1 + \frac{1}{2}\sqrt[3]{4}^2)(1 + \sqrt[3]{4}^2)(3 + \sqrt[3]{4}^2)$$

Let $v = (-1)^{e_0}(-1 + \frac{1}{2}\sqrt[3]{4}^2)^{e_1}$ then
$v = (-13 + \sqrt[3]{4})(1 + \frac{1}{2}\sqrt[3]{4}^2)^{-1}(1 + \sqrt[3]{4}^2)^{-1}(3 + \sqrt[3]{4}^2)^{-1}$. As the rank of $E(R_K)$ is 1 we choose the embedding $\sigma = id$ and we define,

$$\begin{aligned} l\ :\ K^* &\to \mathbb{R} \\ x &\mapsto \log|x| \end{aligned}$$

Therefore,

$$\begin{aligned} e_1 l(-1 + \frac{1}{2}\sqrt[3]{4}^2) = l(v) &\Rightarrow \\ e_1 \log|-1 + \frac{1}{2}\sqrt[3]{4}^2| = \log|(-13 + \sqrt[3]{4})(1 + \frac{1}{2}\sqrt[3]{4}^2)^{-1}(1 + \sqrt[3]{4}^2)^{-1}(3 + \sqrt[3]{4}^2)^{-1}| &\Rightarrow \\ e_1 \log|-1 + \frac{1}{2}\sqrt[3]{4}^2| = \log|-13 + \sqrt[3]{4}| - \log|1 + \frac{1}{2}\sqrt[3]{4}^2| - \log|1 + \sqrt[3]{4}^2| - \log|3 + \sqrt[3]{4}^2| &\Rightarrow \\ (-1.347)e_1 \simeq 2.68 - 0.815 - 1.258 - 1.708 &\Rightarrow \\ e_1 \simeq 0.817 & \end{aligned}$$

so $e_1 = 1$ if we round it to the closest integer. Then it is easy to see that $e_0 = 1$. Hence, we can now construct the vector $v_{(-13,1)}$ as described in section 1.2.

Finally, as we have only 4 partial relations we can observe that they are combined in two cycles C_1 and C_2 which gives us the following vectors.
(0, 0, -2, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, -2, 0, 2, -1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 3)
(4, 0, 2, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, -2, 0, 0, 1, 1, 0)

Then we reduce all these vectors $\pmod 2$ and using them as columns we form a matrix. The nullspace of this matrix is spanned by
$V_1 = (1,0,0,0,0,0,1,1,0,0,1,1,0,0,0,0,0,1,0,1,0,1,1,1,1,0,1,0,0,0,0,0,1,0)$
$V_2 = (0,1,0,0,0,0,0,1,0,1,1,0,1,0,1,0,1,1,0,0,1,1,1,1,0,1,0,0,0,1,0,1,0,0)$
$V_3 = (0,0,1,0,1,0,0,0,0,0,1,0,1,0,1,1,1,0,1,1,1,1,1,0,0,0,1,0,0,1,0,0,1,0)$
$V_4 = (0,0,0,1,0,0,1,0,0,0,0,1,0,0,1,0,0,1,0,0,1,0,0,0,0,0,0,1,1,0,0,0,1,1,1)$
$V_5 = (0,0,0,0,0,1,1,1,0,0,0,1,1,0,0,1,1,1,1,0,1,0,0,1,0,1,0,0,0,1,0,0,1,0)$
$V_6 = (0,0,0,0,0,0,0,0,1,0,0,1,0,0,0,1,0,0,1,0,1,0,0,1,0,1,1,1,0,1,0,0,0,1)$

We examine
$V_4+V_5 = (0,0,0,1,0,1,0,1,0,0,0,0,1,0,1,1,1,0,1,0,0,0,0,1,0,1,1,1,0,1,0,1,0,1)$
which implies that

$$T = \{(-9,\,1),\,(-2,\,1),\,(3,\,1),\,(4,\,3),\,(13,\,5),\,(-13,\,7),\,(207,\,7),\,(12,\,11),\\ (-32,\,39),\,(-42,\,53),\,(3,\,56),\,(176,\,61),\,(3,\,0),\,(43,\,0),\,C_2\}$$

Which gives us,

$$\prod_{(a,\,b)\in T}(a+b393) = (37068206408665323091200)^2$$

$$\prod_{(a,\,b)\in T}(a+b\sqrt[3]{4}) = (1545140844 - 961510272\sqrt[3]{4} - 291398616\sqrt[3]{4}^2)^2$$

and hence,

$$\varphi(37068206408665323091200) \equiv 31167286 \pmod{60982453}$$

$$\varphi(1545140844 - 961510272\sqrt[3]{4} - 291398616\sqrt[3]{4}^2) \equiv 41211233 \pmod{60982453}$$

which means that we have found a non-trivial congruence of squares and therefore,

$$\gcd(31167286 - 41211233, 60982453) = 7369$$
$$\gcd(31167286 + 41211233, 60982453) = 8237$$

Chapter 2

The General Number Field Sieve

A natural question which arose as soon as the SNFS appeared and began to push the boundaries of factorization (in the spacial form of integers in which it applied) was if it could be generalised for arbitrary integers. The answer proved to yes. The algorithm which we described in the previous chapter can be adjusted in order to factor arbitrary integers. The main idea remains the same, we try to find a non-trivial congruence of squares modulo the number we want to factor. In order to do that we are going to use again a factor base, then find a sufficient number of smooth elements and finally use linear algebra in order to construct two squares. However there are some differences as we will see later. These differences make the GNFS to be a bit slower than the SNFS. The records of each method indicate exactly that. As we mentioned in the beginning of the previous chapter the record of SNFS at the moment is the 320-digit number $2^{1061}-1$ [7] whereas for the GNFS is the 232−digit number RSA-768. The factorization of RSA-768 reported in [13] finished in the end of 2009 and took about three years.

2.1 Description of the algorithm

The main ideas used in the SNFS remain the same for the GNFS as well. However there are some differences. In the SNFS the number n which we attempt to factor is assumed to be of the special form $r^e - s$ for some "small" $r, |s|$. As we saw this enabled us to associate to n a number field K of special form. That is no longer true, in our case the number n is random and we do not assume that it possesses such a property. This has the following effect. The number field in which we are going to work will have a large discriminant and will be computationally infeasible to handle it like in the case of SNFS. In this case we are not able to compute efficiently the class number of the number field, a set of fundamental units and generators of the prime ideals with small norm. In order to tackle this problem we are going to modify the SNFS in a way that it will use ideals instead of algebraic integers. That will be the GNFS. This modification will have

some advantages and disadvantages. Apart from not having to compute generators for the prime ideals and a system of a fundamental units in this case we have the advantage that we can work with $\mathbb{Z}[\theta]$ instead of R_K in case $\mathbb{Z}[\theta] \subsetneq R_K$. But there will be also disadvantages, the construction of a square in $\mathbb{Z}[\theta]$ will be probabilistic at some point and the computation of a square root will be demanded. Another difference is the polynomial selection step. In the case of the SNFS the polynomial selection step is almost immediate whereas in the GNFS is not. In the next section we are going to describe the most simple technique by which somebody could choose a polynomial. However there are more advanced techniques used nowadays, like in [3]. In the following description of the GNFS we do not consider the large prime variation as this was illustrated in the previous chapter.

Step 1) We first choose the degree d of the extension in which we are going to work and then associate a number field $K = \mathbb{Q}(\theta)$ to the number n. This is done through the irreducible polynomial $f(x)$ of θ. We choose an $f(x) \in \mathbb{Z}[x]$ in a specific way as we wish it to have the following property.

$$\text{There is an integer m (of size } n^{1/d}\text{) such that} \quad f(m) \equiv 0 \pmod{n}$$

Then we define,

$$\begin{aligned} \varphi : \mathbb{Z}[\theta] &\to \mathbb{Z}/n\mathbb{Z} \\ \sum_{i=0}^{d-1} a_i\theta^i &\mapsto \sum_{i=0}^{d-1} a_i m^i \pmod{n} \end{aligned}$$

Step 2) As we have chosen the number field K in which we are going to work, the next step is to choose our smoothness bounds B_1, B_2. Then we construct the factor base. Our factor base consists of three sets **P**, **G** and **Q**.

$\mathbf{P} = \{p \in \mathbb{P},\ p \leq B_1\}$
$\mathbf{G} = \{\mathfrak{p} \trianglelefteq \mathbb{Z}[\theta] : \mathfrak{p} \text{ is a prime ideal and such that } f(\mathfrak{p}/p\mathbb{Z}) = 1 \text{ and } N(\mathfrak{p}) \leq B_2\}$
$\mathbf{Q} = \{\mathfrak{q} \trianglelefteq \mathbb{Z}[\theta] : \mathfrak{q} \text{ is a prime ideal and such that } f(\mathfrak{q}/q\mathbb{Z}) = 1\ ,\ f'(\theta) \notin \mathfrak{q} \text{ and } N(\mathfrak{q}) > B_2\}$

where $f(\mathfrak{p}/p\mathbb{Z})$ is the residual degree. We take **Q** to have about $\left[3\frac{\log n}{\log 2}\right]$ elements.

Step 3) We choose two sieving bounds U_1, U_2 and like in the case of SNFS we try to find a sufficient number of relations. We are looking for pairs $(a,\ b)$ where $a,\ b$ are integers with $|a| \leq U_1$ and $0 < b \leq U_2$ such that :
i) $\gcd(a,\ b) = 1$
ii) $|a + bm|$ is B_1-smooth
iii) $a + b\theta$ is B_2-smooth

When we find a pair $(a,\ b)$ that satisfies the above three conditions we say that we have found a relation.

Step 4) Once we have enough relations we form a matrix depending on the factorization of the elements $a+bm$ and $< a+b\theta >$ that each relation corresponds to. Let S be the set of all relations that we found in step 3. Then using linear algebra techniques we attempt to find a subset T of S such that :

$$\prod_{(a,\ b)\in T}(a+bm) = \quad \text{square in } \mathbb{Z}$$

$$\prod_{(a,\ b)\in T}(a+b\theta) \quad \text{such that } l_{\mathfrak{p}}\Big(\prod_{(a,b)\in T}(a+b\theta)\Big) \equiv 0 \pmod 2$$

$$\text{and} \prod_{(a,\ b)\in T}\chi_{\mathfrak{q}}(a+b\theta) = 1 \quad \forall\, \mathfrak{q} \in \mathbf{Q}$$

Step 5) Finally, when step 4 will finish it will give us two elements x, δ where $x \in \mathbb{Z}$ and $\delta \in \mathbb{Z}[\theta]$, $\delta = \beta^2$ for some $\beta \in \mathbb{Z}[\theta]$ such that $x^2 \equiv \varphi(\delta) \pmod n$. In this step we will try to find $\varphi(\beta) \pmod n$.

As we can see there are some differences between the algorithm given for the SNFS and the GNFS. The first is the way we find the polynomial $f(x)$. Another difference occurs in step 2. The algebraic factor base consists of prime ideals instead of prime elements and there is an extra set **Q**. That set will be called the *quadratic character base*. Also as it may happen that $\mathbb{Z}[\theta] \subsetneq R_K$ we do not have unique factorization of ideals in $\mathbb{Z}[\theta]$. We are going to deal with this problem by introducing the functions $l_{\mathfrak{p}}$ (see Proposition 2.3.2). Finally the $\chi_{\mathfrak{q}}$ are characters corresponding to the elements of **Q** as we will see in Proposition 2.3.11. In the next sections we are going to study these differences.

2.2 Polynomial selection

In the case we examine in this chapter the number n which we attempt to factor is not of a special form. Therefore we cannot construct a polynomial of the form $x^d - t$ like in the case of SNFS. In this case we need a different approach. In this section we are going to to describe the most simple technique that can be used in order to obtain a polynomial $f(x)$ as demanded by step 1 of the algorithm. However, there are more advanced techniques, not described in this master thesis for doing so. To indicate that we mention that the factorization of RSA-768 mentioned in [13] included a three month step for the polynomial selection.

The method is the following. We first choose the number m. As we want m to be close to $n^{1/d}$ and set $m = [n^{1/d}]$. Then we write n in base m and hence we get,

$$n = m^d + a_{d-1}m^{d-1} + ... + a_1 m + a_0 \quad \text{where } 0 \leq a_i < m$$

We set $f(x) = x^d + a_{d-1}x^{d-1} + ... + a_1 x + a_0$. Obviously $f(x)$ satisfies $f(m) \equiv 0 \pmod{n}$. In order to be able to define $K = \mathbb{Q}(\theta)$ we wish this polynomial to be irreducible as well. However the polynomial may be reducible. As we will see this would be a very good case as a non-trivial factorization of $f(x)$ in $\mathbb{Z}[x]$ implies a non-trivial factorization of n. In order to prove that we are going to use the following results mentioned in [6] (slightly modified).

Proposition 2.2.1. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with roots $a_1, a_2, ..., a_s \in \mathbb{C}$ and $f(b) = n$ for some $b \in \mathbb{Z}$. We assume that $f(b-1) \neq 0$, $Re(a_i) < b - \frac{1}{2}$ for $i = 1, 2, ..., s$ and $f(x) = g(x)h(x)$ is a non-trivial factorization of $f(x)$. Then $|g(b)|$, $|h(b)|$ are non-trivial factors of n.*

Proof. In order to prove the proposition it suffices to prove that $|g(b)| \geq 2$ and $|h(b)| \geq 2$. Let $a_1, a_2, ..., a_r$, $r < s$ be the roots of $g(x)$ and so $g(x) = \alpha_r \prod_{i=1}^{r}(x - a_i)$. We set $g_1(x) = g(x+b-\frac{1}{2}) = \alpha_r \prod_{i=1}^{r}(x+b-\frac{1}{2}-a_i) = \alpha_r \prod_{i=1}^{r}(x-\beta_i)$ where $\beta_i = -b+\frac{1}{2}+a_i$.
If $a_i \in \mathbb{R}$: $\beta_i = -b + \frac{1}{2} + a_i < 0$
If $a_i \in \mathbb{C}$: $Re(\beta_i) = -b + \frac{1}{2} + Re(a_i) < 0$
But if $g_1(\beta_i) = 0 \Rightarrow g_1(\overline{\beta_i}) = 0$ and hence $\overline{\beta_i}$ is also a root of $g_1(x)$. We have that $(x - \beta_i)(x - \overline{\beta_i}) = x^2 - (\beta_i + \overline{\beta_i})x + |\beta_i|^2 = x^2 - 2Re(\beta_i)x + |\beta_i|^2$ and therefore,

$$g_1(x) = \alpha_r \prod_{\beta_i \in \mathbb{R}} (x - \beta_i) \prod_{\substack{\beta_i \in \mathbb{C} \setminus \mathbb{R} \\ \beta_i \neq \overline{\beta_j}}} \left(x^2 - 2Re(\beta_i)x + |\beta_i|^2\right)^{\lambda_i}$$

is a factorization of $g_1(x)$ in $\mathbb{R}$. Let $g_1(x) = \sum_{i=0}^{r} \alpha_i x^i$, the previous factorization of $g_1(x)$ enables us to conclude that all the α_i have the same sign and $\alpha_i \neq 0$. Furthermore $g_1(-x) = \sum_{i=0}^{r} \alpha_i (-1)^i x^i$ and hence the coefficients of $g(-x + b - \frac{1}{2})$ have strictly alternating signs.
Let $t > 0$: $|g_1(t)| = |\sum_{i=0}^{r} \alpha_i (-1)^i t^i| < |\sum_{i=0}^{r} \alpha_i t^i| = |g_1(t)|$. For $t = \frac{1}{2}$ we get that $|g_1(-\frac{1}{2})| < |g_1(\frac{1}{2})| \Rightarrow |g(b-1)| < |g(b)|$. But $g(b-1) \neq 0 \Rightarrow |g(b-1)| \geq 1 \Rightarrow |g(b)| \geq 2$. In the same way we can show that $|h(b)| \geq 2$ which then implies the result. □

Therefore our next goal is to show that the polynomials which we use satisfy the conditions of the above proposition.

Proposition 2.2.2. *Let* $f(x) = \sum_{k=0}^{n} \alpha_k x^k \in \mathbb{Z}[x]$ *be a polynomial with* $\alpha_n > 0$, $\alpha_{n-1} \geq 0$, $\alpha_{n-2} \geq 0$. *Let* $m = \max\{\frac{|\alpha_k|}{\alpha_n}\}$ *for* $k = 0, 1, \ldots n-2$, r_1 *the real positive root of* $x^2 - x - m$ *and* r_2 *the real positive root of* $x^3 - x^2 - m$ *respectively.* *(*$r_1 = \dfrac{1+\sqrt{4m+1}}{2}$, $\quad r_2 = \dfrac{1}{3} + \sqrt[3]{\dfrac{s+\sqrt{s^2-4}}{54}} + \sqrt[3]{\dfrac{s-\sqrt{s^2-4}}{54}}$ *where* $s = 27m + 2$*). If there is a* $b \in \mathbb{Z}$ *such that* $b > \max\{\frac{r_1}{\sqrt{2}}, r_2\} + \frac{1}{2}$ *then* $Re(a_i) < b - \frac{1}{2}$ *for every* a_i *root of* $f(x)$.

Proof. As $m \geq 0$ it follows that $r_1 \geq 1$ and $r_2 \geq 1$. Let $A = \{z \in \mathbb{C} : Re(z) \leq \max\{\frac{r_1}{\sqrt{2}}, r_2\}\}$. We will show that if $z \in A^c$ then $|f(z)| > 0$ and therefore the roots of $f(x)$ belong to A which implies the result. Let $B = \{z \in \mathbb{C} : Re(z) \leq 0 \text{ or } |z| \leq r_1\}$ and we set $A_1 = A^c \cap B$ and $A_2 = A^c \cap B^c$.
If $z \in A_2$: As $z \in A_2$ we get that $z \in A^c$ and hence $Re(z) > 0$ implying that $Re(\frac{1}{z}) > 0$ as well.

$$\left|\frac{f(z)}{z^n}\right| \geq \left|\alpha_n + \frac{\alpha_{n-1}}{z}\right| - \left|\sum_{k=0}^{n-2} \alpha_k z^{k-n}\right| = \left|\alpha_n + \frac{\alpha_{n-1}}{z}\right| - \left|\sum_{k=2}^{n} \frac{\alpha_{n-k}}{z^k}\right| \Rightarrow$$

$$\left|\frac{f(z)}{z^n}\right| \geq \left|\alpha_n + \frac{\alpha_{n-1}}{z}\right| - \sum_{k=2}^{n} \frac{|\alpha_{n-k}|}{|z|^k} > Re\Big(\alpha_n + \frac{\alpha_{n-1}}{z}\Big) - \sum_{k=2}^{\infty} \frac{m\alpha_n}{|z|^k} \Rightarrow$$

$$\left|\frac{f(z)}{z^n}\right| \geq \alpha_n - m\alpha_n\left(\frac{1}{1-\frac{1}{|z|}} - 1 - \frac{1}{|z|}\right) = \frac{\alpha_n(|z|^2 - |z| - m)}{|z|^2 - |z|} > 0 \Rightarrow$$

$$|f(z)| > 0 \quad \text{as } |z| > r_1$$

If $z \in A_1$: then $Re(z) > \frac{r_1}{\sqrt{2}}$ and $|z| \leq r_1$ which implies that $|\arg(z)| < \frac{\pi}{4}$ and hence $|\arg(\frac{1}{z})| < \frac{\pi}{4}$ and $|\arg(\frac{1}{z^2})| < \frac{\pi}{2}$. Therefore we have that $Re(\frac{1}{z}) \geq 0$ and $Re(\frac{1}{z^2}) \geq 0$. As in the above case we get that :

$$\left|\frac{f(z)}{z^n}\right| \geq \left|\alpha_n + \frac{\alpha_{n-1}}{z} + \frac{\alpha_{n-2}}{z^2}\right| - \sum_{k=3}^{n} \frac{m\alpha_n}{|z|^k} > Re(\alpha_n + \frac{\alpha_{n-1}}{z} + \frac{\alpha_{n-2}}{z^2}) - \sum_{k=3}^{\infty} \frac{m\alpha_n}{|z|^k} \Rightarrow$$

$$\left|\frac{f(z)}{z^n}\right| \geq \alpha_n - m\alpha_n\left(\frac{1}{1-\frac{1}{|z|}} - 1 - \frac{1}{|z|} - \frac{1}{|z|^2}\right) = \frac{\alpha_n(|z|^3 - |z|^2 - m)}{|z|^3 - |z|^2} > 0 \Rightarrow$$

$$|f(z)| > 0 \quad \text{as } |z| > r_2$$

Therefore we can conclude that if $z \in A^c$ then $|f(z)| > 0$. □

Proposition 2.2.3. *Let* $f(x) = \sum_{k=0}^{n} \alpha_k x^k \in \mathbb{Z}[x]$ *be a polynomial with* $\alpha_n > 0$, $\alpha_{n-1} \geq 0$, $\alpha_{n-2} \geq 0$. *Let* $b \in \mathbb{N}$, *we set*

$$B = \begin{cases} 1 & \text{if } b = 2 \\ \dfrac{(2b-1)(2b-1-\sqrt{2})}{2} & \text{if } b \geq 3 \end{cases}$$

If $\frac{|a_k|}{a_n} \leq B$ *for* $k = 0, 1, \dots, n-2$ *then* $b > \max\{\frac{r_1}{\sqrt{2}}, r_2\} + \frac{1}{2}$ *where* r_1, r_2 *are like in the previous proposition.*

Proof. Let r_1^* and r_2^* be the positive roots of $x^2 - x - B$ and $x^3 - x^2 - B$ respectively. Our hypothesis implies that $m = \max\{\frac{|a_k|}{a_n}\} \leq B$ and therefore $r_1 \leq r_1^*$ and $r_2 \leq r_2^*$ respectively. So it is sufficient to show that $b > \max\{\frac{r_1^*}{\sqrt{2}}, r_2^*\} + \frac{1}{2}$. We have that $\frac{r_1^*}{\sqrt{2}}$ is root of $h(x) = 2x^2 - \sqrt{2}x - B$, but $h(b - \frac{1}{2}) = \frac{1}{2}(2b-1)(2b-1-\sqrt{2}) - B > 0$ by the definition of B. Hence we get $b - \frac{1}{2} > \frac{r_1^*}{\sqrt{2}}$. Also if we set $g(x) = x^3 - x^2 - B$ then $g(b - \frac{1}{2}) = (b - \frac{1}{2})^2(b - \frac{3}{2}) - B > 0$ and therefore $b - \frac{1}{2} > r_2^*$. So finally we get $b - \frac{1}{2} > \max\{\frac{r_1}{\sqrt{2}}, r_2\}$.

□

In our case we have that $f(x) = \sum_{k=0}^{d} \alpha_k x^k$ where $\alpha_d = 1$, $0 \leq \alpha_k < b$ for $k = 0, \dots, d-1$ and $f(m) = n$, $m \geq 3$. As $m \geq 3$ and $0 \leq \alpha_k$ not all equal to zero, we get that $f(m-1) = \sum_{k=0}^{d} \alpha_k (m-1)^k > 0$. Additionally $\frac{|\alpha_k|}{\alpha_n} < \frac{m}{1} = m$. Hence if we show that $m \leq \frac{(2m-1)(2m-1-\sqrt{2})}{2} - 1$ the conditions of the above proposition will be satisfied. Indeed, the desired inequality is equivalent to $4m^2 - (6+2\sqrt{2})m + \sqrt{2} - 1 \geq 0$ and the solutions of the quadratic equation $4x^2 - (6+2\sqrt{2})x + \sqrt{2} - 1 = 0$ are

$x_1 = \dfrac{3 + \sqrt{2} - \sqrt{15 + 2\sqrt{2}}}{4} \approx 0.004$ and

$x_2 = \dfrac{3 + \sqrt{2} + \sqrt{15 + 2\sqrt{2}}}{4} \approx 2.15$. Hence as $m \geq 3$ the desired inequality holds and therefore Proposition 2.2.3 as well. Then Proposition 2.2.3 implies Proposition 2.2.2 and Proposition 2.2.2 combined with the fact $f(m-1) \neq 0$ implies Proposition 2.2.1. So, finally we get that a non-trivial factorization of the polynomial induced by the base-m algorithm implies a non-trivial factorization of n.

We are now going to prove two lemmas concerning the polynomial $f(x)$ which we are going to use later. At this point we are going to make the assumption that $n > 2^{d^2}$ which is realistic as in practice when we use the GNFS in order to factor a number n it will be greater than 10^{100} whereas d will be about 5.

Lemma 2.2.4. *Let $f(x) = c_d x^d + c_{d-1}x^{d-1} + ... + c_1 x + c_0$ be the polynomial induced by the base$-m$ algorithm. Then $c_d = 1$ and $c_{d-1} \leq d$.*

Proof.
If $i = 0$ then $\binom{d}{i} = 1 \leq 2^d - 2$
If $i = d$ then $\binom{d}{i} = 1 \leq 2^d - 2$
If $0 < i < d$ then $\binom{d}{i} \leq \sum_{j=1}^{d-1} \binom{d}{j} = 2^d - 2 \leq n^{1/d} - 2 \leq [n^{1/d}] + 1 - 2 = m - 1$

We have that $m^d \leq n \leq (m+1)^d$ so $m^d \leq c_d m^d + \sum_{i=0}^{d-1} c_i m^i < m^d + \sum_{i=0}^{d-1} \binom{d}{i} m^i \Rightarrow$
$0 \leq (c_d - 1)m^d + \sum_{i=0}^{d-1} c_i m^i < \sum_{i=0}^{d-1} \binom{d}{i} m^i$ Hence,
$(c_d - 1)m^d < \sum_{i=0}^{d-1} \binom{d}{i} m^i \leq (m-1) \sum_{i=0}^{d-1} m^i = (m-1)\frac{m^d - 1}{m-1} = m^d - 1 < m^d$
so $(c_d - 1)m^d < m^d \Rightarrow c_d < 2$ which implies that $c_d = 0$ or $c_d = 1$. If $c_d = 0$ then $m^d \leq \sum_{i=0}^{d-1} c_i m^i \leq (m-1) \sum_{i=0}^{d-1} m^i = (m-1)\frac{m^d - 1}{m-1} = m^d - 1$ contradiction. Therefore $c_d = 1$.
As $c_d = 1$ we have that $0 \leq \sum_{i=0}^{d-1} c_i m^i < \sum_{i=0}^{d-1} \binom{d}{i} m^i \Rightarrow c_{d-1}m^{d-1} + \sum_{i=0}^{d-2} c_i m^i <$
$dm^{d-1} + \sum_{i=0}^{d-2} \binom{d}{i} m^i \Rightarrow (c_{d-1} - d)m^{d-1} < \sum_{i=0}^{d-2} \binom{d}{i} m^i \leq (m-1) \sum_{i=0}^{d-2} m^i =$
$(m-1)\frac{m^{d-1} - 1}{m-1} = m^{d-1} - 1 < m^{d-1} \Rightarrow c_{d-1} - d < 1 \Rightarrow c_{d-1} - d \leq 0 \Rightarrow$
$c_{d-1} \leq d$ □

Lemma 2.2.5. *Let $\Delta(f)$ be the discriminant of the polynomial $f(x)$ then $\Delta(f) < d^{2d} n^{2-\frac{3}{d}}$.*

Proof. For the discriminant of $f(x)$ we have that $\Delta(f) = (-1)^{\frac{d(d-1)}{2}} \frac{1}{c_d} Res(f, f')$. Also $Res(f, f') = det(A)$,

$$A = \begin{pmatrix} c_d & c_{d-1} & ... & c_0 & 0 & ... & 0 \\ 0 & c_d & ... & c_1 & c_0 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & ... & c_d & c_{d-1} & ... & c_0 \\ dc_d & (d-1)d_{d-1} & ... & c_1 & 0 & ... & 0 \\ 0 & dc_d & ... & c_2 & c_1 & ... & c_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & ... & dc_d & (d-1)c_{d-1} & ... & c_0 \end{pmatrix}$$

where A is a $(2d-1)\times(2d-1)$ matrix. Next we try to correlate matrix A with one which will have elements of absolute value at most 1. In order to achieve that we do the following.
1) We divide the last d rows by d.
2) We divide the last $2d-3$ columns by m.
3) We subtract c_{d-1} times the first column from the second column.
After these three steps the elements of the resulting matrix A' will have absolute value at most 1. Therefore the first $d-1$ rows vectors will have length at most $\sqrt{d+1}$ and the last d row vectors at most $\sqrt{d}$. Let v_i be the row vectors of the matrix A', it holds that $det(A') \leq \prod_{i=1}^{2d-1} ||v_i||$. Hence we get that $det(A') \leq (d+1)^{\frac{d-1}{2}} d^{\frac{d}{2}}$. Combining that with the fact that $c_d = 1$ as we showed in the previous Lemma we conclude that $|\Delta(f)| \leq d^d m^{2d-3} det(A') \leq d^d n^{2-\frac{3}{d}} det(A') \Rightarrow |\Delta(f)| \leq d^d n^{2-\frac{3}{d}} (d+1)^{\frac{d-1}{2}} d^{\frac{d}{2}} = d^{\frac{3d}{2}} n^{2-\frac{3}{d}} (d+1)^{\frac{d-1}{2}} < d^{2d} n^{2-\frac{3}{d}}$. The last inequality follows by the fact that $(d+1)^{d-1} \leq d^d$. Indeed, in order to prove that it suffices to prove that $(d-1)\log(d+1) \leq d\log d$. If we consider $f(x) = (x-1)\log(x+1) - x\log x$ for $x \geq 1$ and take its derivative $f'(x) = \log(\frac{x+1}{x}) - \frac{2}{x+1}$ we can show that $f'(x) \leq 0$ for $x \geq 1$. The last inequality follows by the fact that $\log x \leq x-1$ for $x \geq 1$. Therefore as $f'(x) \leq 0$ for $x \geq 2$ we have that $f(x) \leq f(2) < f(1) = 0$ which implies the desired result. □

2.3 Sieving

During the sieving step our goal is like in the case of SNFS to find a sufficient number of pairs (a,b) such that $a+bm$ and $a+b\theta$ are smooth. However for the algebraic part we are going to work with ideals of $\mathbb{Z}[\theta]$ instead of algebraic integers. Like in the case of R_K we have that,

Proposition 2.3.1. *Let $f(x)$ be a monic, irreducible polynomial with integer coefficients and $\theta \in \mathbb{C}$ a root of $f(x)$. The set of pairs (r,p) where p is a prime integer and r is an integer such that $f(r) \equiv 0 \pmod{p}$ is in bijective correspondence with the set of all first degree prime ideals of $\mathbb{Z}[\theta]$.*

Proof. Let $\mathfrak{p}$ be a first degree prime ideal of $\mathbb{Z}[\theta]$. Then $[\mathbb{Z}[\theta] : \mathfrak{p}] = p$ for some prime p and hence $\mathbb{Z}[\theta]/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$. There is a canonical ring epimorphism $\phi : \mathbb{Z}[\theta] \to \mathbb{Z}[\theta]/\mathfrak{p}$ such that $\ker\phi = \mathfrak{p}$. Since $\mathbb{Z}[\theta]/\mathfrak{p}$ it follows that ϕ can also be thought as an epimorphism of rings $\phi : \mathbb{Z}[\theta] \to \mathbb{Z}/p\mathbb{Z}$ with $\ker\phi = \mathfrak{p}$. Hence the elements in $\mathfrak{p}$ map to integers which are divisible by p and any such integer is the image of an element in $\mathfrak{p}$.
Let $r = \phi(\theta) \in \mathbb{Z}/p\mathbb{Z}$. If $f(x) = x^d + a_{d-1}x^{d-1} + ... + a_1 x + a_0$ then $\phi(f(\theta)) \equiv 0$

$(\mathrm{mod}\ p)$ as $f(\theta) = 0$ and hence

$$\begin{aligned} 0 &\equiv \phi(f(\theta)) \\ &\equiv \phi(\theta^d + a_{d-1}\theta^{d-1} + ... + a_1\theta + a_0) \\ &\equiv \phi(\theta)^d + a_{d-1}\phi(\theta)^{d-1} + ... + a_1\phi(\theta) + a_0 \\ &\equiv r^d + a_{d-1}r^{d-1} + ... + a_1 r + a_0 \\ &\equiv f(r) \pmod{p} \end{aligned}$$

Therefore r is a root of $f(x)\ (\mathrm{mod}\ p)$ and the ideal $\mathfrak{p}$ determines a unique pair (r, p). Conversely, let p be a prime integer and $r \in \mathbb{Z}/p\mathbb{Z}$ with $f(r) \equiv 0\ (\mathrm{mod}\ p)$. Then there is a natural ring epimorphism that maps polynomials in θ to polynomials in r. In particular $\sum_{i=0}^{d-1} a_i\theta^i \mapsto \sum_{i=0}^{d-1} a_i r^i\ (\mathrm{mod}\ p)$. Let $\mathfrak{p} = \ker\phi$ so that $\mathfrak{p}$ is an ideal of $\mathbb{Z}[\theta]$. Since ϕ is onto and $\mathfrak{p} = \ker\phi$ it follows that $\mathbb{Z}[\theta]/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$ and hence $[\mathbb{Z}[\theta] : \mathfrak{p}] = p$ and $\mathfrak{p}$ is therefore a first degree prime ideal of $\mathbb{Z}[\theta]$. Thus the pair (r, p) determines a unique first degree prime ideal $\mathfrak{p}$ which in turn determines the unique pair (r, p) consistent with the first part of the proof. □

The above result actually enables us to find the sets **G** and **Q** of the factor base as we have already seen in the previous chapter how to determine the pairs (r, p).

In order to examine if $a + b\theta$ is smooth we are going to use its norm once again.

$$\begin{aligned} N(a + b\theta) &= \sigma_1(a + b\theta)\sigma_2(a + b\theta) ... \sigma_d(a + b\theta) \\ &= (a + b\theta^{(1)})(a + b\theta^{(2)}) ... (a + b\theta^{(d)}) \\ &= b^d(\frac{a}{b} + \theta^{(1)})(\frac{a}{b} + \theta^{(2)}) ... (\frac{a}{b} + \theta^{(d)}) \\ &= (-b)^d(-\frac{a}{b} - \theta^{(1)})(-\frac{a}{b} - \theta^{(2)}) ... (-\frac{a}{b} - \theta^{(d)}) \\ &= (-b)^d f(-\frac{a}{b}) \end{aligned}$$

In the case of R_K we had that if $< a + b\theta > = {\mathfrak{p}_1}^{e_1}{\mathfrak{p}_2}^{e_2} ... {\mathfrak{p}_k}^{e_k}$

$$\begin{aligned} |N(a + b\theta)| &= N(< a + b\theta >) \\ &= N({\mathfrak{p}_1}^{e_1}{\mathfrak{p}_2}^{e_2} ... {\mathfrak{p}_k}^{e_k}) \\ &= N(\mathfrak{p}_1)^{e_1} N(\mathfrak{p}_2)^{e_2} ... N({\mathfrak{p}_k}^{e_k}) \\ &= ({p_1}^{f_1})^{e_1}({p_2}^{f_2})^{e_2} ... ({p_k}^{f_k})^{e_k} \end{aligned}$$

But $\mathbb{Z}[\theta]$ may not be a Dedekind domain ($R_K \neq \mathbb{Z}[\theta]$) so we will have to generalize the concept of factorization in ideals in $\mathbb{Z}[\theta]$. We will show that the concept of the exponents e_i can be generalized for first degree prime ideals of $\mathbb{Z}[\theta]$. In order to do that we initially

observe that the exponents e_i can be seen as group homomorphisms $e_{\mathfrak{p}_i} : \mathbb{Q}(\theta)^* \to \mathbb{Z}$. These homomorphisms possess the following properties.
i) $e_{\mathfrak{p}_i}(\beta) \geq 0 \quad \forall \beta \in \mathbb{Z}[\theta]^*$
ii) $e_{\mathfrak{p}_i}(\beta) > 0$ if and only if $\mathfrak{p}_i \mid < \beta >$.
iii) $e_{\mathfrak{p}_i}(\beta) = 0$ for all but finitely many $\mathfrak{p}_i$ of R_K and $|N(\beta)| = \prod N(\mathfrak{p}_i)^{e_{\mathfrak{p}_i}}$
The following result holds.

Proposition 2.3.2. *For every prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\theta]$ there is a group homomorphism $l_{\mathfrak{p}} : K^* \to \mathbb{Z}$ such that:*
i) $l_{\mathfrak{p}}(\beta) \geq 0 \quad \forall \beta \in \mathbb{Z}[\theta]^*$
ii) If $\beta \in \mathbb{Z}[\theta]^*$ then $l_{\mathfrak{p}}(\beta) > 0$ if and only if $\beta \in \mathfrak{p}$.
iii) If $\beta \in K^*$ then $l_{\mathfrak{p}}(\beta) = 0$ for all but finitely many $\mathfrak{p}$ and $|N(\beta)| = \prod N(\mathfrak{p})^{l_{\mathfrak{p}}(\beta)}$ where $\mathfrak{p}$ ranges over the set of all prime ideals of $\mathbb{Z}[\theta]$.

We are going to prove the above proposition more generally for an order A of R_K and then for $A = \mathbb{Z}[\theta]$ we will get the above result. In order to do that we need some concepts of modules.

Definition 2.3.3. *Let R be a commutative ring. An $R-$module is an (additive) abelian group M equipped with a scalar multiplication $R \times M \to M$ denoted by $(r, m) \mapsto rm$ such that the following axioms hold for all $m, m' \in M$ and all $r, r' \in R$.*
i) $r(m + m') = rm + rm'$
ii) $(r + r')m = rm + r'm$
iii)$(rr')m = r(r'm)$
iv) $1m = m$

Definition 2.3.4. *If M is an R-module, then a submodule N of M, denoted by $N \subseteq M$, is an additive subgroup N of M closed under scalar multiplication: $rn \in N$ whenever $n \in N$ and $r \in R$.*

Definition 2.3.5. *An $R-$module M is called simple if it does not have any proper submodules apart from 0.*

Definition 2.3.6. *An $R-$module $M$is said to have finite length if there is a chain*

$$M = M_n \supset ... \supset M_1 \supset M_0 = 0$$

of submodules of M such that M_i/M_{i-1} is a simple $R-$module for $i = 1, ..., n$

Theorem 2.3.7 (Jordan-Holder)**.** *Let M be an $R-$module of finite length and let*

$$M = M_n \supset ... \supset M_1 \supset M_0 = 0 \quad \textit{and}$$

$$M = N_m \supset ... \supset N_1 \supset N_0 = 0$$

be like above. Then $n = m$ and $M_i/M_{i-1} \cong N_i/N_{i-1}$ for $i = 1, ..., n$.

Proposition 2.3.8. *Let K be a number field and A an order of K. For every prime ideal $\mathfrak{p}$ of A there is a group homomorphism $l_{\mathfrak{p}} : K^* \to \mathbb{Z}$ with the following properties. i)* $l_{\mathfrak{p}}(x) \geq 0 \quad \forall\, x \in A^*$
ii) If $x \in A^*$ then $l_{\mathfrak{p}}(x) > 0$ if and only if $x \in \mathfrak{p}$.
iii) Let $x \in K^*$ then $l_{\mathfrak{p}}(x) = 0$ for all but finitely many $\mathfrak{p}$ and $|N(x)| = \prod N(\mathfrak{p})^{l_{\mathfrak{p}}(x)}$ where $\mathfrak{p}$ ranges over the set of all prime ideals of A.

Proof. Initially we construct the functions $l_{\mathfrak{p}}$. Let $\mathfrak{p}$ be a prime ideal of A and $x \in A\,, x \neq 0$. We have that $\#A/xA = |N(x)|$ so there is a finite chain of ideals

$$A = P_0 \supset P_1 \supset \dots P_{t-1} \supset P_t = xA$$

with $P_i \neq P_{i+1}$ for $i = 0, \dots, t-1$ and there is no P' such that $P_i \supset P' \supset P_{i+1}$. We define $l_{\mathfrak{p}} := \#\{i \in \{1, 2, \dots, t\} | P_{i-1}/P_i \cong A/\mathfrak{p}\}$ The map $l_{\mathfrak{p}}$ is well defined as it does not depend on the choice of the above chain. This follows by the Jordan-Holder theorem mentioned above for A/xA. In order to apply the theorem it suffices to show that P_{i-1}/P_i is a simple module. If it was not a simple module then there would exist a B/P_i such that $P_i/P_i \subset B/P_i \subset P_{i-1}/P_i$ which implies that $P_i \subset B \subset P_{i-1}$ contradiction. Hence P_{i-1}/P_i is a simple module. Let $x, y \in A\,,\, x, y \neq 0$ and $A = P_0 \supset P_1 \supset \dots P_{t-1} \supset P_t = xA$ and $A = Q_0 \supset Q_1 \supset \dots Q_{s-1} \supset Q_s = yA$. This two chains can be combined in the following one,

$$A = P_0 \supset P_1 \supset \dots P_{t-1} \supset P_t = xA = xQ_0 \supset xQ_1 \supset \dots xQ_{s-1} \supset xQ_s = xyA$$

and therefore for xy we have that

$$\begin{aligned} l_{\mathfrak{p}}(xy) &= \#\{i \in \{1, 2, \dots, t\} | P_{i-1}/P_i \cong A/\mathfrak{p}\} + \#\{i \in \{1, 2, \dots, s\} | xQ_{i-1}/xQ_i \cong A/\mathfrak{p}\} \\ &= l_{\mathfrak{p}}(x) + l_{\mathfrak{p}}(y) \end{aligned}$$

So we have shown that $l_{\mathfrak{p}}$ is a group homomorphism from A^* to $\mathbb{Z}$. We know that the fractions field of A is K therefore we can extend $l_{\mathfrak{p}}$ in K^* as follows

$$l_{\mathfrak{p}}\left(\frac{x}{y}\right) = l_{\mathfrak{p}}(x) - l_{\mathfrak{p}}(y)$$

Now we are left to prove that for $l_{\mathfrak{p}}$ the properties (i), (ii) and (iii) hold.
By the definition of $l_{\mathfrak{p}}$ we have that $l_{\mathfrak{p}}(x) \geq 0 \quad \forall\, x \in A^*$ so (i) holds.
For (ii): Let $x \in \mathfrak{p}$, we then take $P_1 = \mathfrak{p}$ and hence $l_{\mathfrak{p}}(x) \geq 0$.
Conversely, let $l_{\mathfrak{p}}(x) \geq 0$. If $x \notin \mathfrak{p}$ then as $\mathfrak{p}$ is maximal $xA + \mathfrak{p} = A$ so there are $y \in A$, $z \in \mathfrak{p}$ such that $xy + z = 1 \Rightarrow z - 1 = xy \Rightarrow z \in 1 + xA \Rightarrow z \equiv 1 \pmod{xA}$. Therefore multiplication by z induces the identity map $A/xA \to A/xA$. But $A/xA \cong \prod_{i=1}^{t} P_{i-1}/P_i$ so multiplication by z induces the identity map in all of the

P_{i-1}/P_i. As $l_{\mathfrak{p}}(x) \geq 0$ there is a $j \in \{1, \dots, t\}$ such that $P_{j-1}/P_j \cong A/\mathfrak{p}$. Therefore multiplication by z induces the identity map in $A/\mathfrak{p}$, contradiction. Hence, $x \in \mathfrak{p}$.
For (iii): Let $x \in K^*$ then $x = \frac{y}{z}$ with $y, z \in A$. It suffices to prove (iii) for A^* as $l_{\mathfrak{p}}(x) = l_{\mathfrak{p}}(y) - l_{\mathfrak{p}}(z)$ and then $|N(x)| = \left|\frac{N(y)}{N(z)}\right| = \frac{\prod_{\mathfrak{p}} N(\mathfrak{p})^{l_{\mathfrak{p}}(y)}}{\prod_{\mathfrak{p}} N(\mathfrak{p})^{l_{\mathfrak{p}}(z)}} = \prod N(\mathfrak{p})^{l_{\mathfrak{p}}(y)-l_{\mathfrak{p}}(z)} = \prod N(\mathfrak{p})^{l_{\mathfrak{p}}(x)}$.
Let $x \in A^*$ with $A = P_0 \supset \dots \supset p_{t-1} \supset P_t = xA$. But $|N(x)| = \#A/xA$ and $A/xA \cong \prod_{i=1}^{t} P_{i-1}/P_i \Rightarrow |N(x)| = \prod_{i=1}^{t} \#P_{i-1}/P_i$. Therefore in order to show (iii) it suffices to prove that for each $i = 1, \dots, t$ there is a unique prime ideal $\mathfrak{p}$ of A such that $P_{i-1}/P_i \cong A/\mathfrak{p}$. Let $y \in P_{i-1}$ and $y \notin P_i$. As there is no ideal properly between P_{i-1} and P_i we get that $yA + P_i = P_{i-1}$. Hence multiplication by y induces an epimorphism $\phi : A \to P_{i-1}/P_i$ such that $a \mapsto ya + P_i$. Indeed this homomorphism is onto as we want $\forall\, b \in P_{i-1}$ to $\exists a \in A$ such that $ay \equiv b \pmod{P_i}$ which is true as $yA + P_i = P_{i-1}$. Therefore there is an ideal $\mathfrak{p}(= \ker\phi)$ such that $A/\mathfrak{p} \cong P_{i-1}/P_i$. But P_{i-1}/P_i has no proper submodules and hence $\mathfrak{p}$ is maximal and so prime as well. Finally $\mathfrak{p}$ is the annihilator of P_{i-1}/P_i and therefore uniquely determined. □

Corollary 2.3.9. *Let $\beta \in \mathbb{Z}[\theta]$ with $\beta = a + b\theta$, $\gcd(a, b) = 1$ and $\mathfrak{p}$ a prime ideal of $\mathbb{Z}[\theta]$. Then for the homomorphism $l_{\mathfrak{p}}$ it holds that $l_{\mathfrak{p}}(\beta) = 0$ if $\mathfrak{p}$ is not of degree 1 and if $\mathfrak{p}$ is of degree 1 that corresponds to the pair (r, p) then*

$$l_{\mathfrak{p}}(\beta) = \begin{cases} ord_p N(\beta) & \text{if } a \equiv -br \pmod{p} \\ 0 & \text{otherwise} \end{cases}$$

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\theta]$ with $l_{\mathfrak{p}}(a + b\theta) > 0$ then $\mathfrak{p}$ is the kernel of a canonical epimorphism $\phi : \mathbb{Z}[\theta] \to \mathbb{Z}[\theta]/\mathfrak{p}$. But $\mathbb{Z}[\theta]/\mathfrak{p} \cong \mathbb{F}_q, q = p^e$. We will show that $Im\phi = \mathbb{F}_p$ and hence $\mathbb{Z}[\theta]/\ker\phi \cong \mathbb{F}_p$. But $\ker\phi = \mathfrak{p}$ and so $\mathbb{Z}[\theta]/\mathfrak{p} \cong \mathbb{F}_p$ which implies that $\mathfrak{p}$ is of degree 1. The fact that $l_{\mathfrak{p}}(a + b\theta) > 0$ implies that $a + b\theta \in \mathfrak{p}$ by the previous proposition. Therefore $a + b\theta \in \ker\phi \Rightarrow \phi(a + b\theta) \equiv 0 \pmod{p}$
$\Rightarrow a + b\phi(\theta) \equiv 0 \pmod{p}$. But $p \nmid b$ as if $p \mid b$ then $p \mid a \Rightarrow p \mid \gcd(a, b) = 1$ contradiction. So finally, $\phi(\theta) \equiv -ab^{-1} \pmod{p} \Rightarrow \phi(\mathbb{Z}[\theta]) \subseteq \mathbb{F}_p$ and we also have that $\mathbb{F}_p \subseteq \phi(\mathbb{Z}[\theta])$ hence $\phi(\mathbb{Z}[\theta]) = \mathbb{F}_p$.
In order to prove the second part we will use (iii) of the previous proposition, which states that $|N(\beta)| = \prod_{\mathfrak{p}} N(\mathfrak{p})^{l_{\mathfrak{p}}(\beta)}$. However, by the first part of the corollary we have that $|N(\beta)| = \prod_{\mathfrak{p}, f(\mathfrak{p}/p\mathbb{Z})=1} N(\mathfrak{p})^{l_{\mathfrak{p}}(\beta)}$ where the $\mathfrak{p}$ that appear in the product on the right with $l_{\mathfrak{p}}(\beta) > 0$ correspond to pairs (r, p). For these ideals we get that $N(\mathfrak{p}) \mid N(\beta) \Rightarrow$

$p \mid (-b)^d f(\frac{-a}{b})$ so as $p \nmid b$ this implies that $p \mid f(\frac{-a}{b}) \Rightarrow$
$-ab^{-1} \equiv r \pmod{p} \Rightarrow a \equiv -br \pmod{p}$. Lets assume that there are two ideals $\mathfrak{p}_1, \mathfrak{p}_2$ of degree 1 such that $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$ corresponding to the pairs (r_1, p) and (r_2, p) which appear in the product. Then we would have that $a \equiv -br_1 \pmod{p}$ and $a \equiv -br_2 \pmod{p}$ which imply that $r_1 \equiv r_2 \pmod{p}$ as $p \nmid b$. The pairs (r, p) are in bijective correspondence with the ideals of degree 1 and therefore $\mathfrak{p}_1 = \mathfrak{p}_2$. So finally for each prime p that appear in the factorization of $N(\beta)$ there is exactly one prime ideal $\mathfrak{p}$ with $N(\mathfrak{p}) = p$ and hence

$$l_{\mathfrak{p}}(\beta) = \begin{cases} ord_p N(\beta) & \text{if } a \equiv -br \pmod{p} \\ 0 & \text{otherwise} \end{cases}$$

□

The above corollary indicates for which ideals we will have $l_{\mathfrak{p}}(a + b\theta) > 0$ and therefore justifies our choice for the set **G**. It also gives us a condition (as in the case of SNFS) of when $l_{\mathfrak{p}}(a + b\theta) > 0$ and actually a way to compute that value.
As in the case of SNFS for each pair (a, b) which we keep as a relation the exponents of the primes occurring in the factorization of $a + bm$ and the values $l_{\mathfrak{p}}(a + b\theta)$ are kept for the linear algebra step. However as we work with ideals of $\mathbb{Z}[\theta]$ instead of algebraic integers these will cause some extra obstructions in our way of constructing a square of an element in $\mathbb{Z}[\theta]$.

Proposition 2.3.10. *Let S be a finite set of pairs (a, b) such that $\gcd(a, b) = 1$ and also $\prod_{(a,b)\in S} (a + b\theta) = \gamma^2$ with $\gamma \in \mathbb{Q}(\theta)$ then $\sum_{(a,b)\in S} l_{\mathfrak{p}}(a + b\theta) \equiv 0 \pmod{2}$ for every prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\theta]$.*

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\theta]$. As $l_{\mathfrak{p}}$ is a group homomorphism then

$$\begin{aligned} \sum_{(a,b)\in S} l_{\mathfrak{p}}(a + b\theta) &= l_{\mathfrak{p}}\Big(\prod_{(a,b)\in S} (a + b\theta) \Big) \\ &= l_{\mathfrak{p}}(\gamma^2) \\ &= 2l_{\mathfrak{p}}(\gamma) \equiv 0 \pmod{2} \end{aligned}$$

□

The above result gives a necessary condition for $\prod_{(a,b)\in S} (a + b\theta)$ to be a square of an element in $K = \mathbb{Q}(\theta)$. However this condition is not sufficient. In our way to construct a square in $\mathbb{Z}[\theta]$ given only that $\sum_{(a,b)\in S} l_{\mathfrak{p}}(a + b\theta) \equiv 0 \pmod{2}$ we will face the following obstructions:

1) The ideal $\left(\prod_{(a,b)\in S}(a+b\theta)\right)R_K$ may not be a square of an ideal as we work with prime ideals of $\mathbb{Z}[\theta]$.
2) Even if $\left(\prod_{(a,b)\in S}(a+b\theta)\right)R_K = I^2$ for some ideal I of R_K the ideal I may not be principal.
3) Even if $\left(\prod_{(a,b)\in S}(a+b\theta)\right)R_K = <\gamma>^2$ with $\gamma \in R_K$ it may not hold that $\prod_{(a,b)\in S}(a+b\theta) = \gamma^2$.
4) Even if $\prod_{(a,b)\in S}(a+b\theta) = \gamma^2$ with $\gamma \in R_K$ it may not hold that $\gamma \in \mathbb{Z}[\theta]$.

The easiest of the four obstructions is the last one. Assume that we have found a set S such that $\prod_{(a,b)\in S}(a+b\theta) = \gamma^2$ with $\gamma \in K$. Then $\gamma \in R_K$. Indeed, as $\prod_{(a,b)\in S}(a+b\theta) = \gamma^2$ then $\gamma^2 \in \mathbb{Z}[\theta] \subseteq R_K$. This implies that there is a monic $f(x) \in \mathbb{Z}[x]$ such that $f(\gamma^2) = 0$. If we set $g(x) = f(x^2)$ then $g(x) \in \mathbb{Z}[x]$ and is monic as well and as $g(\gamma) = f(\gamma^2) = 0$ we get that $\gamma \in \tilde{\mathbb{Z}}$. But we also have that $\gamma \in K$ so $\gamma \in R_K$. Moreover $\gamma f'(\theta) \in \mathbb{Z}[\theta]$ by [20, prop. 3-7-14] so $f'(\theta)^2 \prod_{(a,b)\in S}(a+b\theta) = \delta^2$ with $\delta \in \mathbb{Z}[\theta]$. Therefore by doing this modification in the end we showed that it suffices to find a set S of pairs (a,b) such that $\prod_{(a,b)\in S}(a+b\theta) = \gamma^2$ with $\gamma \in K$.

Proposition 2.3.11. *Let S be a finite set of pairs (a,b) such that $\prod_{(a,b)\in S}(a+b\theta) = \gamma^2$ with $\gamma \in K$. Let also $\mathfrak{q}$ be a first degree prime ideal which corresponds to the pair (s,q) and such that $a+bs \not\equiv 0 \pmod q \quad \forall\,(a,b) \in S$ and $f'(s) \not\equiv 0 \pmod q$. It then holds that $\prod_{(a,b)\in S}\chi_{\mathfrak{q}}(a+b\theta) = 1$*

Proof. Initially we define the map $\chi_{\mathfrak{q}}$. Let $\phi : \mathbb{Z}[\theta] \to \mathbb{Z}/q\mathbb{Z}$ such that $\sum_{i=0}^{d-1} a_i\theta^i \mapsto \sum_{i=0}^{d-1} a_i s^i \pmod q$. Then ϕ is a ring homomorphism which is onto and $\ker\phi = \mathfrak{q}$. If we restrict ϕ in $\mathbb{Z}[\theta]\setminus\mathfrak{q}$ then the restriction will be onto for $(\mathbb{Z}/q\mathbb{Z})^*$. We define

$$\begin{aligned}\chi_{\mathfrak{q}} : \mathbb{Z}[\theta]\setminus\mathfrak{q} &\to \{\pm 1\}\\ \gamma &\mapsto \left(\frac{\phi(\gamma)}{q}\right)\end{aligned}$$

where $\left(\frac{\phi(\gamma)}{q}\right)$ denotes the Legendre symbol. As we have already seen

$f'(\theta)^2 \prod_{(a,b)\in S}(a+b\theta) = \beta^2$ with $\beta = f'(\theta)\gamma \in \mathbb{Z}[\theta]$ and $\chi_{\mathfrak{q}}(a+b\theta) = \left(\frac{a+bs}{q}\right)$. Additionally $a+b\theta \notin \mathfrak{q}$ and $f'(\theta)^2 \notin \mathfrak{q}$ by the hypotheses of the proposition, hence $\beta^2 \notin \mathfrak{q}$ which in turn follows that $\beta \notin \mathfrak{q}$. Therefore $\chi_{\mathfrak{q}}(\beta)$ and $\chi_{\mathfrak{q}}(\beta^2)$ are defined. We have that $\chi_{\mathfrak{q}}(\beta^2) = \chi_{\mathfrak{q}}(\beta)^2 = 1$ and so

$$\begin{aligned} 1 &= \chi_{\mathfrak{q}}\Big(f'(\theta)^2 \prod_{(a,b)\in S}(a+b\theta)\Big) \\ &= \left(\frac{\phi(f'(\theta))^2 \phi\Big(\prod_{(a,b)\in S}(a+b\theta)\Big)}{q}\right) \\ &= \left(\frac{\phi(f'(\theta))}{q}\right)^2 \left(\frac{\prod_{(a,b)\in S}\phi(a+b\theta)}{q}\right) \\ &= 1 \cdot \prod_{(a,b)\in S}\left(\frac{a+bs}{q}\right) \end{aligned}$$

which gives us the desired result. □

The above proposition gives us another necessary condition for $\prod_{(a,b)\in S}(a+b\theta)$ being a square in K. The above proposition is the reason we had to add the set **Q** of quadratic characters in our factor base. As we will see later if we have that $\sum_{(a,b)\in S} l_{\mathfrak{p}}(a+b\theta) \equiv 0 \pmod 2$ and $\prod_{(a,b)\in S}\chi_{\mathfrak{q}}(a+b\theta) = 1$ for "enough" prime ideals $\mathfrak{q}$ this implies that there is a very good chance $\prod_{(a,b)\in S}(a+b\theta)$ being a square. So our next goal is to examine how big the set **Q** must be.

Let $V = \{\beta \in K^* : l_{\mathfrak{p}}(\beta) \equiv 0 \pmod 2 \text{ for all prime ideals } \mathfrak{p} \text{ of } \mathbb{Z}[\theta]\}$

As $l_{\mathfrak{p}}$ is a group homomorphism we have that V multiplicative subgroup of K^*. Let $\beta \in K^{*2}$ then there is a $\gamma \in K^*$ such that $\beta = \gamma^2$ and hence $\prod_{\mathfrak{p}} N(\mathfrak{p})^{l_{\mathfrak{p}}(\beta)} = |N(\beta)| = |N(\gamma^2)| = |N(\gamma)|^2$. This implies that $l_{\mathfrak{p}}(\beta) \equiv 0 \pmod 2$ $\forall$ $\mathfrak{p}$ prime ideal of $\mathbb{Z}[\theta]$ and therefore $K^{*2} \subseteq V$. If in our factor base we used only the sets **P** and **G** the elements $\prod_{(a,b)\in S}(a+b\theta)$ induced by the linear algebra step would belong to V. We consider the quotient V/K^{*2} as a vector space over $\mathbb{F}_2$. In order to see how much V differs from K^{*2} we will try to give a bound for $\dim_{\mathbb{F}_2} V/K^{*2}$.

Let A, B be two orders of K such that $A \subset B$, $\mathfrak{q}$ a prime ideal of B and $\mathfrak{p} = \mathfrak{q} \cap A$. By $f(\mathfrak{q}/\mathfrak{p})$ we denote the degree of the extension $B/\mathfrak{q} \diagup A/\mathfrak{p}$. Depending on in which order we work we will use the notation $l_{\mathfrak{p},A}$ or $l_{\mathfrak{q},B}$ instead of $l_{\mathfrak{p}}$.

Proposition 2.3.12. *Let $\mathfrak{p}$ be a prime ideal of A. Then we have that*

$$l_{\mathfrak{p},A}(x) = \sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p}) l_{\mathfrak{q},B}(x) \quad \forall\, x \in K^*$$

. By $\mathfrak{q}|\mathfrak{p}$ we refer to the prime ideals $\mathfrak{q}$ of B lying above $\mathfrak{p}$.

Proof. It suffices to prove the proposition for $x \in A$ as if $x \in K^*$ there will exist $y, z \in A$ such that $x = \frac{y}{z}$ and $l_{\mathfrak{p},A}(x) = l_{\mathfrak{p},A}(y) - l_{\mathfrak{p},A}(z)$. we introduce the following notation. If M is an $A-$module of finite length then by $l_{\mathfrak{p},A}(M)$ we denote the number of M_i/M_{i-1} such that $M_i/M_{i-1} \cong A/\mathfrak{p}$ where $M = M_n \supset M_{n-1} \supset ... \supset M_1 \supset M_0 = 0$. Therefore using this notation gives us that $l_{\mathfrak{p},A}(x) = l_{\mathfrak{p},A}(A/xA)\, \forall\, x \in A^*$. Additionally if $L \subseteq M$ it holds that $l_{\mathfrak{p},A}(M) = l_{\mathfrak{p},A}(L) + l_{\mathfrak{p},A}(M/L)$. It is true that $B/A \cong xB/xA$ so $l_{\mathfrak{p},A}(B/A) = l_{\mathfrak{p},A}(xB/xA)$. Then using the previous relation and the fact that $B/xA \diagup A/xA \cong B/A$ we get that $l_{\mathfrak{p},A}(B/xA) = l_{\mathfrak{p},A}(A/xA) + l_{\mathfrak{p},A}(B/A)$. So $l_{\mathfrak{p},A}(x) = l_{\mathfrak{p},A}(A/xA) = l_{\mathfrak{p},A}(B/xA) - l_{\mathfrak{p},A}(B/A) = l_{\mathfrak{p},A}(B/xA) - l_{\mathfrak{p},A}(xB/xA) = l_{\mathfrak{p},A}(B/xB)$. If we set $M = B/xB$ it then suffices to prove that $l_{\mathfrak{p},A}(M) = \sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p}) l_{\mathfrak{q},B}(M)$. Let $M = M_n \supset M_{n-1} \supset ... \supset M_1 \supset M_0 = 0$ then we have that

$$\begin{aligned} l_{\mathfrak{p},A}(M) &= l_{\mathfrak{p},A}(M_n/M_{n-1}) + l_{\mathfrak{p},A}(M_{n-1}) \\ &= l_{\mathfrak{p},A}(M_n/M_{n-1}) + l_{\mathfrak{p},A}(M_{n-1}/M_{n-2}) + ... + l_{\mathfrak{p},A}(M_1/M_0) \end{aligned}$$

All of the M_i/M_{i-1} are simple and therefore it suffices to prove the equality for them. Let N be a simple $B-$module then $N \cong B/\mathfrak{q}'$ for some prime ideal $\mathfrak{q}$ of B and

$$l_{\mathfrak{q},B}(N) = \begin{cases} 1 & \text{if } \mathfrak{q}' = \mathfrak{q} \\ 0 & \text{if } \mathfrak{q}' \neq \mathfrak{q} \end{cases}$$

Let $\mathfrak{p}' = \mathfrak{q}' \cap A$, as an $A-$module N is the direct sum of $f(\mathfrak{q}'/\mathfrak{p}')$ copies of $A/\mathfrak{p}'$ and therefore

$$l_{\mathfrak{p},A}(N) = \begin{cases} f(\mathfrak{q}'/\mathfrak{p}') & \text{if } \mathfrak{p}' = \mathfrak{p} \\ 0 & \text{if } \mathfrak{p}' \neq \mathfrak{p} \end{cases}$$

So finally we have that

$$\begin{aligned} l_{\mathfrak{p},A}(M) &= \sum_{i=1}^{n} \sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p}) l_{\mathfrak{q},B}(M_i/M_{i-1}) \\ &= \sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p}) \sum_{i=1}^{n} l_{\mathfrak{q},B}(M_i/M_{i-1}) \\ &= \sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p}) l_{\mathfrak{q},B}(M) \end{aligned}$$

□

Proposition 2.3.13. *For all but a finitely many prime ideals* $\mathfrak{p}$ *of* A *it holds that* $\sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p}) = 1$. *Additionally the number* $\prod_{\mathfrak{p}} N(\mathfrak{p})^{-1+\sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p})}$ *divides the index* $[B : A]$, *with* $\mathfrak{p}$ *ranging over all prime ideals of* A.

Proof. Let T be a finite set of prime ideals of A and U the set of prime ideals of B lying above those of T. Let P be the intersection of the ideals in T and Q the intersection of the ideals in U. Hence we have that $P = Q \cap A$ and A/P is a subring of B/Q. By the Chinese remainder theorem we have that $A/P \cong \prod_{\mathfrak{p}\in T} A/\mathfrak{p} \Rightarrow \#A/P = \prod_{\mathfrak{p}\in T} N(\mathfrak{p})$. Similarly we have that $\#B/Q = \prod_{\mathfrak{q}\in U} N(\mathfrak{q}) = \prod_{\mathfrak{p}\in T} N(\mathfrak{p})^{\sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p})}$

We have that $[B/Q : A/P] = \#(B/Q)/\#(A/P) = \prod_{\mathfrak{p}\in T} N(\mathfrak{p})^{-1+\sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p})}$. From the construction of Q and P it follows that Q is the only ideal above P and so $[B/Q : A/P] | [B : A]$. This implies that only for finitely many $\mathfrak{p}$ holds that $\sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p}) \neq 1$ not depending in the choice of T. That proves the first part of the proposition. If we take T to be the set of prime ideals $\mathfrak{p}$ such that $\sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p}) \neq 1$ then the second part of the proposition follows by the above proof. □

Let A be an order, we define
$V_A := \{x \in K^* : l_{\mathfrak{p},A}(x) \equiv 0 \pmod 2 \text{ for all prime ideals } \mathfrak{p} \text{ of } A\}$

Proposition 2.3.14. *Let* A, B *be two orders of* K *such that* $A \subset B$. *Then* $V_B \subset V_A$ *and* $[V_A : V_B] \leq [B : A]$.

Proof. By Proposition 2.3.12 we get that if $x \in V_B$ then $x \in V_A$ as $l_{\mathfrak{p},A}(x) = \sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p}) l_{\mathfrak{q},B}(x)$. Hence we get the first part of the proposition. For every

prime ideal $\mathfrak{p}$ of A we construct a set $S_\mathfrak{p}$ of ideals of B as follows:
If $f(\mathfrak{q}/\mathfrak{p}) \equiv 0 \pmod 2 \quad \forall\, \mathfrak{q}|\mathfrak{p}$ then we set $S_\mathfrak{p}$ to be all the prime ideals $\mathfrak{q}$ of B lying above $\mathfrak{p}$.
If there is at least one $\mathfrak{q}|\mathfrak{p}$ such that $f(\mathfrak{q}/\mathfrak{p}) \equiv 1 \pmod 2$ then we choose such an ideal, lets say $\mathfrak{q}_0$ and we set $S_\mathfrak{p}$ to be all the prime ideals $\mathfrak{q}$ of B lying above $\mathfrak{p}$ except $\mathfrak{q}_0$.
It holds that $\#S_\mathfrak{p} \leq -1 + \sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p})$ as $f(\mathfrak{q}/\mathfrak{p}) \geq 2$ if we are in the first case and $f(\mathfrak{q}/\mathfrak{p}) \geq 1$ if we are in the second case. Therefore by Proposition 2.3.13 the set $S_\mathfrak{p}$ will not be empty only for finitely many $\mathfrak{p}$. Let S be the union of all $S_\mathfrak{p}$ where $\mathfrak{p}$ ranges over all prime ideals of A. Then we have that,

$$2^{\#S} \leq \prod_{\mathfrak{p}} 2^{\#S_\mathfrak{p}} \leq \prod_{\mathfrak{p}} N(\mathfrak{p})^{\#S_\mathfrak{p}} \leq \prod_{\mathfrak{p}} N(\mathfrak{p})^{-1+\sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}/\mathfrak{p})} \leq [B : A] \tag{2.1}$$

The last inequality follows by Proposition 2.3.13. We consider the map

$$\begin{aligned} \vartheta \;:\; V_A &\to \mathbb{F}_2^{\#S} \\ x &\mapsto (l_{\mathfrak{q},B}(x) \pmod 2)_{\mathfrak{q}\in S} \end{aligned}$$

which is a group homomorphism.
$\ker\vartheta = \{x \in V_A \;:\; (l_{\mathfrak{q},B}(x) \equiv 0 \pmod 2 \;\forall\, \mathfrak{q} \in S\}$ We will show that $\ker\vartheta = V_B$.
Let $x \in \ker\vartheta$ then $l_{\mathfrak{p},A}(x) \equiv 0 \pmod 2$ for all $\mathfrak{p}$ in A as $x \in V_A$ and $l_{\mathfrak{q},B}(x) \equiv 0 \pmod 2$ for all $\mathfrak{q}$ in S. Let $\mathfrak{q}'$ be a prime ideal of B and $\mathfrak{p}' = \mathfrak{q}' \cap A$.
If $\mathfrak{q}' \in S$ then $l_{\mathfrak{q}',B}(x) \equiv 0 \pmod 2$.
If $\mathfrak{q}' \notin S$ then we distinguish between two cases:
1) If $\sum_{\mathfrak{q}|\mathfrak{p}'} f(\mathfrak{q}/\mathfrak{p}') = 1$ then there is only one ideal above $\mathfrak{p}'$ namely $\mathfrak{q}'$. So by Proposition 2.3.12 we get $l_{\mathfrak{p}',A}(x) = f(\mathfrak{q}'/\mathfrak{p}')l_{\mathfrak{q}',B}(x)$ which in turn implies that $l_{\mathfrak{q}',B}(x) = l_{\mathfrak{p}',A}(x) \equiv 0 \pmod 2$.
2) If $\sum_{\mathfrak{q}|\mathfrak{p}'} f(\mathfrak{q}/\mathfrak{p}') > 1$ then by the fact that $\mathfrak{q}' \notin S$ and $S_\mathfrak{p} \subseteq S$ we have that

$$\sum_{\mathfrak{q}|\mathfrak{p}'} f(\mathfrak{q}/\mathfrak{p}')l_{\mathfrak{q}',B}(x) = f(\mathfrak{q}'/\mathfrak{p}')l_{\mathfrak{q}',B}(x) + \sum_{\mathfrak{q}\in S_{\mathfrak{p}'}} f(\mathfrak{q}/\mathfrak{p}')l_{\mathfrak{q},B}(x)$$

So by Proposition 2.3.12 we get that

$$l_{\mathfrak{p}',A}(x) = f(\mathfrak{q}'/\mathfrak{p}')l_{\mathfrak{q}',B}(x) + \sum_{\mathfrak{q}\in S_{\mathfrak{p}'}} f(\mathfrak{q}/\mathfrak{p}')l_{\mathfrak{q},B}(x)$$

As $\mathfrak{q}' \notin S$ we have that $f(\mathfrak{q}'/\mathfrak{p}') \equiv 1 \pmod 2$, as $\mathfrak{q} \in S_{\mathfrak{p}'} \subseteq S$ we get that $l_{\mathfrak{q},B}(x) \equiv 0 \pmod 2$ and finally as $x \in V_A$ it follows that $l_{\mathfrak{p}',A}(x) \equiv 0 \pmod 2$. Combining all these in the previous relation it follows that $l_{\mathfrak{q}',B}(x) \equiv 0 \pmod 2$. Therefore we

showed that for any prime ideal $\mathfrak{q}'$ of B we have $l_{\mathfrak{q}',B}(x) \equiv 0 \pmod 2$ and hence $\ker\vartheta \subseteq V_B$. Additionally, as $V_B \subset V_A$ it is straightforward that $V_B \subseteq \ker\vartheta$ so finally $\ker\vartheta = V_B$. By the first isomorphism theorem we get that $V_A/V_B \cong Im\vartheta \leq \mathbb{F}_2^{\#S}$. This implies that $\left|V_A/V_B\right| \leq 2^{\#S}$ and so $[V_A : V_B] \leq 2^{\#S}$. Combining that with the inequality in 2.1 we get that $[V_A : V_B] \leq [B : A]$. □

Lemma 2.3.15. *The following inequalities hold:*
i) $\frac{d!}{d^d}(\frac{4}{\pi})^{d/2} < 1$ *with* $d \geq 2$
ii) $d - 1 + d\log d < \frac{3}{2d}\log n$ *with* $d \geq 2$ *and* $n > d^{2d^2}$
iii)$2d(2\log n)^{d-1} < n^{\frac{3}{2d}}$ *with* $d \geq 2$ *and* $n > d^{2d^2}$

For this we refer to [16].

Theorem 2.3.16. *Let* $K = \mathbb{Q}(\theta)$, $d = [K : \mathbb{Q}(\theta)]$ *and* n *such that* $n > d^{2d^2}$. *Let* m , $f(x)$ *be as before, i.e. induced by the base−*m *algorithm and*
$V = \{\beta \in K^* : l_{\mathfrak{p}}(\beta) \equiv 0 \pmod 2$ *for all prime ideals* $\mathfrak{p}$ *of* $\mathbb{Z}[\theta]\}$. *It holds that* $\dim_{\mathbb{F}_2} V/K^{*2} < \frac{\log n}{log2}$.

Comment 2.3.17. *The condition* $n > d^{2d^2}$ *is consistent with the condition needed for Lemma 2.2.4 and in practice will be satisfied as* n *will be very large and therefore we do not have to bother about it.*

Proof. It suffices to prove that $|V/K^{*2}| = [V : K^{*2}] < 2^{\frac{\log n}{log2}} = n$. We set,

$$W = \{\gamma \in K^* : \gamma R_K = I^2 \text{ for some ideal } I \text{ of } R_K\}$$

Using Proposition 2.3.14 with $A = \mathbb{Z}[\theta]$ and $B = R_K$ we get that $W = V_B \subset V_A = V$ and $[V : W] \leq [R_K : \mathbb{Z}[\theta]]$. Let $Y = E(R_K)K^{*2}$, then we get the chain

$$V \supset W \supset Y \supset K^{*2}$$

This chain represents the first three obstructions that we had in our try to construct a square in K^* by an element of V.
We consider the map

$$\begin{aligned} \psi : W &\to Cl(K) \\ \gamma &\mapsto [I] \quad \text{where } \gamma R_K = I^2 \end{aligned}$$

which is a group homomorphism. We now examine the kernel of ψ.

$$\begin{aligned} \ker\psi &= \{\gamma \in W : [I] = 1_{Cl(K)}\} = \{\gamma \in W : I = \langle\delta\rangle\} = \\ &= \{\gamma \in K^* : \gamma R_K = \langle\delta\rangle^2\} = \{\gamma \in K^* : \gamma = \varepsilon\delta^2 , \varepsilon \in E(R_K)\} = Y \end{aligned}$$

Therefore we have that $W/Y \cong Im\psi \leq Cl(K) \Rightarrow [W : Y] \leq h_K$ where h_K is the class number of K. Next we define,

$$\begin{aligned} \phi \ : \ Y &\rightarrow E(R_K)/E(R_K)^2 \\ \varepsilon a^2 &\mapsto \varepsilon E(R_K)^2 \end{aligned}$$

The map ϕ is onto and $\ker \phi = K^{*2}$ and hence we have that $Y/K^{*2} \cong E(R_K)/E(R_K)^2$. If $d = 2s + t$ then by Theorem 1.4.6 the group $E(R_K)$ is spanned by $(s + t - 1) + 1 = s + t = d - s$ elements. Therefore we get that $\dim_{\mathbb{F}_2} E(R_K)/E(R_K)^2 = d - s$.
We are now going to combine all the above results in order to obtain the bound for $\dim_{\mathbb{F}_2} V/K^{*2}$. We have that $V \supset W \supset Y \supset K^{*2}$ so,

$$[V : K^{*2}] = [V : W][W : Y][Y : K^{*2}]$$

Using what we have proved so far we get that,

$$[V : K^{*2}] \leq [R_K : \mathbb{Z}[\theta]]h_k 2^{d-s}$$

Let D_K denote the discriminant of K, then by [11] we have that $h \leq M\dfrac{(d - 1 + \log M)^{d-1}}{(d-1)!}$ where $M = \dfrac{d!}{d^d}\left(\dfrac{4}{\pi}\right)^s \sqrt{|D_K|}$ is the Minkowski constant. Let $\Delta(f)$ be the discriminant of $f(x)$, we have that,

$$M \leq \sqrt{|D_K|} \leq \sqrt{|D_K|}[R_K : \mathbb{Z}[\theta]] = \sqrt{|\Delta(f)|} < d^d n^{1-\frac{3}{2d}}$$

by Lemma 2.2.5.

$$\begin{aligned} [V : K^{*2}] &\leq [R_K : \mathbb{Z}[\theta]]h_k 2^{d-s} \\ &\leq [R_K : \mathbb{Z}[\theta]]\frac{d!}{d^d}\left(\frac{4}{\pi}\right)^s \sqrt{|D_K|}\frac{(d - 1 + \log M)^{d-1}}{(d-1)!}2^{d-s} \\ &\leq \sqrt{|\Delta(f)|}\frac{d!}{d^d(d-1)!}\left(\frac{4}{\pi}\right)^s 2^{d-s}(d - 1 + \log \sqrt{|\Delta(f)|})^{d-1} \\ &\leq \sqrt{|\Delta(f)|}\frac{1}{d^{d-1}}\left(\frac{2}{\pi}\right)^s 2^d(d - 1 + \log \sqrt{|\Delta(f)|})^{d-1} \\ &\leq d^d n^{1-\frac{3}{2d}}\frac{2^d}{d^{d-1}}\left(\frac{2}{\pi}\right)^s (d - 1 + d\log d + (1 - \frac{3}{2d})\log n)^{d-1} \\ &\leq dn^{1-\frac{3}{2d}}2^d(\log n)^{d-1} = n^{1-\frac{3}{2d}}2d(2\log n)^{d-1} \\ &< n^{1-\frac{3}{2d}}n^{\frac{3}{2d}} = n \end{aligned}$$

□

Proposition 2.3.18. *Let k, r be non-negative integers and E a $\mathbb{F}_2$—vector space of dimension k. Then if we choose independently $k+r$ elements of E with the uniform distribution, the probability that these $k+r$ elements span E is at least $1-2^{-r}$.*

Proof. For each hyperplane H of E the probability that all of the $k+r$ elements to belong in H is $(\frac{1}{2})^{k+r}$. Each such hyperplane is the kernel of a uniquely determined non-zero linear map $l : E \to \mathbb{F}_2$. The number of these l is $2^k - 1$ as E is a $\mathbb{F}_2$—vector space of dimension k. Therefore we will have that many hyperplanes as well. That follows that the probability of the $k+r$ vectors which we chose to be in the same hyperplane is $\frac{2^k-1}{2^{k+r}} = 2^{-r} - 2^{-(k+r)} < 2^{-r}$. The $k+r$ which we chose will span E exactly when they do not all lie in the same hyperplane, thus the probability to span E is at least $1-2^{-r}$. □

In the second step of the algorithm, when we defined the set **Q** we demanded it to have about $[3\frac{\log n}{log2}]$ elements, now we are going to justify this choice. Let V be the multiplicative subgroup of K^* as described in Theorem 2.3.16. Let as well $\mathfrak{q}$ be a prime ideal and $\chi_\mathfrak{q}$ a quadratic character as described in Proposition 2.3.11. Any $\beta \in V$ can be written as $\beta = \beta_1\beta_2^2$ with $\beta_1 \in \mathbb{Z}[\theta]\setminus\mathfrak{q}$ and $\beta_2 \in K^*$. In order to show that, it suffices to prove that the $\beta_1 \in \mathbb{Z}[\theta]\setminus\mathfrak{q}$ form a full system of representatives for the residual classes $(\mathrm{mod}\ K^{*2})$. Let $\beta \in V$ then by definition of V we will have that $l_\mathfrak{q}(\beta) \equiv 0 \pmod 2$. We multiply β by an even power of an element $x \in R_K$ such that $\mathfrak{q}$ does not appear in the factorization of $< y >$ and $\beta x^2 \in K^*\setminus\mathfrak{q}$. Afterwards we multiply the previous product by a square of an element $y \in R_K\setminus\mathfrak{q}$ such that $\beta x^2 y^2 \in \mathbb{Z}[\theta]\setminus\mathfrak{q}$. Hence if we set $\beta_1 = \beta x^2 y^2$ and $\beta_2 = (xy)^{-1}$ we get that $\beta = \beta_1\beta_2^2$ with $\beta_1 \in \mathbb{Z}[\theta]\setminus\mathfrak{q}$ and $\beta_2 \in K^*$. We can show that $\chi_\mathfrak{q}(\beta_1)$ is independent of this representation and therefore $\chi_\mathfrak{q}$ induces a map,

$$\chi'_\mathfrak{q} : V/K^{*2} \to \{\pm 1\}$$

Our goal is to use Proposition 2.3.18 for the $\mathbb{F}_2$—vector space $Hom(V/K^{*2}, \{\pm 1\})$ We know that $\dim_{\mathbb{F}_2} Hom(V/K^{*2}, \{\pm 1\}) = \dim_{\mathbb{F}_2} V/K^{*2}$ and therefore by Theorem 2.3.16 we conclude that $\dim_{\mathbb{F}_2} Hom(V/K^{*2}, \{\pm 1\}) < \frac{\log n}{log2}$. Then the Cebotarev density theorem (Appendix A) implies that if $\mathfrak{q}$ ranges over all first degree prime ideals of $\mathbb{Z}[\theta]$ with $f'(\theta) \notin \mathfrak{q}$ with increasing norm then the $\chi'_\mathfrak{q}$ are asymptotically uniformly distributed over $Hom(V/K^{*2}, \{\pm 1\})$. So the $\chi_\mathfrak{q}$ which the algorithm uses can be seen as random elements of $Hom(V/K^{*2}, \{\pm 1\})$. Having this in mind, then Proposition 2.3.18 and Theorem 2.3.16 imply that the $[3\frac{\log n}{log2}]$ elements of **Q** have a probability of at least $1-2^{-[2\frac{\log n}{\log 2}]}$ to span $Hom(V/K^{*2}, \{\pm 1\})$. If that is the case then for a $\beta \in V$ it would hold that

$$\beta \in K^{*2} \Leftrightarrow \chi_\mathfrak{q}(\beta) = 1 \quad \forall\, \mathfrak{q} \in Q.$$

Hence we get a necessary and sufficient condition for when an element of V belongs to K^{*2}.

So for each pair (a, b) stored by the sieving step when we will construct the vector $v_{(a,b)}$ its coordinates will include the following:
1) The first $|\mathbf{P}|$ coordinates of $v_{(a,b)}$ will be equal to the exponent vector over $\mathbf{P}$ of $a+bm \pmod 2$.
2) The next $|\mathbf{G}|$ coordinates of $v_{(a,b)}$ will be equal to the value $l_{\mathfrak{p}}(a+b\theta) \pmod 2$ for all $\mathfrak{p} \in \mathbf{Q}$.
3) The last $[3\frac{\log n}{log2}]$ of $v_{(a,b)}$ will be equal to 0 or 1 as follows:
For each $\mathfrak{q} \in Q$ we compute $\chi_{\mathfrak{q}}(a+b\theta)$. If $\chi_{\mathfrak{q}}(a+b\theta) = 1$ we store 0 in the corresponding coordinate of $v_{(a,b)}$. If $\chi_{\mathfrak{q}}(a+b\theta) = -1$ we then store 1 in the corresponding coordinate of $v_{(a,b)}$. Thus after the linear algebra step we will get a set T such that,

$$l_{\mathfrak{p}}\Big(\prod_{(a,b)\in T}(a+b\theta)\Big) \equiv 0 \pmod 2 \quad \forall\, \mathfrak{p} \in \mathbf{P}$$

$$\chi_{\mathfrak{q}}\Big(\prod_{(a,\,b)\in T}(a+b\theta)\Big) = 1 \quad \forall\, \mathfrak{q} \in \mathbf{Q}$$

So we get an element in $\mathbb{Z}[\theta]$ which with a very high probability will be a square in K^*.

2.4 The square root step

The last step of our algorithm is the square root step. In this section we describe an algorithm that solves this problem according to a paper included in [16]. Let $\beta^2 \in \mathbb{Z}[\theta]$ with $\beta \in \mathbb{Z}[\theta]$ and φ as in section 2.1. Let $\beta = a_{d-1}\theta^{d-1} + ... + a_1\theta + a_0$ and $x = a_{d-1}m^{d-1} + ... + a_1 m + a_0$. We wish to compute

$$\varphi(\beta) \equiv x \pmod n$$

by only knowing $\delta = \beta^2$. As $\delta \in \mathbb{Z}[\theta]$ it then can be written as a polynomial of θ with integer coefficients and degree less than d. However in practice δ will be a product of thousands of elements of the form $a + b\theta$ and hence its coefficients will be huge making it completely impractical to use them. In order to deal with this difficulty we will compute $x \pmod{p_i}$ for several primes p_i and using the Chinese remainder theorem in a clever way we will compute $x \pmod n$. By the Chinese remainder theorem we get a $z = \sum_{i=1}^{k} a_i x_i P_i$ such that $z \equiv x \pmod P$ where $\prod_{i=1}^{k} p_i = P$, $P_i = \dfrac{P}{p_i}$, $a_i \equiv P_i^{-1} \pmod{p_i}$, $z \equiv pmodp_i$. The fact than $z \equiv x \pmod P$ implies that $x = z - rP \Rightarrow z - x = rP \Rightarrow r = \frac{z-x}{P} \Rightarrow r = \lfloor \frac{1}{2} + \frac{z}{P} \rfloor$.
Also $x \equiv z - rP \pmod n \Rightarrow x \equiv \sum_{i=1}^{k} a_i x_i P_i - rP \pmod n$.

$\frac{z}{P} = \frac{\sum_{i=1}^{k} a_i x_i P_i}{P} = \frac{\sum_{i=1}^{k} a_i x_i \frac{P}{P_I}}{P} = \sum_{i=1}^{k} \frac{a_i x_i}{P_i}$ hence we can compute r using the previous equation. It is only left to compute the x_i in order to able to compute $x \pmod n$.
Let p be a prime such that $f(x)$ is irreducible in $\mathbb{F}_p[x]$ and θ_p a root of $f(x)$ in its splitting field over $\mathbb{F}_p$. We consider the map

$$\begin{aligned} \tau_p : \mathbb{Z}[\theta] &\to \mathbb{F}_p(\theta_p) \\ \sum_{i=0}^{d-1} a_i \theta^i &\mapsto \sum_{i=0}^{d-1} a_i {\theta_p}^i \end{aligned}$$

Let $\delta = \beta^2$ we then have that $\delta_p = \tau_p(\delta) = \tau_p(\beta^2) = \tau_p(\beta)^2 = \beta_p^2$. So we can think of β_p as β with its coefficients reduced modulo p. This still allows us to compute to compute $x \pmod p$. Hence it is sufficient to find β_p as a polynomial of θ_p and then substitute θ_p by m and reduce the result modulo p. That introduces a new problem. For each prime p we have to be able to decide if $\tau_p(\beta) = \beta_p$ or $\tau_p(\beta) = -\beta_p$ so all of the congruences which we collect coincide. In order to be able to do that we will assume that the degree of the extension is odd. If we assume that we have that we can use the norm in order to be able to distinguish between the two cases.
If the degree of the extension is odd then $N(-\beta) = -N(\beta)$ so either β or $-\beta$ has positive norm. We assume that β has positive norm. Hence in any case we for the β_p we have found it suffices to compute the norm or the element it corresponds to. In order to do that we will use the norm N_p of $\mathbb{F}_p(\theta_p)$ for which we have that $N(a) \equiv N_p(\tau_p(a)) \pmod p$ for $a \in \mathbb{Z}[\theta]$.
The extension $\mathbb{F}_p(\theta_p)/\mathbb{F}_p$ is a cyclic extension and $Gal(\mathbb{F}_p(\theta_p)/\mathbb{F}_p)$ is generated by the automorphism of Frobenius,

$$\begin{aligned} \sigma_p : \mathbb{F}_p(\theta_p) &\to \mathbb{F}_p(\theta_p) \\ a &\mapsto a^p \end{aligned}$$

This implies that

$$\begin{aligned} N_p(a) &= \sigma_1(a)\sigma_2(a) \dots \sigma_d(a) \\ &= \sigma_p(a)\sigma_p^2(a) \dots \sigma_p^d(a) \\ &= a^p a^{p^2} \dots a^{p^d} \\ &= a^{1+p+\dots+p^{d-1}} \\ &= a^{\frac{p^{d-1}-1}{p-1}} \end{aligned}$$

Therefore we compute $y_1 \equiv N(\beta) \pmod p$ and $y_2 \equiv \beta_p{}^{\frac{p^d-1}{p-1}} \pmod p$. Then

$$\tau_p(\beta) = \begin{cases} \beta_p & \text{if } y_1 \equiv y_2 \pmod p \\ -\beta_p & \text{if } y_1 \equiv -y_2 \pmod p \end{cases}$$

Remark 2.4.1. *Note that even though we do not know β we can compute its norm. This can be done by using the following formula*

$$N(\beta) = |N(f'(\theta))| \sqrt{|\prod_{(a,b)\in T} N(a+b\theta)|} = |N(f'(\theta))| \prod_{\substack{p\,:\exists \mathfrak{p}\in \boldsymbol{G} \\ p=N(\mathfrak{p})}} p^{e_p}$$

where $e_p = \frac{1}{2} \sum_{(a,b)\in T} l_{\mathfrak{p}}(a+b\theta)$

Therefore the only thing left is to compute the $x_i \equiv x \pmod{p_i}$. For doing that it is sufficient to compute the β_{p_i}.

Proposition 2.4.2. *Let $\mathbb{F}_q$ be a finite field with $q = p^d$. An element $\delta \in \mathbb{F}_q^*$ is a square in $\mathbb{F}_q^*$ if and only if $\delta^{\frac{q-1}{2}} = 1$ and respectively δ is not a square in $\mathbb{F}_q^*$ if and only if $\delta^{\frac{q-1}{2}} = -1$.*

Proof. Let $\gamma \in \mathbb{F}_q^*$ be a generator of $\mathbb{F}_q^*$ and δ a square, hence $\delta = (\gamma^k)^2 = \gamma^{2k}$ for some $k \in \mathbb{Z}$. Then $\delta^{\frac{q-1}{2}} = \gamma^{\frac{2k(q-1)}{2}} = (\gamma^{q-1})^k = 1$. If δ is not a square then $\delta = \gamma^{2k+1}$ for some $k \in \mathbb{Z}$ and $\delta^{\frac{q-1}{2}} = \gamma^{2k+1\,\frac{(q-1)}{2}} = \gamma^{\frac{(2k+1)(q-1)}{2}} = \gamma^{\frac{2k(q-1)}{2}}\gamma^{\frac{q-1}{2}} = (\gamma^{q-1})^k\gamma^{\frac{q-1}{2}} = 1(-1) = -1$.
But $\delta^{q-1} = 1 \Rightarrow \delta^{\frac{q-1}{2}} = \pm 1$. If $\delta^{\frac{q-1}{2}} = 1$ and assume that $\delta = \gamma^{2k+1}$ then $1 = \delta^{\frac{q-1}{2}} = \gamma^{\frac{(2k+1)(q-1)}{2}} = -1$ contradiction, so δ is a square. If $\delta^{\frac{q-1}{2}} = -1$ and we assume that $\delta = \gamma^{2k}$ then $\gamma^{2k\,\frac{q-1}{2}} = -1 \Rightarrow \gamma^{(q-1)k} = -1$ contradiction, so δ is not a square. □

Proposition 2.4.3. *Let $\mathbb{F}_q$ be a finite field with $q = p^d$ and $q-1 = 2^r s$. If $\eta \in \mathbb{F}_q^*$ is not a square in $\mathbb{F}_q^*$ then $ord(\eta^s) = 2^r$. Additionally the Sylow $2-$subgroup of $\mathbb{F}_q^*$ will be the $S_{2^r} =< \eta^s >$.*

Proof. Let k be the order of η^s and $\eta^{\frac{q-1}{2}} = -1$ by the previous proposition as η is not a square. Hence $-1 = \eta^{\frac{q-1}{2}} = \eta^{\frac{2^r s}{2}} = \eta^{2^{r-1}s} = (\eta^s)^{2^{r-1}}$ which implies that $(\eta^s)^{2^r} = 1$. Therefore $k \mid 2^r$. Also $(\eta^s)^{2^m} \neq 1$ for $0 \leq m < r-1$ as if that did not occur we would have that $1 = (\eta^s)^{2^{m+1}} = ... = (\eta^s)^{2^{r-1}}$, contradiction. Thus η^s generates a subgroup of order 2^r. As $\mathbb{F}_q^*$ is abelian there is only one Sylow $2-$ subgroup of $\mathbb{F}_q^*$ and hence $S_{2^r} =< \eta^s >$. □

The idea we will use in order to find a square root δ is the following. We will construct two sequences of elements ω_i and λ_i respectively such that $\omega_i^2 = \lambda_i \delta$, $ord(\lambda_{i+1}) < ord(\lambda_i)$ and $ord(\lambda_i)|2^{r-1}$ for all i. If we manage to find such two sequences the eventually for some j we will get $\lambda_j = 1$. Therefore we will have $\omega_j^2 = \delta$ and hence we get a square root of δ. In the worst case i.e. if $ord(\lambda_0) = 2^{r-1}$ it will take us r steps until we get $\lambda_j = 1$.

Proposition 2.4.4. *Let ζ be a generator of the Sylow $2-$subgroup of $\mathbb{F}_q^*$ S_{2^r}. If $ord(\lambda_i) = 2^m$ and $\lambda_{i+1} = \lambda_i \zeta^{2^{r-m}}$ then $ord(\lambda_{i+1})|2^{m-1}$. Additionally, if we have $\omega_i^2 = \lambda_i \delta$ and $\omega_{i+1} = \omega_i \zeta^{2^{r-m-1}}$ then $\omega_{i+1}^2 = \lambda_{i+1}\delta$.*

Proof. As $ord(\lambda_i) = 2^m \Rightarrow {\lambda_i}^{2^m} = 1 \Rightarrow {\lambda_i}^{2^{m-1}} = -1$. Also $ord(\zeta) = 2^r \Rightarrow \zeta^{2^r} = 1 \Rightarrow \zeta^{2^{r-1}} = -1$. So $\lambda_{i+1}^{2^{m-1}} = \lambda_i^{2^{m-1}} (\zeta^{2^{r-m}})^{2^{m-1}} = (-1)\zeta^{2^{r-m+m-1}} = -\zeta^{2^{r-1}} = (-1)(-1) = 1 \Rightarrow ord(\lambda_{i+1})|2^{m-1}$. Finally, $\omega_{i+1}^2 = \omega_i^2 (\zeta^{2^{r-m-1}})^2 = \omega_i^2 \zeta^{2^{r-m}} = \lambda_i \delta \zeta^{2^{r-m}} = \lambda_{i+1}\delta$. □

Let $\lambda = \delta^s$ and $\omega = \delta^{\frac{s+1}{2}}$ then $\omega^2 = \lambda\delta$ and $(\delta^s)^{2^{r-1}} = \delta^{2^{r-1}s} = \delta^{\frac{q-1}{2}} = 1$ as δ is a square. Therefore we have that $ord(\delta^s)|2^{r-1}$. So according to the previous proposition we will construct ω_i and λ_i as follows:

$$\lambda_0 = \delta^s \qquad \omega_0 = \delta^{\frac{s+1}{2}}$$
$$\lambda_{i+1} = \lambda_i \zeta^{2^{r-m_i}} \qquad \omega_{i+1} = \omega_i \zeta^{2^{r-m_i-1}}$$

where $\zeta = \eta^s$ for some η that is not a square in $\mathbb{F}_q^*$ and $ord(\lambda_i) = 2^{m_i}$.

2.5 A working example

In order to understand and illustrate what we have studied so far in this chapter we give an example. In this section we are going to try to factor the number $n = 12353161739$. In practice in order to factor a number of this magnitude we do not need a so powerful algorithm like the GNFS but here it will help us illustrate the procedure.
The first step is to choose the degree d of the extension $K/\mathbb{Q}$ in which we are going to work. We choose $d = 3$. The next step is to find an irreducible polynomial $f(x)$. According to section 2.2 we proceed as follows. We compute
$m = [n^{1/d}] = [12353161739^{1/3}] = 2311$ and then find the base$-m$ expansion of n.

$$12353161739 = 2311^3 + 2 \cdot 2311^2 + 32 \cdot 2311 + 114$$

The base$-m$ expansion of n suggests that we must set $f(x) = x^3 + 2x^2 + 32x + 114$. This polynomial is irreducible. Indeed, this can be easily induced by applying the Eisenstein

criterion for the prime number $p = 2$. Therefore if we denote by θ a root of $f(x)$ then $K = \mathbb{Q}(\theta)$ is a third degree extension of $\mathbb{Q}$. We define

$$\begin{aligned} \varphi : \mathbb{Z}[\theta] &\to \mathbb{Z}/12353161739\mathbb{Z} \\ \sum_{i=0}^{2} a_i\theta^i &\mapsto \sum_{i=0}^{2} a_i 2311^i \pmod{12353161739} \end{aligned}$$

Afterwards we choose our smoothness bounds B_1 and B_2. We set $B_1 = 100$ and $B_2 = 101$. Thus we get

$\mathbf{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$

$\mathbf{G} = \{(0,2), (0,3), (3,5), (6,11), (4,13), (3,17), (0,19), (7,19), (10,19), (19,23), (31,37), (7,41), (10,43), (14,43), (17,43), (64,71), (27,73), (34,79), (57,79), (65,79), (82,83), (58,89), (2,97), (33,97), (60,97), (8,101), (27,101), (64,101)\}$

$\mathbf{Q} = \{(59,103), (89,127), (62,131), (89,139)\}$

As it can be seen the quadratic character base is chosen to be much smaller than suggested in section 2.2. If we used the suggested size for $\mathbf{Q}$ which is $[3\frac{\log n}{\log 2}]$ we should take $\mathbf{Q}$ to have 100 elements. This is not so good as it implies that in the sieving step we have to find "many" relations. Fortunately in this case we can do something better. The size $[3\frac{\log n}{\log 2}]$ was induced by Theorem 2.3.16. However in the proof of this theorem we showed that the following inequality holds as well,

$$[V : K^{*2}] \leq [R_K : \mathbb{Z}[\theta]] h_K 2^{d-s}$$

As the number field K is not too "big" we can use SAGE to compute the parameters in the right hand side of the inequality.

In SAGE we give the orders,

```
R.<x> = QQ []
K.<a> = NumberField (x^3 +2*x^2+32*x+114)
h=K.class_number() ; h
OK = K.maximal_order()
OK.basis()
K.signature()
```

The output of the above orders gives us that $[R_K : \mathbb{Z}[\theta]] = 1$, $h_K = 4$ and $s = 1$. Hence we get that $[V : K^{*2}] \leq 1 \cdot 4 \cdot 2^{3-1} = 2^4$ and therefore a set $\mathbf{Q}$ of size 12 is sufficient. However even a choice for $\mathbf{Q}$ with 4 elements proved to be sufficient for our example. So finally we have that $|\mathbf{P}| + |\mathbf{G}| + |\mathbf{Q}| = 25 + 28 + 4 = 57$ and we can start sieving. We choose the sieving bounds to be $U_1 = 700$ and $U_2 = 150$ and we deduce the above 63 relations mentioned in table 2.1.

The next step is to form the matrix which we are going to use in the linear algebra step. In order to do that we form the vectors $v_{(a,b)}$ that correspond to each relation (a, b). For

Relations							
b	a	$A_1(a)$	$A_2(a)$	b	a	$A_1(a)$	$A_2(a)$
1	-57	1	-1	9	13	1	-1
1	-48	1	-1	11	-278	1	-1
1	-33	1	-1	11	19	1	-1
1	-17	1	-1	11	35	1	-1
1	-10	1	-1	12	-61	1	-1
1	-8	1	-1	13	-608	1	-1
1	-7	1	-1	17	-237	1	-1
1	1	1	-1	17	-157	1	-1
1	3	1	-1	17	52	1	-1
1	7	1	1	17	58	1	1
1	9	1	1	17	114	1	1
1	14	1	1	19	113	1	1
1	119	1	1	20	-587	1	-1
1	677	1	1	21	67	1	1
2	-71	1	-1	24	73	1	-1
2	-57	1	-1	25	76	1	-1
2	-23	1	-1	29	508	1	1
2	19	1	1	31	-46	1	-1
2	31	1	1	31	39	1	-1
2	109	1	1	43	126	1	-1
2	123	1	1	47	319	1	1
3	35	1	1	53	-219	1	-1
5	-107	1	-1	55	-609	1	-1
5	-12	1	-1	56	257	1	1
5	-3	1	-1	59	163	1	-1
5	16	1	1	59	271	1	1
6	-1	1	-1	75	238	1	-1
7	-317	1	-1	83	171	1	-1
7	5	1	-1	103	579	1	1
8	-19	1	-1	104	393	1	1
8	-15	1	-1	121	369	1	-1
8	27	1	1				

Table 2.1: Relations

example we take $(a, b) = (-57, 1)$ and we show how to compute $v_{(a,b)}$. The first 25 coordinates of $v_{(a,b)}$ will be the exponents of the factorization of $-57 + 1 \cdot 2311 = 2254$ over **P** reduced modulo 2.

$$2254 = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^2 \cdot 11^0 \cdot 13^0 \cdot 17^0 \cdot 19^0 \cdot 23^1 \cdot 29^0 \cdot 31^0 \cdot 37^0 \cdot 41^0 \cdot 43^0 \cdot 47^0 \cdot 53^0 \cdot 59^0 \cdot 61^0 \cdot 67^0 \cdot 71^0 \cdot 73^0 \cdot 79^0 \cdot 83^0 \cdot 89^0 \cdot 97^0$$

so modulo 2 we get the vector

$$(1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$$

The norm of an element $a + b\theta$ is given by the following formula,

$$N(a + b\theta) = a^3 - 2a^2b + 32ab^2 - 114b^3$$

so for $(a, b) = (-57, 1)$ we get $N(-57 + \theta) = -193629$.

$$-193629 = -3 \cdot 19 \cdot 43 \cdot 79$$

Therefore checking for which pairs (c, p) in **G** it holds that $-57+1\cdot c \equiv 0 \pmod{p}$ and reducing modulo 2 the respective $l_{\mathfrak{p}}(-57 + \theta)$, we get the following vector.

$$(0,1,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,1,0,0,0,0,0,0,0,0,0)$$

Finally we compute $\left(\dfrac{-57 + s}{q}\right)$ for (s, q) in **Q** and we get the vector

$$(0,0,0,1)$$

By concatenating the above three vectors we form $v_{(a,b)}$ and hence the first column of the matrix which we are going to use in the linear algebra step. We do the same for the rest of the pairs (a, b) and form a 57×63 matrix. Then we try to find vectors in the nullspace of this matrix. An algorithm like Block Lanczos could be used for this step. However as the size of the matrix we want to handle is not too large standard Gaussian elimination can be used. Again we use SAGE for this by giving the following orders.
M = MatrixSpace(GF(2),63,57)
A=M([]).transpose()
A.transpose().kernel()
where in [] we put the matrix. The dimension of the resulting nullspace is 10 and one vector in the nullspace is the following

$$(0,0,1,0,0,0,0,0,0,1,1,0,0,0,1,0,1,1,0,1,0,0,0,0,1,0,1,0,0,1,1,1,1,0,0,1,1,1,1,1,0,1,0,0,0,1,1,0,0,1,1,0,0,0,1,1,0,1,1,0,1,0,0,1,1)$$

This vector implies a set T of relations.

$$\begin{aligned} T = \{&(1,-33),(1,7),(1,9),(2,-71),(2,-23),(2,19),(2,109),(5,-3),(6,-1),\\ &(8,-19),(8,-15),(8,27),(11,19),(11,35),(12,-61),(13,-608),(17,-157),\\ &(19,113),(20,-587),(25,76),(29,508),(47,319),(53,-219),(56,257),(59,163),\\ &(75,238),(104,393),(121,369)\} \end{aligned}$$

Using this set we get

$$f'(2311)^2 \prod_{(a,b)\in T}(a+b2311) =$$

$$8087308854437939950600498285211228651347692108758362363953119232000002 \quad \text{and}$$

$$f'(\theta)^2 \prod_{(a,b)\in T}(a+b\theta) =$$

$$165426272508618432776464147346342224215536627939434239934402 0\theta^2 +$$
$$113110929126537401218119171267992156443731091745657583431266 32\theta +$$
$$192455348857613524411166614771607837253128183162291726014287 84$$

At this point we have to note that in practice when the GNFS is used we do not compute the above results as we care only about their image under φ. What we would have computed using repeated multiplications $\pmod{12353161739}$ is

$$\varphi(8087308854437939950600498285211228651347692108758362363953119232000 00) \equiv 11624226379 \pmod{12353161739}.$$

This can be done efficiently as we can use the exponent vectors of $a+b2311$ for $(a,b)\in T$ which we have already computed. By adding these vectors and then dividing by 2 each coordinate we take the exponent vector of

$$8087308854437939950600498285211228651347692108758362363953119232000000$$

Then by modular exponentiation and multiplication $\pmod{12353161739}$ we can compute its image under φ efficiently.
This can not be done for $\delta = f'(\theta)^2 \prod_{(a,b)\in T}(a+b\theta)$ as we have already seen that in this case we can not find the square root of this element efficiently. Therefore we have to use the techniques of section 2.4. However in this case we can use again SAGE in order to compute the square root of δ. We give the order:
δ.is_square(True)
and we get

$$(\text{True}, 5911893323624826013329750234\theta^2 - 1293869310951621452979819242506\theta - 4182528496250969872573845109548)$$

If we denote by β the above square root of δ then we have that

$$\varphi(\beta) \equiv 1749634778 \pmod{12353161739}$$

Additionally $11624226379 \not\equiv \pm 1749634778 \pmod{12353161739}$ so we can conclude the following prime factors of n.

$$\gcd(11624226379 - 1749634778, 12353161739) = 97039$$

$$\gcd(11624226379 + 1749634778, 12353161739) = 127301$$

We are now going to try to illustrate the procedure that we would have followed if we had used the method described in section 2.4 for computing $\varphi(\beta) \pmod{n}$.

Let $\beta = a_2\theta^2 + a_1\theta + a_0$ and $x = a_2m^2 + a_1m + a_0$. Obviously $\varphi(\beta) \equiv x \pmod{n}$. The first step is to find a sufficient number of primes p such that $f(x)$ is irreducible in $\mathbb{F}_p[x]$ and the product of these primes to exceed x . In order to do that we need an estimate for x which we can get in general. In this case we know that

$$x = 285794583171374562630275408849378 00$$

and therefore we obtain that the following set of primes will work

$$\mathrm{A} = \{227, 251, 293, 307, 347, 359, 397, 421, 433, 443, 461, 467, 479, 509, 569\}$$

The next step is to compute $x \pmod{p}$ for $p \in A$. We use the method described in section 2.4. We are going to show how this can be done for one prime in A. We will consider the prime 227. Initially we have to find an element that is not a square in $\mathbb{F}_p(\theta_p)$. One such element is $\eta = \theta_p^2 + 3\theta_p + 1$. We have that $227^3 - 1 = 2 \cdot 5848541$ and hence

$$S_2 = \{1, \eta^{5848541}\} = \{1, -1\}$$

Afterwards we compute the reduction modulo 227 of δ which turns out to be $\delta_p = 35\theta_p^2 + 9\theta_p + 163$. Now we are ready to construct the two sequences that will give us the square root of δ_p in $\mathbb{F}_p(\theta_p)$.

$$\lambda_0 = \delta_p^{5848541} = 1 \qquad \omega_0 = \delta_p^{\frac{5848541+1}{2}} = 214\theta_p^2 + 207\theta_p + 150$$

As $\lambda_0 = 1$ we conclude that ω_0 is a square root of δ_p in $\mathbb{F}_p(\theta_p)$. Now we have to apply the norm test in order to determine if it is the one we want.

$$N(\beta) \equiv 172 \pmod{227} \qquad N_p(\omega_0) = \omega_0^{\frac{227^3-1}{227-1}} \equiv 172 \pmod{227}$$

p	227	251	293	307	347	359	397	421	433	443	461
$x \pmod p$	177	126	235	92	114	304	291	96	161	393	36

p	467	479	509	569
$x \pmod p$	445	251	204	42

Therefore we found the right square root. Now we can compute $x \pmod{227}$. We have that $x \equiv 214 \cdot 2311^2 + 207 \cdot 2311 + 150 \equiv 177 \pmod{227}$. We do the same for the rest of the primes $p \in A$ and we conclude that

We set $P = \prod_{p_i \in A} p_i$ and $P_i = \frac{P}{p_i}$. The next step is to compute the $a_i \equiv P_i^{-1} \pmod{p_i}$.

p_i	227	251	293	307	347	359	397	421	433	443	461
a_i	29	220	17	252	46	107	105	352	54	133	300

p_i	467	479	509	569
a_i	428	310	182	335

$$\sum_{i=1}^{15} \frac{a_i x_i}{p_i} = 1530.00$$

Thus we get that $r = 1530$ and we can now compute $x \pmod n$ as follows.

$$x \equiv \sum_{i=1}^{15} a_i x_i P_i - rP \pmod n \Rightarrow x \equiv 1749634778 \pmod{12353161739}$$

Appendix A

The Cebotarev density theorem

Let L/K be a Galois extension of number fields, S, R the respective rings of integers of L, K. Let $P \in \mathbb{P}(K)$ and $Q \in \mathbb{P}(L)$ such that $Q|P$.

$$G_Z = G_Z(Q/P) = \{\sigma \in Gal(L/K) \,|\, \sigma(Q) = Q\}$$

is the decomposition group of Q/P ,

$$G_T = G_T(Q/P) = \{\sigma \in Gal(L/K) \,|\, \sigma(a) \equiv a \pmod{Q} \; \forall \; a \in S\}$$

is the inertia group and $\overline{G} = Gal(S/Q \diagup R/P)$. It is well known that the following short sequence is exact.

$$1 \longrightarrow G_T \longrightarrow G_Z \longrightarrow \overline{G} \longrightarrow 1$$

If Q is not ramified in L/K then $G_T = \{1\}$ and so $G_Z \cong \overline{G}$. The Galois group $\overline{G}$ is cyclic and is generated by the automorphism of Frobenius,

$$\begin{aligned} \overline{\sigma} \; : \; & S/Q \to S/Q \\ & s + Q \mapsto s^{N_K(P)} + Q \end{aligned}$$

It follows that there is exactly one $K-$automorphism of L , $\sigma \in G_Z$ such that $\sigma(s) \equiv s^{N_K(P)} \pmod{Q} \; \forall s \in S$. This automorphism will be called symbol of the Frobenius and will be denoted by $\left[\frac{L/K}{Q}\right]$. If we take $\sigma \in Gal(L/K)$ then $\left[\frac{L/K}{\sigma(Q)}\right] = \sigma\left[\frac{L/K}{Q}\right]\sigma^{-1}$. So if Q ranges over all the prime ideals of L lying over the not ramified prime ideal P of K then the $\left[\frac{L/K}{Q}\right]$ ranges over a conjugate class of $Gal(L/K)$. We denote this class by $\left[\frac{L/K}{P}\right]$.

Definition A.0.1. *Let $A \subseteq \mathbb{P}(K)$ be a subset of the prime ideals of K such that there exists a positive real number $\delta = \delta(A) > 0$ for which*

$$\sum_{P \in A} \frac{1}{N(P)^S} = -\delta \log(s-1) + O(1) \quad \text{as } s \to 1^+$$

Then the number δ will be called Dirichlet density of A.

Theorem A.0.2 (Cebotarev Density Theorem)**.** *Let C be a conjugate class of the group $Gal(L/K)$, $c = \#C$ and $\mathcal{A}_{L/K,C} := \left\{ P \in \mathbb{P}(K) \mid P \text{ not ramified in } L/K,\ \left[\frac{L/K}{P}\right] = C \right\}$. Then $\mathcal{A}_{L/K,C}$ has Dirichlet density $\delta(\mathcal{A}_{L/K,C}) = \frac{c}{n}$ where $n = [L : K]$.*

The above theorem has also the following form.

Theorem A.0.3. *If $x \in \mathbb{R}$ and $N_{\mathcal{A}_{L/K,C}} = \#\{P \in \mathbb{P}(K) | P \in \mathcal{A}_{L/K,C}$ and $N_{K/\mathbb{Q}(P)} \leq x\}$ then $N_{\mathcal{A}_{L/K,C}} = \left(\frac{c}{n} + o(1)\right) \frac{x}{\log x}$.*

For more details about the above theorems we refer to [1] or [19].

The subgroup V of K^* has the property that V/K^{*2} is of finite dimension over the field of two elements. We set $L = K(\sqrt{v} | v \in V)$. Let $B = \{vK^{*2}\}$ be a base of V/K^{*2} over $\mathbb{F}_2$ for some $v \in V$. Then we have that $L = K(\sqrt{v} | vK^{*2} \in B)$. The L/K is a finite abelian Galois extension of exponent 2. According to the Kummer theory the map

$$\begin{aligned} V/K^{*2} &\to Hom(Gal(L/K), \{\pm 1\}) \\ vK^{*2} &\mapsto \chi_v \end{aligned}$$

where $\chi_v(\sigma) = \frac{\sigma(\sqrt{v})}{\sqrt{v}}$ for each $v \in V$ is an isomorphism [12, Theorem 4.4 p.412]. This can be written also as a pairing

$$\begin{aligned} Gal(L/K) \times V/K^{*2} &\to \{\pm 1\} \\ (\sigma, vK^{*2}) &\mapsto \frac{\sigma(\sqrt{v})}{\sqrt{v}} \end{aligned}$$

and by duality, since L/K is finite $Gal(L/K) \cong V/K^{*2}$. This means that the characters $\chi_{\mathfrak{q}}$ of V/K^{*2} coming from a prime ideals of degree 1, $\mathfrak{q} \nmid \langle f'(\theta) \rangle$ from which it follows that $\mathfrak{q}$ is unramified in L/K is nothing but the Artin-symbol $\left[\frac{L/K}{\mathfrak{q}}\right]$. According to the Cebotarev's density theorem they are equidistributed over $Gal(L/K) = Hom(V/K^{*2}, \{\pm 1\})$.

Bibliography

[1] Jannis A. Antoniadis. *Algebraic number theory II (L-series) (in Greek)*. Heraklion 1999.

[2] Jannis A. Antoniadis. Notes in algebraic number theory (in greek).

[3] Shi Bai. *Polynomial Selection for the Number Field Sieve*. PhD thesis, Australian National University, 2011.

[4] Adrian Bondy and U.S.R. Murty. *Graph theory*, volume 244 of *Graduate texts in mathematics*. Springer, 2008.

[5] Matthew E. Briggs. An introduction to the general number field sieve. Master's thesis, Virginia Polytechnic Institute and State University, 1998.

[6] John Brillhart, Michael Filaseta, and Andrew Oldyzko. On an irreducibility theorem of A. Cohn. *Canadian Journal of Mathematics*, 33(5):1055–1059, 1981.

[7] Greg Childers. Factorization of a 1061-bit number by the special number field sieve, 2012. https://eprint.iacr.org/2012/444.pdf.

[8] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, 1993.

[9] D. Coppersmith. Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm. *Mathematics of Computation*, 62:333–350, 1994.

[10] A. Fröhlich and M. J. Taylor. *Algebraic number theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1992.

[11] H.W. Lenstra, Jr. Algorithms in algebraic number theory. *Bulletin of the American Mathematical Society*, 26(2):211–244, 1992.

[12] G. Kaprilovsky. *Topics in Field Theory*. North-Holland, 1989. Amsterdam.

[13] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thome, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768-bit RSA modulus, 2010. https://eprint.iacr.org/2010/006.pdf.

[14] Mihalis Kolountzakis. Notes in discrete mathematics (in greek), 2011.

[15] A. K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, and J.M. Pollard. The factorization of the ninth fermat number. *Mathematics of Computation*, 61(203):319–349, 1993.

[16] A. K. Lenstra and H.W. Lenstra, Jr. (eds.). *The development of the number field sieve, Lecture Notes in Mathematics*, volume 1554. Springer-Verlag, 1993.

[17] A. K. Lenstra and M. S. Manasse. Factoring with two large primes. *Mathematics of Computation*, 63(208):785–798, 1994.

[18] Peter L. Montgomery. A block Lanczos algorithm for finding dependencies over GF(2). *Lecture Notes in Computer Science, Springer-Verlag*, 921:106–120, 1995.

[19] Wladyslaw Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Monographs in Mathematics. Springer-Verlag, third edition, 2004.

[20] Edwin Weiss. *Algebraic number theory*. McGraw-Hill, 1976.