Università degli Studi di Trento

DIPARTIMENTO DI MATEMATICA
Corso di Dottorato di Ricerca in Matematica
XXXI CICLO

A thesis submitted for the degree of Doctor of Philosophy

An investigation on Integer Factorization applied to Public Key Cryptography

Supervisor:
Prof. Massimiliano Sala

Ph.D. Candidate:
Giordano Santilli

"I was just guessing at numbers and figures, pulling your puzzles apart..."
(The Scientist - Coldplay)

To all the people that told me their secrets and asked me their questions.

Contents

Introduction

Public-key or asymmetric cryptography allows two or more users to communicate in a secure way on an insecure channel, using two different keys: a public key, which has the function to encrypt the messages, and a private key, employed in the decryption of the ciphertexts. Because of the importance of these keys in the protocol, their generation is a sensible issue and it is often based on an underlying mathematical problem, which is considered hard to solve by the scientific community. Among the difficult number-theoretic problems, the Integer Factorization Problem (IFP) is one of the most famous: given a composite integer number, recovering its factors is commonly believed to be hard (worst-case complexity). Many asymmetric algorithms such as RSA ([RSA78]), Rabin's cryptosystem ([Rab79]) or Goldwasser-Micali cryptosystem ([GM84]) found their mathematical security on IFP. Due to its rather simple formulation, IFP has been extensively examined ever since: many factorization methods have been developed to solve this problem, such as Dixon's algorithm ([Dix81]) or the quadratic sieve ([Pom82]), but, at the moment, the most efficient one is the General Number Field Sieve (GNFS), which is fully described in [LLMP93a].
The aim of this thesis is to discuss some number-theoretic techniques to investigate IFP from new points of view.

The thesis will be organized as follows:

- in Chapter 1 we will present the factorization problem and discuss its involvement in Public-key Cryptography. We will also recall some of the most famous factorization methods, give a description of the state of the art and survey the actual records on integer factorization. Furthermore, the number-theoretic techniques we will employ belong to three main fields: firstly we will examine relevant properties of the floor function and the ceiling function, then we will recall some important

results in Algebraic Number Theory about ring of integers and their ideals, while Groebner bases will be the main topic of the last part.

- Starting from the results recalled in the first chapter, in Chapter 2 we will describe an original work on integer factorization based on some elementary properties of the remainders of a fixed positive integer N modulo successive numbers. We will show that it is possible to define a formula that computes all the remainders of N starting with just three initial consecutive remainders. Later, we will also prove that this formula does not change even as considering the second-degree interpolating polynomial between the starting remainders. This interesting regularity was originally noticed and analysed by Dr. Matteo Piva. We will exihibit an equivalence between the integer factorization problem and the solution of the aforementioned formula and we will finally explore the future developments of this approach, explaining with an example how we would like to generalize this approach.

- The main theme of Chapter 3 is the General Number Field Sieve algorithm, depicted in great details. We will report the classical formulation of GNFS, including the Rational Factor Base, the Algebraic Factor Base and the Quadratic Characters Base, which permit to get a non-trivial factor of a semiprime N. Additionally, the complexity of the algorithm will be stated and analysed, employing some functions borrowed from Analytic Number Theory. By the end of the chapter, the successive improvements on GNFS will be inspected, especially the different strategies developed in the polynomial selection and in the sieving step.

- The last two chapters will again contain some original material. In Chapter 4 we will examine a way to generalize GNFS to bivariate polynomials, based on a joint work with Dr. Daniele Taufer. The structure we will handle in this chapter is the following: we will consider two simple quadratic extensions of the rational numbers that do not have any intersection between them, except for the rational numbers themselves, and a larger extension of degree 4 that contains both. We will prove that the first-degree prime ideals in the smaller extensions may be used to generate the same kind of ideals in the larger one and, adding some additional hypotheses, we will show that also the converse is true. Moreover, a potential scheme of an application to GNFS is theorized and we will explain at the end of the chapter why

this approach will not completely work for our situation in its present formulation.

Finally, Chapter 5 addresses the issue of finding some elements for GNFS that lead to a successful factorization of N, through the solution of some multivariate systems, solved using Groebner bases. We will provide this way an algorithm for integer factorization, also with a very detailed example.

In Appendix A and Appendix B we will report MAGMA programs used to test some of our algorithms.

Chapter 1

Preliminaries

Notation. We will denote with $\mathbb{N}$ the set of natural numbers

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

and with $\mathbb{N}^+$ all the positive integers.

1.1 Historical Overview

One of the most ancient and famous theorems about prime numbers is the Fundamental Theorem of Arithmetic, which was first described in Euclid's Elements in Book IX, [Hea56].

Theorem 1.1. *Every positive integer $N \in \mathbb{N}^+$ such that $N > 1$ can be represented in a unique way as a product of prime powers:*

$$N = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k},$$

where $k \in \mathbb{N}^+$, $p_1 < p_2 < \ldots < p_k$ are prime numbers and $e_1, e_2, \ldots, e_k \in \mathbb{N}$.

A natural problem arising from this theorem is, given a positive integer number $N \in \mathbb{N}^+$, to find its prime factorization.

From a computational point of view, while there are several ways to decide (in polynomial-time) whether an integer is a prime, it is still unknown if there exist a non-quantum polynomial-time algorithm that finds its prime factors. This issue is called *Integer Factorization Problem* (IFP). The clarification "non-quantum" is needed, since in 1994 Schor ([Sho94]) presented an algo-

rithm for quantum computers that finds all prime factors of a given integer in polynomial-time. Since a classical polynomial-time algorithm that solves IFP might never be found, it is considered to be a hard problem. Due to this hardness, IFP guarantees the security of many public-key cryptography algorithms, starting from RSA.

1.1.1 RSA

The RSA cryptosystem was proposed in 1977 by Rivest, Shamir and Adleman ([RSA78]) and addresses the issue of secure data transmissions: suppose Bob wants to send a message m to Alice and he does not want anyone else to intercept the message m that he sent. In order to do so, Alice needs to generate a pair of prime integers p and q and multiply them together to obtain N. Then, she also need an integer $1 < e < \varphi(n)$ such that $\gcd(e, \varphi(N)) = 1$. Finally she computes $d \equiv e^{-1} \bmod \varphi(N)$, where φ is Euler's totient function. The value e is called *public exponent*, the pair (N, e) is called *public key* and Alice publicly shares it. On the other hand, the value d, called *private exponent*, must be kept secret, as well as the triplet (p, q, d), which is called *private key*. Bob can now communicate with Alice, sending to her $c \equiv m^e \bmod N$. When Alice gets the ciphertext c, she may compute $c^d \equiv m \bmod N$ to recover the original message. This is an easy application of Fermat's Little Theorem. The security of this protocol is assured by the Integer Factorization Problem, since it is proved in [RSA78] that finding p and q is equivalent to finding $\varphi(N)$ knowing only N, which in turn is equivalent to solving the congruence $x^e \equiv c \bmod N$.

1.1.2 A quick review on Factorization Methods

In this section we will discuss about different factorization methods. In order to analyse their performance we will introduce the big-O notation:
Definition 1.2. Let $f, g : \mathbb{R} \to \mathbb{R}$ two functions. We write that

$$f(x) = O(g(x)), \quad \text{for } x \to \infty$$

if and only if there exists a value $M \in \mathbb{N}^+$ and $x_0 \in \mathbb{R}$ such that

$$|f(x)| \leq Mg(x)$$

for every $x \geq x_0$.

The problem of factoring integers is way older than RSA: while Eratosthenes described a method to find all primes more than 2200 years ago, the most intuitive and natural factorization algorithm was described by Fibonacci in his Liber Abaci ([Sig03]) and is called *Trial Division*. This algorithm consists in dividing the integer N by every prime between 2 and $\left\lfloor \sqrt{N} \right\rfloor$. If we consider N to have n digits in base-2 representation, the interval in which we have to check has width

$$\pi\left(2^{\frac{n}{2}}\right) \approx \frac{2^{\frac{n}{2}}}{\frac{n}{2}\log(2)},$$

where $\pi(x)$ is the prime-counting function, which counts all the prime numbers up to x and may be approximated to $\frac{x}{\log(x)}$ by the Prime Number Theorem. So, the cost of trying every factor is, using the "big-O" notation, $O\left(2^{\frac{n}{2}}\right) = O\left(\sqrt{N}\right)$. We may notice that this algorithm stops when the smallest prime factor of N is found. A different approach to factorization is to consider a method proposed by Fermat: the problem of the factorization of N may be transformed in finding two integers x and y such that

$$x^2 \equiv y^2 \bmod N \qquad \text{and} \qquad x \not\equiv \pm y \bmod N.$$

In this way, we obtain that

$$N \mid (x^2 - y^2) = (x - y)(x + y),$$

so that $\gcd(N, x - y)$ and $\gcd(N, x + y)$ may be equal to non-trivial factors of N. If $N = p \cdot q$, we may summarize all possible cases in the following table:

$p \mid (x-y)$	$p \mid (x+y)$	$q \mid (x-y)$	$q \mid (x+y)$	$\gcd(x-y, N)$	$\gcd(x+y, N)$	Factorization
✓	✓	✓	✓	N	N	✗
✓	✓	✓	✗	N	p	✓
✓	✓	✗	✓	p	N	✓
✓	✗	✓	✓	N	q	✓
✓	✗	✓	✗	N	1	✗
✓	✗	✗	✓	p	q	✓
✗	✓	✓	✗	q	p	✓
✗	✓	✗	✓	1	N	✗
✗	✓	✓	✓	q	N	✓

Table 1.1: Output for $x^2 \equiv y^2 \bmod N$.

Therefore, if we find these two values $x, y \in \mathbb{Z}$, we have 67% chances of re-

covering a prime factor of N.
These two methods allows a first distinction between the factorization algorithms [BW00, p. 168-169]:

- **First category algorithms** are the methods that return the smallest prime divisor of the number we need to factor. These algorithms work well if there is a prime divisor between 7 and 40 digits and they are extremely effective at finding divisors of less than 20 digits.
- **Second category algorithms or Kraitchick family** are the methods based on Fermat's idea explained above. These algorithms do not take into account the size of the factors of N and depend only on its size. They are used when N has more than 100 digits and no small factors.

First Category Algorithms		
Factorization Method	**Execution Time**	**Reference**
Trial Division	$O\left(N^{\frac{1}{2}}\right)$	[Coh13, p. 425]
Pollard's $p-1$ Algorithm	$O\left(N^{\frac{1}{2}}\right)$	[Pol74]
Pollard's ρ	$O\left(N^{\frac{1}{4}}\right)$	[Pol75]
Shanks' Class Group Method	$O\left(N^{\frac{1}{4}}\right)$	[Sha71]
Lenstra's Elliptic Curves Method (ECM)	$O\left(e^{\sqrt{2\log N \log\log N}}\right)$	[LJ87]
Second Category Algorithms		
Factorization Method	**Execution Time**	**Reference**
Lehman's method	$O\left(N^{\frac{1}{3}}\right)$	[Leh74]
Shanks' Square Forms Factorization (SQUFOF)	$O\left(N^{\frac{1}{4}}\right)$	[GWJ08]
Dixon's Factorization Method	$O\left(e^{2\sqrt{2\log N \log\log N}}\right)$	[Dix81]
Continued Fractions Method (CFRAC)	$O\left(e^{\sqrt{2\log N \log\log N}}\right)$	[LP31]
Quadratic Sieve	$O\left(e^{\sqrt{\log N \log\log N}}\right)$	[Pom82]
Multiple Polynomial Quadratic Sieve (MPQS)	$O\left(e^{\sqrt{\log N \log\log N}}\right)$	[Sil87]
General Number Field Sieve (GNFS)	$O\left(e^{\sqrt[3]{\frac{64}{9}\log N(\log\log N)^2}}\right)$	[LLMP93a]

Table 1.2: Recap of some factorization methods for $N = p \cdot q$.

1.1.3 Factorization Records

As we stated above, the problem of factorization guarantees the mathematical security for the RSA protocol, therefore the RSA Laboratories on March 18, 1991 started a competition to promote the research in this topic, [RSAa]. A long list of semiprimes was published on [RSAb], known as *RSA numbers* or *RSA moduli* and a cash prize was assigned to each of them for the successful factorization. The challenge was ended in 2007, but many of the numbers and the search for their factors still continues nowadays. We report a list of the factored numbers:

RSA-Number	**Binary Digits**	**Date of Factorization**	**Method used**	**Reference**
RSA-100	330	1 April 1991	MPQS	N/A
RSA-110	364	14 April 1992	MPQS	[DL93]
RSA-120	397	9 July 1993	MPQS	[DDLM93]
RSA-129	426	26 April 1994	MPQS	[AGLL94]
RSA-130	430	10 April 1996	GNFS	[CDEH$^+$96]
RSA-140	463	2 February 1999	GNFS	[CDL$^+$99]
RSA-150	496	16 April 2004	GNFS	[AKSU04]
RSA-155	512	22 August 1999	GNFS	[CDL$^+$00]
RSA-160	530	1 April 2003	GNFS	[BBF$^+$03]
RSA-170	563	29 December 2009	GNFS	[BK10]
RSA-576	576	3 December 2003	GNFS	[FK03]
RSA-180	596	8 May 2010	GNFS	[DP10]
RSA-190	629	8 November 2010	GNFS	[PT10]
RSA-640	640	2 November 2005	GNFS	[BBFK05b]
RSA-200	663	9 May 2005	GNFS	[BBFK05a]
RSA-210	696	26 September 2013	GNFS	[Pop13]
RSA-704	704	2 July 2012	GNFS	[BTZ12]
RSA-220	729	13 May 2016	GNFS	[BGK$^+$16]
RSA-230	762	15 August 2018	GNFS	[Gro17]
RSA-768	768	12 December 2009	GNFS	[KAF$^+$10]

Table 1.3: Known factorizations of RSA moduli.

It is evident from Table 1.2 and Table 1.3 that, at the moment, the best theoretical and practical factorization method is GNFS, that we will discuss in Chapter 3. However, it is interesting to note that only methods of the second category lead to a succesful factorization for RSA numbers, in according to what we specified about the size of the numbers we deal with the two categories of algorithms.

1.2 Preliminaries on Elementary Number Theory

In this chapter we will recall some results on selected topics in elementary Number Theory that we will exploit in Chapter 2.

1.2.1 Basics on Floor and Ceiling

In Chapter 2 we will explore a novel approach to factorization that involves the use of the floor and the ceiling functions, so we will now recall the properties of these two functions. Our main reference for this section is [GKP94]. We will add the proofs for all the statements that are not explicitly proved in [GKP94].

1.2.2 Definitions and basic properties

Definition 1.3. The *floor* function is defined as

$$\begin{aligned} \lfloor \cdot \rfloor : \mathbb{R} &\to \mathbb{Z} \\ x &\mapsto \max_{i \in \mathbb{Z}} \{i \leq x\}, \end{aligned}$$

while the *ceiling* function is

$$\begin{aligned} \lceil \cdot \rceil : \mathbb{R} &\to \mathbb{Z} \\ x &\mapsto \min_{i \in \mathbb{Z}} \{i \geq x\}. \end{aligned}$$

Using just the definitions, it is possible to highlight some useful inequalities for the floor and the ceiling functions:

Lemma 1.4. *Let x be a real number and $n \in \mathbb{Z}$. Then,*

$$\lfloor x \rfloor = n \quad \text{if and only if} \quad n \leq x < n+1, \tag{1.1}$$

$$\lfloor x \rfloor = n \quad \text{if and only if} \quad x - 1 < n \leq x, \tag{1.2}$$

$$\lceil x \rceil = n \quad \text{if and only if} \quad n - 1 < x \leq n, \tag{1.3}$$

$$\lceil x \rceil = n \quad \text{if and only if} \quad x \leq n < x + 1. \tag{1.4}$$

We can even say something on inequalities that involves directly floors and ceilings.

Lemma 1.5. *Let x be a real number and $m \in \mathbb{Z}$. Then,*

$$\lfloor x \rfloor < m \quad \text{if and only if} \quad x < m, \tag{1.5}$$
$$\lfloor x \rfloor \geq m \quad \text{if and only if} \quad x \geq m, \tag{1.6}$$
$$\lceil x \rceil \leq m \quad \text{if and only if} \quad x \leq m, \tag{1.7}$$
$$\lceil x \rceil > m \quad \text{if and only if} \quad x > m. \tag{1.8}$$

Using these simple relations it is possible to prove the following result for the floor and the ceiling of a sum.

Proposition 1.6. *For every $x, y \in \mathbb{R}$,*

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1, \tag{1.9}$$
$$\lceil x \rceil + \lceil y \rceil - 1 \leq \lceil x + y \rceil \leq \lceil x \rceil + \lceil y \rceil . \tag{1.10}$$

Proof. We will prove it for the floors. Suppose $\lfloor x \rfloor = a \in \mathbb{Z}$ and $\lfloor y \rfloor = b \in \mathbb{Z}$, then by (1.1), we obtain that

$$\begin{cases} a \leq x < a + 1 \\ b \leq y < b + 1. \end{cases}$$

Summing these two inequalities, we obtain $a + b \leq x + y < a + b + 2$. The result follows applying (1.5) and (1.6) respectively. □

There are also some clear links between the floor and the ceiling function:

Lemma 1.7. *Let x be a real number. Then,*

$$\lfloor x \rfloor = x \quad \text{if and only if} \quad x \in \mathbb{Z} \quad \text{if and only if} \quad \lceil x \rceil = x, \tag{1.11}$$
$$\lceil x \rceil - \lfloor x \rfloor = \begin{cases} 1 \text{ if } x \in \mathbb{R} \setminus \mathbb{Z}, \\ 0 \text{ if } x \in \mathbb{Z}, \end{cases} \tag{1.12}$$
$$\lfloor -x \rfloor = - \lceil x \rceil, \tag{1.13}$$
$$\lceil -x \rceil = - \lfloor x \rfloor. \tag{1.14}$$

The first non-trivial result is a theorem given by McEliece:

Theorem 1.8. *[GKP94, pag.71] Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function such that:*

- *f is strictly monotonically increasing (if $x_1 < x_2$, then $f(x_1) < f(x_2)$),*

- *if* $f(x_0) \in \mathbb{Z}$*, then* $x_0 \in \mathbb{Z}$*.*

Then for every $x \in \mathbb{R}$*,*

$$\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor \qquad \textit{and} \qquad \lceil f(x) \rceil = \lceil f(\lceil x \rceil) \rceil .$$

Proof. We prove the theorem for the floors, since the procedure for the ceiling is analogous and can be found in [GKP94]. If $\lfloor x \rfloor = x$, this means by (1.11) that $x \in \mathbb{Z}$ and the thesis follows. We can suppose $x \notin \mathbb{Z}$: we know by (1.1) that $\lfloor x \rfloor \leq x$ and since f is monotonic, $f(\lfloor x \rfloor) \leq f(x)$. Applying the floor function to both sides, we obtain that

$$\lfloor f(\lfloor x \rfloor) \rfloor \leq \lfloor f(x) \rfloor .$$

Suppose $\lfloor f(\lfloor x \rfloor) \rfloor < \lfloor f(x) \rfloor$, then, since f is continous, there must be an element $y \in \mathbb{R}$ such that $f(y) = \lfloor f(x) \rfloor$ and $\lfloor x \rfloor < y \leq x$. Due to the second property of f, since $f(y) \in \mathbb{Z}$, then $y \in \mathbb{Z}$, so y is an integer between $\lfloor x \rfloor$ and x, which cannot be. Then,

$$\lfloor f(\lfloor x \rfloor) \rfloor = \lfloor f(x) \rfloor .$$

□

A similar argument can be applied to monotonically decreasing functions.

Theorem 1.9. *Let* $f : \mathbb{R} \to \mathbb{R}$ *be a continuous function such that:*

- f *is monotonically decreasing (if* $x_1 < x_2$*, then* $f(x_1) > f(x_2)$*),*
- *if* $f(x_0) \in \mathbb{Z}$*, then* $x_0 \in \mathbb{Z}$*.*

Then for every $x \in \mathbb{R}$*,*

$$\lfloor f(x) \rfloor = \lfloor f(\lceil x \rceil) \rfloor \qquad \textit{and} \qquad \lceil f(x) \rceil = \lceil f(\lfloor x \rfloor) \rceil .$$

Proof. Suppose that $x \notin \mathbb{Z}$, otherwise the theorem is obvious. We can define $g(x) = -f(x)$ and since f is a continuous monotonically decreasing function, g is a continuous monotonically increasing function. Furthermore, if $g(x_0) = -f(x_0) \in \mathbb{Z}$, then also x_0 is an integer. So we can apply Theorem 1.8 and obtain that

$$\lfloor g(x) \rfloor = \lfloor g(\lfloor x \rfloor) \rfloor$$
$$\lceil g(x) \rceil = \lceil g(\lceil x \rceil) \rceil .$$

From the first identity and using (1.13), we get that

$$\begin{aligned} \lfloor -f(x) \rfloor &= \lfloor -f\left(\lfloor x \rfloor\right) \rfloor \\ \lceil f(x) \rceil &= \lceil f\left(\lfloor x \rfloor\right) \rceil . \end{aligned}$$

From the second one, using (1.14), we obtain that

$$\begin{aligned} \lceil -f(x) \rceil &= \lceil -f\left(\lceil x \rceil\right) \rceil \\ \lfloor f(x) \rfloor &= \lfloor f\left(\lceil x \rceil\right) \rfloor . \end{aligned}$$

□

Consider the function

$$f : \mathbb{R} \to \mathbb{R} \qquad x \mapsto \frac{x+n}{m},$$

with $n \in \mathbb{Z}$ and $m \in \mathbb{N}^+$. This function is of course continuous and strictly monotonically increasing, since its derivative is $\frac{1}{m} > 0$. Furthermore, if $\frac{x+n}{m} \in \mathbb{Z}$, this also means that $x + n \in m\mathbb{Z}$ and so $x \in \mathbb{Z}$. So, we can apply Theorem 1.8 to f and find that:

Lemma 1.10. *For every $x \in \mathbb{R}$, $n \in \mathbb{Z}$ and $m \in \mathbb{N}^+$ we have that:*

$$\left\lfloor \frac{x+n}{m} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + n}{m} \right\rfloor , \tag{1.15}$$

$$\left\lceil \frac{x+n}{m} \right\rceil = \left\lceil \frac{\lceil x \rceil + n}{m} \right\rceil . \tag{1.16}$$

Another interesting property that links floors and ceilings is the following:

Proposition 1.11. *Let $n \in \mathbb{Z}$ and $m \in \mathbb{N}^+$, then*

$$\left\lfloor \frac{n}{m} \right\rfloor = \left\lceil \frac{n-m+1}{m} \right\rceil = \left\lceil \frac{n+1}{m} \right\rceil - 1, \tag{1.17}$$

$$\left\lceil \frac{n}{m} \right\rceil = \left\lfloor \frac{n+m-1}{m} \right\rfloor = \left\lfloor \frac{n-1}{m} \right\rfloor + 1. \tag{1.18}$$

Proof. We prove the formula (1.17), since (1.18) is analogous. First of all, if $\left\lceil \frac{n-m+1}{m} \right\rceil = k \in \mathbb{Z}$, then by (1.3), $k \leq \frac{n-m+1}{m} < k+1$, which implies that $k+1 \leq \frac{n+1}{m} < k+2$ and again by (1.3) it becomes $\left\lceil \frac{n+1}{m} \right\rceil = k+1$. So the last equality of (1.17) is proved. For the other part, since n and m are integers, we can perform Euclid's algorithm and obtain that $n = mt + r$, with $t \in \mathbb{Z}$

and $0 \leq r < m$. So, $\frac{n}{m} = t + \frac{r}{m}$ and by the discussion on the value of the remainder

$$t \leq t + \frac{r}{m} \leq t + \frac{m-1}{m} < t + 1,$$

which by (1.1) implies $\left\lfloor \frac{n}{m} \right\rfloor = t$. In contrast, $n + 1 = mt + r + 1$, so that $\frac{n+1}{m} = t + \frac{r+1}{m}$ and

$$t < t + \frac{1}{m} \leq t + \frac{r+1}{m} \leq t + 1,$$

that by (1.3) means that $\left\lceil \frac{n+1}{m} \right\rceil = t + 1$, which is exactly what we wanted to show. □

Finally, we present a result on the floor and the ceiling of an integer multiple of a real number:

Proposition 1.12. *For every $x \in \mathbb{R}$ and every $m \in \mathbb{N}^+$,*

$$\lfloor mx \rfloor = \sum_{i=0}^{m-1} \left\lfloor x + \frac{i}{m} \right\rfloor, \tag{1.19}$$

$$\lceil mx \rceil = \sum_{i=0}^{m-1} \left\lceil x - \frac{i}{m} \right\rceil. \tag{1.20}$$

Proof. We will prove this proposition for floors. We will show that

$$n = \sum_{i=0}^{m-1} \left\lfloor \frac{n+i}{m} \right\rfloor,$$

for any $n \in \mathbb{Z}$ and any $m \in \mathbb{N}^+$. In this way, substituting $\lfloor mx \rfloor$ instead of n and applying (1.15), we will obtain the desired result. Fix the value for n and m. We can apply the Euclidean division and obtain that $n = qm + r$, with $q \in \mathbb{Z}$ and $0 \leq r < m$. Then for every $0 \leq i \leq m - 1$, it follows that $n + i = qm + r + i$, which divided by m gives $\frac{n+i}{m} = q + \frac{r+i}{m}$. We want to find for which i, $\left\lfloor q + \frac{r+i}{m} \right\rfloor = q$. This is equivalent by (1.1) to asking when

$$\begin{cases} q + \frac{r+i}{m} < q + 1 \\ q + \frac{r+i}{m} \geq q, \end{cases}$$

which happens when $-r \leq i < m - r$. However both r and i are non-negative, so that $\left\lfloor q + \frac{r+i}{m} \right\rfloor = q$ for $0 \leq i < m - r$. We study now when

$\left\lfloor q + \frac{r+i}{m} \right\rfloor = q + 1$. As before using (1.1), this happens when

$$\begin{cases} q + \frac{r+i}{m} < q + 2 \\ q + \frac{r+i}{m} \geq q + 1, \end{cases}$$

which it is reached when $m - r \leq i < 2m - r$. However, since $m > r$, then $2m - r > m$, it turns out that $\left\lfloor q + \frac{r+i}{m} \right\rfloor = q + 1$ when $m - r \leq i < m$. So

$$\sum_{i=0}^{m-1} \left\lfloor \frac{n+i}{m} \right\rfloor = \sum_{i=0}^{m-1} \left\lfloor \left(q + \frac{r+i}{m} \right) \right\rfloor = q(m-r) + (q+1)r = qm + r = n,$$

as stated. □

1.2.3 Integer solutions of a General Quadratic Diophantine Equation having as discriminant a square

In this section we will briefly explain how to find the integer solutions of a special family of equations:

Definition 1.13. A *General Quadratic Diophantine Equation* defined in $\mathbb{Z}$ is a general polynomial $Q \in \mathbb{Z}[x, y]$ of degree 2 equal to zero, namely

$$Q : ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{1.21}$$

where a, b, c, d, e, $f \in \mathbb{Z}$ are called *coefficients* and it cannot happen that $a = b = c = 0$. The quantity $\Delta = b^2 - 4ac$ is called the *discriminant* of Q.

We will discuss now how to find all the integer solutions of $Q = 0$, following [Edw96], [SSW08] and [Rob03] in the case when $\Delta > 0$ is a square.
Suppose that $a = c = 0$ in (1.21), so that the equation of Q becomes

$$Q : bxy + dx + ey + f = 0. \tag{1.22}$$

In this case the discriminant $\Delta = b^2 > 0$, since $b \neq 0$, otherwise the equation would be linear. So, we may multiply by b (1.22) and obtain

$$(bx + e)(by + d) = ed - bf.$$

We may define $N := ed - bf$, now N can be written as $N = pq$, with p, $q \in \mathbb{Z}$ into finitely many ways, due to the Fundamental Theorem of Arithmetic, so

the system

$$\begin{cases} bx + e = p \\ by + d = q, \end{cases}$$

where p and q vary between the divisors of N, contains the solutions we were looking for:

$$\begin{cases} x = \frac{p-e}{b} \\ y = \frac{q-d}{b}. \end{cases} \tag{1.23}$$

Of course, we need x and y to be integers, so both $p - e$ and $q - d$ must be multiples of b.

We will show now how to always reduce an equation of the form (1.21) into one of the form (1.22), when $\Delta = r^2 \in \mathbb{N}^+$. We may suppose that at least one between a and c is not zero. Suppose it is a, otherwise we can switch x with y so that $a \neq 0$. Multiplying (1.21) by $4a$ we get

$$\begin{aligned} (2ax + by)^2 - (b^2 - 4ac)y^2 + 4adx + 4aey + 4af = 0 \\ (2ax + by + ry)(2ax + by - ry) + 4adx + 4aey + 4af = 0. \end{aligned} \tag{1.24}$$

Using the linear change of variables

$$\begin{cases} S := 2ax + by + ry \\ T := 2ax + by - ry \end{cases} \qquad \begin{cases} x = \frac{bT+rS+rT-bS}{4ar} \\ y = \frac{S-T}{2r} \end{cases} \tag{1.25}$$

and multiplying by r, the equation (1.24) becomes

$$rST + (adr - abd + 2ae)S + (abd + adr - 2ae)T + 4afr = 0, \tag{1.26}$$

which is an equation of the form (1.22) in the new variables S and T. So we may prove the following Proposition:

Proposition 1.14. *Let $Q : ax^2 + bxy + cy^2 + dx + ey + f = 0$ be a General Quadratic Diophantine Equation with discriminant $\Delta = r^2$, where $r \in \mathbb{Z}$. Then, the integer solutions of the equation are given by the integer solutions of*

$$\begin{cases} x = \frac{b(q-p+2abd-4ae)+r(p+q-2adr)}{4ar^2} \\ y = \frac{p-q+4ae-2abd}{2r^2}, \end{cases}$$

where $p, q \in \mathbb{Z}$ are divisors of $N = (adr - abd + 2ae)(abd + adr - 2ae) - 4afr^2$ such that $p \cdot q = N$.

Proof. The solution of (1.26), using the solutions given by (1.23), are

$$\begin{cases} S = \frac{p+2ae-abd-adr}{r} \\ T = \frac{q+abd-adr-2ae}{r}, \end{cases}$$

where $p, q \in \mathbb{Z}$ are divisors of N as defined above. Then, performing the substitutions in (1.25) we get that

$$\begin{aligned} x &= \left(b \left(\frac{q + abd - adr - 2ae}{r} \right) + p + 2ae - abd - adr + q + abd + \right. \\ &\quad \left. - adr - 2ae - b \left(\frac{p + 2ae - abd - adr}{r} \right) \right) \frac{1}{4ar} = \\ &= \left(b \left(\frac{q - p + 2abd - 4ae}{r} \right) + p + q - 2adr \right) \frac{1}{4ar} = \\ &= \frac{b\,(q - p + 2abd - 4ae) + r\,(p + q - 2adr)}{4ar^2} \end{aligned}$$

and

$$\begin{aligned} y &= \left(\frac{p + 2ae - abd - adr}{r} - \frac{q + abd - adr - 2ae}{r} \right) \frac{1}{2r} = \\ &= \frac{p - q + 4ae - 2abd}{2r^2}. \end{aligned}$$

□

1.3 Algebraic Number Theory Background

In the following chapters we will treat in great detail the GNFS algorithm that relies upon some Algebraic Number Theory theorems. We state some basic definition to fix the notation. All these results are taken from [ST01], unless otherwise specified.

1.3.1 Number Fields and Ring of Integers

Definition 1.15. A number $\alpha \in \mathbb{C}$ is called *algebraic* (over $\mathbb{Q}$) if there exists a polynomial $f \in \mathbb{Q}[x]$ with $\deg(f) \geq 1$, such that $f(\alpha) = 0$.

It can be proved that the set of all algebraic numbers

$$A = \{\alpha \in \mathbb{C} : \alpha \text{ is an algebraic number}\}$$

is a field.

Definition 1.16. A *number field* K is a finite-degree field extension of $\mathbb{Q}$, namely $[K : \mathbb{Q}]$ is finite.

An important characterization is the following:

Theorem 1.17. *If K is a number field, then there exists some $\theta \in \mathbb{K}$ algebraic number, such that $K = \mathbb{Q}(\theta)$.*

This theorem essentially states that every number field has a defining element in K that generates the extension. A very important subset of any number field is the set of algebraic integers.

Definition 1.18. An element $\alpha \in \mathbb{C}$ is called *algebraic integer* if there exists a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. In other words, if there exist $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0.$$

We define also the set of all algebraic integers as

$$B = \{\alpha \in \mathbb{C} : \alpha \text{ is an algebraic integer}\}.$$

It turns out that the set B has a more sophisticated algebraic structure:

Theorem 1.19. *The set of all algebraic integers B is a subring of the field of all algebraic numbers A.*

Instead of considering all the ring B, it is more interesting to study a particular restriction of it.

Definition 1.20. Fon any number field K, we define the *ring of integers* of K, as the set

$$\mathfrak{O}_K = K \cap B,$$

namely all the algebraic integers contained in K.

It easily follows from the previous definition that $\mathfrak{O}_K$ is a subring of K. A corollary of the previous theorem can be now stated:

Corollary 1.21. *If K is a number field then $K = \mathbb{Q}(\theta)$, where θ is an algebraic integer.*

Remark 1.1. Fixed an element $\theta \in B$, we define

$$\mathbb{Z}[\theta] = \{f(\theta) : f(x) \in \mathbb{Z}[x]\}.$$

If we consider the number field $\mathbb{Q}(\theta)$, the element θ is an algebraic integer, meaning that $\theta \in \mathfrak{O}_{\mathbb{Q}(\theta)}$, then $\mathbb{Z}[\theta] \subseteq \mathfrak{O}_{\mathbb{Q}(\theta)}$. However, usually $\mathbb{Z}[\theta] \neq \mathfrak{O}_{\mathbb{Q}(\theta)}$. For example, if we consider $\mathbb{Q}(\sqrt{5})$ as number field, and an element

$$\alpha = \frac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5}),$$

then $\alpha \notin \mathbb{Z}[\sqrt{5}]$, but α is a root of the polynomial $f(x) = x^2 - x - 1 \in \mathbb{Z}[x]$, therefore $\alpha \in \mathfrak{O}_{\mathbb{Q}(\sqrt{5})}$. So, in this case

$$\mathbb{Z}[\sqrt{5}] \subsetneq \mathfrak{O}_{\mathbb{Q}(\sqrt{5})} \subsetneq \mathbb{Q}(\sqrt{5}).$$

For quadratic fields, that is $[K : \mathbb{Q}] = 2$, it is possible to identify directly the ring of integers, as stated below.

Theorem 1.22. *Let $d \in \mathbb{Z}$ be a squarefree integer. Then, $\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}$ is equal to*

- $\mathbb{Z}[\sqrt{d}]$ *if* $d \not\equiv 1 \bmod 4$,
- $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *if* $d \equiv 1 \bmod 4$.

Example 1.1. In the previous example, in fact, since $5 \equiv 1 \bmod 4$, then

$$\mathfrak{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right].$$

1.3.2 Norm of an element

Theorem 1.23. *Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. Let $f \in \mathbb{Q}[x]$ be the minimal polynomial of K and call $\theta_1, \ldots, \theta_n$ its roots. Then there are exactly n distinct injective homomorphisms from K to $\mathbb{C}$ that fix $\mathbb{Q}$: for every $i \in \{1, \ldots, n\}$*

$$\begin{aligned} \sigma_i : K &\to \mathbb{C} \\ \theta &\mapsto \theta_i. \end{aligned}$$

From this theorem we obtain a useful definition:

Definition 1.24. Keeping the same notation as the previous theorem, fix $\alpha \in K$, we call $\{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$ the *K-conjugates* of α.

This notion of conjugates it is important to define a crucial quantity for GNFS.

Definition 1.25. Given $\alpha \in \mathbb{Q}(\theta)$, we define the *norm* of α as the product of all its conjugates:

$$N(\alpha)_{\mathbb{Q}(\theta)/\mathbb{Q}} = N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

The norm has some very useful properties that may be summarized in the following proposition.

Proposition 1.26. *(i) For every $\alpha \in \mathbb{Q}(\theta) \setminus \{0\}$, then $N(\alpha) \neq 0$.*

(ii) For every $\alpha, \beta \in \mathbb{Q}(\theta)$, then $N(\alpha\beta) = N(\alpha)N(\beta)$.

(iii) For every $\alpha \in \mathbb{Q}(\theta)$, then $N(\alpha) \in \mathbb{Q}$. In particular if $\alpha \in \mathfrak{O}_{\mathbb{Q}(\theta)}$, then $N(\alpha) \in \mathbb{Z}$.

1.3.3 Ideals in the Ring of Integers

In this section we are going to explain why we will consider ideal factorization in GNFS, instead of the standard factorization of an element in a number field.

Notation. We denote the ideals in $\mathfrak{O}_K$ with gothic lowercase letters.

We will present some results on ring theory. Throughout this section, we will always suppose to deal with commutative rings.

Definition 1.27. An *integral domain* (or just domain) D is a nonzero ring in which, for every $x, y \in D$ if $x \cdot y = 0$, then either $x = 0$ or $y = 0$.

A domain R is a Unique Factorization Domain (UFD) if every non-zero $x \in R$ can be written as the product of irreducible elements $p_1, \ldots, p_n \in R$ ($n \geq 0$) and a unit $u \in R$:

$$x = u \cdot p_1 \cdot p_2 \cdots p_n$$

and this representation is unique, namely if $q_1, \ldots, q_s \in R$ are irreducible and $w \in R$ is a unit such that

$$x = w \cdot q_1 \cdot q_2 \cdots q_s,$$

then $m = s$ and every p_i is associated to some q_j for $1 \leq i, j \leq n$.

We recall the definition of the product between ideals as well as the notion of divisibility between ideals:

Definition 1.28. Given two ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{O}_K$, then their *product* is

$$\mathfrak{ab} = \left\{ a_1 b_1 + \ldots + a_n b_n \, : \, a_1, \ldots, a_n \in \mathfrak{a};\, b_1, \ldots, b_n \in \mathfrak{b}; n \in \mathbb{N}^+ \right\},$$

where the sums considered in the set are finite.
We can also establish a notion of *ideal divisibility* in the following way:

$$\mathfrak{a} \mid \mathfrak{b} \quad \text{if and only if} \quad \mathfrak{a} \supseteq \mathfrak{b}.$$

We remind that an ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ is called *maximal* if $\mathfrak{a}$ is a proper ideal of $\mathfrak{O}_K$ and there are no ideals of $\mathfrak{O}_K$ strictly between $\mathfrak{a}$ and $\mathfrak{O}_K$. An ideal $\mathfrak{p} \neq \mathfrak{O}_K$ is *prime* if, for every $\mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{O}_K$ such that $\mathfrak{ab} \subseteq \mathfrak{p}$, then either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$. This last condition may also be rewritten using the notion of ideal divisibility as $\mathfrak{p} \mid \mathfrak{ab}$ implies $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$. We also report the following fundamental definition:

Definition 1.29. Let D be a domain. Then D is *Noetherian* if one of the following equivalent properties is verified:

- Every ideal I in D is finitely generated.
- Given an ascending chain of ideals in D

  $$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots,$$

  there exists a $N \in \mathbb{N}$ for which $I_n = I_N$ for every $n \geq N$.
- Every non-empty set of ideals, partially ordered by inclusion, has a maximal element, that is, an ideal which is not properly contained in any other ideal in the set.

One of the main properties of a Noetherian domain is expressed by the following theorem:

Theorem 1.30. *If a domain D is Noetherian, then every non-zero, non-invertible $x \in D$ is a product of a finite number of irreducible elements.*

It can be proved that the ring of integers $\mathfrak{O}_K$ is Noetherian, meaning that every element of this ring can be expressed as a product of irreducible elements. To spot irreducible elements or units in the ring of integers, we

employ the norm.

Proposition 1.31. *Let $\mathfrak{O}_K$ be the ring of integers of a number field K and let $x, y \in \mathfrak{O}_K$. Then:*

- *x is a unit if and only if $N(x) = \pm 1$.*
- *If $N(x) = \pm p$, where $p \in \mathbb{N}^+$ is a prime, then x is irreducible.*
- *If x and y are associate, then $N(x) = \pm N(y)$.*

However, $\mathfrak{O}_K$ is not necessarily a UFD:
Example 1.2. In $\mathbb{Q}(\sqrt{-5})$, we have that

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

We want to prove that all these four factors are irreducible in $\mathfrak{O}_{\mathbb{Q}(\sqrt{-5})}$, using the known fact that every element in $\mathfrak{O}_{\mathbb{Q}(\sqrt{-5})}$ is of the form $a+b\sqrt{-5}$, where a,$b \in \mathbb{Z}$. The norm is given by

$$N(a + b\sqrt{-5}) = a^2 + 5b^2,$$

so

$$N(2) = 4, \quad N(3) = 9, \quad N(1 + \sqrt{-5}) = 6 \qquad \text{and} \qquad N(1 - \sqrt{-5}) = 6.$$

So if $2 = x \cdot y$, with $x, y \in \mathfrak{O}_{\mathbb{Q}(\sqrt{-5})}$ (non-unit), then $N(x) = N(y) = \pm 2$. In the same way non-trivial factors for 3 must have norm equal to ± 3, while two irreducible divisors of $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$, must have norm equal to ± 2 and ± 3 respectively. So the problem is to solve

$$a^2 + 5b^2 = \pm 2 \text{ or } \pm 3.$$

But this Diophantine equation has no solution in $\mathbb{Z}$ and so all the elements above are irreducible. Moreover these four elements are not associate, otherwise $N(2) = 4$ would be equal to $N(1 + \sqrt{-5}) = 6$, but this does not happen. So, there are at least two different ways of writing 6 as the product of irreducible elements.

Although $\mathfrak{O}_K$ is not necessarily a UFD, the concept of unique factorization can be extended in some sense to ideals of $\mathfrak{O}_K$. Indeed, it is possible to prove that $\mathfrak{O}_K$ has some important properties reguarding ideals:

Theorem 1.32. *The ring of integers $\mathfrak{O}_K$ of a number field K is a Dedekind*

Domain, meaning equivalently one of the two following definitions:

1. *All the followings hold:*
   - *(i)* $\mathfrak{O}_K$ *is a domain, with field of fractions* K.
   - *(ii)* $\mathfrak{O}_K$ *is Noetherian.*
   - *(iii) If* $\alpha \in K$ *is a root of a monic polynomial equation with coefficients in* $\mathfrak{O}_K$*, then* $\alpha \in \mathfrak{O}_K$.
   - *(iv) Every non-zero prime ideal of* $\mathfrak{O}_K$ *is maximal.*
2. *every non-zero ideal of* $\mathfrak{O}_K$ *can be written as a product of powers of prime ideals, uniquely up to the order of the factors.*

The following definition can be derived from the previous theorem:
Definition 1.33. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a non-zero ideal, then the finite quantity

$$\mathscr{N}(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|$$

is called the *Norm* of the ideal $\mathfrak{a}$.

We would like to point out some properties for this norm of ideals.
Proposition 1.34. *Let* K *be a number field of degree* n.

- *(i) For every* $\mathfrak{a} \subseteq \mathfrak{O}_K$ *non-zero ideal, then* $\mathscr{N}(\mathfrak{a}) \in \mathbb{N}^+$ *and* $\mathscr{N}(\mathfrak{a}) \in \mathfrak{a}$.
- *(ii) For every* $\mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{O}_K$ *non-zero ideals, then* $\mathscr{N}(\mathfrak{ab}) = \mathscr{N}(\mathfrak{a})\mathscr{N}(\mathfrak{b})$.
- *(iii) If* $\mathfrak{a} = \langle a \rangle$ *is a principal ideal in* $\mathfrak{O}_K$*, then* $\mathscr{N}(\mathfrak{a}) = |N_{K/\mathbb{Q}}(a)|$.
- *(iv) Let* $\mathfrak{a}$ *be a non-zero ideal of* $\mathfrak{O}_K$*, then if* $\mathscr{N}(\mathfrak{a})$ *is prime, then* $\mathfrak{a}$ *is a prime ideal.*
- *(v) Conversely, if* $\mathfrak{p}$ *is a prime ideal, then there exist* $p \in \mathbb{N}^+$ *prime number and* $m \in \mathbb{N}^+$ *such that* $\mathscr{N}(\mathfrak{p}) = p^m$*, where* $m \leq n$*. The number* m *is called the degree of the ideal* $\mathfrak{p}$.

Remark 1.2. Suppose that $\mathfrak{a} = \langle a \rangle$ is a principal ideal in $\mathfrak{O}_K$. Then using the previous proposition we get that

$$|N(a)| = \mathscr{N}(\mathfrak{a}).$$

Furthermore, we know that $\mathfrak{a}$ factorizes into prime ideals with a given expo-

nent, say $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$, with $e_1, \ldots, e_k \in \mathbb{N}^+$. So,

$$\begin{aligned} |N(a)| = \mathscr{N}(\mathfrak{a}) = \mathscr{N}\left(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}\right) = \\ = \mathscr{N}(\mathfrak{p}_1)^{e_1} \cdots \mathscr{N}(\mathfrak{p}_k)^{e_k} = \\ = p_1^{e_1 m_1} \cdots p_k^{e_k m_k}, \end{aligned}$$

where the last passage is obtained using the last point of the previous proposition for suitable $m_1, \ldots, m_k \in \mathbb{N}^+$ and $p_1, \ldots, p_k \in \mathbb{N}^+$ not necessarily distinct prime numbers. In GNFS we will only consider *first-degree prime ideals*, i.e. prime ideals for which $m_1 = \ldots = m_k = 1$. We will develop this theory in Chapter 3.

1.4 Groebner Bases Theory

In Chapter 5, we will use the theory of Groebner Bases to describe a new approach for GNFS. We will now recall some of the most important results about this topic.

1.4.1 Multivariate polynomials

We begin with giving some basic definitions and setting the notation. All the results of this section are presented in [CLO13].

Definition 1.35. A *monomial* in $x_1, \ldots, x_n$ is a product of the form

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

where all the exponents $\alpha_1, \alpha_2, \ldots, \alpha_n$ are positive integers. The *total degree* of the monomial is $\alpha_1 + \alpha_2 + \ldots + \alpha_n$.

Notation. We can identify each monomial in a more direct way: calling $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{N}^+)^n$, then

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

We indicate with $|\alpha| = \alpha_1 + \ldots + \alpha_n$ the total degree of the monomial.

Definition 1.36. Let $\mathbb{K}$ be a field. A *polynomial* $f \in \mathbb{K}[x_1, \ldots, x_n]$ is a

finite linear combination of monomials with coefficients in $\mathbb{K}$:

$$f = \sum_{\alpha} a_\alpha x^\alpha,$$

where $a_\alpha \in \mathbb{K}$ and the sum is defined over a finite number of $\alpha \in (\mathbb{N}^+)^n$. We call a_α the *coefficient* of the monomial x^α. If $a_\alpha \neq 0$, then we say that $a_\alpha x^\alpha$ is a *term* of f and we define the *total degree* of f as

$$\deg(f) = \max_{\alpha \in (\mathbb{N}^+)^n} \{|\alpha| : a_\alpha \neq 0\}.$$

Definition 1.37. Let $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. The *ideal generated* by $f_1, \ldots, f_s$ is

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=0}^{s} h_i f_i : h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n] \right\}.$$

Remark 1.3. Suppose we have $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ and the system

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_s(x_1, \ldots, x_n) = 0. \end{cases}$$

If we consider some polynomials $h_1, h_2, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n]$, we may obtain the new equation

$$h_1 f_1 + h_2 f_2 + \ldots + h_s f_s = 0,$$

in which the left-side term is exactly an element of $\langle f_1, \ldots, f_s \rangle$. Thus, we may identify $\langle f_1, \ldots, f_s \rangle$ with all the possible polynomial equations that arise from the starting system. Of course if we succeed in finding a "minimal" (in some sense) set of generators for this ideal, we obtain the "smallest" condition we need the solutions of the system to fulfill.
We will explain now how to introduce these measurement on the polynomials.

1.4.2 Monomial Orderings

We already said how to define a one-to-one correspondence between each monomial in $\mathbb{K}[x_1, \ldots, x_n]$ and $(\mathbb{N}^+)^n$. So, if we establish an ordering $>$ on $(\mathbb{N}^+)^n$, this leads naturally to an order for monomials, in fact if $\alpha > \beta$, then $x^\alpha > x^\beta$.

Definition 1.38. A *monomial ordering* on $\mathbb{K}[x_1, \ldots, x_n]$ is any relation in $(\mathbb{N}^+)^n$ such that:

(i) $>$ is a total ordering on $(\mathbb{N}^+)^n$.

(ii) For every $\alpha, \beta, \gamma \in (\mathbb{N}^+)^n$, if $\alpha > \beta$, then $\alpha + \gamma > \beta + \gamma$.

(iii) $>$ is a well-odering on $(\mathbb{N}^+)^n$, namely for any non-empty subset $S \subseteq (\mathbb{N}^+)^n$, there exists $\alpha \in S$ such that $\alpha < \beta$, for every $\beta \in S$.

The first condition enables us to compare every pair of monomials, so given $x^\alpha, x^\beta \in \mathbb{K}[x_1, \ldots, x_n]$ only one between

$$x^\alpha > x^\beta \qquad x^\alpha = x^\beta \qquad x^\alpha < x^\beta$$

can be true.

The second property preserves the multiplicative structure of monomials: if $x^\alpha > x^\beta$, then multiplying by the same monomial x^γ to both sides, $x^{\alpha+\gamma} > x^{\beta+\gamma}$ does still hold.

The last condition, finally, is equivalent to asking that every strictly decreasing sequence in $(\mathbb{N}^+)^n$

$$\alpha_1 > \alpha_2 > \ldots$$

eventually terminates. This proposition assures that algorithms that act on monomial orderings must terminate if they produce a strictly decreasing sequence.

We will now give a brief description of the most-used monomial orderings:

- *Lexicographic Order*:
  Definition 1.39. Let $\alpha, \beta \in (\mathbb{N}^+)^n$. Then we define the *lexicographic order* $>_{lex}$ as the relation such that $\alpha >_{lex} \beta$ if and only if the leftmost non-zero entry of $\alpha - \beta$ is positive.

  With this ordering each variable in $\mathbb{K}[x_1, \ldots, x_n]$ is alphabetically ordered, in fact $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$. Of course if we change the order of the variables, also the lexicographic ordering will change.

- *Graded Lexicographic Order*:
  Definition 1.40. Let $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in (\mathbb{N}^+)^n$. Then we define the *graded lexicographic order* $>_{grlex}$ as the relation such that $\alpha >_{grlex} \beta$ if and only if

$$\begin{cases} |\alpha| > |\beta| & \text{if } |\alpha| \neq |\beta| \\ \alpha >_{lex} \beta & \text{if } |\alpha| = |\beta|. \end{cases}$$

  This ordering initially considers the sum of the degrees of each monomial, in case of tie it is equivalent to the lexicographic order. Even in this case $x_1 >_{grlex} x_2 >_{grlex} \ldots >_{grlex} x_n$ and again the graded lexicographic order depends on the order of the variables.

- *Graded Reverse Lexicographic Order*:
  Definition 1.41. Let $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in (\mathbb{N}^+)^n$. Then we define the *graded reverse lexicographic order* $>_{grevlex}$ as the relation such that $\alpha >_{grevlex} \beta$ if and only if

$$\begin{cases} |\alpha| > |\beta| & \text{if } |\alpha| \neq |\beta| \\ \text{the rightmost non-zero entry of } \alpha - \beta \text{ is negative} & \text{if } |\alpha| = |\beta|. \end{cases}$$

  Grevlex is similar to grlex, because it considers again the sum of all the exponents of a monomial, but it breaks the ties in favor of the rightmost variable with the smaller exponent. Again all the variables are ordered in the familiar way $x_1 >_{grevlex} x_2 >_{grevlex} \ldots >_{grevlex} x_n$ and changing the order of the variables drastically change also the order of grevlex.

With the notion of monomial ordering we can give new definitions reguarding multivariate polynomials.
Definition 1.42. Let $f = \sum_\alpha a_\alpha x^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$ and $>$ a monomial ordering. The *multidegree* of f is

$$\text{multideg}(f) = \max\left\{\alpha \in (\mathbb{N}^+)^n : a_\alpha \neq 0\right\},$$

where the maximum is taken with respect to $>$.
The *leading coefficient* of f is

$$\text{LC}(f) = a_{\text{multideg}(f)} \in \mathbb{K}.$$

The *leading monomial* of f is

$$\mathrm{LM}(f) = x^{\mathrm{multideg}(f)} \in \mathbb{K}[x_1, \ldots, x_n].$$

The *leading term* of f is

$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f) = a_{\mathrm{multideg}(f)} x^{\mathrm{multideg}(f)} \in \mathbb{K}[x_1, \ldots, x_n].$$

The main reason for the introduction of monomial orderings is to produce an algorithm for the division in $\mathbb{K}[x_1, \ldots, x_n]$.

Theorem 1.43. *Let $>$ be a monomial ordering in $(\mathbb{N}^+)^n$ and define $F = \{f_1, \ldots, f_s\}$ as an ordered set of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Then, for every polynomial $g \in \mathbb{K}[x_1, \ldots, x_n]$ there exist $a_1, \ldots, a_s, r \in \mathbb{K}[x_1, \ldots, x_n]$ such that*

$$g = a_1 f_1 + \ldots a_s f_s + r.$$

Moreover, r can be either equal to 0 or a linear combination of monomials not divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. The polynomial r is called remainder of the division of g by F. Furthermore if $a_i \neq 0$, then

$$\mathrm{multideg}(g) \geq \mathrm{multideg}(a_i f_i),$$

for $1 \leq i \leq s$.

However, this definition does not preserve some of the nice properties of the univariate Euclidean division, such as the uniqueness of the remainder. Therefore, as we saw in Section 1.3, a standard technique is considering ideals instead of elements.

1.4.3 Groebner Bases

For the rest of this section suppose that we fix a monomial ordering $>$. A first fundamental theorem on ideals is the following:

Theorem 1.44 (Hilbert's Basis Theorem)**.** *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. Then there exist $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_s \rangle$.*

This means that every ideal in $\mathbb{K}[x_1, \ldots, x_n]$ is finitely generated and its generators are called a *basis* for the ideal. Clearly a basis for a fixed ideal is not uniquely determined and among them we search for a special one.

Definition 1.45. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be a non-zero ideal. The *set of the*

leading terms of I is

$$\mathrm{LT}(I) = \{cx^\alpha : \text{ there exists } f \in I \text{ such that } \mathrm{LT}(f) = cx^\alpha\}.$$

This definition is needed in order to define a Groebner basis.

Definition 1.46. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal different from $\{0\}$, then a finite subset $G = \{g_1, \ldots, g_s\} \subset I$ is called a *Groebner basis* if

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle = \langle \mathrm{LT}(I) \rangle$$

It can be proved that such a basis exists.

Proposition 1.47. *Every ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ different from $\{0\}$ has a Groebner basis. Furthermore, any Groebner basis for an ideal I is also a basis for I.*

If we employ Grobner bases in the algorithm for divisions, it can be proved that the remainder is uniquely determined:

Proposition 1.48. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and $G = \{g_1, \ldots, g_s\}$ be one of its Groebner bases. Let $f \in \mathbb{K}[x_1, \ldots, x_n]$, then there exists a unique $r \in \mathbb{K}[x_1, \ldots, x_n]$ such that:*

- *every term of r is not divisible by any element of $\{\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\}$,*
- *there exists $g \in \mathbb{K}[x_1, \ldots, x_n]$ such that $f = g + r$.*

An immediate consequence of this proposition is a criterion to establish when a polynomial belongs to a given ideal:

Corollary 1.49. *Let $G = \{g_1, \ldots, g_s\}$ be a Groebner basis for the ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Let $f \in \mathbb{K}[x_1, \ldots, x_n]$, then $f \in I$ if and only if the remainder of the division of f by G is zero.*

Indeed, we would like to give a simpler condition to check whether a basis for an ideal is also a Groebner basis. In order to do that, we need the following definition:

Definition 1.50. Let $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ be non-zero polynomials with $\alpha = (\alpha_1, \ldots, \alpha_n) = \mathrm{multideg}(f)$ and $\beta = (\beta_1, \ldots, \beta_n) = \mathrm{multideg}(g)$. Then the *S-polynomial* of f and g is the polynomial

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g,$$

where $\gamma = (\gamma_1, \ldots, \gamma_n)$ and $\gamma_i = \max\{\alpha_i, \beta_i\}$ for every $1 \leq i \leq n$.

Using the S-polynomials it is possible to prove the following theorem:

Theorem 1.51 (Buchberger's First Criterion)**.** *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and $G = \{g_1, \ldots, g_s\}$ a basis for it. Then G is a Groebner basis if and only if the remainder of the division between $S(g_i, g_j)$ and G is equal to 0 for every $1 \leq i < j \leq n$.*

Starting from this theorem, Buchberger provided also an effective algorithm to compute a Groebner basis of an ideal ([Buc65]):

Theorem 1.52 (Buchberger's Algorithm)**.** *Let $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ be non-zero polynomials and $I = \langle f_1, \ldots, f_s \rangle$ be the ideal generated by them. Then a Groebner basis for I can be constructed in a finite number of steps using Algorithm 1.1.*

Algorithm 1.1 Buchberger's Algorithm

Input: The basis $F = (f_1, \ldots, f_s)$ for the ideal I.
Output: A Groebner basis $G = (g_1, \ldots, g_t)$ fot the ideal I, with $F \subset G$.

```
1:  G = F
2:  repeat
3:      G' = G
4:      for p, q ∈ G with p ≠ q do
5:          S = the remainder of the division between S(p, q) and G'
6:          if S ≠ 0 then
7:              G = G ∪ {S}
8:          end if
9:      end for
10: until G = G'
```

The Groebner bases computed with Algorithm 1.1 may contain more elements than needed.

Lemma 1.53. *Let G be a Groebner basis for the ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Let $g \in G$ be a polynomial such that $\mathrm{LT}(g) \in \langle \mathrm{LT}(G \setminus \{g\}) \rangle$. Then $G \setminus \{g\}$ is also a Groebner basis for I.*

So we may cut out from any Groebner basis the elements that do satisfy the previous lemma.

Definition 1.54. A *minimal Groebner basis* G for an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is a Groebner basis such that for every $g \in G$

(i) $\mathrm{LC}(g) = 1$,

(ii) $\mathrm{LT}(g) \notin \langle \mathrm{LT}(G \setminus \{g\}) \rangle$.

However for a fixed ideal there is more than one minimal Groebner basis. To avoid this situation it can be defined another special Groebner basis.

Definition 1.55. A *reduced Groebner basis* G for an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is a minimal Groebner basis such that for every $g \in G$, none of the monomials of g lies in $\langle \mathrm{LT}(G \setminus \{g\}) \rangle$.

It can be proved the following:

Proposition 1.56. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. Then I has a unique reduced Groebner basis.*

Remembering what we said in Remark 1.3, in order to solve a polynomial system, we may fix a monomial ordering and find a (reduced) Groebner basis for the ideal generated by the equations. Then the solutions of the system must satisfy the equations of the polynomial in the Groebner basis. We would like to obtain polynomials that depend only on one variable, so that it is possible to find a solution and, from that, to find the value of all the other variables. This process is called elimination and will be discussed in the following section.

1.4.4 Elimination Theory

We begin giving formal definitions for the procedure explained above.

Definition 1.57. Let $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. Then for every $0 \leq l \leq n$, the *l-th elimination ideal* I_l is the ideal in $\mathbb{K}[x_{l+1}, \ldots, x_n]$ defined by

$$I_l = I \cap \mathbb{K}[x_{l+1}, \ldots, x_n].$$

If $l = 0$, then $I_0 = I$, while if $l = n$, then $I_n = \{0\}$.

So, when we said that we want to remove all the variables except one from the ideal generated by a Groebner basis, actually we were talking about finding the $n-1$-th elimination ideal. If we fix a lexicographic order, there is more that can be said on elimination ideals.

Theorem 1.58 (The Elimination Theorem)**.** *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and let G be a Groebner basis for I with respect to a lexicographic ordering in which $x_1 > x_2 > \ldots > x_n$. Then, for every $0 \leq l \leq n$, the set*

$$G_l = G \cap \mathbb{K}[x_{l+1}, \ldots, x_n]$$

is a Groebner basis for the l-th elimination ideal.

Moreover, if the ideal is zero-dimensional, the reduced Groebner basis of $G \cap K[x_n]$ contains one univariate polynomial. So going back to the example of the system, it is possible to find firstly a Groebner basis using the lexicographic ordering for the ideal and then consider the Groebner basis for the consecutive elimination ideals to reduce the number of variables until we reach the univariate polynomial. Then we find a partial solution for the system, starting from the univariate polynomial and, finally, recover all the other solutions for the system.

Chapter 2

An elementary approach to factorization

In this chapter we will explain an approach to integer factorization, based on elementary Number Theory.

2.1 Successive moduli

As usual, call $N \in \mathbb{N}^+$ the number to be factorized and let $m \in \mathbb{N}^+$ be such that $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor \leq m \leq \left\lfloor \sqrt{N} \right\rfloor$. Suppose also that

$$\begin{cases} N \equiv a_0 \bmod m \\ N \equiv a_1 \bmod (m+1) \\ N \equiv a_2 \bmod (m+2), \end{cases}$$

where $a_0, a_1, a_2 \in \mathbb{N}^+$ are the smallest non-negative integers that verify this congruences and assume as additional requirement that

$$a_2 \geq a_1 \geq a_0 \geq 0.$$

In this setting, the first congruence can be rewritten as

$$N = a_0 + ml \qquad \text{with} \qquad l := \left\lfloor \frac{N}{m} \right\rfloor \geq 0, \tag{2.1}$$

so that substituting in the second equation this one, we obtain that

$$\begin{aligned} a_1 &\equiv a_0 + ml \bmod (m+1) \\ a_1 - a_0 &\equiv -l \bmod (m+1). \end{aligned}$$

Since $a_1 \geq a_0$ and $m+1 > a_1$, it follows that $m+1 > a_1 - a_0 \geq 0$, so $a_1 - a_0$ is the least non-negative integer modulo $m+1$, that is congruent to $-l$. We can define

$$k := a_1 - a_0 \geq 0$$

and thus $k \equiv -l \bmod (m+1)$, that means that

$$-l = k + (m+1)s \qquad \text{with} \qquad s := \left\lfloor \frac{-l}{m+1} \right\rfloor \leq 0. \tag{2.2}$$

We can iterate the same argument and consider the third equation to obtain that

$$\begin{aligned} a_2 &\equiv a_0 + ml \bmod (m+2) \\ a_2 &\equiv a_0 - 2l \bmod (m+2) \\ a_2 &\equiv a_0 + 2k + 2(m+1)s \bmod (m+2) \\ a_2 &\equiv a_0 + 2k - 2s \bmod (m+2) \\ a_2 - a_0 - 2k &\equiv -2s \bmod (m+2) \\ (a_2 - a_1) - (a_1 - a_0) &\equiv -2s \bmod (m+2). \end{aligned}$$

Since $m+1 \geq a_2$ and $a_2 - a_1 \geq 0$, we obtain the following inequality for this quantity:

$$-m \leq (a_2 - a_1) - (a_1 - a_0) \leq m+1.$$

As a consequence, we can define a quantity w, that we call the *world*, as

$$w := \begin{cases} a_2 - 2a_1 + a_0 & \text{if } a_2 - 2a_1 + a_0 \geq 0, \\ a_2 - 2a_1 + a_0 + m + 2 & \text{if } a_2 - 2a_1 + a_0 < 0. \end{cases}$$

to be the least positive integer such that $w \equiv -2s \bmod m+2$. So we may write

$$-2s = w + (m+2)t \qquad \text{with} \qquad t := \left\lfloor \frac{-2s}{m+2} \right\rfloor.$$

Therefore, we have found a formula for w, which is

$$w = -2s - (m+2)t. \tag{2.3}$$

We treat the two terms in the right part of the equation (2.3) separately: the first term is equal to

$$-2s = -2\left\lfloor \frac{-l}{m+1} \right\rfloor = 2\left\lceil \frac{l}{m+1} \right\rceil,$$

substituting the definition of s and (1.13). Moreover

$$-2s = 2\left\lceil \frac{\lfloor \frac{N}{m} \rfloor}{m+1} \right\rceil = 2\left(\left\lfloor \frac{\lfloor \frac{N}{m} \rfloor - 1}{m+1} \right\rfloor + 1 \right),$$

due to the definition of l and (1.18). Finally,

$$-2s = 2\left(\left\lfloor \frac{\frac{N}{m} - 1}{m+1} \right\rfloor + 1 \right) = 2\left(\left\lfloor \frac{N-m}{m(m+1)} \right\rfloor + 1 \right),$$

employing the identity (1.15). For the second term in (2.3), we use the definition of t and the last equation, obtaining that

$$t = \left\lfloor \frac{-2s}{m+2} \right\rfloor = \left\lfloor \frac{2\left(\left\lfloor \frac{N-m}{m(m+1)} \right\rfloor + 1 \right)}{m+2} \right\rfloor.$$

We prove the following proposition:

Proposition 2.1. *Let $N \in \mathbb{N}^+$ and let m be a positive integer such that $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor \leq m \leq \left\lfloor \sqrt{N} \right\rfloor$. Then, for every $N \geq 50$, we have that*

$$t = \left\lfloor \frac{2\left(\left\lfloor \frac{N-m}{m(m+1)} \right\rfloor + 1 \right)}{m+2} \right\rfloor = 0.$$

Proof. To show that $t = 0$, it is enough to show that

$$0 \leq \frac{2\left(\left\lfloor \frac{N-m}{m(m+1)} \right\rfloor + 1 \right)}{m+2} < 1. \tag{2.4}$$

As regards the left side of (2.4), it is clear:

$$\frac{2\left(\left\lfloor\frac{N-m}{m(m+1)}\right\rfloor+1\right)}{m+2}\geq 0,$$

since $N > m > 0$. On the other hand, we want to prove that

$$\begin{aligned}\frac{2\left(\left\lfloor\frac{N-m}{m(m+1)}\right\rfloor+1\right)}{m+2}&<1\\ 2\left(\left\lfloor\frac{N-m}{m(m+1)}\right\rfloor+1\right)&<m+2\\ \left\lfloor\frac{N-m}{m(m+1)}\right\rfloor&<\frac{m}{2},\end{aligned}\tag{2.5}$$

since m is a positive integer. In order to prove (2.5), we can notice that, applying the inequality (1.1),

$$\left\lfloor\frac{N-m}{m(m+1)}\right\rfloor\leq\frac{N-m}{m(m+1)},$$

so all the pairs $(N,m)\in(\mathbb{N}^+)^2$ that satisfy $\frac{N-m}{m(m+1)}<\frac{m}{2}$ will also fulfill (2.5). The last inequality becomes

$$\begin{aligned}N-m&<\frac{m^2(m+1)}{2}\\ N&<\frac{m^2(m+1)}{2}+m.\end{aligned}\tag{2.6}$$

Remember that $\left\lfloor\sqrt{\frac{N}{2}}\right\rfloor\leq m\leq\left\lfloor\sqrt{N}\right\rfloor$ and consider separately the two inequalities:

- Using the first one, we can say that

$$\sqrt{\frac{N}{2}}-1<\left\lfloor\sqrt{\frac{N}{2}}\right\rfloor\leq m,$$

therefore

$$\begin{aligned}\sqrt{\frac{N}{2}}&<m+1\\ N&<2(m+1)^2.\end{aligned}\tag{2.7}$$

- Considering instead the second one, we can find that

$$m \leq \left\lfloor \sqrt{N} \right\rfloor \leq \sqrt{N},$$

leading to

$$m^2 \leq N. \tag{2.8}$$

Combining together (2.7) and (2.8) and since m^2 is always smaller than $2(m+1)^2$ if $m > 0$, we obtain that

$$m^2 \leq N < 2(m+1)^2. \tag{2.9}$$

To find a solution for (2.5), we study when (2.6) and (2.9) hold at the same time:

$$\begin{cases} N < m + \frac{m^2(m+1)}{2} \\ m^2 \leq N < 2(m+1)^2. \end{cases}$$

If $m^2 \leq 2(m+1)^2 \leq m + \frac{m^2(m+1)}{2}$, then the solutions of the system are exactly all the elements in the interval (2.9). To obtain the desired bound, we have to study when $m^2 \leq m + \frac{m^2(m+1)}{2}$, $m^2 \leq 2(m+1)^2$ and when $2(m+1)^2 \leq m + \frac{m^2(m+1)}{2}$. The first two are attained for every $m \geq 0$, while the third one holds for every $m > 4.522$, but remembering that m is a positive integer, we may assume that $m \geq 5$. By hypothesis if $N \geq 50$, it follows that $m \geq \left\lfloor \sqrt{\frac{N}{2}} \right\rfloor \geq \left\lfloor \sqrt{\frac{50}{2}} \right\rfloor = 5$ and the thesis follows. □

The previous proposition gives us a new equality for the world w:

Corollary 2.2. *Let $N \in \mathbb{N}^+$ such that $N \geq 50$ and let $m \in \mathbb{N}^+$ with $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor \leq m \leq \left\lfloor \sqrt{N} \right\rfloor$, then*

$$w = -2s = 2\left(\left\lfloor \frac{N-m}{m(m+1)} \right\rfloor + 1 \right).$$

A more precise statement can be proved about this quantity:

Proposition 2.3. *Let $N \in \mathbb{N}^+$ be a positive integer such that $N \geq 50$ and let $m \in \mathbb{N}^+$ with $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor \leq m \leq \left\lfloor \sqrt{N} \right\rfloor$, then*

$$w \in \{2, 4, 6\}.$$

If we have also that $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 \leq m \leq \left\lfloor \sqrt{N} \right\rfloor - 1$*, then*

$$w = 4.$$

Proof. We will prove that

$$\left\lfloor \frac{N-m}{m(m+1)} \right\rfloor = \begin{cases} 0 \\ 1 \\ 2 \end{cases},$$

which is also equivalent (by (1.1)) to proving that

$$0 \leq \frac{N-m}{m(m+1)} < 3. \tag{2.10}$$

Since N and m are both positive and $m < N$, we know that $\frac{N-m}{m(m+1)} > 0$. To prove the other side, we need to write a system of inequalities as in Proposition 2.1, where one of them is (2.9), which holds because we are using the same hypothesis as before. The other inequality is, as explained above,

$$\begin{aligned} \frac{N-m}{m(m+1)} &< 3 \\ N - m &< 3m(m+1) \\ N &< 3m^2 + 4m. \end{aligned}$$

So, summarizing, we have to find when

$$\begin{cases} N < 3m^2 + 4m \\ m^2 \leq N < 2(m+1)^2. \end{cases}$$

As before, we will check when the expressions in m are such that the interval given by the second inequality is contained in the first one. In this way, (2.10) will hold for every N and m as in the hypotesis of the proposition. Then, $m^2 \leq 3m^2 + 4m$ and $m^2 \leq 2(m+1)^2$ for every $m \geq 0$, while we have $2(m+1)^2 < 3m^2 + 4m$ for every $m > 1.7$, that means that (2.10) holds if $m \geq 2$, which it is always attained for $N \geq 50$.
For the second part of the theorem we can proceed similarly, noting that, in

this case, we have to prove that

$$1 \leq \frac{N-m}{m(m+1)} < 2. \tag{2.11}$$

On one side,

$$\frac{N-m}{m(m+1)} < 2,$$

it is equivalent to the condition

$$\begin{aligned} \frac{N-m}{m(m+1)} &< 2 \\ N - m &< 2m(m+1) \\ N &< 2m^2 + 3m; \end{aligned}$$

on the other side

$$\frac{N-m}{m(m+1)} \geq 1,$$

which is equal to

$$N \geq m^2 + 2m.$$

Once again this interval is properly defined, since $m^2 + 2m \leq 2m^2 + 3m$ for every $m \geq 0$. We also have to change the interval inequalities for N: an upper bound is given by

$$\begin{aligned} m \geq \left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 > \left(\sqrt{\frac{N}{2}} - 1 \right) + 1 = \sqrt{\frac{N}{2}} \\ 2m^2 > N, \end{aligned}$$

while a lower bound is

$$\begin{aligned} m \leq \lfloor \sqrt{N} \rfloor - 1 \leq \sqrt{N} - 1 \\ (m+1)^2 \leq N, \end{aligned}$$

so (2.9) is replaced by

$$(m+1)^2 \leq N < 2m^2.$$

This interval is well defined when $(m+1)^2 \leq 2m^2$, that is verified when $m \geq 2.41$, which is again achieved for $N \geq 50$. Therefore in this case the

system is

$$\begin{cases} m^2 + 2m \leq N < 2m^2 + 3m \\ (m+1)^2 \leq N < 2m^2. \end{cases}$$

Again our aim is to check when the second interval is contained in the first one: it is clear that $2m^2 \leq 2m^2 + 3m$ and $(m+1)^2 \geq m^2 + 2m$ for every $m \geq 0$. This proves that for every $N \geq 50$, the relation (2.11) holds. □

If we consider the world to be $w = 4$, we can track back our definitions and obtain the following

Corollary 2.4. *Let $N \in \mathbb{N}^+$ be a positive integer such that $N \geq 50$ and let $m \in \mathbb{N}^+$ with $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 \leq m \leq \left\lfloor \sqrt{N} \right\rfloor - 1$, then*

$$N = a_0 + 2m^2 - (k-2)m,$$

where a_0 and k are defined as above.

Proof. By the previous theorem we know that the world $w = 4$, so Corollary 2.2 assures us that $s = -2$. We may substitute the value of s in (2.2) to get that $l = -k + 2(m+1)$ and using this value in (2.1), we obtain the stated result. □

Remark 2.1. The condition of requiring increasing remainders, that is $a_2 \geq a_1 \geq a_0 \geq 0$, may be replaced by the condition of decreasing remainders, i.e. $a_2 \leq a_1 \leq a_0 \leq 0$, and we obtain a formula similar to Proposition 2.3. It is also possible to consider a more general situation, which is explored in Section 2.4.

2.2 A formula for successive moduli

We can now conclude our excursus on successive remainders, proving a formula for all the residues of N modulo every integer greater than m.

Theorem 2.5. *Let $N \in \mathbb{N}^+$ be such that $N \geq 50$ and $m \in \mathbb{N}^+$ such that*

$\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor \leq m \leq \left\lfloor \sqrt{N} \right\rfloor$. *Define*

$$\begin{cases} N \equiv a_0 \bmod m \\ N \equiv a_1 \bmod (m+1) \\ N \equiv a_2 \bmod (m+2), \end{cases}$$

with a_0, a_1, $a_2 \in \mathbb{N}$ *the least non-negative integers that verifies these congruences and such that* $0 \leq a_0 \leq a_1 \leq a_2$. *Define also*

$$k := a_1 - a_0 \qquad \text{and}$$
$$w := \begin{cases} a_2 - 2a_1 + a_0 & \text{if } a_2 - 2a_1 + a_0 \geq 0, \\ a_2 - 2a_1 + a_0 + m + 2 & \text{if } a_2 - 2a_1 + a_0 < 0. \end{cases}$$

Then, we have the following formula: for every $i \in \mathbb{N}$,

$$N \equiv \left(a_0 + ik + w \sum_{j=1}^{i-1} j \right) \bmod (m+i).$$

Proof. From (2.1), we know that $N = a_0 + ml$. So,

$$N = a_0 + ml \equiv a_0 - l \equiv a_0 + k \bmod (m+1)$$

which is the first step of our formula. Now, employing (2.2) and Corollary 2.2, we can simplify the third equation and obtain

$$\begin{aligned} N = a_0 + ml &\equiv a_0 - 2l \bmod (m+2) \\ &\equiv a_0 + 2k + 2(m+1)s \bmod (m+2) \\ &\equiv a_0 + 2k - 2s \bmod (m+2) \\ &\equiv a_0 + 2k + w \bmod (m+2). \end{aligned}$$

This proves the formula for $i = 2$.

Generalising the same strategy, we get that

$$\begin{aligned} N = a_0 + ml &\equiv a_0 - il \bmod (m+i) \\ &\equiv a_0 + i(k + (m+1)s) \bmod (m+i) \\ &\equiv a_0 + ik - i(i-1)s \bmod (m+i) \\ &\equiv a_0 + ik + \frac{i(i-1)}{2} w \bmod (m+i) \\ &\equiv a_0 + ik + w \sum_{j=1}^{i-1} j \bmod (m+i). \end{aligned}$$

□

Of course we may give a more precise formulation, since we already computed the value of the world in Proposition 2.3.

Corollary 2.6. *Using the same notation of the previous theorem, if*

$$\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 \leq m \leq \left\lfloor \sqrt{N} \right\rfloor - 1,$$

then for every $i \in \mathbb{N}$

$$N \equiv \left(a_0 + ik + 2i^2 - 2i\right) \bmod (m+i).$$

Proof. From Theorem 2.5, since in this case $w = 4$ and $w \sum_{j=1}^{i-1} j = 2i(i-1)$, the result trivially follows. □

Example 2.1. Suppose we consider the number $N = 955191388807$. If we perform a search for the $m \in \mathbb{N}^+$ in the interval $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 \leq m \leq \left\lfloor \sqrt{N} \right\rfloor - 1$, we obtain that $m = 691083$ satisfies the following:

$$\begin{cases} N \equiv a_0 := 654112 \bmod m \\ N \equiv a_1 := 654115 \bmod (m+1) \\ N \equiv a_2 := 654122 \bmod (m+2), \end{cases}$$

where $0 \leq a_0 \leq a_1 \leq a_2$. Setting $k := 3$, it is possible to write the formula:

$$N \equiv \left(654112 + 3i + 2i^2 - 2i\right) \bmod (m+i).$$

For example, for $i = 724$, we obtain

$$1703188 \equiv 319574 \bmod (m + i)$$

which is exactly $N \bmod (m + i)$.
If we take as $i = 253810$, we obtain that

$$N \equiv \left(654112 + 3i + 2i^2 - 2i\right) \equiv 128839940122 \equiv 0 \bmod (m + i),$$

in fact $m + i = 944893$ is a factor of N. This example gives us an idea of what we would like to obtain from this formula.

2.3 Successive moduli in factorization

Suppose N is an odd number. Our aim is now to find a positive integer i such that the congruence

$$N \equiv \left(a_0 + ik + 2i^2 - 2i\right) \equiv 0 \bmod (m + i) \tag{2.12}$$

holds. However solving a congruence of this kind is as difficult as solving the congruence

$$N \equiv 0 \bmod x$$

for $x \in \mathbb{N}^+$. We therefore need to develop a different strategy to use this formula.
We can define $k' := k - 2$, so that (2.12) becomes

$$2i^2 + ik' + a_0 \equiv 0 \bmod (m + i),$$

which is equivalent to

$$\begin{aligned} 2i^2 + ik' + a_0 &= x(m + i) \\ 2i^2 + i(k' - x) + a_0 - xm &= 0, \end{aligned}$$

with $x \in \mathbb{Z}$. We want to solve this last equation for i in order to find a factor of N, so

$$i_{1/2} = \frac{x - k' \pm \sqrt{(k')^2 + x^2 - 2xk' - 8a_0 + 8mx}}{4}. \tag{2.13}$$

Remember that i must be and integer, so that the following conditions have to be verified

$$\begin{cases} (k')^2 + x^2 - 2xk' - 8a_0 + 8mx = y^2 \quad \text{with } y \in \mathbb{Z} \\ x - k' \pm y \equiv 0 \bmod 4. \end{cases}$$

Let us focus on the first one for the moment. We need to find all integer solutions $(x, y) \in \mathbb{Z}^2$ of the General Quadratic Diophantine Equation

$$x^2 - y^2 + \left(8m - 2k'\right) x + \left(k'\right)^2 - 8a_0 = 0$$

with discriminant $\Delta = -4 \cdot 1 \cdot (-1) = 4$, which is a square. So we may apply Proposition 1.14 and obtain that the solutions of this equation are the integers that satisfies

$$\begin{cases} x = \frac{2(p+q)-8(8m-2k')}{16} = \frac{(p+q)}{8} - (4m - k') \\ y = \frac{p-q}{8}, \end{cases}$$

where p and q are factors of

$$\begin{aligned} &4\left[(8m - 2k')^2 - 4\left(\left(k'\right)^2 - 8a_0\right)\right] = \\ =&4\left[64m^2 - 32mk' + 32a_0\right] = \\ =&128\left(2m^2 - mk' + a_0\right), \end{aligned}$$

but from Corollary 2.4 the last term is equal to N, so that p and q must be factors of $128N$ such that $pq = 128N$. However x and y must be integers, so both p and q must be multiple of 8: in this way $p+q$ and $p-q$ are multiple of 8. However, since we don't know the factorization of N (that we supposed to be odd) the only possibilities left for (p, q) are (employing the fact that the solutions are symmetric):

- $(p, q) = (8, 16N)$,
- $(p, q) = (16, 8N)$.

In the first case we obtain the solution:

$$\begin{cases} x = 1 + 2N - 4m + k' \\ y = 1 - 2N, \end{cases}$$

which implies that (substituting in (2.13))

$$i = \frac{1 + 2N - 4m + k' - k' \pm (1 - 2N)}{4} = \begin{cases} \frac{1-2m}{2} \\ N - m. \end{cases}$$

Since the first value is not an integer, the only possible value for i is the second one, obtaining that $N \equiv 0 \bmod N$, which is obvious.
The second case instead gives rise to

$$\begin{cases} x = 2 + N - 4m + k' \\ y = 2 - N, \end{cases}$$

which again leads to

$$i = \frac{2 + N - 4m + k' - k' \pm (2 - N)}{4} = \begin{cases} 1 - m \\ \frac{N-2m}{2}. \end{cases}$$

In this case the only integer beween them is the first value, so $i = 1 - m$, but again this is useless, meaning that $N \equiv 0 \bmod 1$.
Thus, to solve (2.12) it is needed to know the factorization of N in order to obtain a non-trivial solution. This proves the following theorem:

Theorem 2.7. *Let N be an odd integer and let $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 \leq m \leq \left\lfloor \sqrt{N} \right\rfloor - 1$ such that*

$$\begin{cases} N \equiv a_0 \bmod m \\ N \equiv a_1 \bmod (m+1) \\ N \equiv a_2 \bmod (m+2) \end{cases}$$

with $0 \leq a_1 \leq a_2 \leq a_2$. Call $k = a_1 - a_0$, then producing the factorization of N is equivalent to finding an integer $i \in \mathbb{N}^+$ for which

$$N \equiv \left(a_0 + ik + 2i^2 - 2i\right) \equiv 0 \bmod (m + i).$$

This last theorem states that, at the moment, the strategy of using the successive moduli does not improve significately the factorization strategy, however it enstablishes a new non-obvious equivalent problem, which may be interesting to study.

2.4 Interpolation

We will now explain how interpolating polynomials can predict the remainders in the same way as the formula in Corollary 2.6.

2.4.1 Successive Remainders and Interpolation

Starting again from our three values a_0, a_1, $a_2 \in \mathbb{Z}$ and

$$\begin{cases} N \equiv a_0 \bmod m \\ N \equiv a_1 \bmod (m+1) \\ N \equiv a_2 \bmod (m+2), \end{cases}$$

we would like to find the interpolating polynomial $f \in \mathbb{Q}[x]$ of degree 2, namely f must satisfy the following:

$$\begin{cases} f(0) = a_0 \\ f(1) = a_1 \\ f(2) = a_2. \end{cases} \tag{2.14}$$

The reason we need f to be a polynomial in $\mathbb{Q}[x]$ is that to find an interpolation between nodes, we need to work in a field, so we will consider rational coefficients. So suppose $f(x) = \alpha \cdot x^2 + \beta \cdot x + \gamma$ with α, β, $\gamma \in \mathbb{Q}$, a simple evaluation in the three points gives

$$\begin{cases} \gamma = a_0 \\ \alpha + \beta + \gamma = a_1 \\ 4\alpha + 2\beta + \gamma = a_2, \end{cases}$$

which can be inverted to obtain the values for the coefficients of f:

$$\begin{cases} \alpha = \frac{a_2 - 2a_1 + a_0}{2} \\ \beta = 2a_1 - \frac{3}{2}a_0 - \frac{a_2}{2} \\ \gamma = a_0. \end{cases} \tag{2.15}$$

We can now prove the following proposition:

Proposition 2.8. *Let N be an odd integer and let*

$\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 \leq m \leq \left\lfloor \sqrt{N} \right\rfloor - 1$ *such that*

$$\begin{cases} N \equiv a_0 \bmod m \\ N \equiv a_1 \bmod (m+1) \\ N \equiv a_2 \bmod (m+2) \end{cases}$$

with $0 \leq a_0 \leq a_1 \leq a_2$ *or* $0 \leq a_2 \leq a_1 \leq a_0$. *Then, the interpolating polynomial* $f \in \mathbb{Q}(x)$ *defined as in* (2.14) *with coefficients as in* (2.15) *is such that, for every* $i \in \mathbb{Z}$,

$$N \equiv f(i) \bmod (m+i).$$

Proof. We will show that $f = \alpha x^2 + \beta x + \gamma$ has the same form of the formula in Corollary 2.6 for the case $a_2 \geq a_1 \geq a_0 \geq 0$, while the case $0 \leq a_2 \leq a_1 \leq a_0$ can be proved similarly and we omit the adapted proof (see Remark 2.1). The coefficient α is equal to $\frac{w}{2}$, which in turn, due to Proposition 2.3, gives that $\alpha = 2$. As reguards β, using the same argument,

$$\beta = 2a_1 - \frac{3}{2}a_0 - \frac{a_2}{2} = a_1 - a_0 - \frac{a_0 - 2a_1 + a_2}{2} = a_1 - a_0 - \frac{w}{2} = k - 2,$$

using the definition of k and again Proposition 2.3. This proves that

$$f(i) = 2i^2 + (k-2)i + a_0,$$

which is exactly the second term of the formula in Corollary 2.6. □

So, it seems that the interpolating polynomial between three nodes expresses the behaviour of the successive remainders of the number N.
A natural question that arises is the following: will the interpolating polynomial approximates the successive remainders even if $a_0 \leq a_1 \leq a_2$ does not hold?
The following example shows the negative answer:
Example 2.2. Fix $N = 577 \cdot 727 = 419479$. Then we consider for m only the values between $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 = 458$ and $\left\lfloor \sqrt{N} \right\rfloor - 1 = 646$. Take $m = 462$, so that

$$\begin{cases} a_0 = 445 \\ a_1 = 1 \\ a_2 = 23. \end{cases}$$

Then the interpolating polynomial is $f(x) = 233x^2 - 677x + 445$. So

$$f(3) = 511 \equiv 46 \bmod m+3 \qquad \text{and} \qquad f(-2) = 2731 \equiv 426 \bmod m-1,$$

while

$$N \equiv 49 \bmod m+3 \qquad \text{and} \qquad N \equiv 419 \bmod m-2.$$

2.4.2 A conjecture on interpolating polynomials

It seems that the request of having growing remainders is necessary. Actually, from experimental results, we state the following conjecture:

Conjecture. Let N be an odd integer and let $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 \leq m \leq \left\lfloor \sqrt{N} \right\rfloor - 1$ such that

$$\begin{cases} N \equiv a_0 \bmod m \\ N \equiv a_1 \bmod (m+1) \\ N \equiv a_2 \bmod (m+2). \end{cases}$$

Then, the interpolating polynomial $f \in \mathbb{Q}(x)$ defined as in (2.14) is such that, for every $i \in \mathbb{Z}$,

$$N \equiv f(i) \bmod (m+i)$$

if and only if $a_0 \leq a_1 \leq a_2$ or $a_0 \geq a_1 \geq a_2$.

If the previous conjecture is true, then we may relax our requests and consider just a monotonic set of three successive remainders. The approach of the interpolating polynomial is useful to find an exact factorization, since if we succeed in finding the roots for it, the corresponding values found for i prove that $m+i$ is a divisor for N.

Example 2.3. Suppose we consider $N = 955191388807$. Then the interval for m is

$$691083 \leq m \leq 977337.$$

We choose $m = 944879$, then

$$\begin{cases} a_0 = 9242080 \\ a_1 = 858247 \\ a_2 = 792216. \end{cases}$$

The interpolating polynomial is

$$f(x) = x^2 - 66034x + 924280,$$

which has two integers roots

$$f(14) = f(66020) = 0.$$

This proves that N should have factors equal to $m + 14 = 944893$ and $m + 66020 = 1010899$ and, in fact,

$$944893 \cdot 1010899 = 955191388807 = N.$$

This example shows the limits of this method: we may find a root for f only when we consider three starting remainders that are in a sequence that grows up to N or decreases to 0. In fact, in the previous example, the successive remainders starting from m are

$$\begin{aligned}
N &\equiv 924280 \bmod m & N &\equiv 858247 \bmod (m+1)\\
N &\equiv 792216 \bmod (m+2) & N &\equiv 726187 \bmod (m+3)\\
N &\equiv 660160 \bmod (m+4) & N &\equiv 594135 \bmod (m+5)\\
N &\equiv 528112 \bmod (m+6) & N &\equiv 462091 \bmod (m+7)\\
N &\equiv 396072 \bmod (m+8) & N &\equiv 330055 \bmod (m+9)\\
N &\equiv 264040 \bmod (m+10) & N &\equiv 198027 \bmod (m+11)\\
N &\equiv 132016 \bmod (m+12) & N &\equiv 66007 \bmod (m+13)\\
N &\equiv 0 \bmod (m+14)
\end{aligned}$$

Therefore, we were already close to one of the factors of N with the value of m. If we choose m to be distant from the factors of N and such that the first three remainders are monotonic, then we would obtain a different polynomial without integer roots, so that we still have to deal with the issue of getting a right value for m in order to obtain a factor of N using the interpolating polynomial.
A possible application of this property could be to find a method to understand when we choose m such that we are in a descending or ascending chain of remainders leading to 0 or N respectively, so that then it is easy to find at least one of the factors.

Chapter 3

The General Number Field Sieve

In this chapter we will describe the classical General Number Field Sieve algorithm as formulated in [BLP93].
A first simpler version of this algorithm was proposed in 1988 by Pollard ([Pol93a]), who presented a factorization for the seventh Fermat Number $F_7 = 2^{128} + 1$, using the ring of integers $\mathbb{Z}[\sqrt[3]{2}]$ of the number field $\mathbb{Q}(\sqrt[3]{2})$. This example does not employ any sieving phase, but eventually led to the development of the (Special) Number Field Sieve ([LLMP93b]), a generalization of Pollard's idea for the factorization of integers of the form $r^e \pm s$, where $r, s \in \mathbb{N}^+$ are small integers and $e \in \mathbb{N}^+$ is large. In the same article it was also presented a first heuristic estimate for the complexity, which showed that the algorithm was sub-exponential.
Finally, in 1993, a more complete version of the algorithm was provided ([BLP93]). It holds for all integers and was therefore called General Number Field Sieve (for a complete history of the evolution of algorithm, we refer to [LLMP93a] and [Pom08]). This is the version that we will entirely report in this chapter: we will present the most important steps of the algorithm, describing the construction of the Rational Factor Base, the Algebraic Factor Base and the Quadratic Characters Base. We will also give some hints on the computation of the heuristic complexity of the algorithm, based on some theorems in Analytic Number Theory. We will always refer to it as the *classical* version of GNFS.
Since the description of this idea, many changes have been made, especially

in the choice of the polynomial and the sieving phase. We will discuss these new developments at the end of the chapter, focusing on the most important changes with respect to the older versions of the sieve. On one hand, we will see how to generalize the polynomials used in GNFS and some criteria to establish if a given polynomial would lead to an adequate number of pairs in the sieving phase; on the other side, we will also present how the techniques of sieving have been improved in order to increase the speed of this phase. In this thesis we will refer to classical GNFS as a starting point to develop new strategies that will be explained in the next chapters.

3.1 Choice of the polynomial

From now on, we will call N the number we want to factorize. The first problem in GNFS is to determine a monic irreducible polynomial $f \in \mathbb{Z}[x]$ of degree d such that there exists $m \in \mathbb{Z}$, which verifies $f(m) \equiv 0 \bmod N$. A common way to create this polynomial is to fix a degree d for the polynomial and take an $m \in \mathbb{Z}$, such that $m \approx N^{\frac{1}{d}}$ in order to obtain that $N = m^d + r$, where $0 \leq r < m^d$. Then we consider the base-m representation of N as

$$N = \sum_{i=0}^{d-1} a_i m^i + m^d,$$

with $0 \leq a_i < m$, for every $i \in \{0, \ldots, d-1\}$. More generally, we can consider the base-m representation of any kN, with $k \in \mathbb{Z}$. The polynomial we consider is then

$$f(x) = a_0 + a_1 x + \ldots + a_{d-1} x^{d-1} + x^d,$$

which returns exactly the value N (or kN), when evaluated in m. Choosing the polynomial in this way, it might (very rarely) happen that f is a reducible polynomial, say $f = gh$, with $g, h \in \mathbb{Z}[x]$ and $\deg(g), \deg(h) < d$. In this case

$$N = f(m) = g(m)h(m),$$

so that $g(m)$ and $h(m)$ are factors for N. If $g(m)$ and $h(m)$ are non-trivial, then we have obtained a factorization for N, while if one of them, say $g(m)$, is equal to N and $h(m) = 1$, then we can take g instead of f as defining polynomial for GNFS. We may therefore assume that f is irreducible.

In the modern implementation of the algorithm, the condition of f being monic has been removed and instead of a single polynomial, two bivariate polynomials $f_1, f_2 \in \mathbb{Z}[x, y]$ are fixed with a common root modulo N. Moreover, some other indicators are computed (such as α-value and Murphy's E-score, [Mur99]) to witness the probability of having chosen "good" polynomials, where f is considered good if it satisfies some properties that will be discussed in Section 3.8.

3.1.1 Producing a difference of squares

Given f, we call $\theta \in \mathbb{C}$ one of its roots and define the number field $\mathbb{Q}(\theta)$. We also consider $\mathbb{Z}[\theta]$, which is a subring of its ring of integers $\mathfrak{O}_{\mathbb{Q}(\theta)}$. The next proposition defines a map from $\mathbb{Z}[\theta]$ to $\mathbb{Z}_N$.

Proposition 3.1. *Given $f \in \mathbb{Z}[x]$ an irreducible monic polynomial, let $\theta \in \mathbb{C}$ be one of its roots and $m \in \mathbb{Z}$ a root of f modulo N. Then, the function ϕ*

$$\begin{aligned} \phi :& \mathbb{Z}[\theta] \to \mathbb{Z}_N \\ & a + b\theta \mapsto a + bm \bmod N \end{aligned}$$

is a surjective ring homomorphism.

We recall from Chapter 1 that GNFS is a method of the second category, meaning that we find two values $x, y \in \mathbb{Z}$ such that $x^2 \equiv y^2 \bmod N$ and $x \not\equiv \pm y \bmod N$. In GNFS, to provide x and y we search for a set $U \subset \mathbb{Z} \times \mathbb{Z}$ such that

$$\prod_{(a,b)\in U} (a + b\theta) = \beta^2 \in \mathbb{Z}[\theta] \qquad \text{and} \qquad \prod_{(a,b)\in U} (a + bm) = y^2 \in \mathbb{Z}.$$

So if we define $x = \phi(\beta) \bmod N$, we obtain that

$$\begin{aligned} x^2 \equiv \phi(\beta)^2 = \phi\left(\beta^2\right) = \\ = \phi\left(\prod_{(a,b)\in U} (a + b\theta)\right) = \prod_{(a,b)\in U} \phi(a + b\theta) \equiv \\ \equiv \prod_{(a,b)\in U} (a + bm) = y^2 \bmod N, \end{aligned}$$

producing the difference of squares we need (however we still must check that $x \not\equiv \pm y \bmod N$). Hence the aim of GNFS is to find a set $U \subseteq \mathbb{Z} \times \mathbb{Z}$

for which

$$\prod_{(a,b)\in U} (a + bm) \tag{3.1}$$

is a square in $\mathbb{Z}$ and, at the same time,

$$\prod_{(a,b)\in U} (a + b\theta) \tag{3.2}$$

is a square in $\mathbb{Z}[\theta]$. For implementative needs, U will actually be a subset of S, namely

$$S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : \gcd(a, b) = 1, |a| \leq \mu, 0 < b \leq \eta\}, \tag{3.3}$$

where $\mu, \eta \in \mathbb{N}^+$ are two parameters chosen at the beginning of the algorithm, that depend on N and define the *sieving region*. To find U, we need to define three special sets, called *bases*:

- The *Rational Factor Base*,
- The *Algebraic Factor Base*,
- The *Quadratic Characters Base*.

The first one addresses the issue of searching for a square in $\mathbb{Z}$ and will be explained in Section 3.2, while the others face the more complicated problem of finding a square in $\mathbb{Z}[\theta]$ and will be discussed in Section 3.3 and Section 3.4.

3.2 The Rational Factor Base

The search for a square in the integers is a procedure employed in many factorization methods, for example in Dixon's Factorization or in the Quadratic Sieve.

Definition 3.2. Given $N \in \mathbb{N}^+$, $f \in \mathbb{Z}[x]$ an irreducible monic polynomial and m a root of f modulo N, we fix a threshold value $B \in \mathbb{N}^+$ and define the *Rational Factor Base* $\mathcal{R}$ as

$$\mathcal{R} = \left\{(m \bmod p_i, p_i) : p_i \in \mathbb{N}^+ \;\middle|\; p_i \leq B \text{ and } p_i \text{ is prime}\right\}.$$

The set $\mathcal{R}$ is essentially the set of all prime numbers up to B, where the first term of each element is noted for implementative reasons.

3.2.1 The Rational Sieve

We search for all the elements with $(a, b) \in S$ of the form $a + bm$, that are *smooth* in $\mathcal{R}$ or equivalently that are B-*smooth*, meaning that all the prime divisors of $a + bm$ are in $\mathcal{R}$, namely all the prime divisors of $a + bm$ are not greater than B. So for each fixed integer $b \in \{1, \ldots, \eta\}$, an array of length $2\mu + 1$ is initialized with the integers $a + bm$ for $-\mu \leq a \leq \mu$. Then for each prime $p \in \mathcal{R}$ we want to track all the a's such that $a + bm \equiv 0 \bmod p$ (and this is why we precomputed each $m \bmod p$ in the definition of $\mathcal{R}$), but this is equivalent to finding all the a in the interval such that $a = -bm + hp$, for any $h \in \mathbb{Z}$ (remember that b, m and p are fixed). So,

$$\begin{aligned} -\mu \leq a &\leq \mu \\ -\mu \leq -bm + hp &\leq \mu \\ \frac{-\mu + bm}{p} \leq h &\leq \frac{\mu + bm}{p} \end{aligned}$$

We run h through all the integers between $\left\lceil \frac{-\mu+bm}{p} \right\rceil$ and $\left\lfloor \frac{\mu+bm}{p} \right\rfloor$ and identify in the array all the $a = -bm + hp$. We divide each $a + bm$ by the highest power of p that divides it and we replace it with the quotient in the same position of the array. We repeat this procedure for all the primes in $\mathcal{R}$. At the end of this process, if there is a position in the array that contains ± 1, then that the corresponding $a + bm$ is smooth in $\mathcal{R}$. If also $\gcd(a, b) = 1$, then we store this value in a set T_1. At the end of the whole sieving step, the set T_1 will consist of

$$T_1 = \{(a, b) \in S : a + bm \text{ is smooth in } \mathcal{R}\}.$$

This sieving part can be speeded up by initializing $-\log_2(|a + bm|)$ in each position of the array and adding $\log_2(p)$ each time, instead of dividing by p. At the end of the phase, if the result in an entry of the array is approximately close to 0, we may assume $a + bm$ is smooth in $\mathcal{R}$. We will see how the problem of finding a subset U for which (3.1) holds is linked to the set T_1 in Section 3.5.

3.3 The Algebraic Factor Base

Our aim for this section is to set a strategy for finding the subset U, in order to obtain a square in $\mathbb{Z}[\theta]$, as described in (3.2). When $\mathbb{Z}[\theta]$ is a Unique Factorization Domain, then we apply a similar process as done in the previous section and obtain a square. However $\mathbb{Z}[\theta]$ is rarely a UFD (exactly if and only if $\mathbb{Z}[\theta] = \mathfrak{O}_{\mathbb{Q}(\theta)}$, [LLMP93b]), which is the case treated by the Special Number Field Sieve. When $\mathbb{Z}[\theta]$ is not a UFD, we use principal ideals in $\mathbb{Z}[\theta]$ of the form $\langle a + b\theta \rangle$. We will mainly work with first-degree prime ideals, as defined in Chapter 1 and it is useful to state the following theorem:

Theorem 3.3. *Let $f \in \mathbb{Z}[x]$ be an irreducible monic polynomial and $\theta \in \mathbb{C}$, one of its roots. Then, for every positive prime p there exists a bijection between*

$$\{(r, p) : r \in \mathbb{Z}_p \mid f(r) \equiv 0 \bmod p\}$$

and

$$\{\mathfrak{p} : \mathfrak{p} \text{ is a first-degree prime ideal in } \mathbb{Z}[\theta] \mid \mathscr{N}(\mathfrak{p}) = p\}.$$

Proof. Given the importance of this theorem, we will give a proof for it.
Suppose $\mathfrak{p}$ is a first-degree prime ideal in $\mathbb{Z}[\theta]$. This means that the norm $\mathscr{N}(\mathfrak{p}) = [\mathbb{Z}[\theta] : \mathfrak{p}] = p$, with $p \in \mathbb{N}^+$ prime number, so that $\mathbb{Z}[\theta]/\mathfrak{p} \cong \mathbb{Z}_p$. It is therefore possible to consider the canonical projection $\pi : \mathbb{Z}[\theta] \to \mathbb{Z}_p$ (which is surjective), with kernel equal to $\mathfrak{p}$. If we consider the polynomial f to be $f = \sum_{i=0}^{d-1} a_i x^i + x^d$, then of course $\pi(f(\theta)) = \pi(0) = 0$, but, on the other hand,

$$\begin{aligned} 0 = \pi(f(\theta)) &= \pi(a_0 + a_1\theta + \ldots + a_{d-1}x^{d-1} + x^d) \equiv \\ &\equiv a_0 + a_1\pi(\theta) + \ldots + a_{d-1}\pi(\theta)^{d-1} + \pi(\theta)^d \bmod p \equiv \\ &\equiv f(\pi(\theta)) \bmod p, \end{aligned}$$

hence $\pi(\theta) = r \in \mathbb{Z}_p$ must be a root of f modulo p.
On the contrary, suppose that p is a prime number and $r \in \mathbb{Z}_p$ is a root for f modulo p. Let $\pi' : \mathbb{Z}[\theta] \to \mathbb{Z}_p$ be the surjective homomorphism that maps θ to r mod p. Let $\mathfrak{p} = \ker \pi'$ be an ideal of $\mathbb{Z}[\theta]$, so by the first isomorphism theorem $\mathbb{Z}[\theta]/\mathfrak{p} \cong \mathbb{Z}_p$, meaning also that $|\mathbb{Z}[\theta]/\mathfrak{p}| = p$, so that $\mathfrak{p}$ is a first-degree prime ideal of $\mathbb{Z}[\theta]$. It is obvious that $\pi' = \pi$, leading to a bijective correspondence between the two sets analysed. □

There are two possible scenarios: $\mathbb{Z}[\theta] = \mathfrak{O}_{\mathbb{Q}(\theta)}$ or the more common case $\mathbb{Z}[\theta] \subsetneq \mathfrak{O}_{\mathbb{Q}(\theta)}$. Suppose we are in the first case.
Recalling what we explained in Remark 1.2, if $\alpha \in \mathbb{Z}[\theta]$ and $\mathfrak{a} = \langle \alpha \rangle$ is a principal ideal of $\mathbb{Z}[\theta]$, then

$$p_1^{m_1} \cdots p_h^{m_h} = |N(\alpha)| = \mathscr{N}(\mathfrak{a}) = \mathscr{N}\left(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}\right), \tag{3.4}$$

where $\{p_1, \ldots, p_h\}$ are prime numbers, while $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ are prime ideals and $\{e_1, \ldots, e_k, m_1, \ldots, m_h\} \in \mathbb{N}^+$. Since in $\mathfrak{O}_{\mathbb{Q}(\theta)}$ every ideal has a unique factorization into prime ideals, it is obvious that α is a square in $\mathbb{Z}[\theta]$ if and only if every $e_1, \ldots, e_k$ is even. In particular if α is a square, then also every m_i is even for every $i \in \{1, \ldots, h\}$. However on the contrary, supposing every m_i to be even does not assure α to be a square. In fact, two undesirable things may happen:

(i) for some p_i there exist more than one prime ideal, say $\mathfrak{p}_{i_1}$ and $\mathfrak{p}_{i_2}$, with corresponding exponents e_{i_1} and e_{i_2} odd, such that

$$\mathscr{N}\left(\mathfrak{p}_{i_1}^{e_{i_1}}\right) \cdot \mathscr{N}\left(\mathfrak{p}_{i_2}^{e_{i_2}}\right) = p_i^{e_{i_1}} \cdot p_i^{e_{i_2}} = p_i^{m_i};$$

(ii) for some p_i there exist an ideal $\mathfrak{p}_j$, with corresponding exponent e_j odd, such that

$$\mathscr{N}\left(\mathfrak{p}_j^{e_j}\right) = p_j^{e_j \cdot u} = p_j^{m_i},$$

with $u \in \mathbb{N}^+$.

The case (ii) can be prevented, by restricting to ideals of a special form.

Proposition 3.4. *Let $a, b \in \mathbb{Z}$ be coprime. Then every prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\theta]$ that divides $\langle a + b\theta \rangle$ is a first-degree prime ideal.*

Proof. Let $\mathfrak{p}$ be a prime ideal that divides $\langle a + b\theta \rangle$. In particular $a + b\theta \in \mathfrak{p}$. Since $\mathscr{N}(\mathfrak{p}) = p^m$, with $m \in \mathbb{N}^+$ and p a prime number, then $\mathbb{Z}[\theta]/\mathfrak{p} \cong \mathbb{F}_{p^m}$ the finite field with p^m elements. Let $\pi : \mathbb{Z}[\theta] \to \mathbb{F}_{p^m}$ be the canonical projection, then $a + b\theta \in \mathfrak{p} = \ker(\pi)$, so $\pi(a + b\theta) \equiv 0 \bmod p$. Suppose now $b \equiv 0 \bmod p$, but then $0 \equiv \pi(a + b\theta) \equiv a + br \equiv a \bmod p$, meaning that also a is a multiple of p and this is not possible, since a and b are coprime. So $b \not\equiv 0 \bmod p$, implying that $\pi(\theta) \equiv -\frac{a}{b} \bmod p$. This last condition is equivalent to $\pi(\mathbb{Z}[\theta]) = \mathbb{F}_p$, but since the projection is surjective, this implies that $m = 1$, proving the desired result. □

To prevent (i), we add constraints on r, where r comes from the correspondence defined earlier by Theorem 3.3.

Proposition 3.5. *Let $a, b \in \mathbb{Z}$ such that $\gcd(a,b) = 1$. Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial and call $\theta \in \mathbb{C}$ on of its roots. Then, the first-degree prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\theta]$, corresponding to the pair (r,p) as in Theorem 3.3, divides $\langle a + b\theta \rangle$ with exponent equal to*

$$e_{p,r}(a+b\theta) = \begin{cases} \operatorname{ord}_p\left(|N(a+b\theta)|\right) & \text{if } a + br \equiv 0 \bmod p \\ 0 & \text{otherwise,} \end{cases} \tag{3.5}$$

where $\operatorname{ord}_p(k)$ is the maximum exponent of p in the factorization of k.

To prove the previous proposition, we need a useful link between the norm of an element in $\mathbb{Q}(\theta)$ and the polynomial defining the number field.

Proposition 3.6. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree d and call $\theta \in \mathbb{C}$ one of its roots. Then, given for every $a, bin\mathbb{Z}$, with $b \neq 0$,*

$$N(a+b\theta) = (-b)^d f\left(-\frac{a}{b}\right).$$

Proof. Call $\theta = \theta_1, \ldots, \theta_d$ the conjugates of θ in $\mathbb{Q}(\theta)$, then

$$\begin{aligned} N(a+b\theta) &= (a+b\theta_1)\cdot(a+b\theta_2)\cdots(a+b\theta_d) = \\ &= (-b)^d\left(-\frac{a}{b}-\theta_1\right)\cdots\left(-\frac{a}{b}-\theta_d\right) = (-b)^d f\left(-\frac{a}{b}\right). \end{aligned}$$

□

We can now prove Proposition 3.5:

Proof of Proposition 3.5. Consider the projection $\pi : \mathbb{Z}[\theta] \to \mathbb{Z}_p$ such that $\pi(\theta) = r \bmod p$ as in the proof of Theorem 3.3, then $\mathfrak{p} \mid \langle a + b\theta \rangle$ if and only if $\langle a + b\theta \rangle \subseteq \mathfrak{p}$ and in particular, $a + b\theta \in \mathfrak{p}$. This translates into $\pi(a + b\theta) \equiv 0 \bmod p$, since $\mathfrak{p}$ is the kernel of π. But the last condition is equivalent to $a + b\pi(\theta) \equiv a + br \equiv 0 \bmod p$. So we have proved that $\mathfrak{p} \mid \langle a + b\theta \rangle$ if and only if $a + br \equiv 0 \bmod p$.

Remembering that, from the proof of Proposition 3.6, $b \not\equiv 0 \bmod p$, it turns out that $N(a + b\theta) \equiv 0 \bmod p$ if and only if $f\left(-\frac{a}{b}\right) \equiv 0 \bmod p$, so that $a \equiv -br \bmod p$, since, by definition, r is a root of f modulo p. Now, to complete the result, we would like to show that the problem highlighted previously does not occur: suppose there exist another first-degree prime

ideal $\mathfrak{p}_2 \neq \mathfrak{p}$, corresponding to the pair (r_2, p), such that $\mathfrak{p}_2 \mid \langle a + b\theta \rangle$. But, this is equivalent to saying that $a + br_2 \equiv 0 \bmod p$ and so $r \equiv r_2 \bmod p$, which is impossible since $\mathfrak{p} \neq \mathfrak{p}_2$. Thus, for any prime p there it can be at most one first-degree prime ideal $\mathfrak{p}$ with norm p that divides $\langle a + b\theta \rangle$, hence, if this happens, it must have exponent equal to the maximum power of p that divides $|N(a + b\theta)|$, which is exactly $\operatorname{ord}_p(|N(a + b\theta)|)$. □

We have now established an exact correspondence between the first-degree prime ideals $\mathfrak{p}$ that divides principal ideals of the form $\langle a + b\theta \rangle \subseteq \mathbb{Z}[\theta]$ and the exponents $e_{p,r}$ when $\mathfrak{O}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta]$, namely recalling (3.4), the relation becomes

$$p_1^{e_{p_1,r_1}(a+b\theta)} \cdots p_k^{e_{p_k,r_k}(a+b\theta)} = |N(a + b\theta)| = \mathscr{N}(\langle a + b\theta \rangle) = \mathscr{N}\left(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}\right), \tag{3.6}$$

where each ideal $\mathfrak{p}_i$ corresponds to the pair (r_i, p_i) using Theorem 3.3 and each $e_i = e_{p_i,r_i}(a + b\theta)$ for every $1 \leq i \leq k$. In this specific setting, $a + b\theta$ is a square if and only if every $e_{p_i,r_i}(a + b\theta)$ is even.

We can now define another fundamental base for GNFS:

Definition 3.7. Given $N \in \mathbb{N}^+$, $f \in \mathbb{Z}[x]$ an irreducible monic polynomial and $\theta \in \mathbb{C}$ one of its roots, we fix a threshold value $C \in \mathbb{N}^+$ and define the *Algebraic Factor Base* $\mathcal{A}$ as

$$\mathcal{A} = \{\mathfrak{p} : \mathfrak{p} \text{ is a first-degree prime ideal of } \mathbb{Z}[\theta] \text{ with } \mathscr{N}(\mathfrak{p}) \leq C\}.$$

Equivalently, using Theorem 3.3,

$$\mathcal{A} = \{(r, p) : p \in \{2, \ldots, C\} \text{ is a prime number and } f(r) \equiv 0 \bmod p\}.$$

It remains to deal with the more consistent case, when $\mathbb{Z}[\theta] \neq \mathfrak{O}_{\mathbb{Q}(\theta)}$ and will be discussed in detail in Section 3.4.

3.3.1 The Algebraic Sieve

We say that an element $a + b\theta \in \mathbb{Z}[\theta]$ is *smooth* in $\mathcal{A}$ if the ideal $\langle a + b\theta \rangle$ factorizes completely into first-degree prime ideals in $\mathcal{A}$, which also means that $|N(a + b\theta)|$ is C-smooth in the sense that we have already defined for

rational numbers. We are now searching for a set

$$T_2 = \{(a,b) \in S : a + b\theta \text{ is smooth in } \mathcal{A}\}.$$

The sieving is performed in a similar way as explained in Section 3.2.1, with minor changes to adapt to ideals. First of all, fixed a value for $b \in \{1, \ldots, \eta\}$, an array of length $2\mu + 1$ is initialized having in each entry the quantity $|N(a+b\theta)|$. For each $\mathfrak{p} = (r, p) \in \mathcal{A}$, we search for the ideals $\langle a+b\theta\rangle$'s that are divisible by $\mathfrak{p}$, that, as we have seen in Proposition 3.5, are those satisfying the condition $a + br \equiv 0 \bmod p$, which can be rewritten as $a = -br + hp$, with $h \in \mathbb{Z}$. Then again, since $-\mu \leq a \leq \mu$, we consider all the $a = -br+hp$, where

$$\left\lceil \frac{-\mu + br}{p} \right\rceil \leq h \leq \left\lfloor \frac{\mu + br}{p} \right\rfloor.$$

For all the a's found in this way, we divide the corresponding $|N(a + b\theta)|$ by the highest power of p that divides it and replace the entry with the result. We repeat the process for all the elements in $\mathcal{A}$. At the end of the procedure, we look for all the elements equal to 1, which are exactly the smooth elements we were looking for, if also $\gcd(a, b) = 1$, we store that pair (a, b) in the set T_2. Then, we move on with the next b. As before, the sieving can be speeded up inizializing the vector with $\log N(a+b\theta)$ for every a and b and then subtract $\log p$, when we found a first-degree prime ideal with norm equal to p that divides $\langle a + b\theta\rangle$. In Section 3.5 we will see how to employ T_2 to find the set U we are searching for.

3.4 General Ring of Integers

We now deal with the general case when $\mathfrak{O}_{\mathbb{Q}(\theta)} \neq \mathbb{Z}[\theta]$. There are some problems in this case: in (3.6) we used the property that the factorization of ideals in $\mathfrak{O}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta]$ is unique, however if $\mathbb{Z}[\theta]$ is different from the whole ring of integers, then it is not a UFD anymore. First of all, we need to define a new function that links the exponent of the factorization in prime ideals in $\mathbb{Z}[\theta]$ to the ones in the factorization in $\mathfrak{O}_{\mathbb{Q}(\theta)}$:

Proposition 3.8. *For each prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\theta]$ we can define a group homomorphism $l_{\mathfrak{p}} : \mathbb{Q}(\theta)^* \to \mathbb{Z}$, such that the following holds:*

(i) For every non-zero $\beta \in \mathbb{Z}[\theta]$, then $l_{\mathfrak{p}}(\beta) \geq 0$.

(ii) If $\beta \in \mathbb{Z}[\theta]$, with $\beta \neq 0$, then $l_{\mathfrak{p}}(\beta) > 0$ if and only if $\beta \in \mathfrak{p}$.

(iii) For all $\alpha \in \mathfrak{O}_{\mathbb{Q}(\theta)}$*, we have* $l_{\mathfrak{p}}(\alpha) = 0$ *for all but finitely many* $\mathfrak{p}$ *and*

$$\prod_{\mathfrak{p}} \mathscr{N}(\mathfrak{p})^{l_{\mathfrak{p}}(\alpha)} = |N(\alpha)|,$$

where $\mathfrak{p}$ *ranges over all the prime ideals in* $\mathbb{Z}[\theta]$*.*

In the case when $\mathfrak{O}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta]$, the function $l_{\mathfrak{p}_i}$ for each prime ideal $\mathfrak{p}_i$ of $\mathbb{Z}[\theta]$ is exactly the exponent e_i, using the notations of (3.6).

Corollary 3.9. *Let* $a, b \in \mathbb{Z}$ *with* $(a, b) = 1$ *and let* $\mathfrak{p}$ *be a prime ideal of* $\mathbb{Z}[\theta]$*. If* $\mathfrak{p}$ *is not a first-degree prime ideal, then* $l_{\mathfrak{p}}(a + b\theta) = 0$*. Instead, if* $\mathfrak{p} = (r, p)$ *is a first-degree prime ideal, then* $l_{\mathfrak{p}}(a + b\theta) = e_{p,r}(a + b\theta)$*.*

Proof. In Proposition 3.4 we already proved the first part of this corollary. The second result, follows from the last point of the previous proposition, comparing the exponents on the left and on the right sides of the equation. □

In this way we have obtained again an exact correspondence between the integer factorization of $|N(a+b\theta)|$ and the ideal factorization of $\langle a+b\theta\rangle$ and we have the following:

Proposition 3.10. *Let* $f \in \mathbb{Z}[x]$ *be a monic irreducible polynomial and call* $\theta \in \mathbb{C}$ *one of its roots and let* $U \subseteq S$*, where* S *is defined as in* (3.3)*. Suppose that*

$$\prod_{(a,b)\in U} (a + b\theta) = \gamma^2 \in \mathfrak{O}_{\mathbb{Q}(\theta)},$$

then for each first-degree prime ideal $\mathfrak{p}$ *corresponding to the pair* (r, p) *we have*

$$\sum_{(a,b)\in U} e_{p,r}(a + b\theta) \equiv 0 \bmod 2.$$

Proof. Since $l_{\mathfrak{p}}$ is a group homomorphism, we obtain that

$$\sum_{(a,b)\in U} e_{p,r}(a + b\theta) = \sum_{(a,b)\in U} l_{\mathfrak{p}}(a + b\theta) = l_{\mathfrak{p}}\left(\prod_{(a,b)\in U} (a + b\theta)\right) =$$
$$= l_{\mathfrak{p}}(\gamma^2) = 2l_{\mathfrak{p}}(\gamma) \equiv 0 \bmod 2.$$

□

Actually, one could wish the converse to hold as well, in order to find a

sufficient condition for an element to be a square in $\mathfrak{O}_{\mathbb{Q}(\theta)}$, but unfortunately this is not the case. However, the number of elements for which the converse fail can be estimated ([BLP93, Theorem 6.7]) and we will explain a way to overcome this situation in Section 3.4.1.

Moreover, we may highlight other four different issues for which this solution might not be enough:

1. The ideal $\left\langle \prod_{(a,b)\in U}(a+b\theta)\right\rangle$ of $\mathfrak{O}_{\mathbb{Q}(\theta)}$ may not be the square of an ideal, since we are working with prime ideals in $\mathbb{Z}[\theta]$ and not in $\mathfrak{O}_{\mathbb{Q}(\theta)}$.
2. Even if $\left\langle \prod_{(a,b)\in U}(a+b\theta)\right\rangle = \mathfrak{a}^2$ for some $\mathfrak{a}$ ideal of $\mathfrak{O}_{\mathbb{Q}(\theta)}$, the ideal $\mathfrak{a}$ may not be principal.
3. Even if $\left\langle \prod_{(a,b)\in U}(a+b\theta)\right\rangle = \langle\gamma^2\rangle$ for some $\gamma \in \mathfrak{O}_{\mathbb{Q}(\theta)}$, it is not necessary that $\prod_{(a,b)\in U}(a+b\theta) = \gamma^2$.
4. Even if $\prod_{(a,b)\in U}(a+b\theta) = \gamma^2$ for some $\gamma \in \mathfrak{O}_{\mathbb{Q}(\theta)}$, it is not guaranteed that $\gamma \in \mathbb{Z}[\theta]$.

If $\mathfrak{O}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta]$, then the first and the last conditions cannot happen. Moreover the last obstruction can be avoided by searching for a $\gamma \in \mathfrak{O}_{\mathbb{Q}(\theta)}$ such that

$$\prod_{(a,b)\in U}(a+b\theta) = \gamma^2,$$

instead of the request given in (3.2). We know that if $\gamma \in \mathfrak{O}_{\mathbb{Q}(\theta)}$, then $\beta = \gamma f'(\theta) \in \mathbb{Z}[\theta]$ (as stated in [Wei98, Proposition 3-7-14]). Keeping the condition that $\prod_{(a,b)\in U}(a+bm) = z^2$ is a square in $\mathbb{Z}$ and using this new definition of β, we can define

$$y = f'(m)z \in \mathbb{Z} \qquad \text{and} \qquad x = \phi(\beta) \in \mathbb{Z}_N.$$

In this way, we can obtain a difference of squares, in fact:

$$\begin{aligned} x^2 \equiv \phi\left(\beta\right)^2 = \phi\left(\beta^2\right) = \\ = \phi\left(f'(\theta)^2 \prod_{(a,b)\in U}(a+b\theta)\right) = \phi\left(f'(\theta)^2\right) \prod_{(a,b)\in U} \phi\left(a+b\theta\right) \equiv \\ \equiv f'(m)^2 \prod_{(a,b)\in U}(a+bm) = f'(m)^2 z^2 = y^2 \bmod N, \end{aligned} \tag{3.7}$$

obtaining again the desired relation.

3.4.1 The Quadratic Characters Base

The three problems left can be addressed by using quadratic characters as suggested by Adelman in [Adl91]. To explain this idea, we present a simpler situation: suppose that X is a finite set of prime numbers and that $l \in \mathbb{Z}^*$ is such that every prime in its factorization that does not belong to X has an even exponent. Suppose also that we cannot know in advance the sign of l and the exponents of its prime factors in X. A test for the squareness of l can be the following: if p is an odd prime number such that $p \notin X$ and $p \nmid l$, then we check the Legendre symbol $\left(\frac{l}{p}\right)$. If it is equal to -1, then l is not a square; on the contrary if the symbol is always 1 for a number of primes greater than $\#X$ it is extremely probable that l is a square. In the same way, replacing $\mathbb{Z}$ with $\mathbb{Z}[\theta]$, we can find a necessary condition for $a+b\theta$ being a square.

Theorem 3.11. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial and call $\theta \in \mathbb{C}$ one of its roots. Let $U \subseteq S$ such that $\prod_{(a,b)\in U}(a+b\theta) = \gamma^2 \in \mathfrak{O}_{\mathbb{Q}(\theta)}$ and let $\mathfrak{q}$ be a first-degree prime ideal corresponding to the pair (s,q) such that for every $(a,b) \in U$, we have that $a+bs \not\equiv 0 \bmod q$ (that is $\mathfrak{q} \nmid \langle a+b\theta \rangle$) and $f'(s) \not\equiv 0 \bmod q$. Then,*

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

Proof. Let $\pi : \mathbb{Z}[\theta] \to \mathbb{Z}[\theta]/\mathfrak{q} \cong \mathbb{F}_q$ be the canonical ring projection that maps θ to $s \bmod q$. If we consider the Legendre symbol modulo q to be a map $\psi_q : \mathbb{F}_q \setminus \{0\} \to \{\pm 1\}$, we can now define the composition $\chi_{\mathfrak{q}} : \psi_q \circ \pi$, where clearly

$$\begin{aligned} \chi_{\mathfrak{q}} &: \mathbb{Z}[\theta] \setminus \mathfrak{q} \to \{\pm 1\} \\ \chi_{\mathfrak{q}}&(a+b\theta) = \left(\frac{a+bs}{q}\right). \end{aligned}$$

As we saw in (3.7), it exists $\beta \in \mathbb{Z}[\theta]$ such that

$$\beta^2 = f'(\theta)^2 \prod_{(a,b)\in U} (a+b\theta).$$

When we apply π to β^2, we obtain that

$$\pi(\beta^2) = \pi\left(f'(\theta)^2 \prod_{(a,b)\in U}(a+b\theta)\right) = f'(s)^2 \prod_{(a,b)\in U}(a+bs) \not\equiv 0 \bmod q,$$

by hypothesis. Thus, we may apply $\chi_{\mathfrak{q}}$ to β^2 and obtain:

$$\begin{aligned}\chi_{\mathfrak{q}}\left(\beta^2\right) &= \chi_{\mathfrak{q}}\left(f'(\theta)^2 \prod_{(a,b)\in U}(a+b\theta)\right) = \psi_q\left(f'(s)^2 \prod_{(a,b)\in U}(a+bs)\right) = \\ &= \left(\frac{f'(s)^2 \prod_{(a,b)\in U}(a+bs)}{q}\right) = \left(\frac{f'(s)^2}{q}\right)\left(\frac{\prod_{(a,b)\in U}(a+bs)}{q}\right) = \\ &= \prod_{(a,b)\in U}\left(\frac{a+bs}{q}\right).\end{aligned}$$

On the other side,

$$\chi_{\mathfrak{q}}\left(\beta^2\right) = \left(\frac{\pi(\beta)^2}{q}\right) = 1,$$

so that the thesis follows. □

Again we proved a necessary, but not sufficient condition for an element to be a square in $\mathfrak{O}_{\mathbb{Q}(\theta)}$. Nevertheless, if a non-zero element $\beta \in \mathbb{Z}[\theta]$ satisfies $\chi_{\mathfrak{q}}(\beta) = 1$ for a large number of first-degree prime ideals $\mathfrak{q}$, it is very likely to be a square in $\mathfrak{O}_{\mathbb{Q}(\theta)}$. In this way all the obstructions presented above can be bypassed. Thus, we can define the last base needed by the algorithm:

Definition 3.12. Let $N \in \mathbb{N}^+$, $f \in \mathbb{Z}[x]$ be an irreducible monic polynomial and $\theta \in \mathbb{C}$ be one of its roots. Let $\mathcal{A}$ be the Algebraic Factor Base as in Definition 3.7 with threshold $C = C(N)$ and define another threshold value $D = D(N)$, we define the *Quadratic Characters Base* $\mathcal{Q}$ as

$$\mathcal{Q} = \left\{(s,q) : f(s) \equiv 0 \bmod q,\ C < q \leq D \text{ and } f'(s) \not\equiv 0 \bmod q\right\}.$$

With this definition, we collect in $\mathcal{Q}$ each of the first-degree prime ideals $\mathfrak{q}$ of $\mathbb{Z}[\theta]$ with $C < \mathcal{N}(\mathfrak{q}) \leq D$ (so that $\mathfrak{q} \notin \mathcal{A}$), corresponding to the pair (s,q) such that $f'(s) \not\equiv 0 \bmod q$. As explained above, we use the elements in this base to check the squareness of the products of the elements found with the Algebraic Factor Base. We will explain this concept in the next section.

3.5 Linear Algebra

After the Rational Sieve and the Algebraic Sieve (described in Section 3.2.1 and Section 3.3.1) we obtained two sets:

$$T_1 = \{(a,b) \in S : a + bm \text{ is smooth in } \mathcal{R}\}$$

and

$$T_2 = \{(a,b) \in S : a + b\theta \text{ is smooth in } \mathcal{A}\}.$$

Recall we are looking for a set $U \subseteq S$ such that

$$\prod_{(a,b)\in U} (a + bm) = y^2 \in \mathbb{Z} \quad \text{and} \quad \prod_{(a,b)\in U} (a + bm) = \gamma^2 \in \mathfrak{O}_{\mathbb{Q}(\theta)},$$

so $U \subseteq T = T_1 \cap T_2$. We also remember the three bases and write explicitly their elements:

- The Rational Factor Base is (essentially) the set of all prime integers up to B:
$$\mathcal{R} = \{p_1, \ldots, p_M\},$$
with M the number of the elements in this set, i.e. $M = \pi(B)$, where in this case π is the prime-counting function.

- The Algebraic Factor Base is the set of all pairs (r,p), with p a prime up to C and r is a root of f modulo p:
$$\mathcal{A} = \{(r_1,p_1), \ldots, (r_{M_1},p_{M_1})\},$$
where M_1 is the dimension of this set. Notice that the primes p_i's with $1 \leq i \leq M_1$ can be repeated.

- The Quadratic Character Base is defined as the set of all pairs (s,q), with $C < q \leq D$ a prime, s a root of f modulo q and $f'(s) \not\equiv 0 \bmod q$, then
$$\mathcal{Q} = \{(s_1,q_1), \ldots, (s_{M_2},q_{M_2})\},$$
where M_2 is the size of the set. Even in this case each q_i $(1 \leq i \leq M_2)$ can appear more than once.

We call $n = 1 + M + M_1 + M_2$ and associate to each element $(a,b) \in T$, a vector $v = (v_1, \ldots, v_n) \in (\mathbb{F}_2)^n$ in the following way:

- $\boldsymbol{v_1}$:
  this value represents the sign of $a + bm$ and we set

$$v_1 = \begin{cases} 0 & \text{if } a + bm > 0 \\ 1 & \text{if } a + bm < 0. \end{cases}$$

- $\boldsymbol{v_2, \ldots, v_{(1+M)}}$:
  since $(a, b) \in T$, then $a + bm$ completely factorizes into the primes in $\mathcal{R}$. But again we are interested in finding a square in $\mathbb{Z}$, so we may consider the exponents of the factorization of $a + bm$ modulo 2: for every $1 \leq i \leq M$

$$v_{(1+i)} = \text{ord}_{p_i}(a + bm) \bmod 2,$$

  where p_i ranges over all the elements in $\mathcal{R}$.

- $\boldsymbol{v_{(2+M)}, \ldots, v_{(1+M+M_1)}}$:
  $(a, b) \in T$, so that the principal ideal $\langle a + b\theta \rangle$ completely factorizes into first-degree prime ideals in $\mathcal{A}$. As we saw in Corollary 3.9, there is a correspondence between the exponents of the ideals and $e_{p,r}(a + b\theta)$, defined in (3.5) for every (r, p) first-degree prime ideal. Thus, for every $1 \leq i \leq M_1$

$$v_{(1+M+i)} = e_{p_i,r_i}(a + bm) \bmod 2,$$

  where (r_i, p_i) varies among all the ideals in $\mathcal{A}$.

- $\boldsymbol{v_{(2+M+M_1)}, \ldots, v_n}$:
  as we explained in Section 3.4.1 to ensure that $\prod_{(a,b)\in U}(a + b\theta)$ is a square in $\mathfrak{O}_{\mathbb{Q}(\theta)}$, we employ the quadratic characters, so these last bits of the vector are set as

$$v_{(1+M+M_1+i)} = \begin{cases} 1 & \text{if } \left(\frac{a+bs_i}{q_i}\right) = -1 \\ 0 & \text{if } \left(\frac{a+bs_i}{q_i}\right) = 1, \end{cases}$$

  for every $1 \leq i \leq M_2$ and where (s_i, q_i) are all the first-degree prime ideals in $\mathcal{Q}$.

It is now possible to write such a vector for every pair $(a, b) \in T$ and arrange them in a matrix $G \in M_{\#T\times n}(\mathbb{F}_2)$ and if $\#T > n$, then there exists at least one non-zero solution $x \in (\mathbb{F}_2)^{\#T}$ for the homogeneous system $xG = 0$. The

non-zero entries of x are exactly the pairs in T that belongs to U, in fact in this way $\prod_{(a,b)\in U}(a+bm)$ is a positive integer, since the first bit is 0 and all the primes appearing in its factorization have even exponents because the successive M entries are null as well, so it is exactly a square in $\mathbb{Z}$. In a similar way $\prod_{(a,b)\in U}(a+b\theta)$ is a square in $\mathfrak{O}_{\mathbb{Q}(\theta)}$, since the exponents in the ideal factorizations are all even and the quadratic characters are all equal to 1.

3.6 Finding The Square Roots

After having obtained a value $\beta^2 \in \mathbb{Z}[\theta]$, we need to compute its square root. In the original paper [BLP93], this is achieved by using the Hensel lifting modulo several prime powers, however this computation may be very time consuming because the integers involved in the last lifting are huge. Couveignes proposed in [Cou93] another method that exploits the Chinese Remainder Theorem, given the condition that the degree of f is odd. The best efficient algorithm to compute the square root of β was given by Montgomery in [Mon93] and later refined in [Ngu98]. This method is based upon fractional ideals and the construction of a lattice, which is then reduced using LLL algorithm.

3.7 Complexity of GNFS

We will now concisely explain the analysis of the performances of GNFS, using results from some well-known functions developed in Analytic Number Theory.

3.7.1 Some analytic considerations

Definition 3.13. For $x \geq 1$ and $y \geq 1$, define the function

$$\psi(x,y) = |\{m \in \mathbb{N} : m \leq x \text{ and } m \text{ is } y\text{-smooth}\}|,$$

where y-smooth means that every prime factor of m is smaller than y.

Using the ψ function, we can define another important function ([Dic30]):

Definition 3.14. For $u \in \mathbb{R}^+$, the *Dickman function* $\rho : \mathbb{R}^+ \to \mathbb{R}^+$ is

$$\rho(u) = \begin{cases} \lim_{r\to\infty} \frac{\psi\left(r, r^{\frac{1}{u}}\right)}{r} & \text{for } u > 1 \\ 1 & \text{otherwise.} \end{cases}$$

This function measures the asymptotic probability that a random value has its largest prime factor at most $r^{\frac{1}{u}}$. In other words it corresponds to the asymptotic probability that the random value is y-smooth, where $u = \frac{\log r}{\log y}$. A survey of results on Dickman's function can be found in [Nor71]. Consider a random integer i uniformly extracted in $[1, x]$. The probability of i being y-smooth is $\frac{\psi(x,y)}{x}$, so the expected number of elements we need to pick to obtain a y-smooth value is $\frac{x}{\psi(x,y)}$. If we want to apply this process k times, we need to consider roughly $\frac{xk}{\psi(x,y)}$ elements. We would like to consider a generalized version of this quantity and minimize it. Before doing that, we need a famous definition:

Definition 3.15. Suppose that $v, w \in \mathbb{R}$ and $0 \leq v \leq 1$. The *L-function* is defined as

$$L_x[v, w] = \exp\left((w + o(1)) (\log x)^v (\log\log x)^{1-v}\right).$$

Theorem 3.16. *Let $g(y)$ be a function defined for $y \geq 2$ such that $g(y) \geq 1$ and $g(y) = y^{1+o(1)}$ for $y \to \infty$. Then, as $x \to \infty$,*

$$\frac{xg(y)}{\psi(x, y)} \geq L_x\left[\frac{1}{2}, \sqrt{2}\right]$$

uniformly for all $y \geq 2$. Moreover,

$$\frac{xg(y)}{\psi(x, y)} = L_x\left[\frac{1}{2}, \sqrt{2}\right]$$

if and only if $y = L_x\left[\frac{1}{2}, \frac{\sqrt{2}}{2}\right]$ for $x \to \infty$.

Remark 3.1. This theorem is used in the analysis of many factoring algorithms (see Table 1.2), in fact if an algorithm $\mathscr{A}$ produces x auxiliary numbers and hopes to find y of them which are y-smooth, then we should check roughly $\frac{xy}{\psi(x,y)}$ of these values to obtain the integers we need. If the time to check each value is $y^{o(1)}$, the expected total time for this step is $\frac{xy^{1+o(1)}}{\psi(x,y)}$. Using Theorem 3.16 it is possible to reduce the computational time choosing $y = L_x\left[\frac{1}{2}, \frac{\sqrt{2}}{2}\right]$, obtaining a total computational time for the sieving phase of

$L_x\left[\frac{1}{2}, \sqrt{2}\right]$. Regarding the linear algebra phase of $\mathscr{A}$, the matrix built after the sieving phase has approximately y rows and y columns, so if the analysis of this matrix has cost $y^{2+o(1)}$, we obtain a total computational time for $\mathscr{A}$ of $L_x\left[\frac{1}{2}, \sqrt{2}\right]$.

This remark gives rise to the following important heuristic principle:
Conjecture. If $x = x(N)$ is the bound on integers which are required to be smooth by some algorithm $\mathscr{A}$ for factoring N, then with an optimal choice of parameters the asymptotic run-time of $\mathscr{A}$ is

$$L_x\left[\frac{1}{2}, \sqrt{2}\right].$$

In the case of GNFS this heuristic complexity can be lowered as we will report in the next section.

3.7.2 Heuristic Complexity

As we saw in Section 1.1.2, the complexity of GNFS is subexponential and its evaluation exploits the results given by Theorem 3.16. To be more specific, the optimal choice for the degree d of the polynomial f is thought to be given by [BLP93, Conjecture 11.4]

$$d = \left(3^{\frac{1}{3}} + o(1)\right)\left(\frac{\log N}{\log\log N}\right)^{\frac{1}{3}}$$

as $N \to \infty$. In this setting the asymptotic run-time is

$$\exp\left((1+o(1))\left(d\log d + \sqrt{(d\log d)^2 + 4\log\left(N^{\frac{1}{d}}\right)\log\log\left(N^{\frac{1}{d}}\right)}\right)\right),$$

which may be transformed, after some manipulations, into

$$\exp\left(\left(\left(\frac{64}{9}\right)^{\frac{1}{3}} + o(1)\right)(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}\right) = L_N\left[\frac{1}{3}, \left(\frac{64}{9}\right)^{\frac{1}{3}}\right].$$

For more details about the heuristic analysis for GNFS we refer to [BLP93] and [LLMP93b].

3.8 Further Developments in GNFS for the Polynomial Choice

The polynomial choice of GNFS has been widely investigated since the formulation we presented above. We will now briefly explain the several modifications that has changed this phase of the algorithm during the last 25 years.

3.8.1 Homogeneous polynomials

The constraint of considering only monic polynomials has the advantage that the root $\theta \in \mathfrak{O}_{\mathbb{Q}(\theta)}$ and so $\mathbb{Z}[\theta]$ has a structure such that is possible to apply Proposition 3.8. However, this choice has the downside effect of considering polynomials with bigger coefficients that may slow the execution time of the algorithm. Trying to overcome this issue, in [BLP93], it is described a new improvement of GNFS: instead of considering a monic univariate polynomial of fixed degree d such that there exists a root m modulo N, we consider a bivariate homogeneous irreducible polynomial $F \in \mathbb{Z}[x, y]$ of degree d

$$F(x, y) = c_d x^d + c_{d-1} x^{d-1} y + \ldots + c_1 x y^{d-1} + c_0 y^d, \tag{3.8}$$

such that there exist two elements $m_1, m_2 \in \mathbb{Z}$ for which $F(m_1, m_2) \neq 0$ and $F(m_1, m_2) \equiv 0 \bmod N$. In this setting, we need a new identification theorem for first-degree prime ideals. Let $\omega \in \mathbb{C}$ be a root of $F(x, c_d)$ and call $f \in \mathbb{Z}[x]$ the polynomial $f(x) = c_d x^d + c_{d-1} x^{d-1} + \ldots c_1 x + c_0$, then it is a straightforward computation seeing that $F(x, y) = y^d f\left(\frac{x}{y}\right)$ and that $\frac{\omega}{c_d} = \theta$ is such that
$F(\theta, 1) = f(\theta) = 0$. In this case θ is not an algebraic integer if $c_d \neq \pm 1$, but ω has this property, since ω is a root of $\frac{F(x, c_d)}{c_d}$, which is a monic polynomial. It can be proved that $A = \mathbb{Z}[\theta] \cap \mathbb{Z}[\theta^{-1}]$ is actually an *order* of $\mathbb{Q}(\theta)$.

Definition 3.17. Let $\mathbb{Q}(\theta)$ be a number field. A subring $A \subset \mathfrak{O}_{\mathbb{Q}(\theta)}$ is called an *order* of $\mathbb{Q}(\theta)$ if the index of the additive group of A with respect to the additive group of $\mathfrak{O}_{\mathbb{Q}(\theta)}$ is finite, i.e.

$$\left[\mathfrak{O}_{\mathbb{Q}(\theta)} : A\right] < \infty.$$

In this setting, we have the following generalization of Theorem 3.3:

Theorem 3.18. *Let $F \in \mathbb{Z}[x,y]$ be an irreducible homogeneous polynomial of degree d as in (3.8), $\omega \in \mathbb{C}$ a root of $F(x, c_d)$ and $\theta = \frac{\omega}{c_d}$. Then, for every p prime number, if $A = \mathbb{Z}[\theta] \cap \mathbb{Z}[\theta^{-1}]$ there exists a bijection between*

$$\left\{ \left(r = \frac{r_1}{r_2}, p \right) : (r_1, r_2) \in \mathbb{Z}_p^2 \;\middle|\; F(r_1, r_2) \equiv 0 \bmod p \right\} \cup \{(\infty, p)\}$$

and

$$\{\mathfrak{p} : \mathfrak{p} \text{ is a first-degree prime ideal in } A \mid \mathscr{N}(\mathfrak{p}) = p\}.$$

We will just give an idea of the function that guarantees the bijection. Consider the ring homomorphism

$$\begin{aligned} \pi_1 : \mathbb{Z}[\alpha] &\to \mathbb{F}_p \\ a + b\alpha &\mapsto a + br \bmod p. \end{aligned}$$

Then if $r_2 \neq 0$ it is possible to identify $\mathfrak{p} = \ker(\pi_1) \cap A$. If $r_2 = 0$ instead, we consider the homomorphism

$$\begin{aligned} \pi_2 : \mathbb{Z}[\alpha^{-1}] &\to \mathbb{F}_p \\ a + b\alpha^{-1} &\mapsto a \bmod p, \end{aligned}$$

so that $\mathfrak{p} = \ker(\pi_2) \cap A$. Notice that in this case if $r_2 = 0$, we identify the first-degree prime ideal with the pair (∞, p). Since we are working with orders now, it is possible to give also a generalization of Proposition 3.8:

Proposition 3.19. *Let $A \subseteq \mathfrak{O}_{\mathbb{Q}(\theta)}$ be an order of $\mathbb{Q}(\theta)$. For each $\mathfrak{p}$ of A prime ideal we can define a group homomorphism $l_\mathfrak{p} : \mathbb{Q}(\theta)^* \to \mathbb{Z}$, such that the following holds:*

(i) For every non-zero $\beta \in A$, then $l_\mathfrak{p}(\beta) \geq 0$.

(ii) If $\beta \in A$, with $\beta \neq 0$, then $l_\mathfrak{p}(\beta) > 0$ if and only if $\beta \in \mathfrak{p}$.

(iii) For all $\alpha \in \mathfrak{O}_{\mathbb{Q}(\theta)}$, we have $l_\mathfrak{p}(\alpha) = 0$ for all but finitely many $\mathfrak{p}$ and

$$\prod_{\mathfrak{p}} \mathscr{N}(\mathfrak{p})^{l_\mathfrak{p}(\alpha)} = |N(\alpha)|,$$

where $\mathfrak{p}$ ranges over all the prime ideals in A.

It is also possible to obtain a similar relation between the norm of elements

in $\mathbb{Q}(\theta)$ and the homogeneous polynomial F, as in Proposition 3.6:

Proposition 3.20. *Let $F \in \mathbb{Z}[x, y]$ be a homogeneous irreducible polynomial as in (3.8) of degree d, call $\omega \in \mathbb{C}$ one of its roots and $\theta = \frac{\omega}{c_d}$. Then, given $a - b\theta \in \mathbb{Q}(\theta)$,*

$$N(a - b\theta) = \frac{F(a, b)}{c_d}.$$

Let $a, b \in \mathbb{Z}$ with $(a, b) = 1$. As before we define the exponent $e_{p,r}$ as the exponent of the prime p in the factorization of $F(a, b)$, i.e.

$$e_{p,r}(a - b\theta) = \begin{cases} \operatorname{ord}_p(a - b\theta) & \text{if } a - br \equiv 0 \bmod p \\ 0 & \text{otherwise.} \end{cases}$$

Finally, we can also retrieve the link between $l_{\mathfrak{p}}(a - b\theta)$ and $e_{p,r}(a, b)$ as in Corollary 3.9:

Corollary 3.21. *Let $a, b \in \mathbb{Z}$ with $(a, b) = 1$ and let $\mathfrak{p}$ be a prime ideal of A. If $\mathfrak{p}$ is not a first-degree prime ideal, then $l_{\mathfrak{p}}(a - b\theta) = 0$. Instead, if $\mathfrak{p}$ is a first-degree prime ideal corresponding to the pair (r, p), then*

$$e_{p,r}(a - b\theta) = \begin{cases} l_{\mathfrak{p}}(a - b\theta) & \text{if } r \neq \infty \\ l_{\mathfrak{p}}(a - b\theta) + \operatorname{ord}_p(c_d) & \text{if } r = \infty. \end{cases}$$

Therefore with homogeneous non-monic bivariate polynomials it is again possible to establish a correspondence between norm and ideal factorization which leads to a sieving method.

3.8.2 GNFS with multiple polynomials

Another improvement in polynomial selection was obtained considering two polynomials instead of only one (see for example [BBKZ16] and [Mur99]). Define two irreducible polynomials $f_1, f_2 \in \mathbb{Z}[x]$ and suppose that there exists an integer m such that

$$f_1(m) \equiv f_2(m) \equiv 0 \bmod N,$$

so that m is a common root for f_1 and f_2 modulo N. Call θ_1 and θ_2, two complex roots respectively of f_1 and f_2. It is therefore possible to define the

two number fields $\mathbb{Q}(\theta_1)$ and $\mathbb{Q}(\theta_2)$. Consider two ring homomorphisms

$$\phi_i : \mathbb{Z}[\theta_i] \to \mathbb{Z} \qquad \theta_i \mapsto m \bmod N \qquad \text{for } i = 1, 2$$

and suppose we recover as usual a set $U \subseteq S$ such that

$$\prod_{(a,b)\in U} (a - b\theta_1) = \beta_1^2$$
$$\prod_{(a,b)\in U} (a - b\theta_2) = \beta_2^2,$$

for some $\beta_1 \in \mathbb{Z}[\theta_1]$ and $\beta_2 \in \mathbb{Z}[\theta_2]$. Then,

$$\phi_1\left(\beta_1^2\right) = \prod_{(a,b)\in U} \left(\phi_1\left(a - b\theta_1\right)\right) \equiv \prod_{(a,b)\in U} (a - bm) \bmod N$$
$$\phi_2\left(\beta_2^2\right) = \prod_{(a,b)\in U} \left(\phi_2\left(a - b\theta_2\right)\right) \equiv \prod_{(a,b)\in U} (a - bm) \bmod N,$$

so

$$\phi_1\left(\beta_1^2\right) \equiv \phi_2\left(\beta_2^2\right) \bmod N.$$

In this way we remove the request of finding a square in $\mathbb{Z}$, by using the Rational Factor Base, but instead we consider two separate Algebraic Factor Bases. Notice that the case $f_2(x) = x - m$ leads to the classical GNFS setting. In practice, the most common situation nowadays is to use a non-linear polynomial of degree 5/6 and another polynomial of degree 1.
In [EH96b] this process is generalized and k irreducible polynomials are considered with a common root $m \in \mathbb{Z}$ modulo N. However, in the same article it is experimentally proved that using two polynomials provides a faster sieving phase rather than taking into account more polynomials.

3.8.3 How to choose polynomials

A full report of the properties that the non-linear polynomials in GNFS should fullfil can be found in [Mur99]. We can define some tests in order to control the "goodness" of the polynomial f before performing the sieving phase. To check whether a polynomial is likely to perform well during GNFS, we analyse:

- *Size property*
  By size we refer to the magnitude of the values taken by the polynomial.

In fact, the dimension of the coefficients of the polynomial f and its degree d influences the sieving region Ω and the time of convergence of the algorithm: the coefficients of f become very large at small d, while at higher degree, the dimension of the matrix in the linear algebra phase is bigger. We may distinguish two different types of polynomials: the *non-skewed* and the *skewed*. The first class corresponds to polynomials with small coefficients which allows us to consider a sieving region of the form $-K \leq a \leq K$, $1 \leq b \leq K$, with $K \in \mathbb{N}^+$. Instead, in skewed polynomials we require only some of the coefficients to be small: if we consider non-monic polynomials as in (3.8), the coefficients a_d, a_{d-1} and a_{d-2} are chosen to be sensibly small and usually $|a_{i-1}| \geq |a_i|$ for every $0 \leq i \leq d$. In this case the sieving region is a rectangle S and the ratio $s > 1$ between the a-length and the b-width is called *skewness*.

- *Root property*
  If a polynomial F has many roots modulo small prime powers, the probability of finding smooth values for the norm is greater than considering random integers. There are some additional techniques that grant skewed-polynomial to have excellent root properties. This is the main reason for their introduction. We will now explain in short how to distinguish a polynomial with good root properties from a random one.

  Definition 3.22. Let S be a sample. Then, the quantity $\text{cont}_p(v)$ (called *contribution*) is the expected value of $\text{ord}_p(v)$ for values of v that ranges through S. If the sample S is the image of a polynomial F, we denote $\text{cont}_p(v)$ as $\text{cont}_p(F)$ and it is called *typical F-value*.

  If we consider a random element i_r, the average contribution of p to i_r is

  $$\text{cont}_p(i_r) = \frac{1}{p-1}.$$

  Instead, if $f \in \mathbb{Z}[x]$ is a univariate monic polynomial, the typical f-value is

  $$\text{cont}_p(f) = \frac{n_p}{p-1}, \tag{3.9}$$

  where n_p is the number of distinct roots of f modulo p, while if $F \in \mathbb{Z}[x, y]$ is a bivariate homogeneous polynomial as in (3.8), the

typical F-value is

$$\mathrm{cont}_p(F) = n_p \left(\frac{p}{p^2 - 1} \right), \tag{3.10}$$

where again we denote with n_p the number of distinct roots $(\overline{x}, \overline{y})$ of F modulo p. During the sieving phase (see Section 3.3.1), the contribution of each prime $p \leq C$ is removed from each value being sieved, removing $\log p$ from the previous value. So, a random element i_r would appear as

$$\log i_r - \sum_{p \leq C} \frac{\log p}{p-1},$$

while each polynomial value of the form $f(x) = v$ or $F(x, y) = v$ after the sieving becomes

$$\log v - \sum_{p \leq C} \mathrm{cont}_p(v) \cdot \log p.$$

The difference between these two quantities is called the *α-value* of a polynomial f (or F) and it is defined as

$$\alpha = \sum_{p \leq C} \left(\frac{1}{p-1} - \mathrm{cont}_p(v) \right) \log p,$$

which may be specialized using (3.9) and (3.10)

$$\alpha(f) = \sum_{p \leq C} (1 - n_p) \frac{\log p}{p-1}$$
$$\alpha(F) = \sum_{p \leq C} \left(1 - n_p \frac{p}{p+1} \right) \frac{\log p}{p-1}.$$

So from these formulas

$$\log f(x) = \log i_r + \alpha(f)$$
$$\log F(x, y) = \log i_r + \alpha(F).$$

This means that each value $F(x, y) = v$ acts like a random integer of size $F(x, y) \cdot e^{\alpha(F)}$. In fact when $\alpha(F) < 0$, v has more chances of being smooth than a random element of the same size. We see that $\alpha(F)$ is smaller when n_p is bigger for p small primes, namely when F has more

roots modulo p.

- *Murphy's E-score*
  Suppose we are in the setting of having two homogeneous defining polynomials for GNFS as described in Section 3.8.2 and suppose we are working with non-skewed polynomials F_1 and F_2. Since the polynomial F_j is homogeneous, we can write it in its projective coordinates as

  $$F_j(x, y) = r^d F_j(\cos\psi, \sin\psi).$$

  Our aim is to estimate $F_j(\cos\psi, \sin\psi)$. Define

  $$u_{F_j}(\psi) = \frac{\log|F_j(\cos\psi, \sin\psi| + \alpha(F_j)}{\log C_j},$$

  where C_j is the smoothness bound for F_j. We divide the interval $[0, \pi]$ uniformly into K sub-intervals and set a collection of

  $$\psi_i = \frac{\pi}{K}\left(i - \frac{1}{2}\right),$$

  for $i = 1, \ldots, K$. In this way ψ_i is the mean of the i-th interval. Now, we can define the following quantity called *Murphy's E-score*:

  $$E(F_1, F_2) = \sum_{i=1}^{K} \rho\left(u_{F_1}(\psi_i)\right) \rho\left(u_{F_2}(\psi_i)\right),$$

  where ρ is the Dickman function as defined in Definition 3.14. Murphy's E-value can be defined similarly for skewed polynomials. This quantity tests the goodness of polynomials for GNFS without performing the sieving. The E-score takes into account both the root and the size properties and compares the estimates on the possible smooth values over the sieving region. The higher the value $E(F_1, F_2)$ is, the more probable the pair (F_1, F_2) would lead to a sufficient number of coprime sieving pairs to perform the sieving step in GNFS.

We are therefore interested in polynomials with small coefficients, so that we can obtain small values when evaluated, and with many roots modulo small prime powers. The most important and famous algorithm to obtain polynomials in such a way is the so-called Kleinjung's algorithm ([Kle06]), that was also used to implement GNFS for the biggest RSA number factorized so far, RSA-768 [KAF$^+$10]. This method consists of creating many skewed

polynomials of the form (3.8), such that the coefficients $|c_d|$ and $|c_{d-1}|$ are very small, while $|c_{d-2}|$ is small. The other coefficients are not controlled, but the skewness, the α-value and Murphy's E-score are computed to analyse the behaviour of the polynomials.
This algorithm, presented in 2006, is the last notable improvement in the polynomial selection for GNFS. Other successive articles on this topic, such as [BBKZ16] or [Cox15], are mainly based on Kleinjung's work to obtain some refinements on some other coefficients. However these further improvements have not led to a successful factorization for a number with more than 768 binary digits.

3.9 Other sieving methods

The ideas of rational and algebraic sieve presented in Section 3.2.1 and Section 3.3.1 are the first ones proposed in [BLP93] and are often called *classical sieving*. However nowadays this procedure is no longer used, since more refined and faster sieving techniques have been developed. We will shortly describe some of them in this section.

3.9.1 Lattice Sieving

The lattice sieving was proposed by John Pollard in [Pol93b]. We fix a prime q for which F has at least one root modulo q. This means that the elements q we are considering are the norm of some first-degree prime ideals in the algebraic factor base $\mathcal{A}$. Suppose also that $m \not\equiv 0 \bmod q$. The prime q is called *special prime*. The sieving is done only on coprime pairs $(a, b) \in \mathbb{Z}^2$ such that $a + bm \equiv 0 \bmod q$, namely we consider the set

$$L_q = \{(a, b) : a + bm \equiv 0 \bmod q \mid \gcd(a, b) = 1\}.$$

This set is a lattice on the (a, b) plane. Then we consider a basis for L_q

$$V_1 = (a_1, b_1) \qquad \text{and} \qquad V_2 = (a_2, b_2)$$

made of short vectors. In this way, for every $(a, b) \in L_q$, there exist $c, d \in \mathbb{Z}$

$$(a, b) = (c \cdot a_1 + d \cdot a_2, c \cdot b_1 + d \cdot b_2).$$

We can therefore consider any point of L_q as a point in the plane with coordinates (c, d), which are the coordinates with respect to the basis $\{V_1, V_2\}$. If $\gcd(a, b) = 1$ it is straightforward that $(c, d) = 1$. However if $(c, d) = 1$ then $(a, b) = 1$, unless $a \equiv b \equiv 0 \bmod q$. In this latter case, we may consider $\frac{a}{q}$ and $\frac{b}{q}$ instead. Then, it is possible to consider only coprime pairs (c, d). The lattice sieve then starts building a two-dimension array A in the following way: suppose $(c, d) \in [-\mu, \mu] \times [1, \eta]$, then we may write

$$A = \left(\begin{array}{ccc|c} -\mu & \cdots & \mu & 1 \\ -\mu & \cdots & \mu & 2 \\ \vdots & \ddots & \vdots & \vdots \\ -\mu & \cdots & \mu & \eta \end{array}\right),$$

where we indicate each entry $A[c, d]$ as the elements $(c, d) \in L$. The sieving array A is used twice: firstly for the factorization of $a + bm$, then for the factorization of $N(a + b\theta)$. Let us consider just the first one, since the second case is analogous. The array A is set to 0, then we sum $\log(p)$ for those primes p that divide $(a + bm)$, where each corresponding pair (a, b) has a representation (c, d) in the base $\{V_1, V_2\}$, remembering that we are considering only (c, d) coprime. To do so, consider the array element $A[c, d]$, which represents the integer

$$a + bm = c \cdot u_1 + d \cdot u_2,$$

where

$$u_1 = a_1 + b_1 m$$
$$u_2 = a_2 + b_2 m.$$

Since V_1 and V_2 are elements of the lattice L_q then $u_1 \equiv u_2 \equiv 0 \bmod q$. In our assumptions, since $\gcd(c, d) = 1$, it means that $\gcd(u_1, u_2) = q$. So, the element $A[c, d]$ is to be sieved if and only if

$$c \cdot u_1 + d \cdot u_2 \equiv 0 \bmod p,$$

and it cannot happen that $u_1 \equiv u_2 \equiv 0 \bmod p$. We treat separately the different cases:

- Case $u_1 \equiv 0 \bmod p$.

In this case every element in the row with $d \equiv u_2^{-1} \bmod p$ is sieved.

- Case $u_2 \equiv 0 \bmod p$.
  In this case every element in the column with $c \equiv u_1^{-1} \bmod p$ is sieved.
- Case $u_1 \not\equiv 0 \bmod p$ and $u_2 \not\equiv 0 \bmod p$.
  In this case we may proceed into two different ways:

  (i) *Sieving by rows.*
  For every $d \in \{1, \ldots, \eta\}$, we find the least positive integer such that $c \equiv -du_2u_1^{-1} \bmod p$ and sieve that element, call it $A[c, d]$. Then we sieve also every p elements on the same row from $A[c, d]$. This method is similar to that used in classical sieving and it performs well on small primes.

  (ii) *Sieving by vectors.*
  The points to be sieved form a sub-lattice

$$L_{q_p} = \{(c, d) \in L_q : c \cdot u_1 + d \cdot u_2 \equiv 0 \bmod p\}.$$

  Again, if possible, we would like to find a short basis for this lattice, call it $\{W_1 = (c_1, d_1), W_2 = (c_2, d_2)\}$. Then every element of the lattice L_{q_p} has the form for $e, f \in \mathbb{Z}$

$$(c, d) = (e \cdot c_1 + f \cdot c_2, e \cdot d_1 + f \cdot d_2),$$

  for some $e, f \in \mathbb{Z}$. Considering only the points with $\gcd(e, f) = 1$ allows us to find all the pairs we wanted and the corresponding (a, b). This approach is faster for big p, however if it is not possible to find a small basis for the lattice L_{q_p}, we sieve by rows.

The sieve terminates when the process is repeated for every p in the rational base. The same is done for the norm and the algebraic base.
The advantage of using this procedure of sieving is that we are considering smaller sets of elements to be sieved (just the elements in the lattice L_q) and we still obtain most of the pairs considered by the classical sieve. In this way the time spent in the sieving phase can be drastically reduced. More details on lattice sieving can be found in [GLM94].

3.9.2 Line Sieving

A variation of lattice sieving is the line sieving. In this case b is fixed, so that the lattice sieving is applied to the lattice L_q, with q special prime and a is the only parameters that varies. Typically, the polynomials generated for the line sieving are skewed polynomials designed for changing b rarely. For a full implementation of GNFS with the line sieving, see [EH96a].

Chapter 4

A first attempt to a bivariate GNFS

In this chapter we try to pass from a univariate formulation for GNFS to a bivariate one, in a different way from the method explained in Section 3.8.1: a suitable bivariate polynomial is considered, which defines two different univariate polynomials of degree two, on which the classical algorithm is applied. The simultaneous analysis of the number fields generated by these two polynomials eventually leads to a description of the biquadratic extension they generate. A special focus is given to the relation between ideals in the ring of integers of the degree-four extension and those of the two quadratic number fields. Exploiting this connection, a new version of the algorithm may be developed, avoiding computations in number fields with a high degree. In turn, this might well translate into an overall speed up and in a parallelizable implementation. However, at the moment we are not able to identify a suitable polynomial class for the algorithm, in fact using small degree polynomials of this particular shape is probably too restrictive.

4.1 A bivariate version for GNFS

Suppose that $N \in \mathbb{N}^+$ is a semiprime we need to factorize. We work in the following setting: let us consider a polynomial $F(x, y) \in \mathbb{Z}[x, y]$ of the form

$$F(x, y) = x^2 + y^2 + c,$$

where $c \in \mathbb{N}$ and suppose that there exist two values $A, B \in \mathbb{Z}$, $A \neq \pm B$, such that

$$F(A, B) = A^2 + B^2 + c = N. \tag{4.1}$$

Then, we define θ_1 and θ_2 as purely imaginary complex numbers such that

$$F(\theta_1, B) = \theta_1^2 + B^2 + c = 0,$$
$$F(A, \theta_2) = \theta_2^2 + A^2 + c = 0.$$

Clearly, we have that $\theta_1 \neq \pm\theta_2$ and we define the two minimal polynomials of θ_1 and θ_2 in $\mathbb{Z}[z]$ to be

$$f_1(z) = z^2 + B^2 + c \text{and} f_2(z) = z^2 + A^2 + c,$$

respectively. In this setting we construct the two extensions $\mathbb{Q}(\theta_1)$ and $\mathbb{Q}(\theta_2)$ of degree 2 over $\mathbb{Q}$ and recall the following theorem:

Theorem 4.1. *[Lan02, Theorem 4.6, p. 243] Let E be a finite extension of a field K. There exists an element $\alpha \in E$ such that $E = K(\alpha)$ if and only if there exists a finite number of fields F such that $K \subset F \subset E$. If E is separable over K, then there exists such an element α.*

Any extension of $\mathbb{Q}$ is separable, since it has characteristic 0 ([Lan02, Prop. 6.1, p.247]), so we know that there exists an element $\theta \in \mathbb{C}$ such that $\mathbb{Q}(\theta_1, \theta_2) = \mathbb{Q}(\theta)$ and, since it is a biquadratic extension, we also know that this primitive element is $\theta = \theta_1 + \theta_2$ and its minimal polynomial is $f(z) = z^4 + 2(N + c)z^2 + (A^2 - B^2)^2$. Thus, we are in this situation:

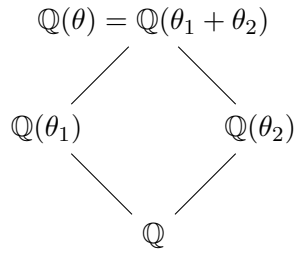

Figure 4.1: The subfield lattice generated for our bivariate version of GNFS.

We also need to define the following morphism:

$$\psi : \mathbb{Z}[\theta] \to \mathbb{Z}_N \qquad u + v\theta \mapsto u + v(A + B) \bmod N. \tag{4.2}$$

This function is the analogous of the ϕ defined for the classic GNFS, since

$\psi(\theta) = (A + B) \bmod N$ and taking the minimal polynomial of θ and substituting $A + B$, we obtain:

$$\begin{aligned} f(A+B) &= (A+B)^4 + 2(N+c)(A+B)^2 + (A^2 - B^2)^2 \\ &= 4N(A+B)^2 \equiv 0 \bmod N, \end{aligned}$$

so $A + B$ plays the role of m in the classical framework.
We define the projection also for the quadratic fields as:

$$\psi_{\theta_i} : \mathbb{Z}[\theta_i] \to \mathbb{Z}_p \qquad a + b\theta_i \mapsto a + br \bmod p,$$

for $i = 1, 2$.

4.2 The Algebraic Factor Base

In this section we will describe how to treat the ideals to build the Algebraic Factor Base required by GNFS. We will define the correspondence between first-degree prime ideals in $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$ and those in $\mathbb{Z}[\theta]$. Then, we will study a divisibility criterion for principal ideals in $\mathbb{Z}[\theta]$.

4.2.1 The identification of first-degree prime ideals

First, we look at the relation between the first-degree prime ideals in $\mathbb{Z}[\theta]$ and the first-degree prime ideals in $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$. We prove the following:
Theorem 4.2. *Let (r, p) be an ideal of $\mathbb{Z}[\theta_1]$ and (s, p) an ideal of $\mathbb{Z}[\theta_2]$, where p is a prime number and $r, s \in \mathbb{Z}_p$, then $(r + s, p)$ represents a first-degree prime ideal of $\mathbb{Z}[\theta]$.*

Proof. By Theorem 3.3, we know that

$$r^2 + A^2 + c \equiv 0 \bmod p \qquad \text{and} \qquad s^2 + B^2 + c \equiv 0 \bmod p. \tag{4.3}$$

We want to prove that

$$f(r+s) = (r+s)^4 + 2(c+N)(r+s)^2 + (A^2 - B^2)^2 \equiv 0 \bmod p.$$

Indeed, performing the computation, using (4.3) and (4.1), we get

$$\begin{aligned}
f(r+s) &= r^4 + 4r^3s + 6r^2s^2 + 4rs^3 + s^4 + 2(c+N)(r^2+s^2+2rs) + \\
&+ (A^2 - B^2) \equiv \\
&\equiv (-A^2 - c)^2 + 4rs(-A^2 - c) + 6(-A^2 - c)(-B^2 - c) + \\
&+ 4rs(-B^2 - c) + (-B^2 - c)^2 + 2(c+N)(-A^2 - B^2 - 2c - 2rs) + \\
&+ (A^2 - B^2) \bmod p = \\
&= 4rs(-A^2 - c - B^2 + N) + A^4 + c^2 + 2A^2c + \\
&+ 6(A^2B^2 + A^2c + B^2c + c^2) + B^4 + c^2 + 2B^2c - 2A^2c - 2A^2N + \\
&- 2B^2c - 2B^2N - 4c^2 - 4cN + A^4 + B^4 - 2A^2B^2 \bmod p = \\
&= 2A^4 + 2B^4 + 4c^2 + 4A^2B^2 + 6A^2c + 6B^2c - 2A^2(A^2 + B^2 + c) + \\
&- 2B^2(A^2 + B^2 + c) - 4c(A^2 + B^2 + c) \bmod p = \\
&= 2A^4 + 2B^4 + 4c^2 + 4A^2B^2 + 6A^2c + 6B^2c - 2A^4 - 2A^2B^2 + \\
&- 2A^2c - 2A^2B^2 - 2B^4 - 2B^2c - 4A^2c - 4B^2c - 4c^2 \bmod p = \\
&= 0 \bmod p.
\end{aligned}$$

□

We will focus our study on the first-degree prime ideals of $\mathbb{Z}[\theta]$ that come from two first-degree prime ideals of the underlying rings $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$.

Definition 4.3. We will refer to the ideal $(r+s, p) \subseteq \mathbb{Z}[\theta]$ as the *combination* of the ideals $(r, p) \subseteq \mathbb{Z}[\theta_1]$ and $(s, p) \subseteq \mathbb{Z}[\theta_2]$.

Therefore, finding all the first-degree prime ideals with the same norm p in the two smaller extensions is equivalent to finding at least some of the first-degree prime ideals in $\mathbb{Z}[\theta]$ that have norm equal to p. We also claim a slightly weaker version of the converse:

Theorem 4.4. *Let (t, p) be a first-degree prime ideal in $\mathbb{Z}[\theta]$. If either $p = 2$ or $t \not\equiv 0 \bmod p$, then there exists a unique pair $r, s \in \mathbb{Z}_p$ such that $t = r + s$ and (r, p) and (s, p) are first-degree prime ideals respectively of $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$.*

Proof. We treat separately the case if $p = 2$ and $p \neq 2$.

- **Case:** $p \neq 2$ **and** $t \not\equiv 0 \bmod p$:
  Since (t, p) is a first-degree prime ideal in $\mathbb{Z}[\theta]$, this means that

$$f(r+s) = t^4 + 2(A^2 + B^2 + 2c)t^2 + (A^2 - B^2)^2 \equiv 0 \bmod p. \quad (4.4)$$

Performing the computations in (4.4), we obtain

$$f(t) = t^4 + 2A^2t^2 + 2B^2t^2 + 4ct^2 + A^4 + B^4 + 2A^2B^2 \equiv 0 \bmod p. \tag{4.5}$$

We will look for a solution for $f_1(x) \bmod p$: since the previous polynomial is symmetric in A and B, the result for f_2 will follow in the same way. We can now notice that

$$(t^2 + A^2 + c)^2 = t^4 + A^4 + c^2 + 2t^2A^2 + 2A^2c + 2ct^2 \qquad \text{and}$$
$$(B^2 + c)^2 = B^4 + c^4 + 2B^2c,$$

so (4.5) becomes

$$(t^2 + A^2 + c)^2 + (B^2 + c)^2 - 2(c^2 + A^2c + B^2c + A^2B^2) + \\ +2t^2(B^2 + c) \equiv 0 \bmod p \tag{4.6}$$

We can also notice that

$$(t^2 + A^2 + c)(B^2 + c) = t^2B^2 + ct^2 + A^2B^2 + A^c + B^2c + c^2$$
$$(t^2 + A^2 + c)(B^2 + c) - t^2(B^2 + c) = c^2 + A^2c + B^2c + A^2B^2$$

and we substitute this last equation into (4.6), getting

$$(t^2 + A^2 + c)^2 + (B^2 + c)^2 - 2(t^2 + A^2 + c)(B^2 + c) + \\ +4t^2(B^2 + c) \equiv 0 \bmod p$$
$$\left[(t^2 + A^2 + c) - (B^2 + c)\right]^2 + 4t^2(B^2 + c) \equiv 0 \bmod p$$
$$-B^2 - c \equiv \left(\frac{t^2 + A^2 - B^2}{2t}\right)^2 \bmod p.$$

Since $2t \not\equiv 0 \bmod p$, we can define

$$r = \frac{t^2 + A^2 - B^2}{2t},$$

in this way, we obtain that $r^2 + B^2 + c = f_1(r) \equiv 0 \bmod p$, so (r, p) is a first-degree prime ideal for $\mathbb{Z}[\theta_1]$.

- **Case** $p = 2$:
  If $p = 2$, then (4.4) becomes

$$\begin{aligned} f(t) = t^4 + A^4 + B^4 &\equiv 0 \bmod 2 \\ (t + A + B)^4 &\equiv 0 \bmod 2 \\ t &\equiv A + B \bmod 2. \end{aligned}$$

  So if $r \equiv B + c \bmod 2$ and $s \equiv A + c \bmod 2$, we get

$$\begin{aligned} f_1(r) &\equiv B^2 + c^2 + B^2 + c \equiv c^2 + c \equiv 0 \bmod 2 \qquad \text{and} \\ f_2(s) &\equiv A^2 + c^2 + A^2 + c \equiv c^2 + c \equiv 0 \bmod 2, \end{aligned}$$

  since every element $x \in \mathbb{F}_2$ is such that $x^2 + x \equiv 0 \bmod 2$, and also

$$r + s = B + c + A + c \equiv A + B \equiv t \bmod 2.$$

□

The only first-degree prime ideals in $\mathbb{Z}[\theta]$ not treated in Theorem 4.4 are those of the form $(0, p)$ with $p \neq 2$. They can be characterized by the following proposition:

Proposition 4.5. *Let $(0, p)$ be a first-degree prime ideal of $\mathbb{Z}[\theta]$ and let $r \in \mathbb{Z}_p$, then the following are equivalent:*

1. $f_1(r) \equiv 0 \bmod p$.
2. $f_2(s) \equiv 0 \bmod p$.
3. (r, p) *and* $(-r, p)$ *are first-degree prime ideals of* $\mathbb{Z}[\theta_1]$.
4. (r, p) *and* $(-r, p)$ *are first-degree prime ideals of* $\mathbb{Z}[\theta_2]$.

Proof.

- $1 \iff 2$ and $3 \iff 4$:
  From $f(0) \equiv 0 \bmod p$ we get that

$$f(0) = (A^2 - B^2)^2 \equiv 0 \bmod p \implies A^2 \equiv B^2 \bmod p.$$

  Hence $f_1 \equiv f_2 \bmod p$, therefore r is a root of f_1 modulo p if and only if f_2 has the same root.

- $3 \implies 1$:
  It follows directly using Theorem 3.3.

- $1 \implies 3$:
  If $f_1(r) \equiv 0 \bmod p$, then also $f_1(-r) \equiv 0 \bmod p$, implying that $(\pm r, p)$ are the first-degree prime ideals of $\mathbb{Z}[\theta_1]$.

□

Remark 4.1. The above proposition is trivial for $p = 2$. In fact, if $(0, 2)$ is a first-degree prime ideal of $\mathbb{Z}[\theta]$, then all the above equivalent condition are satisfied for $r = A^2 + c = B^2 + c$.

According to Proposition 4.5, one of the following situations takes place, depending on the number ν of roots of f_1 modulo p:

$\nu = 0$: $(0, p) \subseteq \mathbb{Z}[\theta]$ cannot be found as a combination of first-degree prime ideals of $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$.

$\nu = 1$: $(0, p) \subseteq \mathbb{Z}[\theta]$ is the combination of $(0, p) \subseteq \mathbb{Z}[\theta_1]$ and $(0, p) \subseteq \mathbb{Z}[\theta_2]$.

$\nu = 2$: $(0, p) \subseteq \mathbb{Z}[\theta]$ is determined by two different combinations of first-degree prime ideals of $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$.

The following example shows that all the above cases may actually occur:
Example 4.1. Let $f_1 = z^2 - 50$ and $f_2 = z^2 - 155$ generate by combination the quadratic fields $\mathbb{Q}[\theta_1]$ and $\mathbb{Q}[\theta_2]$, so that the composite biquadratic field $\mathbb{Q}[\theta]$ is generated by the polynomial $f = z^4 - 410z^2 + 11025$.

The unique first-degree prime ideal in $\mathbb{Z}[\theta]$ with norm $p = 3$ is $(0, 3)$, but there are no such ideals neither in $\mathbb{Z}[\theta_1]$ nor in $\mathbb{Z}[\theta_2]$, then $(0, 3)$ cannot be a combination of any of them.

The unique first-degree prime ideal of norm $p = 5$ in $\mathbb{Z}[\theta]$ is $(0, 5)$, which is determined uniquely as a combination of the ideals $(0, 5)$ in $\mathbb{Z}[\theta_1]$ and $(0, 5)$ in $\mathbb{Z}[\theta_2]$.

There are 3 first-degree prime ideals of norm $p = 7$ in $\mathbb{Z}[\theta]$: $(0, 7), (2, 7)$ and $(5, 7)$. The first-degree prime ideals of the same norm for both $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$ are $(1, 7)$ and $(6, 7)$. As prescribed by Theorem 4.4 we observe that $(2, 7)$ and $(5, 7)$ are uniquely determined by the combinations of $((1, 7), (1, 7))$ and $((6, 7), (6, 7))$, whereas $(0, 7)$ arises from the combinations of $((1, 7), (6, 7))$ and $((6, 7), (1, 7))$.

4.2.2 Divisibility of principal ideals

We have proven that the first-degree prime ideals with the same norm p in $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$ generate almost every first-degree prime ideal in $\mathbb{Z}[\theta]$ with the same norm p. Hence, we can consider $\mathcal{A}_1$ and $\mathcal{A}_2$ to be the algebraic factor bases in $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$ respectively and from them build the algebraic factor base $\mathcal{A}$ in $\mathbb{Z}[\theta]$, by simply considering

$$\mathcal{A} = \{(r+s, p) \mid (r,p) \in \mathcal{A}_1 \text{ and } (s,p) \in \mathcal{A}_2\}.$$

In order to define a divisibility criterion for a principal ideal I in $\mathbb{Z}[\theta]$, we need to investigate the intersections between I and $\mathbb{Z}[\theta_i]$ for $i = 1, 2$.

Proposition 4.6. *Let a, b be non-zero integers and $I = \langle a + b\theta \rangle \subseteq \mathbb{Z}[\theta]$. Then $I \cap \mathbb{Z}[\theta_1]$ is a principal ideal and*

$$I \cap \mathbb{Z}[\theta_1] = \langle (a + b\theta_1 + b\theta_2)(a + b\theta_1 - b\theta_2) \rangle .$$

Proof. $\supseteq$) The generator of the ideal $(a + b\theta_1 + b\theta_2)(a + b\theta_1 - b\theta_2)$ is an element of I and it is equal to $(a + b\theta_1)^2 - (b\theta_2)^2$, which belongs to $\mathbb{Z}[\theta_1]$.
$\subseteq$) Since a basis for $\mathbb{Q}(\theta)$ is formed by $\{1, \theta_1, \theta_2, \theta_1\theta_2\}$, every $x \in I$ has the form $x = (a + b\theta_1 + b\theta_2)(\gamma_0 + \gamma_1\theta_1 + \gamma_2\theta_2 + \gamma_3\theta_1\theta_2)$, where $\gamma_i \in \mathbb{Z}$. Since $x \in \mathbb{Z}[\theta_1]$, the coefficients of θ_2 and $\theta_1\theta_2$ need to vanish, so

$$\begin{cases} a\gamma_3 + b\gamma_2 + b\gamma_1 = 0 \\ a\gamma_2 - b(B^2 + c)\gamma_3 + b\gamma_0 = 0. \end{cases} \tag{4.7}$$

On the other side, we would like to prove that

$$x = (a + b\theta_1 + b\theta_2)(a + b\theta_1 - b\theta_2)(C + D\theta_1),$$

for some $C, D \in \mathbb{Z}$, meaning that

$$\gamma_0 + \gamma_1\theta_1 + \gamma_2\theta_2 + \gamma_3\theta_1\theta_2 = (a + b\theta_1 - b\theta_2)(C + D\theta_1).$$

By comparing the coefficients, we get that

$$\begin{cases} \gamma_0 = aC - bD(B^2 + c) \\ \gamma_1 = aD + bC \\ \gamma_2 = -bC \\ \gamma_3 = -bD. \end{cases}$$

We check that these coefficients verify (4.7):

$$\begin{aligned} &a(-bD) + b(-bC) + b(aD + bC) = 0 \\ &a(-bC) - b(B^2 + c)(-bD) + b\left[aC - bD(B^2 + c)\right] = 0. \end{aligned}$$

Thus, we may invert the system and obtain that

$$x = (a + b\theta_1 + b\theta_2)(a + b\theta_1 - b\theta_2)\left(-\frac{\gamma_2 + \gamma_3\theta_1}{b}\right),$$

as required. □

The previous proposition enables us to prove the following theorem on divisibility of principal ideals:

Theorem 4.7. *Let $a, b \in \mathbb{Z}$ be coprime and let $I = \langle a + b\theta \rangle$ be a principal ideal in $\mathbb{Z}[\theta]$. Let $I_1 = I \cap \mathbb{Z}[\theta_1]$ and $I_2 = I \cap \mathbb{Z}[\theta_2]$. If the ideals $(r, p) \subseteq \mathbb{Z}[\theta_1]$ and $(s, p) \subseteq \mathbb{Z}[\theta_2]$ divide I_1 and I_2, respectively, then the first-degree prime ideal $(r + s, p) \subseteq \mathbb{Z}[\theta]$ divides I, unless*

$$\begin{cases} p \neq 2 \\ n \equiv 0 \bmod p \\ r + s \not\equiv 0 \bmod p. \end{cases}$$

Proof. By Theorem 4.2, $(r + s, p)$ is a first-degree prime ideal in $\mathbb{Z}[\theta]$, then it is enough to show that under the aforementioned conditions we have

$$a + b(r + s) \equiv 0 \bmod p. \tag{4.8}$$

From Proposition 4.6, we find that

$$I_1 = \langle a^2 + b^2(A^2 - B^2) + 2ab\theta_1 \rangle \subseteq \mathbb{Z}[\theta_1], \tag{4.9}$$

$$I_2 = \langle a^2 + b^2(B^2 - A^2) + 2ab\theta_2 \rangle \subseteq \mathbb{Z}[\theta_2]. \tag{4.10}$$

We treat each case separately:

- **Case** $p = 2$:
  By Eq. (4.9), the generator g_1 of I_1 is such that

$$\begin{aligned}\psi_{\theta_1}(g_1) &= a^2 + b^2(A^2 - B^2) + 2abr \equiv \\ &\equiv a^2 + b^2(A^2 + B^2) \equiv a + b(r + s) \bmod 2.\end{aligned}$$

  Then (4.8) is satisfied if and only if $(r, 2)$ divides I_1.

- **Case** $p \neq 2 \wedge a \not\equiv 0 \bmod p$:
  By hypothesis $(r, p) \mid I_1$ and $(s, p) \mid I_2$, meaning

$$\begin{cases} a^2 + b^2(A^2 - B^2) + 2abr \equiv 0 \bmod p \\ a^2 + b^2(B^2 - A^2) + 2abs \equiv 0 \bmod p. \end{cases}$$

  Summing together the above relations we get

$$2a^2 + 2abr + 2abs = 2a[a + b(r + s)] \equiv 0 \bmod p.$$

  Since $2a \not\equiv 0 \bmod p$, this implies (4.8).

- **Case** $p \neq 2 \wedge a \equiv 0 \bmod p \wedge r + s \equiv 0 \bmod p$:
  In this case (4.8) is trivially satisfied.

Thus, we conclude that $(r + s, p)$ is a first-degree prime ideal of $\mathbb{Z}[\theta]$ dividing I, except for the case when $p \neq 2 \wedge a \equiv 0 \bmod p \wedge r + s \not\equiv 0 \bmod p$. □

The next example shows that, in the case highlighted by Theorem 4.7, the combination does not maintain ideal divisibility.

Example 4.2. Let $f_1(z) = z^2 + 4$ and $f_2(z) = z^2 - 6$ generate the quadratic fields $\mathbb{Q}(\theta_1)$ and $\mathbb{Q}(\theta_2)$, so that the composite biquadratic field $\mathbb{Q}(\theta)$ is generated by the polynomial $f(z) = z^4 - 4z^2 + 100$.
The first-degree prime ideals of $\mathbb{Z}[\theta]$ with norm $p = 5$ are $(0, 5)$, $(2, 5)$ and $(3, 5)$, while $(1, 5)$ and $(4, 5)$ are those of $\mathbb{Z}[\theta_1]$ and the same pairs are also first-degree prime ideals of $\mathbb{Z}[\theta_2]$.
Suppose that $I = \langle 5 + \theta \rangle \subseteq \mathbb{Z}[\theta]$. By Proposition 4.6 we have

$$I_1 = \langle 15 + 10\theta_1 \rangle \subseteq \mathbb{Z}[\theta_1], \qquad I_2 = \langle 35 + 10\theta_2 \rangle \subseteq \mathbb{Z}[\theta_2].$$

It is easy to see that both $(1, 5)$ and $(4, 5)$ divide I_1 and I_2. Besides, the

combination of $(1,5)$ and $(4,5)$ is $(0,5)$, which divides I. However, the other options are exactly the exceptions prescribed by Theorem 4.7, since the combination between $(1,5)$ and $(1,5)$ is $(2,5)$, which does not divide I. The same holds for $(3,5)$, which is the combination of $(4,5)$ and $(4,5)$.

On the other hand, whenever a first-degree prime ideal of $\mathbb{Z}[\theta]$ dividing a principal ideal I is obtained as a combination of two first-degree prime ideals, these last two ideals divide the intersections of I with $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$ respectively.

Theorem 4.8. *Let $I = \langle a+b\theta \rangle$ be a principal ideal in $\mathbb{Z}[\theta]$ with $\gcd(a,b) = 1$. Let (t,p) be a first-degree prime ideal in $\mathbb{Z}[\theta]$ that divides I. If there exist two first-degree prime ideals $(r,p) \subseteq \mathbb{Z}[\theta_1]$ and $(s,p) \subseteq \mathbb{Z}[\theta_2]$ such that their combination $r + s \equiv t \bmod p$, then (r,p) divides $I_1 = I \cap \mathbb{Z}[\theta_1]$ and (s,p) divides $I_2 = I \cap \mathbb{Z}[\theta_2]$.*

Proof. If these ideals exist, from $(t,p) \mid I$ we get

$$0 \equiv a + bt \equiv a + br + bs \bmod p.$$

Let I_1 and I_2 be described as in (4.9) and (4.10). From the above equation we have

$$\begin{aligned} &a^2 + b^2(A^2 - B^2) + 2abr \equiv 0 \bmod p \iff \\ &a^2 + b^2(A^2 - B^2) - 2a^2 - 2abs \equiv 0 \bmod p \iff \\ &a^2 + b^2(B^2 - A^2) + 2abs \equiv 0 \bmod p. \end{aligned}$$

Hence, (r,p) divides I_1 if and only if (s,p) divides I_2, so it is sufficient to show that $(r,p) \mid I_1$. Substituting $a \equiv -br - bs \bmod p$, $r^2 \equiv -B^2 - c \bmod p$ and $s^2 \equiv -A^2 - c \bmod p$, we obtain that

$$\begin{aligned} &a^2 + b^2(A^2 - B^2) + 2abr \equiv \\ \equiv &(-br - bs)^2 + b^2(r^2 - s^2) + 2br(-br - bs) \equiv 0 \bmod p, \end{aligned}$$

therefore $(r,p) \mid I_1$. □

The following corollary summarizes the previous results, providing an almost-unique decomposition of first-degree prime ideals by combination, which respects divisibility of principal ideals.

Corollary 4.9. *Let $I = \langle a+b\theta \rangle$ be a principal ideal in $\mathbb{Z}[\theta]$ with $\gcd(a,b) = 1$*

and let (t, p) be a first-degree prime ideal in $\mathbb{Z}[\theta]$ that divides I, with $t \neq 0$ if $p \neq 2$. Then there exist two unique first-degree prime ideals $(r, p) \subseteq \mathbb{Z}[\theta_1]$ and $(s, p) \subseteq \mathbb{Z}[\theta_2]$ such that $r + s \equiv t \bmod p$ and (r, p) divides $I_1 = I \cap \mathbb{Z}[\theta_1]$ and (s, p) divides $I_2 = I \cap \mathbb{Z}[\theta_2]$.

Proof. It follows immediately from Theorem 4.4 and Theorem 4.8. □

Hence we search for first-degree prime ideals in $\mathcal{A}$ that factorize I by checking the factorization of the two smaller ideals obtained by intersecting I with the two extensions of degree two.
Finally, we would like to retrieve the exponents of the ideals we are considering. Since those exponents are just the exponents of the corresponding primes appearing in the norm factorization of the generator similarly to what we saw in Corollary 3.9, it is enough to study how the norm changes between I, I_1 and I_2.

Proposition 4.10. *Let $I = \langle a + b\theta \rangle$ be a principal ideal in $\mathbb{Z}[\theta]$, with $\gcd(a, b) = 1$. Let $I_1 = I \cap \mathbb{Z}[\theta_1]$ and $I_2 = I \cap \mathbb{Z}[\theta_2]$. Then,*

$$\begin{aligned} N_{\mathbb{Q}(\theta)/\mathbb{Q}}(a + b\theta) &= N_{\mathbb{Q}(\theta_1)/\mathbb{Q}}(a^2 + b^2(A^2 - B^2) + 2ab\theta_1) \\ &= N_{\mathbb{Q}(\theta_2)/\mathbb{Q}}(a^2 + b^2(B^2 - A^2) + 2ab\theta_2). \end{aligned}$$

Proof. We know that

$$\begin{aligned} N_{Q(\theta)/\mathbb{Q}}(a + b\theta) &= (-b^4)\left(-\frac{a}{b}\right)^4 + 2(c + N)b^4\left(-\frac{a}{b}\right)^2 + b^4(A^2 - B^2)^2 \\ &= a^4 + 2(c + N)a^2b^2 + b^4(A^2 - B^2)^2. \end{aligned}$$

We compute the norm of the other two elements in $\mathbb{Q}(\theta_1)$ and $\mathbb{Q}(\theta_2)$ over $\mathbb{Q}$, using their minimal polynomials:

$$\begin{aligned} &N_{\mathbb{Q}(\theta_1)/\mathbb{Q}}(a^2 + b^2(A^2 - B^2) + 2ab\theta_1) = \\ &\qquad = 4a^2b^2\left(-\frac{a^2 + b^2(A^2 - B^2)}{2ab}\right)^2 + 4a^2b^2(A^2 + c) \\ &\qquad = a^4 + 2(c + N)a^2b^2 + b^4(A^2 - B^2)^2. \\ &N_{\mathbb{Q}(\theta_2)/\mathbb{Q}}(a^2 + b^2(B^2 - A^2) + 2ab\theta_2) = \\ &\qquad = 4a^2b^2\left(-\frac{a^2 + b^2(B^2 - A^2)}{2ab}\right)^2 + 4a^2b^2(B^2 + c) \\ &\qquad = a^4 + 2(c + N)a^2b^2 + b^4(A^2 - B^2)^2. \end{aligned}$$

□

This last condition implies that the exponent of the first-degree prime ideal of norm p that appears in the factorization of I in $\mathbb{Z}[\theta]$ is exactly the same as the exponent of the first-degree prime ideals of norm p that appear in the factorizations of I_1 in $\mathbb{Z}[\theta_1]$ and of I_2 in $\mathbb{Z}[\theta_2]$.
In this way, we have completely characterized the elements in $\mathcal{A}$, by using only informations that can be read from $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$.

4.3 The Quadratic Characters Base

As regards the Quadratic Character Base $\mathcal{Q}$ in $\mathbb{Z}[\theta]$, this is still formed by first-degree prime ideals. Hence, we analyse again the behaviour of the first-degree prime ideals of $\mathbb{Z}[\theta]$ belonging to $\mathcal{Q}$, comparing to the ideals in $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$, belonging to the two Quadratic Character Bases $\mathcal{Q}_1$ and $\mathcal{Q}_2$ respectively.

Proposition 4.11. *Let (r, q) be an ideal in the Quadratic Character Base of $\mathbb{Z}[\theta_1]$ and (s, q) be an ideal in the Quadratic Character Base of $\mathbb{Z}[\theta_2]$, with the same q ($C < q \leq D$, where C and D are the same as in Definition 3.12). Then, if $r \not\equiv -s \bmod q$, $(r + s, q)$ represents a first-degree prime ideal in the Quadratic Character Base of $\mathbb{Z}[\theta]$.*

Proof. Since, by Theorem 4.2, (r, q) and (s, q) are first-degree prime ideals in $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$, we only need to check the condition that $f'(r+s) \not\equiv 0 \bmod q$. We know that

$$\begin{cases} f_1(r) = r^2 + B^2 + c \equiv 0 \bmod q \\ f_2(s) = s^2 + A^2 + c \equiv 0 \bmod q. \end{cases}$$

Moreover, since they are in the Quadratic Character Base, also

$$\begin{cases} f_1'(r) = 2r \not\equiv 0 \bmod q \\ f_2'(s) = 2s \not\equiv 0 \bmod q. \end{cases} \tag{4.11}$$

Therefore, since q is an odd prime number, we have that

$$\begin{cases} r \not\equiv 0 \bmod q \\ s \not\equiv 0 \bmod q. \end{cases}$$

Now, the derivative of f is $f'(x) = 4x^3 + 4(c+N)x$, that computed in $r+s$ gives the following:

$$\begin{aligned} f'(r+s) &= 4(r+s)^3 + 4(c+N)(r+s) = \\ &= 4(r+s)\left[(r+s)^2 + c + N\right] = \\ &= 4(r+s)\left[r^2 + s^2 + 2rs + c + N\right]. \end{aligned}$$

Now using (4.1) and (4.11) we get that

$$\begin{aligned} f'(r+s) &= 4(r+s)\left[r^2 + s^2 + 2rs + c + A^2 + B^2 + c\right] = \\ &= 4(r+s)\left[(r^2 + B^2 + c) + (s^2 + A^2 + c) + 2rs\right] \equiv \\ &\equiv 8rs(r+s) \bmod q. \end{aligned}$$

So, in order to get that this quantity is different from 0, we must have that $r \not\equiv -s \bmod q$, since r and s are not divisible by q and $\gcd(8, q) = 1$, because q is an odd prime. □

Using this proposition, we just need to compute all Legendre symbols of the form $\left(\frac{a+br+bs}{q}\right)$ for every element in the quadratic character base of $\mathbb{Z}[\theta]$, where $r, s \in \mathbb{Z}_q$ are recovered from the first-degree prime ideals in $\mathbb{Z}[\theta_1]$ and $\mathbb{Z}[\theta_2]$.

4.4 Further works and Limits of this approach

We presented how to find first-degree prime ideals in the ring of integers of a special quartic extension of $\mathbb{Q}$ by studying first-degree prime ideals in the ring of integers of two quadratic extensions. We also provided a precise condition to determine when such prime ideals divide the principal ideals considered in the GNFS algorithm. While this is interesting in an algebraic perspective, we have tried to implement a bivariate version of GNFS hoping to improve the time of convergence, at least in some cases, using these properties. Such as the classical GNFS, a crucial part regards the choice of the starting polynomial $F(x, y)$ in a way that allows us to find enough first-degree prime ideals when performing the sieving phase. However, since we are only considering monic polynomials of degree 2 without any linear term, when $N \to \infty$, the size of the coefficients of F drastically increases. As said in Section 3.8.3, this affects the chances of finding enough elements

in the sieving phase. In fact, in the examples we made, we were not be able to obtain enough smooth elements. We are currently working on a generalization of this process, in order to broaden our results to extensions of any degree. In Appendix A we report a version of the Magma code used to test this version of the algorithm. Another approach that may be worthy to be analysed is the use of non-monic polynomials in the process, obtaining polynomials with smaller coefficients. Nevertheless, in this case, as a downside effect, we should consider Theorem 3.18 to establish an identification between first-degree prime ideals and the modular roots of the polynomials, which may complicate the form of the field extensions we should consider.

Chapter 5

Finding GNFS relations using Groebner bases

We exihibit a novel approach to obtain the elements required by GNFS for a number $N \in \mathbb{N}^+$. The setting is the same as before, but we want to generalize the computations and gain some information about the choice of the parameters for the algorithm. Our aim is to find some relations that arise from the bounds we need to satisfy in GNFS, setting a system with these equations and try to find some constraints on the solutions. We will present a strategy to employ this system: given a suitable polynomial for GNFS, we would like to obtain directly an element $x \in \mathbb{Z}[\theta]$ such that x is a perfect square and also $\phi(x)$ is a perfect square in $\mathbb{Z}$. The system created this way is analysed using the theory of Groebner basis and modular arithmetic to gain some hints on the shape of its solutions.

5.1 The generation of the system

Suppose, as in GNFS, that we have a monic irreducible polynomial $f \in \mathbb{Z}[x]$ of degree d and an element $m \in \mathbb{Z}$ such that $f(m) = N$. If we write explicitly the polynomial as

$$f(x) = x^d + A_{d-1}x^{d-1} + A_{d-2}x^{d-2} + \ldots + A_1 x + A_0, \quad \text{with } A_0, \ldots, A_{d-1} \in \mathbb{Z},$$

this last condition can be rewritten as:

$$f(m) = m^d + A_{d-1}m^{d-1} + A_{d-2}m^{d-2} + \ldots + A_1 m + A_0.$$

For sake of simplicity throughout all this chapter we will focus on cases when $d = 2$. So in our case the polynomial is $f(x) = x^2 + Ax + B$, where $A, B \in \mathbb{Z}$ and the first condition to impose is

$$f(m) = m^2 + Am + B = N. \tag{5.1}$$

The condition of being irreducible can be expressed analysing the discriminant of the polynomial which is $A^2 - 4B$: if $A^2 - 4B \neq C^2$, for any $C \in \mathbb{Z}$, the roots are non-integers, thus f it is irreducible in $\mathbb{Z}$. So an additional bound for the coefficients of f is

$$A^2 - 4B \neq C^2.$$

From now on we may suppose this is the case.
Let us call θ one of the roots of f and consider the number field $\mathbb{Q}(\theta)$ and $\mathbb{Z}[\theta]$, the usual subring of $\mathfrak{O}_{\mathbb{Q}(\theta)}$. Let $\alpha = a_0 + a_1\theta \in \mathbb{Z}[\theta]$, with $(a_0, a_1) \in \mathbb{Z} \times \mathbb{Z}^*$, raise α to the square and reduce it modulo f to get

$$\begin{aligned}\beta :&= b_0 + b_1\theta = \\ &= (a_0 + a_1\theta)^2 = \\ &= {a_0}^2 + 2a_0a_1\theta + {a_1}^2\theta^2 = \\ &= {a_0}^2 - B{a_1}^2 + a_1\theta(2a_0 - a_1A).\end{aligned}$$

Comparing the coefficients of degree 0 and 1 of the two terms of the previous equation, we obtain the following:

$$b_0 = {a_0}^2 - B{a_1}^2 \tag{5.2}$$

$$b_1 = a_1(2a_0 - a_1A). \tag{5.3}$$

The two elements α and β represent exactly what we hope to find using GNFS. In fact, if we call $\phi : \mathbb{Z}[\theta] \to \mathbb{Z}_N$ the surjective homomorphism that sends θ in m, we need to add the condition that $\phi(\beta)$ is a perfect square in $\mathbb{Z}$, so

$$\phi(\beta) \equiv b_0 + b_1 m = {d_1}^2 \bmod N, \tag{5.4}$$

where $d_1 \in \mathbb{Z}$. Hence, in this case we can obtain the difference of squares given by

$$d_1{}^2 \equiv \phi(\alpha)^2 \bmod N$$

and this may lead to a successful factorization for N.

Proposition 5.1. *Let $N \in \mathbb{N}^+$ be a semiprime. If the integer variables $m, A, B, b_0, b_1, a_0, a_1, d_1$ satisfy the system*

$$\begin{cases} m^2 + Am + B = N \\ b_0 = a_0{}^2 - Ba_1{}^2 \\ b_1 = a_1(2a_0 - a_1 A) \\ b_0 + b_1 m = d_1{}^2, \end{cases} \tag{5.5}$$

then $\gcd(a_0 + a_1 m - d_1, N)$ and $\gcd(a_0 + a_1 m + d_1, N)$ are the factors of N, found using GNFS using the polynomial $f = x^2 + Ax + B \in \mathbb{Z}[x]$.

Proof. Gathering together (5.1),(5.2),(5.3) and (5.4) we obtain the system. □

However, finding solutions of a non-linear system could be tough, so we introduce the use of Groebner basis to try to solve the system in (5.5).

5.1.1 Inequalities on the parameters

In this paragraph we will find some constraints in the interval in which all the parameters are defined. We may suppose that all the parameters in the first equation of (5.1) are positive and of course smaller than N, in particular

$$\begin{cases} 0 < m \leq \left\lfloor \sqrt{N} \right\rfloor \\ 0 < A < N \\ 0 < B < N. \end{cases}$$

We may also suppose that $0 \leq \phi(\alpha) \leq N$, that may be rewritten as

$$0 \leq a_0 + a_1 m \leq N,$$

noting that $a_1 \neq 0$. Specifying the dependence of a_0 from a_1,

$$-a_1 m \leq a_0 \leq N - a_1 m. \tag{5.6}$$

Instead, considering $\beta = b_0 + b_1\theta$ and the definitions given by (5.2) and (5.3), we may argue some considerations about these coefficients: on one side, using also (5.6),

$$b_0 = a_0^2 - B{a_1}^2 \leq \max\left\{{a_1}^2(m^2 - B), {a_1}^2(m^2 - B) - 2a_1Nm + N^2\right\},$$

on the other side,

$$b_0 \geq -B{a_1}^2,$$

concluding

$$-B{a_1}^2 \leq b_0 \leq \max\left\{{a_1}^2(m^2 - B), {a_1}^2(m^2 - B) - 2a_1Nm + N^2\right\}. \quad (5.7)$$

We may use the same approach to deduce an analogous inequality for b_1:

$$b_1 = 2a_0a_1 - {a_1}^2A \leq a_1\left(2N - 2a_1m - a_1A\right).$$

The other side of the inequality for b_1 is

$$b_1 \geq -{a_1}^2\left(2m + A\right).$$

Summarizing,

$$-{a_1}^2\left(2m + A\right) \leq b_1 \leq a_1\left(2N - 2a_1m - a_1A\right). \quad (5.8)$$

It remains to give some considerations on ${d_1}^2$, so

$$\begin{aligned}
{d_1}^2 &= {a_0}^2 - B{a_1}^2 + m(2a_0a_1 - {a_1}^2A) \leq \\
&\leq \max\left\{{a_1}^2(m^2 - B), {a_1}^2(m^2 - B) - 2a_1Nm + N^2\right\} + \\
&+ a_1\left(2N - 2a_1m - a_1A\right) \leq \\
&\leq \max\left\{2a_1mN - {a_1}^2\left(m^2 + Am + B\right), N^2 - {a_1}^2\left(B + ma + m^2\right)\right\} \leq \\
&\leq \max\left\{a_1N\left(2m - a_1\right), N\left(N - {a_1}^2\right)\right\},
\end{aligned}$$

where we employed (5.1). Thus,

$$|d_1| \leq \max\left\{\sqrt{a_1N\left(2m - a_1\right)}, \sqrt{N\left(N - {a_1}^2\right)}\right\}. \quad (5.9)$$

5.2 The Algorithm for finding Perfect Squares in the Number Field

In this scenario we suppose that the polynomial $f = x^2 + Ax + B$ is known and we also fix $m \in \mathbb{Z}$, that satisfies $f(m) = N$. Thus, the variables that are left to be found in the system (5.5) are $a_0, a_1, b_0, b_1, d_1 \in \mathbb{Z}$. We fix a value for a_1 and if we cannot find a solution for the system, we update a_1 with another value until we obtain an integer solution. As we can see in (5.5), b_0 and b_1 depends only on a_0 and the last equation can be rewritten as

$$d_1{}^2 = a_0{}^2 - Ba_1{}^2 + ma_1(2a_0 - a_1A)$$

such that also d_1 depends only on a_0. Thus the system we need to solve becomes

$$\begin{cases} d_1^2 = a_0{}^2 - Ba_1^2 + ma_1(2a_0 - a_1A) \\ b_0 = a_0{}^2 - Ba_1^2 \\ b_1 = 2a_0a_1 - a_1^2A \end{cases} \tag{5.10}$$

We can choose a monomial ordering and compute the Groebner basis G_p (see Section 1.4) over different finite fields $\mathbb{F}_p$ imposing the field equations

$$\{a_0{}^p - a_0, b_0{}^p - b_0, b_1{}^p - b_1, d_1{}^p - d_1\}$$

for different p's, small prime numbers. In these $\mathbb{F}_p$'s the system (5.10) may have a simpler formulation and can give us some linear modular substitution to simplify the original system in $\mathbb{Q}$. We may notice that in system (5.10) the variables d_1, b_0 and b_1 involve only a_0 in the equations, so we would like to consider in G_p some special equations to be used as substitution. We want to highlight every possible substitution for each variable, indicating with $i^{(j)}$ the value of the variable $i \in \{a_0, d_1, b_0, b_1\}$ at its j-th substitution.

- For a_0 we would like to consider only linear equations $g \in G_p$ that do not involve any other variable,

  $$g : a_0 \equiv g_0 \bmod p, \qquad g_0 \in \mathbb{F}_p.$$

  Therefore the possible changes for a_0 are of the form

  $$a_0^{(j)} = g_0 + p \cdot a_0^{(j+1)}.$$

- As regards b_0, we consider linear equations $g \in G_p$ that involve at most the variable a_0

$$g : b_0 \equiv g_0 + g_1 \cdot a_0 \bmod p, \qquad g_0, g_1 \in \mathbb{F}_p.$$

  The substitution is then defined as

$$b_0^{(j)} = g_0 + g_1 a_0^{(k)} + p \cdot b_0^{(j+1)}.$$

- In a similar way, for b_1 we only take into account equations $g \in G_p$ that include only a_0:

$$g : b_1 \equiv g_0 + g_1 \cdot a_0 \bmod p, \qquad g_0, g_1 \in \mathbb{F}_p.$$

  The analogous substitution is

$$b_1^{(j)} = g_0 + g_1 a_0^{(k)} + p \cdot b_1^{(j+1)}.$$

- In the same way for d_1, we will treat only equations $g \in G_p$ of the form

$$g : b_1 \equiv g_0 + g_1 \cdot a_0 \bmod p, \qquad g_0, g_1 \in \mathbb{F}_p.$$

  The corresponding substitution is

$$d_1^{(j)} = g_0 + g_1 a_0^{(k)} + p \cdot d_1^{(j+1)}.$$

Clearly, not all the relations that appear in these Groebner bases over $\mathbb{F}_p$ are interesting: the field equations do not give any information, but it can also happen that in $\mathbb{Q}$, after some replacements, one of the equation could become univariate and of degree one. We call this kind of equations *linear forms*, they fix the value for a variable and it is not necessary to reduce them anymore. During this process, we need to keep track of the various substitutions we have performed and how the variables have been modified. Another important aspect that we have to consider is the interval in which every variable must be. These intervals (called I_{a_0}, I_{b_0}, I_{b_1}, I_{d_1}) are defined at the beginning as in respectively (5.6), (5.7), (5.8), (5.9) and after each substitution that have to be updated, using the reduction defined above. After each substitution of a_0, the interval I_{a_0} are reduced by a factor p, while the other intervals may depend on a_0. For example, suppose we perform a

reduction on a_0 of the kind:

$$a_0 = g_0 + p \cdot a_0^{(\mathrm{I})} \qquad \text{and} \qquad I_{a_0} = [-a_1 m, N - a_1 m],$$

therefore the new interval $I_{a_0^{(\mathrm{I})}}$ becomes

$$\frac{-a_1 m - g_0}{p} \leq a_0^{(\mathrm{I})} \leq \frac{N - a_1 m - g_0}{p}.$$

However, at some point it can happen that there will not be any linear modular equations, meaning that in all the Groebner bases G_p over the different $\mathbb{F}_p$'s with small p, there will only be at least quadratic equation. In this case, we try to factorize every equation and use any linear relation found in the factorization to continue with the algorithm highlighting the choice made. We call each of this choices a *branch*. To remember that, we define the quantity $BranchNum = 1$ at the beginning of the algorithm and when we need to make a choice we add to it the number of linear factors of the equation we decided to consider minus 1. In this way, this variable will count the number of active branches. The reduction-substitution process is continued until the size of the intervals I_{a_0}, I_{b_0} and I_{b_1} are small enough to perform a brute force choice for the equations in (5.10), meaning that we try every integer value for the variable i in the interval I_i and see if the equations hold in $\mathbb{Z}$. If it is not possible to find an integer solution in that interval, we need to go back and choose a different branch, so we decrease the value of $BranchNum$ by one and then come back to the last choice made with other linear factors and choose one of them instead. When every branch is analysed and no integer solution is found, this means that there are no elements that have the property of being a perfect square in the number field defined by f, having that particular a_1. Consequently, it is necessary to change a_1 and reapply the computation again.

Algorithm 5.1 Find solutions for (5.10)

Input: Fixed N, $f = x^2 + Ax + B$ and m s.t. $f(m) = N$.

1: Choose any value for a_1;
2: Compute I_{a_0}, I_{b_0}, I_{b_1}, I_{d_1};
3: $BranchNum = 0$;
4: Compute G, the Groebner basis over $\mathbb{Q}$;
5: **for** p small prime **do**
6: Compute G_p, the Groebner basis over $\mathbb{F}_p$;
7: **end for**
8: **for** p small prime **do**
9: **for** i in G_p **and** i not a field equation **and** i not a linear form in G **and** $\deg(i) = 1$ **do**
10: **if** i involves only a_0 **then**
11: Substitute $a_0 = i_0 + p \cdot a_0$;
12: Update I_{a_0};
13: **go to** 4;
14: **else if** i involves a_0 and b_0 **then**
15: Substitute $b_0 = i_0 + i_1 \cdot a_0 + p \cdot b_0$;
16: Update I_{b_0};
17: **go to** 4;
18: **else if** i involves a_0 and b_1 **then**
19: Substitute $b_1 = i_0 + i_1 \cdot a_0 + p \cdot b_1$;
20: Update I_{b_1};
21: **go to** 4;
22: **else if** i involves a_0 and d_1 **then**
23: Substitute $d_1 = i_0 + i_1 \cdot a_0 + p \cdot d_1$;
24: Update I_{d_1};
25: **go to** 4;
26: **end if**
27: **end for**
28: **end for**
29: **if** I_{a_0}, I_{b_0}, I_{b_1} are still too "big" **then**
30: **for** p small prime **do**
31: **for** i in G_p **and** i not a field equation **and** i not a linear form in G **do**
32: Factorize i;
33: **if** i has a factor of degree 1 **then**
34: $BranchNum = BranchNum + \#\{\text{factors of } i\} - 1$;
35: $i =$ a factor of degree 1 of i;
36: **go to** 10

Algorithm 5.1 Find solutions for (5.10) (Part 2)

```
            else
                There are no solutions.
                if BranchNum ≠ 0 then
                    Go back to BranchNum = BranchNum − 1 and take another choice.
                    go to 10;
                else
                    go to 1;
                end if
            end if
        end for
    end for
else
    for (a_0, b_0, b_1, d_1) in I_{a_0} × I_{b_0} × I_{b_1} × I_{d_1} do
        Find values that satisfy all the equations in G;
    end for;
    if There are no integer solutions then
        go to 38;
    else
        return ((a_0, b_0, b_1, d_1));
    end if
end if
```

5.2.1 An example of the Algorithm

Suppose we want to factorize $N = 201589669$ ($\lfloor \log_2 N \rfloor = 27$) using Algorithm 5.1. All the computations described in this example were implemented in Magma and are reported in Appendix B. In this case $m \in \mathbb{Z}$ and the coefficients A, $B \in \mathbb{Z}$ of the polynomial f are already defined, using other strategies, as

$$\begin{cases} A = 17236 \\ B = 712 \\ m = 7991, \end{cases}$$

in fact $f(m) = 7991^2 + 17236 \cdot 7991 + 712 = 201589669 = N$. First, suppose $a_1 = 1$. We will consider small primes p in the set $\{2, 3, 5\}$. Then we fix the following lexicographic ordering: $d_1 < b_0 < b_1 < a_0$. For this particular case in order to simplify the computations, we may suppose that each parameter is in the interval $I = [-N, N]$, thus $I_{a_0} = I_{b_0} = I_{b_1} = I_{d_1} = I$. We compute the Groebner basis G in the field of Rationals. This corresponds to the starting system

$$G : \begin{cases} d_1^2 - a_0^2 - 15982a_0 + 137733588 = 0 \\ b_0 - a_0^2 + 712 = 0 \\ b_1 - 2a_0 + 17236 = 0. \end{cases}$$

1st Reduction: $BranchNum = 1$

Computing G_2, the Groebner basis over $\mathbb{F}_2$, we obtain the following system

$$G_2 : \begin{cases} d_1 + a_0 = 0 \\ b_0 + a_0 = 0 \\ b_1 = 0 \\ a_0^2 + a_0 = 0. \end{cases}$$

The last one is a field equation, while the other ones have degree 1, so if we choose the third one, we can perform the substitution

$$b_1 = 2b_1^{(\mathrm{I})} \qquad \Pi_{b_1} = 2. \tag{5.11}$$

2nd Reduction: $BranchNum = 1$

This transforms the starting system into:

$$G : \begin{cases} d_1^2 - a_0^2 - 15982a_0 + 137733588 = 0 \\ b_0 - a_0^2 + 712 = 0 \\ b_1^{(\mathrm{I})} - a_0 + 8618 = 0. \end{cases}$$

If we consider G_3, the Groebner basis over $\mathbb{F}_3$, we get

$$G_3 : \begin{cases} d_1 = 0 \\ b_0 + a_0 + 1 = 0 \\ b_1^{(\mathrm{I})} + 2a_0 + 2 = 0 \\ a_0^2 + a_0 = 0. \end{cases}$$

So, the first equation leads to

$$d_1 = 3d_1^{(\mathrm{I})} \qquad \Pi_{d_1} = 3. \tag{5.12}$$

3rd Reduction: $BranchNum = 1$

The system in $\mathbb{Q}$ becomes:

$$G : \begin{cases} 9\left(d_1^{(\mathrm{I})}\right)^2 - a_0^2 - 15982a_0 + 137733588 = 0 \\ b_0 - a_0^2 + 712 = 0 \\ b_1^{(\mathrm{I})} - a_0 + 8618 = 0 \end{cases}$$

Now we can compute G_5, the Groebner basis over $\mathbb{F}_5$

$$G_5 : \begin{cases} \left(d_1^{(\mathrm{I})}\right)^2 + a_0^2 + 2a_0 + 2 = 0 \\ d_1^{(\mathrm{I})} a_0 + d_1^{(\mathrm{I})} = 0 \\ b_0 + 4a_0^2 + 2 = 0 \\ b_1^{(\mathrm{I})} + 4a_0 + 3 = 0 \\ a_0^3 + 3a_0^2 + 4a_0 + 2 = 0. \end{cases}$$

So, the fourth equation can be rewritten as

$$b_1^{(\mathrm{I})} = a_0 + 2 + 5b_1^{(\mathrm{II})} \qquad \Pi_{b_1} = 10. \tag{5.13}$$

After this substitution, the original system becomes:

$$\begin{cases} 9\left(d_1^{(\mathrm{I})}\right)^2 - a_0^2 - 15982a_0 + 137733588 = 0 \\ b_0 - a_0^2 + 712 = 0 \\ b_1^{(\mathrm{II})} + 1724 = 0. \end{cases}$$

The third equation is a linear form, so $b_1^{(\mathrm{II})} = -1724$ and this value is fixed, therefore we do not need to consider any substitution for it anymore.

The next computation are obtained in the same way and we will just report the reductions made:

$\underline{4^{\text{th}}\text{ Reduction}}$: $BranchNum = 1$

$$d_1^{(\mathrm{I})} = a_0 + 2d_1^{(\mathrm{II})} \qquad \Pi_{d_1} = 6. \tag{5.14}$$

$\underline{5^{\text{th}}\text{ Reduction}}$: $BranchNum = 1$

$$a_0 = 2a_0^{(\mathrm{I})} \qquad \Pi_{a_0} = 2. \tag{5.15}$$

$\underline{6^{\text{th}}\text{ Reduction}}$: $BranchNum = 1$

$$d_1^{(\mathrm{II})} = 1 + a_0^{(\mathrm{I})} + 2d_1^{(\mathrm{III})} \qquad \Pi_{d_1} = 12. \tag{5.16}$$

$\underline{7^{\text{th}}\text{ Reduction}}$: $BranchNum = 1$

$$b_0 = 2b_0^{(\mathrm{I})} \qquad \Pi_{b_0} = 2. \tag{5.17}$$

$\underline{8^{\text{th}}\text{ Reduction}}$: $BranchNum = 1$

$$b_0^{(\mathrm{I})} = 2b_0^{(\mathrm{II})} \qquad \Pi_{b_0} = 4. \tag{5.18}$$

$\underline{9^{\text{th}}\text{ Reduction}}$: $BranchNum = 1$

$$b_0^{(\mathrm{II})} = a_0^{(\mathrm{I})} + 2b_0^{(\mathrm{III})} \qquad \Pi_{b_0} = 8. \tag{5.19}$$

$\underline{10^{\text{th}}\text{ Reduction}}$: $BranchNum = 1$

$$b_0^{(\mathrm{III})} = 1 + 3b_0^{(\mathrm{IV})} \qquad \Pi_{b_0} = 24. \tag{5.20}$$

Notation. From this moment on, we will remove the apices from the vari-

ables, except when describing linear substitutions. Each variable should be considered as having its latest updated value.

The new Groebner basis G has become

$$G : \begin{cases} 36d_1^2 + 72d_1 \cdot a_0 + 36d_1 + 35a_0^2 - 7955a_0 + 34433406 = 0 \\ 6b_0 - a_0^2 + a_0 + 180 = 0 \\ b_1 + 1724 = 0, \end{cases}$$

while the Groebner Bases G_2, G_3 and G_5 are

$$G_2 : \begin{cases} d_1^2 + d_1 = 0 \\ b_0^2 + b_0 = 0 \\ b_1 = 0 \\ a_0^2 + a_0 = 0 \end{cases}$$

$$G_3 : \begin{cases} d_1^3 + 2d_1 = 0 \\ b_0^3 + 2b_0 = 0 \\ b_1 = 1 \\ a_0^2 + 2a_0 = 0 \end{cases}$$

$$G_5 : \begin{cases} d_1^2 + 3a_0^2 + 3a_0 + 3 = 0 \\ d_1 \cdot a_0 + 3d_1 + a_0^2 + a_0 + 4 = 0 \\ b_0 + 4a_0^2 + a_0 = 0 \\ b_1 = 1 \\ a_0^3 + 4a_0^2 + a_0 + 4 = 0 \end{cases}$$

We notice that we are out of linear equations. Hence, it is necessary to choose a reducible equation with linear factors and use one of them, remembering the choice made. We may observe that in G_2 the only equation different from a field equation is the one in b_1, which is already fixed, while in G_3 the last equation can be factorized and, finally, in G_5 the second and the last equations can be both split. Focusing on the second equation in G_5, we have two different options:

$$a_0^{(\mathrm{I})} \equiv 2 \bmod 5 \qquad \text{or} \qquad d_1^{(\mathrm{III})} \equiv 4a_0^{(\mathrm{I})} + 2 \bmod 5. \tag{5.21}$$

We decide to choose the second option and we remember of this defining $BranchNum = 2$. So, the next substitutions are

11^{th} Reduction: $BranchNum = 2$.

$$d_1^{(\text{III})} = 4a_0^{(\text{I})} + 2 + 5d_1^{(\text{IV})} \qquad \Pi_{d_1} = 60. \tag{5.22}$$

12^{th} Reduction: $BranchNum = 2$.

$$b_0^{(\text{IV})} = 3a_0^{(\text{I})} + 2 + 5b_0^{(\text{V})} \qquad \Pi_{b_0} = 120. \tag{5.23}$$

Again we arrive at a case where there are not any linear equations in the Groebner Bases. We can see that G_3 is the same as in the previous case, so we deal with the following two choices:

$$a_0^{(\text{I})} \equiv 0 \bmod 3 \qquad \text{or} \qquad a_0^{(\text{I})} \equiv 1 \bmod 3. \tag{5.24}$$

We decide to take the first one and remember to increment $BranchNum = 3$.

13^{th} Reduction: $BranchNum = 3$.

$$a_0^{(\text{I})} = 3a_0^{(\text{II})} \qquad \Pi_{a_0} = 6. \tag{5.25}$$

14^{th} Reduction: $BranchNum = 3$.

$$a_0^{(\text{II})} = 3a_0^{(\text{III})} \qquad \Pi_{a_0} = 18. \tag{5.26}$$

15^{th} Reduction: $BranchNum = 3$.

$$b_0^{(\text{V})} = 2 + 3b_0^{(\text{VI})} \qquad \Pi_{b_0} = 360. \tag{5.27}$$

16^{th} Reduction: $BranchNum = 3$.

$$b_0^{(\text{VI})} = 2a_0^{(\text{III})} + 2 + 3b_0^{(\text{VII})} \qquad \Pi_{b_0} = 1080. \tag{5.28}$$

17^{th} Reduction: $BranchNum = 3$.

$$b_0^{(\text{VII})} = 2a_0^{(\text{III})} + 2 + 3b_0^{(\text{VIII})} \qquad \Pi_{b_0} = 3240. \tag{5.29}$$

18^{th} Reduction: $BranchNum = 3$.

$$b_0^{(\text{VIII})} = 3b_0^{(\text{IX})} \qquad \Pi_{b_0} = 9720. \tag{5.30}$$

We are stuck again and the choices are

$$a_0^{(\mathrm{III})} \equiv 0 \bmod 3 \qquad \text{or} \qquad a_0^{(\mathrm{III})} \equiv 2 \bmod 3 \tag{5.31}$$

and we decide to continue with the latter.

19^{th} Reduction: $BranchNum = 4$.

$$a_0^{(\mathrm{III})} = 2 + 3a_0^{(\mathrm{IV})} \qquad \Pi_{a_0} = 54. \tag{5.32}$$

20^{th} Reduction: $BranchNum = 4$.

$$b_0^{(\mathrm{IX})} = 2 + 2a_0^{(\mathrm{IV})} + 3b_0^{(\mathrm{X})} \qquad \Pi_{b_0} = 29160. \tag{5.33}$$

Again we need to make a choice and in G_5 there are two possibilities

$$a_0^{(\mathrm{IV})} \equiv 0 \bmod 5 \qquad \text{or} \qquad a_0^{(\mathrm{IV})} \equiv 4 \bmod 5. \tag{5.34}$$

If we take the first one, the next reductions are:

21^{st} Reduction: $BranchNum = 5$.

$$a_0^{(\mathrm{IV})} = 5a_0^{(\mathrm{V})} \qquad \Pi_{a_0} = 270. \tag{5.35}$$

22^{nd} Reduction: $BranchNum = 5$.

$$a_0^{(\mathrm{V})} = 3 + 5a_0^{(\mathrm{VI})} \qquad \Pi_{a_0} = 1350. \tag{5.36}$$

23^{rd} Reduction: $BranchNum = 5$.

$$b_0^{(\mathrm{X})} = 3 + 5b_0^{(\mathrm{XI})} \qquad \Pi_{b_0} = 145800. \tag{5.37}$$

24^{th} Reduction: $BranchNum = 5$.

$$b_0^{(\mathrm{XI})} = 3a_0^{(\mathrm{VI})} + 1 + 5b_0^{(\mathrm{XII})} \qquad \Pi_{b_0} = 729000. \tag{5.38}$$

25^{th} Reduction: $BranchNum = 5$.

$$b_0^{(\mathrm{XII})} = 4a_0^{(\mathrm{VI})} + 5b_0^{(\mathrm{XIII})} \qquad \Pi_{b_0} = 3645000. \tag{5.39}$$

Again, we need to perform a choice and we have to decide between one of the following:

$$a_0^{(\mathrm{VI})} \equiv 0 \bmod 5 \qquad \text{or} \qquad a_0^{(\mathrm{VI})} \equiv 3 \bmod 5 \qquad \text{or} \qquad a_0^{(\mathrm{VI})} \equiv 4 \bmod 5. \tag{5.40}$$

Let's focus on the first one

26^{th} Reduction: $BranchNum = 7$.

$$a_0^{(\mathrm{VI})} = 5a_0^{(\mathrm{VII})} \qquad \Pi_{a_0} = 6750. \tag{5.41}$$

27^{th} Reduction: $BranchNum = 7$.

$$b_0^{(\mathrm{XIII})} = 5b_0^{(\mathrm{XIV})} \qquad \Pi_{b_0} = 18225000. \tag{5.42}$$

28^{th} Reduction: $BranchNum = 7$.

$$b_0^{(\mathrm{XIV})} = 2a_0^{(\mathrm{VII})} + 5b_0^{(\mathrm{XV})} \qquad \Pi_{b_0} = 91125000. \tag{5.43}$$

It is worthy to report how the system in $\mathbb{Q}$ has become:

$$G : \begin{cases} 4d_1^2+27000d_1a_0+3388d_1+45511875a_0^2+11301945a_0+854628=0 \\ 2b_0 - a_0^2 + a_0 = 0 \\ b_1 + 1724 = 0. \end{cases}$$

At this moment, we should make another choice, but we have reduced the coefficients enough. Since $\left\lceil \log_2 \left(\frac{N}{\Pi_{a_0}} \right) \right\rceil = 15$ and

$$b_0 = 91125000b_0^{(\mathrm{XV})} + 56983500a0^{(\mathrm{VII})} + 715004 \Longrightarrow b_0^{(\mathrm{XV})} \in [-2^{15}, 2^{15}]$$

this means that we can perform a brute force search on the integers for $(b_0, a_0) \in [-2^{15}, 2^{15}] \times [-2^{15}, 2^{15}]$ that satisfies

$$2b_0 = a_0^2 - a_0.$$

Due to the form of this equation, we can reduce also the interval of a_0 to be half of the one for b_0, so $a_0 \in [-2^8, 2^8]$. We find a total of 512 possible solutions. For all these values of a_0 we want to study the corresponding polynomials in the variable d_1 in the first equation of G and check if they

have solutions. It results that they are all irreducible, so there is no solution using these choices. We should decrease $BranchNum$ and go back to (5.40) and take another one.

26^{th} Reduction: $BranchNum = 6$.

$$a_0^{(\text{VI})} = 3 + 5a_0^{(\text{V})} \qquad \Pi_{a_0} = 6750. \tag{5.44}$$

27^{th} Reduction: $BranchNum = 6$.

$$b_0^{(\text{XIII})} = 3 + 5b_0^{(\text{XIV})} \qquad \Pi_{b_0} = 18225000. \tag{5.45}$$

28^{th} Reduction: $BranchNum = 6$.

$$b_0^{(\text{XIV})} = 5b_0^{(\text{XV})} \qquad \Pi_{b_0} = 91125000. \tag{5.46}$$

Similarly as before, we can try to find a solution with brute force. The Groebner basis G is

$$G : \begin{cases} 4d_1^2+27000d_1a_0+19588d_1+45511875a_0^2+65916195a_0+24020070=0 \\ 2b_0 - a_0^2 - a_0 = 0 \\ b_1 + 1724 = 0 \end{cases}$$

Now (b_0, a_0) must be in the interval $[-2^{14}, 2^{14}] \times [-2^7, 2^7]$, obtaining a total of 257 possible values. However, using these values of a_0, neither of the polynomial in the first equation of the system has a solution. So, let us go back again to (5.40) and take the last choice available.

26^{th} Reduction: $BranchNum = 5$.

$$a_0^{(\text{VI})} = 4 + 5a_0^{(\text{VII})} \qquad \Pi_{a_0} = 6750. \tag{5.47}$$

27^{th} Reduction: $BranchNum = 5$.

$$b_0^{(\text{XIII})} = 4 + 5b_0^{(\text{XIV})} \qquad \Pi_{b_0} = 18225000. \tag{5.48}$$

28^{th} Reduction: $BranchNum = 5$.

$$d_1^{(\text{IV})} = 4 + 5d_1^{(\text{V})} \qquad \Pi_{d_1} = 300. \tag{5.49}$$

29^{th} Reduction: $BranchNum = 5$.

$$a_0^{(\text{VI})} = 5a_0^{(\text{VII})} \qquad \Pi_{a_0} = 33750. \tag{5.50}$$

30^{th} Reduction: $BranchNum = 5$.

$$b_0^{(\text{XIV})} = 5b_0^{(\text{XV})} \qquad \Pi_{b_0} = 91125000. \tag{5.51}$$

At this moment the system has become

$$G : \begin{cases} 4d_1^2+27000d_1a_0+5004d_1+45511875a_0^2+16845789a_0+1564952=0 \\ 2b_0 - 25a_0^2 - 7a_0 = 0 \\ b_1 + 1724 = 0 \end{cases}$$

In this case the intervals where to check for the solutions are

$$-2^{14} \leq b_0 \leq 2^{14} \qquad \text{and} \qquad -2^7 \leq a_0 \leq 2^7.$$

In this case we only find 73 possible pairs for (b_0, a_0), which evaluated in the first equation of G, give exactly one non-irreducible polynomial: the pair corresponding to the values $(b_0, a_0) = (0, 0)$ transform the first equation into the polynomial

$$(d_1 + 622)(d_1 + 629) = 0.$$

Therefore we have found two solutions for the system:

$$\begin{cases} a_0^{(\text{VIII})} & = 0 \\ b_0^{(\text{XV})} & = 0 \\ b_1^{(\text{II})} & = -1724 \\ d_1^{(\text{V})} & = -622 \end{cases} \quad \text{or} \quad \begin{cases} a_0^{(\text{VIII})} & = 0 \\ b_0^{(\text{XV})} & = 0 \\ b_1^{(\text{II})} & = -1724 \\ d_1^{(\text{V})} & = -629 \end{cases} \tag{5.52}$$

To recover the initial values for the variables, we need to invert all the relations used so far, obtaining

$$\begin{cases} a_0 & = 33750a_0^{(\text{VIII})} + 6246 \\ b_0 & = 91125000b_0^{(\text{XV})} + 102667500a_0^{(\text{VIII})} + 39011804 \\ b_1 & = 10b_1^{(\text{II})} + 67500a_0^{(\text{VIII})} + 12496 \\ d_1 & = 300d_1^{(\text{V})} + 1012500a_0^{(\text{VIII})} + 187650 \end{cases}$$

and, substituting these equations in (5.52), it follows that

$$\begin{cases} a_0 &= 6246 \\ b_0 &= 39011804 \\ b_1 &= -4744 \\ d_1 &= 1050 \text{ or } -1050. \end{cases}$$

As we expected, we obtained the same absolute value for d_1. To find the factors we need to compute

$$\gcd(a_0 + a_1 \cdot m - d_1, N) = \gcd(6246 + 1 \cdot 7991 - 1050, N) = 13187$$

and

$$\gcd(a_0 + a_1 \cdot m + d_1, N) = \gcd(6246 + 1 \cdot 7991 + 1050, N) = 15287,$$

in fact

$$N = 201589669 = 13187 \cdot 15287.$$

We would like to summarize all the reductions made in this example with the algorithm using a flow chart.

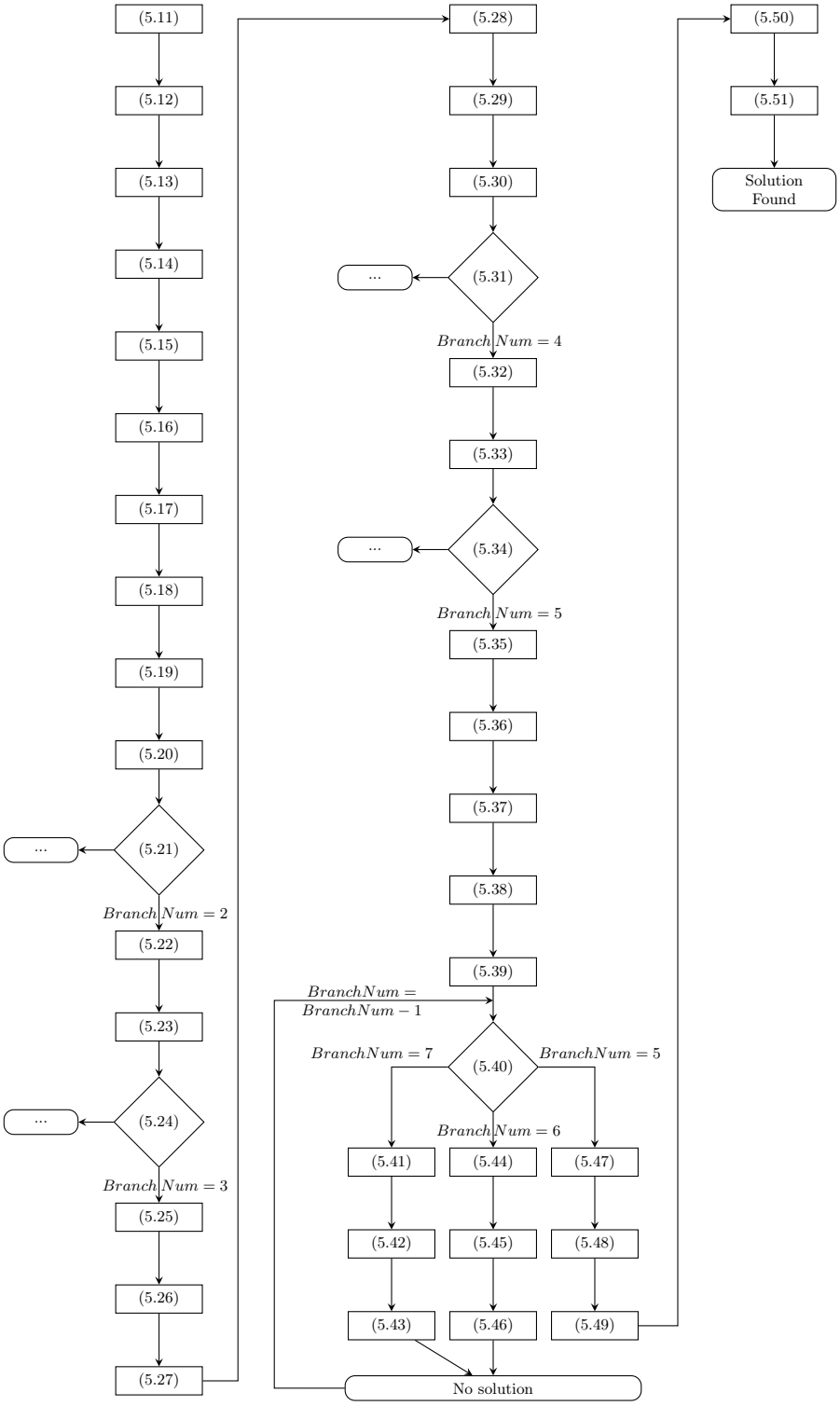

Figure 5.1: Flow chart for the reductions on $N = 201589669$.

5.3 Related Systems

Suppose we have a system like in (5.10) with the additional hypothesis that $a_1 = 1$, so that it becomes

$$\begin{cases} m^2 + Am + B = N \\ {d_1}^2 = {a_0}^2 - B + m(2a_0 - A) \\ b_0 = {a_0}^2 - B \\ b_1 = 2a_0 - A, \end{cases} \tag{5.53}$$

where the first equation is just the definition of the parameters A, B and m. We saw that finding a solution for this system could be complicated, so we need to adopt a different strategy. We may ask ourselves if there exists another integer $\overline{N} \neq N$, such that another system of the form of (5.10) again with $\bar{a}_1 = 1$ can be set, so that

$$\begin{cases} \overline{m}^2 + \overline{A}\overline{m} + \overline{B} = \overline{N} \\ \bar{d_1}^2 = \bar{a}_0{}^2 - \overline{B} + \overline{m}(2\bar{a}_0 - \overline{A}) \\ \bar{b}_0 = \bar{a}_0{}^2 - \overline{B} \\ \bar{b}_1 = 2\bar{a}_0 - \overline{A}. \end{cases} \tag{5.54}$$

We can therefore establish a link between the two sets of variables

$$\begin{cases} \overline{N} &= N + \Delta N \\ \overline{m} &= m + \Delta m \\ \overline{A} &= A + \Delta A \\ \overline{B} &= B + \Delta B \\ \bar{a}_0 &= a_0 + \Delta a_0 \\ \bar{b}_0 &= b_0 + \Delta b_0 \\ \bar{b}_1 &= b_1 + \Delta b_1 \\ \bar{d_1} &= d_1 + \Delta d_1. \end{cases} \tag{5.55}$$

In this way knowing the solutions for (5.54), we hope to recover at least some of the values of the variables in (5.53). For example, suppose that we know N and therefore define A, B and m. Furthermore, if we set $\Delta d_1 = 0$, when

we recover $\bar{d_1}$ from (5.54), we will also obtain the value of $d_1 = \bar{d_1}$ and the second equation of (5.53) could be solved to get, if any, an integer value for a_0. In order to obtain a suitable element in this way, the change of variables expressed in (5.55) does need to not depend on the variables a_0, b_0, b_1 and d_1. However this is not as easy to achieve as we would like.

Proposition 5.2. *Consider the two related systems* (5.53) *and* (5.54). *Suppose that* $\Delta N \neq 0$ *and* $\Delta d_1 = 0$ *defined as in* (5.55). *Then it does not exist any* $\overline{N}$ *for which the change of variable* (5.55) *is independent from* a_0.

Proof. Substituting the relations from (5.55) into (5.54) with $\Delta d_1 = 0$ we obtain

$$\begin{cases} N + \Delta N = & m^2 + (\Delta m)^2 + 2m\Delta m + Am + A\Delta m + m\Delta A + \\ & + \Delta A\Delta m + B + \Delta B \\ {d_1}^2 = & a_0^2 + 2a_0\Delta a_0 + (\Delta a_0)^2 - B - \Delta B + 2ma_0 + 2m\Delta a_0 + \\ & - mA - m\Delta A + 2a_0\Delta m + 2\Delta m\Delta a_0 - A\Delta m - \Delta m\Delta A \\ b_0 + \Delta b_0 = & a_0^2 + 2a_0\Delta a_0 + (\Delta a_0)^2 - B - \Delta B \\ b_1 + \Delta b_1 = & 2a_0 + 2\Delta a_0 - A - \Delta A. \end{cases}$$

We may compare these equations with those in (5.53) and get some simplifications, namely

$$\begin{cases} \Delta N = & (\Delta m)^2 + 2m\Delta m + A\Delta m + m\Delta A + \Delta A\Delta m + \Delta B \\ \Delta B = & 2a_0\Delta a_0 + (\Delta a_0)^2 + 2m\Delta a_0 - m\Delta A + 2a_0\Delta m + 2\Delta m\Delta a_0 + \\ & - A\Delta m - \Delta m\Delta A \\ \Delta b_0 = & 2a_0\Delta a_0 + (\Delta a_0)^2 - \Delta B \\ \Delta b_1 = & 2\Delta a_0 - \Delta A. \end{cases}$$

If we substitute the value of ΔB given by the second equation into the first one, we obtain the following

$$\begin{aligned} \Delta N = & (\Delta m)^2 + 2m\Delta m + 2a_0\Delta a_0 + (\Delta a_0)^2 + 2m\Delta a_0 + \\ & + 2a_0\Delta m + 2\Delta m\Delta a_0 = \\ = & (\Delta m + \Delta a_0)^2 + 2\left(m\Delta m + a_0\Delta a_0 + m\Delta a_0 + a_0\Delta m\right) = \\ = & (\Delta m + \Delta a_0)^2 + 2\left(\Delta m + \Delta a_0\right)(m + a_0) = \\ = & \left(\Delta m + \Delta a_0\right)\left(\Delta m + \Delta a_0 + 2m + 2a_0\right) \end{aligned}$$

and we remember that this quantity, by hypothesis, is different from 0, so in particular $\Delta m \neq -\Delta a_0$. Performing the same substitution in the third equation, the equivalent system becomes

$$\begin{cases} \Delta N = & (\Delta m + \Delta a_0)(\Delta m + \Delta a_0 + 2m + 2a_0) \\ \Delta B = & 2a_0\Delta a_0 + (\Delta a_0)^2 + 2m\Delta a_0 - m\Delta A + 2a_0\Delta m + 2\Delta m\Delta a_0 + \\ & -A\Delta m - \Delta m\Delta A \\ \Delta b_0 = & (\Delta A - 2\Delta a_0)(m + \Delta m) + \Delta m(A - 2a_0) \\ \Delta b_1 = & 2\Delta a_0 - \Delta A. \end{cases}$$

We may see that the only problematic variable that appears in this system is a_0, so we may set that its coefficient is equal to 0. But in the second equation the coefficient of a_0 is $2(\Delta a_0 + \Delta m)$, that is null if and only if $\Delta m = -\Delta a_0$, which is exactly the condition we excluded to obtain $\overline{N} \neq N$. □

This proposition implies that it is not possible to consider another $\overline{N}$ and use it to earn information on the solutions of (5.53), because every change of variables would depend on a_0, which is not known.

5.4 Conclusion and future works

The approach described in this chapter has some evident limits: we still need to develop a good strategy to define the polynomial f that defines the number field; the computational cost of computing Groebner bases is not negligible; the Algorithm 5.1 is not optimized. However this new point of view for the elements arising from GNFS may introduce some improvements for the sieving phase, in fact this new strategy can be seen as a criterion to say something about the shape of the elements α and β we would like to achieve.
We are currently working on a method to check whether we picked a wrong branch after just few computations, avoiding to perform the brute-force step. Another aspect we are investigating is the choice of the primes in which we compute the Groebner bases: in fact we decided to use small primes to simplify the calculations, however choosing bigger primes sensibly reduces the width of the interval, allowing the algorithm to conclude with less reductions.

Appendices

Appendix A

MAGMA Code for the Bivariate Version of GNFS

```
 /*
INPUT: l: the length of the primes
OUTPUT: p,q: two primes of length l
            n: their product (n=p*q)
*/

function primi(_l)
    repeat
        repeat
            p:=RandomPrime(_l);
        until ((p ne 2) and (#Intseq(p,2) eq _l ));
        repeat
            q:=RandomPrime(_l);
        until ((q ne 2) and (#Intseq(q,2) eq _l));
        n:=p*q;
        if p gt q then
            s:=p;
            p:=q;
            q:=s;
        end if;
```

```
    until ((Floor(Sqrt(n/2)) lt p) and (p lt Floor(Sqrt(n))) and (Floor(
    Sqrt(n)) lt q) and (q lt 2*p));
    return p,q,n;
end function;


/*
Our optimized polynomial choice

INPUT: _N: the number we need to factorize
       _R: the ring of polynomials where we need to get the result
OUTPUT: A polynomial P(x,y) of the form x^2+y^2+C and A and B,
    such that P(A,B)=N
*/

function GimmePolyAlpha(_N, _R)
        Vars := MonomialsOfDegree(_R, 1);
        pMAX := 2;
        mm := 1;
        DGbound := Floor(Sqrt(_N/3)*(Sqrt(2)-1));
        repeat
                mm *:= pMAX;
                pMAX := NextPrime(pMAX);
        until mm*pMAX gt DGbound;
        pMAX := PreviousPrime(pMAX);
        halfSq := Floor(Sqrt(_N/3));
        Arange := [Floor(halfSq/2)..halfSq];
        ReqPrimes := Remove(PrimesUpTo(pMAX), 1);
        FinalLength := #ReqPrimes;
        repeat
                A := Random(Arange);
                i := 0;
                repeat
                        i +:= 1;
                until (i eq FinalLength+1) or (LegendreSymbol(A^2-
    _N, ReqPrimes[i]) eq -1);
        until i eq FinalLength+1;
        k := Floor((-A+Sqrt(_N-A^2))/mm);
```

```
        B := A + k*mm;
        c := _N - A^2 - B^2;
        return Vars[1]^2 + Vars[2]^2 + c, A, B, c;
end function;


/*
This function see the polynomial p as an element of the ring R if
    possible .

INPUT: p: a polynomial
        R: a polynomial Ring
OUTPUT: Returns the coefficients of the polynomial p, seen as elements in
    the ring R.
*/

function CoercPoly(_p, _R)
        return _R!Coefficients(_p, 1);
end function;


/*
INPUT:  m: the number chosen at the beginning
         k: the threashold for the primes
OUTPUT  R: the ordered set of Rational Factor Base {@ [m mod p, p] @}
*/

function RationalFactorBase(_m, _k)
        return {@ [_m mod _p, _p] : _p in PrimesUpTo(_k) @};
end function;


/*
INPUT:  f: the polynomial x^2+B^2+c that defines the first extension
         g: the polynomial x^2+A^2+c that defines the second extension
         k: the threashold for the primes
OUTPUT: A1: The Algebraic Factor Base {@ [r_1,p_1], ..., [r_n,p_n] @
    } of the f-extension
```

```
        A2: The Algebraic Factor Base {@ [r_1,p_1], ..., [r_n,p_n] @
    } of the g−extension
        A: The Algebraic Factor Base {@ [r_1,p_1], ..., [r_n,p_n] @}
     of the large quartic extension
*/


function AlgebraicMultiFactorBase(_f, _g, _k)
    // p = 2 is a special case
    A := {@ [Integers()!(Evaluate(_f, 0)+Evaluate(_g, 0)) mod 2, 2]
    @};
    A1 := {@ [Integers()!(Evaluate(_f, 0)) mod 2, 2] @};
    A2 := {@ [Integers()!(Evaluate(_g, 0)) mod 2, 2] @};
    // p > 2
    for _p in Remove(PrimesUpTo(_k), 1) do
        b1, r1 := IsSquare(−Integers(_p)!Evaluate(_f, 0));
        b2, r2 := IsSquare(−Integers(_p)!Evaluate(_g, 0));
        if b1 and b2 then
            J := {r1, −r1};
            H := {r2, −r2};
            for r in J do
                A1 join:= {@ [Integers()!(r), _p] @};
                for s in H do
                    A join:= {@ [Integers()!(r+s),
    _p] @};
                end for;
            end for;
            for s in H do
                A2 join:= {@ [Integers()!(s), _p] @};
            end for;
        end if;
    end for;
    return A1, A2, A;
end function;


/*
INPUT: f: the polynomial x^2+B^2+c that defines the first extension
```

```
        g: the polynomial x^2+A^2+c that defines the second extension
        a,b: the interval in which we search for primes (must be greater
    than k). In particular a > 2.
OUTPUT: Q: the ordered set of Quadratic Characters Base {@ [r,p] @}
*/

function QuadraticCharacterBase(_f, _g, _a, _b)
        Q:= {@ @};
        for _p in PrimesInInterval(_a, _b) do
                b1, r1 := IsSquare(-Integers(_p)!Evaluate(_f, 0));
                b2, r2 := IsSquare(-Integers(_p)!Evaluate(_g, 0));
                if b1 and b2 and (r1*r2 ne 0) and (r1^2 ne r2^2) then
                        J := {r1, -r1};
                        H := {r2, -r2};
                        for r in J do
                                for s in H do
                                        Q join:= {@ [Integers()!(r+s),
    _p] @};
                                end for;
                        end for;
                end if;
        end for;
        return Q;
end function;


/*
INPUT: f: the polynomial that defines the extension
        a,b: the element of the form a+b*theta of which we need to
    compute the norm
OUTPUT: N: the norm of (a+b*theta)
*/

function RapidNorm(_f, _a, _b)
        return Integers()!((-_b)^Degree(_f)*Evaluate(_f,-_a/_b));
end function;
```

```
/*
INPUT: A,B: parameters decided at the beginning
       F: the polynomial that defines Q(theta)
       R: Rational Factor Base for Q(theta)
       A1: Algebraic Factor Base for Q(theta1)
       A2: Algebraic Factor Base for Q(theta2)
       AA: Algebraic Factor Base for Q(theta)
       QQ: Quadratic Characters Base for Q(theta)
       k: the length of the interval [-k..k]
OUTPUT: Good: a list of good (a,b) that can be factorized in the two
    Bases
*/

function MultiSieving(_A, _B, _F, _RB, _AB1, _AB2, _AB, _QB,
    _k)
        m := (_A + _B);
        tot := 1 + #_RB + #_AB + #_QB;
        Good := [];
        b:=1;
        while #Good le tot do
                Good cat:= [ [a,b] : a in [-_k.._k] | { _X[1] : _X in
    Factorization(a+b*m) } subset {_R[2] : _R in _RB} and { _X[1] :
     _X in Factorization(RapidNorm(_F, a, b)) } subset {_R[2] : _R in
     _AB1} ];
                b:=b+1;
                Good;
        end while;
        return Good;
end function;


///// TEST

Q := Rationals();       //Defines the Field of Rationals Q
Acc<z> := PolynomialRing(Q); //Defines the Polynomial Ring in the
    variable z over Q
R<x,y> := PolynomialRing(Q, 2); //Defines the Polynomial Ring in the
    two variables x and y over Q
```

```
p,q,N := primi(8);
f, A, B, c := GimmePolyAlpha(N, R);
F1 := CoercPoly(Evaluate(f, [x,B]), Acc); // min pol of Q(a)
F2 := CoercPoly(Evaluate(f, [A,x]), Acc); // min pol of Q(b)
F := z^4+2*(c+N)*z^2+(A^2-B^2)^2; // min pol of Q(theta)=Q(a+b)

RB := RationalFactorBase(A+B, 30);
AB1, AB2, AB := AlgebraicMultiFactorBase(F1, F2, 100);
QB := QuadraticCharacterBase(F1, F2, 101, 150);

Good := MultiSieving(A, B, F, RB, AB1, AB2, AB, QB, 100);
```

Appendix B

MAGMA Code for the System using Groebner Bases

```
 /*
INPUT: _p, a number
OUTPUT: F_p, the finite field with _p elements or
            Q, the field of rationals if _p is not a prime
*/


KK:=function(_p)
 if IsPrime(_p) then return GF(_p); end if;
 return(Rationals());
end function;

/*
INPUT: _p, a prime
          _f, a polynomial with rational coefficients
OUTPUT: ret, the polynomial _f multiplied by the right power of _p, such
      that _p does not divide any coefficient of ret
*/


Fixx:=function(_f,_p)
 local _C,_M,_ret,_c;
```

```
 _C:=Coefficients(_f);
 _M:=Monomials(_f);
 _ret:=0; _c:=0;
 if #_C ne #_M then
   print("help");
   return(100000000000000000);
 end if;
 for i in [1..#_C] do
   while (Denominator(_C[i]) mod _p^(_c+1) eq 0) do
     _c:=_c+1;
   end while;
 end for;
 _C:=[_C[i]*_p^_c: i in [1..#_C]];

 for i in [1..#_C] do
   _ret:=_ret+_C[i]*_M[i];
 end for;
 return(_ret);
end function;

/*
Fix an integer we want to factorize
*/
NN:=201589669;

/*
Setting the system
*/

p:=0;
QQ<d1,t,b0,b1,m,A,B,a0,a1>:=PolynomialRing(KK(p),9);

F:=t^2+A*t+B;
alpha:=a1*t+a0; beta:=b1*t+b0;
rel:=NormalForm(alpha^2-beta,[F]);  // alpha^2 = beta
rel0:=NormalForm(rel,[t]);
rel1:=(rel-rel0) div t;
```

```
phialpha:=a1*m+a0; phibeta:=b1*m+b0;
extra:=[];

/*
Fix the values of A,B,m and a1
*/

Base:=[rel0,rel1 , m^2+A*m+B-NN,phibeta-d1^2,B-712,A-17236,m
    -7991,a1-1];

//Define the variables to check how they change during the substitutions
Elements:=[F,alpha,beta,d1,t,b0,b1,m,A,B,a0,a1];

////////////////////////////////////////////////////////////
//Adding information by modular reductions (computed below)//
////////////////////////////////////////////////////////////

// b1-->2*b1
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,2*b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,2*b1,m,A,B,a0,a1]);
end for;
// d1 --> 3*d1
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[3*d1,t,b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[3*d1,t,b0,b1,m,A,B,a0,a1]);
end for;
// b1 --> a0+2+5*b1
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,a0+2+5*b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,a0+2+5*b1,m,A,B,a0,a1]);
end for;
```

```
// d1 --> a0+2*d1
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[a0+2*d1,t,b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[a0+2*d1,t,b0,b1,m,A,B,a0,a1]);
end for;
// a0 --> 2*a0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,b1,m,A,B,2*a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,b1,m,A,B,2*a0,a1]);
end for;
// d1 --> 1+a0+2*d1
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[1+a0+2*d1,t,b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[1+a0+2*d1,t,b0,b1,m,A,B,a0,a1]);
end for;
//b0 ---> 2*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,2*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,2*b0,b1,m,A,B,a0,a1]);
end for;
//b0 ---> 2*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,2*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,2*b0,b1,m,A,B,a0,a1]);
end for;
//b0 ---> a0+2*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,a0+2*b0,b1,m,A,B,a0,a1]);
```

```
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,a0+2*b0,b1,m,A,B,a0,a1]);
end for;
//b0 ---> 1+3*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,1+3*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,1+3*b0,b1,m,A,B,a0,a1]);
end for;
// d1 --> 4a0+2+5*d1 *****CHOICE*****
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[4*a0+2+5*d1,t,b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[4*a0+2+5*d1,t,b0,b1,m,A,B,a0,a1]);
end for;
//b0 ---> 3a0+2+5*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,3*a0+2+5*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,3*a0+2+5*b0,b1,m,A,B,a0,a1]);
end for;
// a0 --> 3*a0     *****CHOICE*****
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,b1,m,A,B,3*a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,b1,m,A,B,3*a0,a1]);
end for;
// a0 --> 3*a0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,b1,m,A,B,3*a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,b1,m,A,B,3*a0,a1]);
```

```
end for;
//b0 ---> 2+3*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,2+3*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,2+3*b0,b1,m,A,B,a0,a1]);
end for;
//b0 ---> 2a0+2+3*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,2*a0+2+3*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,2*a0+2+3*b0,b1,m,A,B,a0,a1]);
end for;
//b0 ---> 2a0+2+3*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,2*a0+2+3*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,2*a0+2+3*b0,b1,m,A,B,a0,a1]);
end for;
//b0 ---> 3*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,3*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,3*b0,b1,m,A,B,a0,a1]);
end for;
// a0 --> 2+3*a0     *****CHOICE*****
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,b1,m,A,B,2+3*a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,b1,m,A,B,2+3*a0,a1]);
end for;
//b0 ---> 2a0+2+3*b0
for i in [1..#Base] do
```

```
  Base[i]:=Evaluate(Base[i],[d1,t,2*a0+2+3*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,2*a0+2+3*b0,b1,m,A,B,a0,a1]);
end for;
// a0 --> 5*a0  *****CHOICE******
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,b1,m,A,B,5*a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,b1,m,A,B,5*a0,a1]);
end for;
// a0 ---> 3+5*a0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,b1,m,A,B,3+5*a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,b1,m,A,B,3+5*a0,a1]);
end for;
//b0 ---> 3+5*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,3+5*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,3+5*b0,b1,m,A,B,a0,a1]);
end for;
//b0 ---> 3a0+1+5*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,3*a0+1+5*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,3*a0+1+5*b0,b1,m,A,B,a0,a1]);
end for;
//b0 ---> 4a0+5*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,4*a0+5*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
```

```
  Elements[i]:=Evaluate(Elements[i],[d1,t,4*a0+5*b0,b1,m,A,B,a0,a1]);
end for;
/*// a0 -->5*a0  ***** WRONG CHOICE******
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,b1,m,A,B,5*a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,b1,m,A,B,5*a0,a1]);
end for;
//b0 ---> 5*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,5*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,5*b0,b1,m,A,B,a0,a1]);
end for;
//b0 ---> 2a0+5*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,2*a0+5*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,2*a0+5*b0,b1,m,A,B,a0,a1]);
end for;
*/
/*// a0 -->3+5*a0  *****WRONG CHOICE******
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,b1,m,A,B,3+5*a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,b1,m,A,B,3+5*a0,a1]);
end for;
//b0 ---> 3+5*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,3+5*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,3+5*b0,b1,m,A,B,a0,a1]);
end for;
```

```
//b0 ---> 5*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,5*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,5*b0,b1,m,A,B,a0,a1]);
end for;
*/
// a0 -->4+5*a0  ***** RIGHT CHOICE ******
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,b1,m,A,B,4+5*a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,b1,m,A,B,4+5*a0,a1]);
end for;
//b0 ---> 1+5*b0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,1+5*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,1+5*b0,b1,m,A,B,a0,a1]);
end for;
//d1 --->4+5d1
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[4+5*d1,t,b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[4+5*d1,t,b0,b1,m,A,B,a0,a1]);
end for;
// a0 -->5*a0
for i in [1..#Base] do
  Base[i]:=Evaluate(Base[i],[d1,t,b0,b1,m,A,B,5*a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,b0,b1,m,A,B,5*a0,a1]);
end for;
//b0 ---> 1+5*b0
for i in [1..#Base] do
```

```
  Base[i]:=Evaluate(Base[i],[d1,t,1+5*b0,b1,m,A,B,a0,a1]);
end for;
for i in [1..#Elements] do
  Elements[i]:=Evaluate(Elements[i],[d1,t,1+5*b0,b1,m,A,B,a0,a1]);
end for;


// Compute Rational Groebner Base
if p eq 0 then
  J:=ideal<QQ | Base>;
  time G:=GroebnerBasis(J);
  G;
end if;

////////////////////////////////////////////////////
////////Moduli with additional equations///////////
////////////////////////////////////////////////////

p:=2;
QQ2<d1,t,b0,b1,m,A,B,a0,a1>:=PolynomialRing(KK(p),9);
extra:=[b1^p-b1,b0^p-b0,d1^p-d1,m^p-m,a0^p-a0,a1^p-a1,A^p-A,
    B^p-B];
//Compute the Groebner Base in GF(2) starting from the one calculated
    before
G2:=GroebnerBasis([QQ2!Fixx(_g,p) : _g in G] cat extra);
G2;


p:=3;
QQ3<d1,t,b0,b1,m,A,B,a0,a1>:=PolynomialRing(KK(p),9);
extra:=[b1^p-b1,b0^p-b0,d1^p-d1,m^p-m,a0^p-a0,a1^p-a1,A^p-A,
    B^p-B];
//Compute the Groebner Base in GF(3) starting from the one calculated
    before
G3:=GroebnerBasis([QQ3!Fixx(_g,p) : _g in G] cat extra);
G3;

p:=5;
```

```
QQ5<d1,t,b0,b1,m,A,B,a0,a1>:=PolynomialRing(KK(p),9);
extra:=[b1^p-b1,b0^p-b0,d1^p-d1,m^p-m,a0^p-a0,a1^p-a1,A^p-A,
    B^p-B];
//Compute the Groebner Base in GF(5) starting from the one calculated
    before
G5:=GroebnerBasis([QQ5!Fixx(_g,p) : _g in G] cat extra);
G5;

p:=7;
QQ7<d1,t,b0,b1,m,A,B,a0,a1>:=PolynomialRing(KK(p),9);
extra:=[b1^p-b1,b0^p-b0,d1^p-d1,m^p-m,a0^p-a0,a1^p-a1,A^p-A,
    B^p-B];
//Compute the Groebner Base in GF(7) starting from the one calculated
    before
G7:=GroebnerBasis([QQ7!Fixx(_g,p) : _g in G] cat extra);
G7;


p:=11;
QQ11<d1,t,b0,b1,m,A,B,a0,a1>:=PolynomialRing(KK(p),9);
extra:=[b1^p-b1,b0^p-b0,d1^p-d1,m^p-m,a0^p-a0,a1^p-a1,A^p-A,
    B^p-B];
//Compute the Groebner Base in GF(11) starting from the one calculated
    before
G11:=GroebnerBasis([QQ11!Fixx(_g,p) : _g in G] cat extra);
G11;



/////////Look for the right solution with brute force


//BranchNum=7
p:=0;
QQ<d1,t,b0,b1,m,A,B,a0,a1>:=PolynomialRing(KK(p),9);

time Solutions:=[[_b0,_a0] : _b0 in [-2^15..2^15], _a0 in [-2^8..2^8] |
     Evaluate(QQ!G[2],[d1,t,_b0,b1,m,A,B,_a0,a1]) eq 0];
```

```
//195.8 sec

for i in Solutions do
        if IsIrreducible (Evaluate(QQ!G[1],[d1,t,i [1], b1,m,A,B,i[2],a1]))
    eq false then
                i;
                Factorization(Evaluate(QQ!G[1],[d1,t,i [1], b1,m,A,B,i[2],
    a1]));
        end if;
end for;

//BranchNum=6
p:=0;
QQ<d1,t,b0,b1,m,A,B,a0,a1>:=PolynomialRing(KK(p),9);

time Solutions:=[[_b0,_a0] : _b0 in [-2^14..2^14], _a0 in [-2^7..2^7] |
     Evaluate(QQ!G[2],[d1,t,_b0,b1,m,A,B,_a0,a1]) eq 0];
//50.56 sec

for i in Solutions do
        if IsIrreducible (Evaluate(QQ!G[1],[d1,t,i [1], b1,m,A,B,i[2],a1]))
    eq false then
                i;
                Factorization(Evaluate(QQ!G[1],[d1,t,i [1], b1,m,A,B,i[2],
    a1]));
        end if;
end for;

//BranchNum=5
p:=0;
QQ<d1,t,b0,b1,m,A,B,a0,a1>:=PolynomialRing(KK(p),9);

time Solutions:=[[_b0,_a0] : _b0 in [-2^14..2^14], _a0 in [-2^7..2^7] |
     Evaluate(QQ!G[2],[d1,t,_b0,b1,m,A,B,_a0,a1]) eq 0];
//49.66

for i in Solutions do
        if IsIrreducible (Evaluate(QQ!G[1],[d1,t,i [1], b1,m,A,B,i[2],a1]))
```

```
    eq false then
                i;
                Factorization(Evaluate(QQ!G[1],[d1,t,i [1], b1,m,A,B,i[2],
    a1]));
        end if;
end for;
```

Bibliography

[Adl91] Leonard M. Adleman. Factoring numbers using singular integers. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 64–71. ACM, 1991.

[AGLL94] Derek Atkins, Michael Graff, Arjen K. Lenstra, and Paul C. Leyland. The magic words are squeamish ossifrage. In *International Conference on the Theory and Application of Cryptology*, pages 261–277. Springer, 1994.

[AKSU04] Kazumaro Aoki, Yuji Kida, Takeshi Shimoyama, and Hiroki Ueda. GNFS factoring statistics of RSA-100, 110,..., 150. *IACR Cryptology ePrint Archive*, 2004:95, 2004.

[BBF+03] Friedrich Bahr, M. Böhm, Jens Franke, Thorsten Kleinjung, and Manfred Lochter. Factorization of RSA-160. `https://members.loria.fr/PZimmermann/records/rsa160`, 2003. Accessed: 2019-06-10.

[BBFK05a] Friedrich Bahr, M. Böhm, Jens Franke, and Thorsten Kleinjung. Factorization of RSA-200. `https://web.archive.org/web/20080322125316/http://www.crypto-world.com/announcements/rsa200.txt`, 2005. Accessed with time machine: 2007-01-04.

[BBFK05b] Friedrich Bahr, M. Böhm, Jens Franke, and Thorsten Kleinjung. Factorization of RSA-640. `https://web.archive.org/web/20070104090822/http://www.rsasecurity.com/rsalabs/node.asp?id=2964`, 2005. Accessed with time machine: 2007-01-04.

[BBKZ16] Shi Bai, Cyril Bouvier, Alexander Kruppa, and Paul Zimmer-

mann. Better polynomials for GNFS. *Mathematics of Computation*, 85(298):861–873, 2016.

[BGK+16] Shi Bai, Pierrick Gaudry, Alexander Kruppa, Emmanuel Thomé, and Paul Zimmermann. Factorisation of RSA-220 with CADO-NFS. `https://hal.inria.fr/hal-01315738/document`, 2016. Accessed: 2019-06-10.

[BK10] Dominik Bonenberger and Martin Krone. Factorization of RSA-170. `https://web.archive.org/web/20110719004557/http://public.rz.fh-wolfenbuettel.de/~kronema/pdf/rsa170.pdf`, 2010. Accessed with time machine: 2011-07-19.

[BLP93] Joe P. Buhler, Hendrik W. Lenstra, and Carl Pomerance. Factoring integers with the number field sieve. In *The development of the number field sieve*, pages 50–94. Springer, 1993.

[BTZ12] Shi Bai, Emmanuel Thomé, and Paul Zimmermann. Factorisation of RSA-704 with CADO-NFS. `https://hal.inria.fr/hal-00760322/document`, 2012. Accessed: 2019-06-10.

[Buc65] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Universitat Insbruck, 1965.

[BW00] David M. Bressoud and Stan Wagon. *A course in computational number theory.* Key College Pub., 2000.

[CDEH+96] James Cowie, Bruce Dodson, Marije Elkenbracht-Huizing, Arjen K. Lenstra, Peter L. Montgomery, and Joerg Zayer. A world wide number field sieve factoring record: on to 512 bits. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 382–394. Springer, 1996.

[CDL+99] Stefania Cavallar, Bruce Dodson, Arjen Lenstra, Paul Leyland, Walter Lioen, Peter L. Montgomery, Brian Murphy, Herman Te Riele, and Paul Zimmermann. Factorization of RSA-140 using the number field sieve. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 195–207. Springer, 1999.

[CDL+00] Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Walter Lioen, Peter L. Montgomery, Brian Murphy, Herman Te Riele, Karen Aardal, Jeff Gilchrist, Gérard Guillerm, et al. Factorization of a 512-bit RSA modulus. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 1–18. Springer, 2000.

[CLO13] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013.

[Coh13] Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013.

[Cou93] Jean-Marc Couveignes. Computing a square root for the number field sieve. In *The development of the number field sieve*, pages 95–102. Springer, 1993.

[Cox15] Nicholas Coxon. Montgomery's method of polynomial selection for the number field sieve. *Linear Algebra and its Applications*, 485:72–102, 2015.

[DDLM93] Thomas Denny, Bruce Dodson, Arjen K. Lenstra, and Mark S. Manasse. On the factorization of RSA-120. In *Annual International Cryptology Conference*, pages 166–174. Springer, 1993.

[Dic30] Karl Dickman. On the frequency of numbers containing prime factors of a certain relative magnitude. *Arkiv for matematik, astronomi och fysik*, 22(10):1–14, 1930.

[Dix81] John D. Dixon. Asymptotically fast factorization of integers. *Mathematics of computation*, 36(153):255–260, 1981.

[DL93] Brandon Dixon and Arjen K. Lenstra. Factoring integers using SIMD sieves. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 28–39. Springer, 1993.

[DP10] S.A. Danilov and Ilya A. Popovyan. Factorization of RSA-180. *IACR Cryptology ePrint Archive*, 2010:270, 2010.

[Edw96] Harold M. Edwards. *Fermat's last theorem: a genetic introduction to algebraic number theory*, volume 50. Springer Science & Business Media, 1996.

[EH96a] Marije Elkenbracht-Huizing. An implementation of the number field sieve. *Experimental Mathematics*, 5(3):231–253, 1996.

[EH96b] Marije Elkenbracht-Huizing. A multiple polynomial general number field sieve. In *International Algorithmic Number Theory Symposium*, pages 99–114. Springer, 1996.

[FK03] Jens Franke and Thorsten Kleinjung. Factorization of RSA-576. `https://web.archive.org/web/20061224002937/http://www.rsasecurity.com/rsalabs/node.asp?id=2096`, 2003. Accessed with time machine: 2006-12-24.

[GKP94] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science (2nd Edition)*. Addison-Wesley Professional, mar 1994.

[GLM94] Roger A. Golliver, Arjen K. Lenstra, and Kevin S. McCurley. Lattice sieving and trial division. In *International Algorithmic Number Theory Symposium*, pages 18–27. Springer, 1994.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of computer and system sciences*, 28(2):270–299, 1984.

[Gro17] Samuel S. Gross. Factorization of RSA-230. `https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2018-August/000926.html`, 2017. Accessed: 2019-06-10.

[GWJ08] Jason Gower and Samuel Wagstaff Jr. Square form factorization. *Mathematics of computation*, 77(261):551–588, 2008.

[Hea56] Thomas L. Heath. *The thirteen books of Euclid's Elements*, volume 2. Courier Corporation, 1956.

[KAF+10] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Emmanuel Lenstra, Arjen Kand Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, et al. Factorization of a 768-bit RSA modulus. In *Annual Cryptology Conference*, pages 333–350. Springer, 2010.

[Kle06] Thorsten Kleinjung. On polynomial selection for the general number field sieve. *Mathematics of Computation*, 75(256):2037–2047, 2006.

[Lan02] Serge Lang. *Algebra, volume 211 of Graduate texts in mathematics*. Springer-Verlag, New York,, 2002.

[Leh74] R. Sherman Lehman. Factoring large integers. *Mathematics of Computation*, 28(126):637–646, 1974.

[LJ87] Hendrik W. Lenstra Jr. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987.

[LLMP93a] Arjen K. Lenstra, Hendrik W. Lenstra, Mark S. Manasse, and John M. Pollard. *The development of the number field sieve*. Springer, 1993.

[LLMP93b] Arjen K. Lenstra, Hendrik W. Lenstra, Mark S. Manasse, and John M. Pollard. The number field sieve. In *The development of the number field sieve*, pages 11–42. Springer, 1993.

[LP31] Derrick H. Lehmer and Richard E. Powers. On factoring large numbers. *Bulletin of the American Mathematical Society*, 37(10):770–776, 1931.

[Mon93] Peter L. Montgomery. Square roots of products of algebraic numbers. *Mathematics of Computation*, pages 567–571, 1993.

[Mur99] Brian Antony Murphy. *Polynomial selection for the number field sieve integer factorisation algorithm*. Australian National University, 1999.

[Ngu98] Phong Nguyen. A montgomery-like square root for the number field sieve. In *International Algorithmic Number Theory Symposium*, pages 151–168. Springer, 1998.

[Nor71] Karl K. Norton. *Numbers with small prime factors, and the least k-th power non-residue*, volume 106. American Mathematical Soc., 1971.

[Pol74] John M. Pollard. Theorems on factorization and primality testing. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 76, pages 521–528. Cambridge University Press, 1974.

[Pol75] John M. Pollard. A monte carlo method for factorization. *BIT Numerical Mathematics*, 15(3):331–334, 1975.

[Pol93a] John M. Pollard. Factoring with cubic integers. In *The development of the number field sieve*, pages 4–10. Springer, 1993.

[Pol93b] John M. Pollard. The lattice sieve. In *The development of the number field sieve*, pages 43–49. Springer, 1993.

[Pom82] Carl Pomerance. Analysis and comparison of some integer factoring algorithms. *Computational methods in number theory*, pages 89–139, 1982.

[Pom08] Carl Pomerance. A tale of two sieves. *Biscuits of Number Theory*, 85:175, 2008.

[Pop13] Ryan Popper. Factorization of RSA-210. `https://www.mersenneforum.org/showpost.php?p=354259`, 2013. Accessed: 2019-06-10.

[PT10] Ilya A. Popovyan and Andrey Timofeev. Factorization of RSA-190. `https://mersenneforum.org/showpost.php?p=236114&postcount=1`, 2010. Accessed: 2019-06-10.

[Rab79] Michael O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical report, Massachusetts Inst of Tech Cambridge Lab for Computer Science, 1979.

[Rob03] John P. Robertson. Solving the equation $ax^2+bxy+cy^2+dx+ey+f=0$. `https://web.archive.org/web/20180831180321/http://www.jpr2718.org/ax2p.pdf`, 2003. Accessed with time machine: 2018-08-31.

[RSAa] Announcement of RSA factoring challenge. `https://groups.google.com/forum/#!original/sci.crypt/AA7M9qWWx3w/EkrsR69CDqIJ`. Accessed: 2019-04-12.

[RSAb] The RSA challenge numbers. `https://web.archive.org/web/20070224193029/http://www.rsa.com/rsalabs/node.asp?id=2093`. Accessed with time machine: 2007-02-24.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[Sha71] Daniel Shanks. Class number, a theory of factorization, and genera. In *Proc. of Symp. Math. Soc., 1971*, volume 20, pages 41–440, 1971.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[Sig03] Laurence Sigler. *Fibonacci's Liber Abaci: a translation into modern English of Leonardo Pisano's book of calculation.* Springer Science & Business Media, 2003.

[Sil87] Robert D. Silverman. The multiple polynomial quadratic sieve. *Mathematics of Computation*, 48(177):329–339, 1987.

[SSW08] Reginald E. Sawilla, Alan K. Silvester, and Hugh C. Williams. A new look at an old equation. In *International Algorithmic Number Theory Symposium*, pages 37–59. Springer, 2008.

[ST01] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem.* AK Peters/CRC Press, 2001.

[Wei98] Edwin Weiss. *Algebraic number theory.* Courier Corporation, 1998.