Prime Factorization and Cryptography
A theoretical introduction to the General Number Field Sieve

Barry van Leeuwen
University of Bristol
10 CP Undergraduate Project

Supervisor: Dr. Tim Dokchitser

February 1, 2019
Acknowledgement of Sources

For all ideas taken from other sources (books, articles, internet), the source of the ideas is mentioned in the main text and fully referenced at the end of the report.

All material which is quoted essentially word-for-word from other sources is given in quotation marks and referenced.

Pictures and diagrams copied from the internet or other sources are labelled with a reference to the web page, book, article etc.

Signed: Barry van Leeuwen
Dated: February 1, 2019
Abstract

From a theoretical puzzle to applications in cryptography and computer science: The factorization of prime numbers. In this paper we will introduce a historical retrospect by observing different methods of factorizing primes and we will introduce a theoretical approach to the General Number Field Sieve building from a foundation in Algebra and Number Theory.

We will in this exclude most considerations of efficiency and practical implementation, and instead focus on the mathematical background. In this paper we will introduce the theory of algebraic number fields and Dedekind domains and their importance in understanding the General Number Field Sieve before continuing to explain, step by step, the inner workings of the General Number Field Sieve.
Contents

Abstract 1

Table of contents 2

1 Introduction 3

2 Prime Numbers and the Algebra of Modern Cryptography 5
  2.1 Preliminary Algebra and Number Theory ............... 5
    2.1.1 Algebra: Domains, Ideals, and Algebraicity .... 5
    2.1.2 Number Theory: Primes, Legendre Symbols, and Quadratic Residue ......................... 8
  2.2 Modern Cryptography - RSA .......................... 11

3 An Introduction to Factorization Methods: 14
  3.1 Fermat’s factorization method and Legendre congruences ... 14
  3.2 Continued Fraction Method ............................. 18
  3.3 Morrison-Brillhart ..................................... 22
  3.4 Quadratic Sieve ........................................ 24

4 General Number Field Sieve 28
  4.1 Factor bases and smoothness in Algebraic Number Fields ... 28
    4.1.1 Field Extensions and Algebraicity ............... 28
    4.1.2 Algebraic Number Fields ......................... 34
    4.1.3 Dedekind domains ................................. 41
    4.1.4 Norms of Ideals .................................. 47
  4.2 Sieving for smooth elements ................................
    4.2.1 Base-M Method ................................... 56
    4.2.2 Homomorphism and Smooth elements ............... 57
    4.2.3 Finding the set of solutions, S: ............... 60
  4.3 Hunting for Perfect Squares ............................ 65
    4.3.1 Resolving obstructions: Quadratic Characters: ... 65
    4.3.2 Extracting Square Roots ......................... 68
  4.4 Statement of the Algorithm ............................ 70

5 Conclusion 71

Acknowledgements 72

References 73
1 Introduction

In the last 50 years we, as a society, have seen an extreme increase of computers and automated systems to deal with daily, if not menial, tasks that in the past would have been done by hand. One of the main features that we use every day is the payment card issued by our banks. Here we use a device that we perceive as secure to send our personal data from a shop or website to our bank issuing a payment of the right amount, from the right account, to the right destination, and that all without us having to do more than to enter our details.

The reason we can do this is because public-key cryptography. Public-Key Cryptography is a cryptographical system where there is a public "encryption" key and a private (to anyone but the receiver unknown) "decryption" key. These systems are, in majority, based on two problems which are considered unsolvable in polynomial time: the Diffie-Hellmann Problem and the prime factorization problem. One of the most famous Public-Key Cryptosystems is the RSA-system, which will be introduced more thoroughly in Section 2. Afterwards we will have a look at the history of the prime factorization problem in Section 3: An Introduction to Factorization Methods

The fact that factoring large prime numbers is difficult and an open problem for which a solution is perceived to answer the Millenium Question, P versus NP\(^1\), is the reason that RSA-variants are still used in cryptography today. In our attempt to mathematically solve this long standing problem many efforts have been made by the likes of Fermat, Dixon, and Pomerance, where the latter designed the second fastest general sieve, the Quadratic Sieve, in 1981. We will throw a referencing glance at the Quadratic Sieve in Section 3 as we build up our understanding for our main subject. This is however no longer the fastest way to factorize large primes\(^2\) as the main topic of this paper has taken over: The General Number Field Sieve.

The General Number Field Sieve (GNFS) is currently the fastest factorization method which generalizes many of the ideas we have from the Quadratic Field Sieve to be used in other fields. The GNFS was used to break the 130-digit challenge-integer as posed by RSA, which is the largest integer with cryptographic significance to ever be factored at the time. A specialized version of the GNFS, aptly called the Special Number Field Sieve (SNFS), also

\(^1\)More info on: http://www.claymath.org/millennium-problems/p-vs-np-problem
\(^2\)Note: "Large" is here defined as a composite number of more than 110 digits
exists, but this requires numbers to be of the form $r^e \pm s$ where $r, e, s \in \mathbb{Z}$ and $e > 0$. This has made the SNFS the attack of choice on Fermat numbers, Mersenne primes, and other numbers of the proposed form.

In Section 2 we will be looking at the basic Algebra and Number Theory that is necessary for us to understand the sieving techniques we are discussing in Section 3. While it might seem odd to introduce these "older" sieving techniques they each introduce some concepts which will be used in the GNFS. In Section 4 we will take a look at how the General Number Field Sieve is built up, starting by expanding our theoretical knowledge of algebraic number theory adding such things as field extensions, Dedekind domains, and other algebraic and number theoretical tools to our toolkit which we will need to be able to discuss the GNFS in full. The actual algorithm will then be stated in the final stretch of Section 4.
2 Prime Numbers and the Algebra of Modern Cryptography

2.1 Preliminary Algebra and Number Theory

Before we can start with describing modern cryptography at all we need to have a basis knowledge in place. We will assume basic knowledge of number theory, prime numbers, and algebra but will reiterate some of the, for this paper, important definitions and theorems.

2.1.1 Algebra: Domains, Ideals, and Algebraicity

We will start by developing a basis of algebra so we can expand on this when we talk about number sieves and algebraic number fields. The definitions that we discuss are commonly available in many sources but a reference to these can be found in [1], despite some being adapted slightly to fit our purpose.

To be able to discuss commonalities between different sets we want to define different domains which are subsets of \( \mathbb{C} \). For this we let \( R \) be an arbitrary commutative ring with multiplicative identity.

**Definition 2.1.** Let \( R \) be a ring as above. Then \( R \) is an integral domain if for all \( r, r' \in R \setminus \{0\} \) it holds that

\[
rr' \neq 0
\]

An integral domain is called a field if

\[
\forall r \in R \setminus \{0\} \exists r' \in R \setminus \{0\} : rr' = 1
\]

We will now introduce the following notation and make an observation regarding fields:

**Definition 2.2.** Let \( D \) be an integral domain. The units of \( D \), denoted \( D^* \), are the elements \( d \in D \) for which there exists \( e \in D \) such that \( de = ed = 1 \).

Note that for fields \( K, K^* = K \setminus \{0\} \), and this is in fact not only sufficient but also required for an integral domain to be considered a field.

**Theorem 2.3.** Let \( D \) be an integral domain.

\[
D^* = D \setminus \{0\} \Leftrightarrow D \text{ is a field}
\]
Definition 2.4. A nonzero, nonunit element $a$ of an integral domain $D$ is said to be irreducible, if $a = bc$, where $b, c \in D$, implies that $b \in D^*$ or $c \in D^*$. - A nonzero, non-unit element that is not irreducible is called reducible.

Next we will tackle the basic definition of an important class, namely the ideals. Later on we will be seeing ideals come back in multiple forms, such as ideals in rings of integers and when we discuss Dedekind domains. To get a more complete understanding of ideals reference [1] and [4].

Definition 2.5. Let $D$ be an integral domain. A subset $I \subseteq D$ is called an ideal of $D$ if the following holds:

\[ a \in I, b \in I \Rightarrow a + b \in I \]
\[ a \in I, r \in D \Rightarrow ar \in I \]

Definition 2.6. A nonzero, nonunit element $p \in D$ is called prime if $p | ab \Rightarrow p | a \lor p | b$

From this spawns a whole area of interest, but we will keep us to the following definitions and theorems:

Definition 2.7. An ideal, $I$, of an integral domain $D$ is called a maximal ideal if whenever $J$ is an ideal such that $I \subseteq J \subseteq D$ then $I = J$ or $J = D$.

Definition 2.8. An ideal, $P$, of an integral domain $D$ is called a prime ideal if

\[ a, b \in D \land ab \in P \Rightarrow a \in P \lor b \in P \]

The following bi-implication is an alternate way to define a prime ideal.

Proposition 2.9. Let $P$ be a proper ideal of an integral domain $D$. Then $P$ is a prime ideal if and only if for any two ideals $A$ and $B$ of $D$ satisfying $AB \subseteq P$ either $A \subset P$ or $B \subseteq P$

Definition 2.10. An ideal, $I$, of an integral domain $D$ is called a principle ideal if there exists an element $a \in I$ such that $a$ generates $I$, we denote $I = \langle a \rangle$.

Definition 2.11. An integral domain, $D$, is called a Principle Ideal Domain (PID) if every ideal in $D$ is principal.

These definitions allow us a whole new area of algebra that deepens our understanding of ideal. We will, however, limit us to the key interests regarding the General Number Field Sieve (which should be well known to the reader), summing up a handful results:\n
\[ ^3 \text{Proposition 2.12 is a conglomeration of different theorems and lemmas as seen in [1]} \]
Proposition 2.12. Let $D$ be a PID, then

1. $p \in D$ then $p \in D$ prime $\iff p \in D$ irreducible.
2. $I \subseteq D$ an ideal of $D$, then $D/I$ is a field $\iff I$ is maximal.
3. $I \subseteq D$ a maximal ideal of $D$, then $I$ is a prime ideal of $D$.
4. $\langle a \rangle$ is a maximal ideal of $D$ $\iff a$ is irreducible in $D$.
5. $\langle a \rangle$ is a prime ideal of $D$ $\iff a$ is prime in $D$.

We will highlight one final theorem about rings:

Theorem 2.13. In a ring without zero divisors a polynomial of degree $n$ has at most $n$ (distinct) roots in the ring.

Now that we have recorded the above consequences we want to shift our focus onto the next part of the preliminaries, which is factorization. If we, at a later point, wish to be able to factor large integers into their prime components then we must be sure that such an action can be made, hence we must assure a number can be factored. We do this with the following definitions:

Definition 2.14. Let $D$ be an integral domain. Then $D$ is said to be a unique factorization domain (UFD) if every nonzero, nonunit element of $D$ can be expressed as a finite product of irreducible elements of $D$ up to units.

$$a = u p_1 p_2 p_3 \ldots p_n$$

where $u$ is a unit and $p_k$ is irreducible for all $1 \leq k \leq n$.

The following Theorems are very important to our goal and hence they must be noted despite being elementary algebraic theorems.

Theorem 2.15. $D$ is a field $\Rightarrow D$ is a PID $\Rightarrow D$ is a UFD

Theorem 2.16. Let $D$ be a UFD, then $a \in D$ irreducible $\iff a \in D$ prime.

We can immediately deduce from this that any element $a \in D$, for $D$ a PID, is irreducible if and only if it is prime. Moreover we note that $\mathbb{Z} = \langle 1 \rangle$, hence a PID, so $\mathbb{Z}$ is a UFD and consequently irreducibility in $\mathbb{Z}$ means primality in $\mathbb{Z}$.  

Page 7 of 73
2.1.2 Number Theory: Primes, Legendre Symbols, and Quadratic Residue

Besides a healthy dose of algebra we will also need a basic understanding of number theory. We will not define the absolute basics but restrict us to the theory which is going to be important for this paper. For more information see ([2], Chapter 1 and Appendices 1-3)

Definition 2.17. Let $D$ be an integral domain, let $a, b \in D, a \neq 0, b \neq 0$, and finally let $d|a$ denote that an element $d \in D$ is a divisor of $a$. Then $d \in D$ is called a greatest common divisor of $a$ and $b$, abbreviated as GCD and denoted $\text{gcd}(a, b)$, if the following two conditions hold:

$$d|a \land d|b$$
$$\forall c \in D : c|a \land c|b \Rightarrow c|d$$

It is clear from the definition that $\text{gcd}(a, b) = \text{gcd}(b, a)$. It has also been shown time and time again that there is an effective, though labour intensive, way to find the greatest common divisor between two integers: Euclid’s algorithm.

Algorithm 2.18. Let $a, b \in \mathbb{N}_0$ and let $\forall i \in \mathbb{N} : q_i, r_i \in \mathbb{N}_0$, then the greatest common divisor can be found with the following algorithm:

$$a = q_0b + r_0$$
$$b = q_1r_0 + r_1$$
$$r_{i-1} = q_{i+1}r_i + ri + 1$$

where $r_i = 0$ or $0 < r_i < r_{i-1} < b$. If $0 < r_i$ repeat the sequence, if $r_i = 0$ then $\text{gcd}(a, b) = r_{i-1}$.

Since Euclid described this in ancient Greece we have come a long way in developing our theory on prime numbers. One of the developments that particularly interests us in modern cryptography is the theory of quadratic residues.

Definition 2.19. If for some $a \in \mathbb{Z}/n\mathbb{Z}$ the $\text{gcd}(a, n) = 1$ and the congruence

$$x^2 \equiv a \mod n$$

has solutions $x$, then $a$ is called the quadratic residue modulo $n$. If there are no such $x$ then $a$ is called a quadratic non-residue modulo $n$. 

Page 8 of 73
This seems of little particular interest right now, but it is in fact crucial that we understand these residues well as this congruence relation will be the basis of many prime factorization algorithms including the General Number Field Sieve. One specific mathematician that recognized their importance was Legendre, who in turn developed a specific symbol for quadratic residues modulo a prime \( p \in \mathbb{N} \) called the Legendre symbol:

**Definition 2.20.** Let \( p \in \mathbb{N} \) be prime and let \( a \in \mathbb{N} \). Then the Legendre symbol is defined as follows:

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue mod } p \\
0 & \text{if } p | a \\
-1 & \text{if } a \text{ is a quadratic non-residue mod } p
\end{cases}
\]

At first this was a definition that helped in specific cases, especially when working with small primes where we could simply list all squares, but it was Leonard Euler that found a specific rule all the quadratic residues obeyed called Euler’s Criterion:

**Theorem 2.21.** Let \( a, p \in \mathbb{N} \) such that \( p \) is an odd prime. If \( \gcd(a, p) = 1 \), then

\[
\left( \frac{a}{p} \right) = a^{\frac{p-1}{2}} \mod p
\]

This fact was only expanded upon by the “Law of Quadratic Reciprocity”, which was known to both Legendre and Euler, but was proven by Gauss:

**Theorem 2.22.** Let \( p, q \in \mathbb{N} \) be odd primes, then

\[
\left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) (-1)^{\left( \frac{p-1}{2} \right) \left( \frac{q-1}{2} \right)}
\]

The Legendre symbol was however only defined for cases where \( p \) was prime, and it was another mathematician, Carl Jacobi, who generalized the Legendre symbol with the Jacobi symbol:

**Definition 2.23.** Let \( a, n \in \mathbb{N} \) such that \( n \) is an odd integer with \( \gcd(a, n) = 1 \). Then the Jacobi symbol is defined as follows:

\[
\left[ \frac{a}{n} \right] = \prod_{i=0}^{m} \left( \frac{a}{p_i} \right)^{\alpha_i}
\]

where \( n = p_1^{\alpha_1} \ldots p_n^{\alpha_n} \) for primes \( p_i \in \mathbb{N} \).
As this is an extension of the Legendre symbol it adheres to the same rules and theorems. Another great number theorist was Leonard Euler, who made many strides in mathematics. One of his more basic, yet important, thoughts was that of Euler’s totient function. To be able to formulate this clearly we define what a semiprime is.

**Definition 2.24.** Let \( n \in \mathbb{N} \). Then \( n \) is called a semiprime if there exist \( p, q \in \mathbb{N} \) such that

\[
    n = pq
\]

and \( p, q \) are prime.

From the idea of primes and semiprimes we can define a function that counts the number of integers coprime with an integer \( n \) up to \( n \in \mathbb{N} \). This function is called the Euler totient function:

**Definition 2.25.** Let \( n \in \mathbb{N} \) then then the totient function, or Phi-function, is defined as

\[
    \phi(n) = \# \{ x \in \mathbb{N} | \text{gcd}(x, n) = 1 \}
\]

This definition is a simple one, as with small numbers we can simply count them. However with the composites we are going to work with in RSA this is going to easily run up to 100 digits or more. Then using Euclid’s Algorithm becomes a very frustrating way of finding the number of coprime factors. However there are some things that can help us:

**Theorem 2.26.** Let \( \phi(n) \) be Euler’s totient function and let \( m, n \in \mathbb{N} \) such that \( \text{gcd}(m, n) = 1 \). Then

\[
    \phi(mn) = \phi(m)\phi(n)
\]

Moreover: There are specific formulae we can use for categories of numbers.

**Theorem 2.27.** Let \( p, q \in \mathbb{N} \) be prime, let \( c \) be a semiprime such that \( c = pq \), and let \( k \in \mathbb{N} \). Then the following hold:

1. \( \phi(p) = p - 1 \)
2. \( \phi(c) = (p - 1)(q - 1) \)
3. \( \phi(p^k) = p^{k-1}(p - 1) = p^k \left(1 - \frac{1}{p}\right) \)

Here we have limited us to primes and semiprimes, but what if \( n \in \mathbb{N} \) is composite?
Theorem 2.28. Let \( n \in \mathbb{N} \) and let \( n = \prod_{i=1}^{k} p_i^{\alpha_i} \). Then

\[
\phi(n) = n \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right)
\]

This is of course very useful for us, because now we just need the prime factorization of a number to be able to compute \( \phi(n) \). In fact, Euler made a deduction that is quite effective based on Fermat’s little theorem, here stated first for convenience:

Theorem 2.29. Let \( p \) be a prime number, then for any \( a \in \mathbb{N} \) we have that

\[
a^p \equiv a \quad \text{mod} \ p
\]

Then Euler used his totient function and formulated the following theorem:

Theorem 2.30. Let \( a, n \in \mathbb{N} \) be coprime positive integers, then

\[
a^{\phi(n)} \equiv 1 \quad \text{mod} \ n
\]

Lastly we note the Chinese Remainder Theorem. An important tool for the RSA cryptosystem which we will need in the next section

Theorem 2.31. (Chinese Remainder Theorem) Let \( n = n_1 n_2 ... n_k \) such that \( n, n_i \in \mathbb{N} \) for all \( i \in \{1, 2, ..., k\} \) and such that all \( n_i \) are pairwise coprime. Now let \( a_i \in \mathbb{Z}, i \in \{1, 2, ..., k\} \). Then there exists a unique \( x \in \mathbb{Z} \) such that

\[
\forall i : x \equiv a_i \quad \text{mod} \ n_i
\]

2.2 Modern Cryptography - RSA

We will now take a small dive into what the RSA cryptosystem truly is. We do this to understand the concept that lies behind the number sieves and factorization methods that we will be analyzing in the next chapter. Note that we in the introduction already named that prime factoring being ”difficult” is the main reason for the RSA-Cryptosystem to have gained such a high confidence from the public as a cryptosystem that is considered ”safe”. However with the advancements in technology, and more importantly the mathematical advancements in factoring large primes this notion of security may well be compromised in the near future. For more information on why prime factorization is difficult, RSA safety notions, and rigorous proofs
regarding cryptography the author suggests ([9], Section III, especially chapters 8, 10, and 11).

The RSA cryptosystem was first posited in the late 70’s by Ron Rivest, Adi Shamir, and Leonard Adleman and functions by defining two large prime numbers \( p, q \in \mathbb{N} \) such that \( pq = n \). From here we choose \( d \in \mathbb{N} \) such that \( \gcd(\phi(n), d) = 1 \) where \( \phi(n) \) is Euler’s totient function on \( n \in \mathbb{N} \). We then choose \( e \in \mathbb{N} \) such that \( ed = 1 \mod \phi(n) \). The public key is then released as \((n, e)\) while the private key is \((p, q, d)\).

To encode a message, \( M \), we consider the binary version of \( M \) (padded with zeroes if needed) such that \( \gcd(M, n) = 1 \) and we compute

\[
E = M^e \mod n
\]

using the public key \((n, e)\). We have now obtained the encrypted message, \( E \), which we can send to our recipient. Once this message arrives the recipient (who has the private key) can decrypt the message using the private key \((p, q, d)\). For this we recall Euler’s formula\(^4\) and we recall that we chose \( M \) and \( n \) to be relatively prime, hence:

\[
E^d = (M^e)^d = M^{ed} = M^{1+k\phi(n)} = M \mod n
\]

and the message has been decrypted. Now all that is left to do is run it through the Chinese Remainder Theorem to find the unique message modulo \( n \), so that it can be read by the recipient of the message.

It is important to observe that the factorization is a vital component since a key step for a third party is figuring out (from the public key \((n, e)\)) what \( \phi(n) \) is without knowing \( p \) or \( q \). Hence the problem of finding \( d \) is based completely on the (well-founded) presumption that factoring \( n \) is hard. If we find a quick and efficient way to factor arbitrary integers then the security of the RSA-system is completely nullified.

\(^4\)See Theorem 2.30
Figure 1: A simplified flowchart of RSA where we are successful if $M = M^*$. 

This schematic flowchart is based on the work of Martijn Stam, lecturer at University of Bristol, who used similar flowcharts in his Cryptography A course.
3 An Introduction to Factorization Methods:

With the knowledge we have gained through the first chapters we have now come to a point where we start to consider number sieves and how they have developed over the years. Immediately a brute force method comes to mind which is called Trial Division: When you have a large integer $n$ you attempt, by trial and error to divide every prime up to and including $\sqrt{n}$ and see if a prime integer comes out.

This is a very unproductive way of producing a factorization which can be seen in the following example:

**Example 3.1.** Let $n \in \mathbb{N}$ be a 60 digit integer. To apply the Trial Division method one has to divide all primes up to a size of $10^{30}$. Now assume that 0.1% of all integers up to $10^{30}$ are prime, then we must still make $10^{27}$ divisions. Assuming a computer can make $10^{15}$ divisions per second then it would still take over $3 \cdot 10^5$ years to perform the full computation.

So the question becomes if there are methods that are more efficient than trial division that can get us factorizations of large numbers at a much quicker pace. This is of course a very leading question, because there are: We already mentioned the GNFS. We will now take a dive into how number sieves were used so that we can understand the general number field sieve just that little bit better. This chapter is heavily influenced by ([2], Chapter 5 and 6) including the idea of most examples.

3.1 Fermat’s factorization method and Legendre congruences

After Trial Division the oldest factorization method that was a significant improvement is Fermat’s factorization method. Fermat posited that if we have an odd composite number $N = xy$ and we manage to write it as $N = x^2 - y^2$ then we can use the identity $x^2 - y^2 = (x + y)(x - y)$ to immediately deduce a factorization of $N$. We will see that each odd number $N$ in fact has such a representation.

First we observe that trial division clearly has not worked, hence we are ensured that if such an $x$ and $y$ do exist, then $x > \sqrt{N}$. There is the obvious exception of $N = x^2$, but then $N = x^2 - 0^2$ hence such an $x$ and $y$ exist. Now assume that $N \neq x^2$ then we can define $m = \lfloor \sqrt{N} \rfloor + 1$ such that to find $x$ and $y$ we now have to observe $z = m^2 - N$. If this number is a square then $x = m$ and $y = \sqrt{z}$. If this is not the case we check $m + 1$, which gives
us \((m + 1)^2 - N = m^2 + 2m + 1 - N = z + 2m + 1\). If this is not a perfect square again then we simply continue calculations.

Since there is little theory it is clearest to show the workings of Fermat’s method by an example\(^5\).

**Example 3.2.** Let \(N = 13199\), then \(\sqrt{N} = 114.88\) so \(N \neq x^2\). Hence we start the algorithm:

\[
m = 115, \quad z = 115^2 - 13199 = 26
\]

26 is clearly not a square. We then continue our calculations

\[
m + 1 = 16, \quad z = 116^2 - 13199 = 257
\]

257 is also not a perfect square, hence we continue. The following are the results in table form, where we use that \(z_m = z_{m-1} + 2(m - 1) + 1\) And in

<table>
<thead>
<tr>
<th>(m)</th>
<th>(2m + 1)</th>
<th>(z)</th>
<th>(m)</th>
<th>(2m + 1)</th>
<th>(z)</th>
</tr>
</thead>
<tbody>
<tr>
<td>117</td>
<td>235</td>
<td>490</td>
<td>125</td>
<td>251</td>
<td>2426</td>
</tr>
<tr>
<td>118</td>
<td>237</td>
<td>725</td>
<td>126</td>
<td>253</td>
<td>2677</td>
</tr>
<tr>
<td>119</td>
<td>239</td>
<td>962</td>
<td>127</td>
<td>255</td>
<td>2930</td>
</tr>
<tr>
<td>120</td>
<td>241</td>
<td>1201</td>
<td>128</td>
<td>257</td>
<td>3185</td>
</tr>
<tr>
<td>121</td>
<td>243</td>
<td>1442</td>
<td>129</td>
<td>259</td>
<td>3442</td>
</tr>
<tr>
<td>122</td>
<td>245</td>
<td>1685</td>
<td>130</td>
<td>261</td>
<td>3701</td>
</tr>
<tr>
<td>123</td>
<td>247</td>
<td>1930</td>
<td>131</td>
<td>263</td>
<td>3962</td>
</tr>
<tr>
<td>124</td>
<td>249</td>
<td>2177</td>
<td>132</td>
<td>265</td>
<td>4225</td>
</tr>
</tbody>
</table>

the final line we have 4225 = 65\(^2\) hence we have the immediate factorization that \(N = 132^2 - 65^2 = (132 - 65)(132 + 65) = 67 \cdot 197\).

This is, as can be seen, a very inefficient way to find a factorization of large odd composite integers. It is however a vast improvement over trial division for larger numbers. It can be shown that the efficiency for small numbers is worse than trial division, for more on the performance of the Fermat factorization method see ([2], p.148-149). There is however a much quicker method, but this involves Legendre congruences.

Let us consider Fermat’s factorization method and observe that he was looking for two factors of \(N\) such that \(N = x^2 - y^2\). The reason for this was so

\(^5\)Example taken from [2]
we could use the identity \((x + y)(x - y)\) to find two factors. Legendre found this interesting, but wanted to make a sincere distinction between primes and composites. For this he considered a similar equation:

\[
x^2 \equiv y^2 \pmod{N}
\]

Using this congruence modulo \(N\) we observe that \(x^2 - y^2 = 0 \pmod{N} \iff x^2 - y^2 = kN\) for some \(k \in \mathbb{Z}\). However there is a distinction to be made between prime and composite numbers. It is obvious that \(x^2 = y^2 \pmod{N}\) has the solution \(y = \pm x \pmod{N}\) regardless of our choice of \(N\), and these trivial solutions are not of interest. However for composite numbers these are not the only solutions. These non-trivial solutions are what make Legendre’s observation so important:

**Theorem 3.3.** Let \(p \in \mathbb{Z}\) be an odd prime number, and let \(x, y \in \mathbb{Z}\) be two integers such that

\[
x^2 \equiv y^2 \pmod{p}
\]

then \(y = \pm x \pmod{p}\) and there are no more solutions

**Proof.** Let \(p \in \mathbb{Z}\) be a prime number, and fix an integer \(y\) such that \(y \not\equiv 0 \pmod{p}\). Then since \(p \in \mathbb{Z}\) is prime and \(\mathbb{Z}\) is an integral domain we have that there are at most two solutions to the quadratic congruence.

Now assume \(u \equiv \pm y \pmod{p}\) are solutions to the congruence relation. This assumption is validated by the above, namely that these trivial solutions always exist. Then \(u \equiv y \pmod{p}\) and \(-u \equiv y \pmod{p}\) are valid solutions for the congruence relation.

Now we show that \(u \not\equiv -u \pmod{p}\) by contradiction. Assume that \(u \equiv -u \pmod{p}\), then \(u - (-u) \equiv 0 \pmod{p}\) which means that \(2u \equiv 0 \pmod{p}\). Since \(p\) is assumed to be odd we have \(\gcd(p, 2) = 1\) then this means that \(u \equiv 0 \pmod{p}\) which is a contradiction as we assumed \(y \not\equiv 0 \pmod{p}\). Which proves that the two solutions found are in fact distinct solutions, hence there are exactly two solutions as posited.

Since we have now proven that for any prime \(p \in \mathbb{Z}\) there are two solutions we can consider the case of composite numbers. For this let \(N \in \mathbb{Z}\) be a semi-prime such that \(N = pq\) where both \(p\) and \(q\) are primes in \(\mathbb{Z}\). Then by a simple combinatorial argument we see that \(x^2 \equiv y^2 \pmod{N}\) must have four unique solutions.

**Lemma 3.4.** Let \(p, q\) be primes in \(\mathbb{Z}\) and let \(N = pq\) be a composite integer. Then the equation \(x^2 = y^2 \pmod{N}\) has four solutions.
Proof. Let \( p, q \) be primes and \( N = pq \) as above. Then we know that the equations \( u \equiv y \mod p \) and \( v \equiv y \mod q \) each have two solutions. By observing the combinations of these two solutions for each equation we arrive at four unique solutions for the equation \( x \equiv y \mod N \):

\[
\begin{cases}
  u \equiv y \mod p \\
  v \equiv y \mod q
\end{cases}
\text{ giving } x \equiv y \mod N
\]

\[
\begin{cases}
  u \equiv -y \mod p \\
  v \equiv -y \mod q
\end{cases}
\text{ giving } x \equiv -y \mod N
\]

\[
\begin{cases}
  u \equiv y \mod p \\
  v \equiv -y \mod q
\end{cases}
\text{ giving } x \equiv z \mod N
\]

\[
\begin{cases}
  u \equiv -y \mod p \\
  v \equiv y \mod q
\end{cases}
\text{ giving } x \equiv -z \mod N
\]

Hence we have exactly four solutions as posited. \( \square \)

We have now shown that a semi-prime \( N \) has two non-trivial solutions. We will now embark on an attempt to specify what the two solutions \( \pm z \) are to find a useful factorization of \( N \). Since we know that \( x^2 - y^2 = (x + y)(x - y) \equiv 0 \mod pq \) and \( p \) and \( q \) are prime elements of \( \mathbb{Z} \) we know that either \( p|(x + y) \) or \( p|(x - y) \) and \( q|(x + y) \) or \( q|(x - y) \).

Table 1: Cases for \( x^2 = y^2 \mod n \)

| \( p|x+y? \) | \( p|x-y \) | \( q|x+y \) | \( q|x-y \) | \( \gcd(x+y,n) \) | \( \gcd(x-y,n) \) | Non-trivial factors |
|---|---|---|---|---|---|---|
| Yes | Yes | Yes | Yes | \( n \) | \( n \) | p |
| Yes | Yes | Yes | No | \( n \) | p | |
| Yes | Yes | No | Yes | p | n | p |
| Yes | No | Yes | Yes | n | q | q |
| Yes | No | Yes | No | n | 1 | |
| Yes | No | No | Yes | p | q | p,q |
| No | Yes | Yes | Yes | q | n | q |
| No | Yes | Yes | No | q | p | p,q |
| No | Yes | No | Yes | 1 | | n |

Now we observe that the trivial solutions occur if \( p|(x + y) \land q|(x + y) \) or \( p|(x - y) \land q|(x - y) \), hence we can limit ourselves to the cases where \( p|(x+y) \)
and $q | (x - y)$ or vice versa. And these factors can be extracted by using Euclid’s algorithm on $(x + y)$ and $N$ and then using the found factor $r \in p, q$ to find the other factor by $s = \frac{N}{r}$.

This naturally extends to the case of composite numbers which are not semiprimes. In this case the prime factor found, $p_1$, can be used to calculate a composite factor $\frac{N}{p_1}$, afterwards repeating the process until we end up with the prime

$$q = \frac{N}{p_1 p_2 p_3 \ldots p_m}$$

which gives us the prime factorization $N = p_1 p_2 \ldots p_m q$.

Many important factorization methods rely on Legendre congruences, such as the continued fraction method, which we will be discussing in the next section, and the General Number Field Sieve. We will now however take a look at another method, first devised by Legendre but later expanded upon by Morrison and Brillhart: The continued fraction method.

### 3.2 Continued Fraction Method

To understand what the continued fraction method is we first must understand the basing building blocks of the method: the continued fractions themselves. This follows closely ([2], Appendix 8) for the theory of continued fractions and ([2], Chapter 6, p. 193-196) for Morrison-Brillhart’s method.

**Definition 3.5.** Let $a_i, b_i \in \mathbb{Z}$ for all $i \in \mathbb{N}$. Then a continued fraction is an expression of the form

$$b_0 + \frac{a_1}{b_1 + \frac{a_2}{b_2 + \frac{a_3}{\ddots}}}$$

Where the numbers $a_i$ are called the partial numerators and the numbers $b_i$ (except $b_0$) are called the partial denominators. If all partial numerators are 1 and all $b_i > 0$ then the continued fraction is said to be *regular*.

Regular continued fractions are the simplest to deal with and possess very simple and useful properties. One of these properties is that finding the continued fraction of a real number $x$ can be done algorithmically with the following algorithm:

$$b_0 = \lfloor x \rfloor, \quad x_1 = \frac{1}{x - b_0}$$

$$b_n = \lfloor x_n \rfloor, \quad x_{n+1} = \frac{1}{x_n - b_n}$$
Lemma 3.6. Let $x \in \mathbb{Q}$. Then $x$ is a rational number, if and only if $x_i$ is an integer for some $i$. In other words: $x$ is a rational number, if and only if the continued fraction terminates.

A number $x$ is irrational if it is not rational.

One might be interested to consider the reverse: If we start with a continued fraction, can we then recover the real number $x$ we started with? For this there are two options: backwards, where you intuitively go through the fractions and work your way back, and forwards, such that you start with the first fraction and then move down the line. This can be done with the algorithm below, but first a definition.

**Definition 3.7.** Let

$$\frac{A_n}{B_n} = b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \ldots}}$$

be a regular continued fraction. Then the fraction $\frac{A_s}{B_s}$ is the partial quotient for the continued fraction after $s \in \{1, 2, \ldots, n\}$ steps.

**Theorem 3.8.** Let $b_0$ be the leading integer for a regular continued fraction and let $b_i \in \mathbb{Z}^+$ for all $i$ in the continued fraction

$$\frac{A_n}{B_n} = b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \ldots}}$$

Define $A_{-1} = 1$, $A_0 = b_0$, $B_{-1} = 0$, $B_0 = 1$, then $\frac{A_n}{B_n}$ can be computed by recursion:

$$\begin{align*}
A_s &= b_s A_{s-1} + A_{s-2} \\
B_s &= b_s B_{s-1} + B_{s-2}
\end{align*}$$

**Proof.** Consider the computation of $\frac{A_n}{B_n}$ with the starting conditions as above. We will show that the computation holds by means of induction.

$s = 1$:

$$\frac{A_1}{B_1} = b_0 + \frac{1}{b_1} = \frac{b_0 b_1 + 1}{b_1} = \frac{b_1 A_0 + A_{-1}}{b_1 B_0 + B_{-1}}$$

Now assume that the recursion holds for all $s \leq n$ where $n \in \mathbb{N}$. Now we will take the induction step.

$s = n + 1$ For this consider the following:

$$\begin{align*}
\frac{A_{n+1}}{B_{n+1}} &= \frac{(b_n + \frac{1}{b_{n+1}})A_{n-1} + A_{n-2}}{(b_n + \frac{1}{b_{n+1}})B_{n-1} + B_{n-2}} = \frac{b_n A_{n-1} + A_{n-2} + \frac{A_{n-1}}{b_{n+1}}}{b_n B_{n-1} + B_{n-2} + \frac{B_{n-1}}{b_{n+1}}}
\end{align*}$$
\[
\frac{A_n + \frac{A_{n-1}}{b_{n+1}}}{B_n + \frac{B_{n-1}}{b_{n+1}}} = \frac{b_{n+1}A_n + A_{n-1}}{b_nB_n + B_{n-1}}
\]

Which is exactly of the form we desired \(\square\)

We have now found and proven a theorem that given us the integer we started with or a multiple thereof. It however becomes clear from the following theorem that we will always find the integer we started with as every partial quotient will be in its lowest terms.

**Lemma 3.9.** Let \(A_s\) and \(B_s\) be defined as above. Then

\[
A_{s-1}B_s - A_sB_{s-1} = (-1)^s
\]

This is an ingenuous application of the determinant of the matrix

\[
\begin{bmatrix}
B_s & A_s \\
B_{s-1} & A_{s-1}
\end{bmatrix}
\]

And the fact that if \(\gcd(A_sB_{s-1}, B_sA_{s-1}) = d\) then \(d|A_sB_{s-1} - B_sA_{s-1}\) proves that the partial fractions therefore are always in their lowest terms since \(|\gcd(A_sB_{s-1}, B_sA_{s-1})| = 1\).

We will now take a new step in the theory of continued fractions by asking ourselves how they can be used to find quadratic residues. For this we will first make some basic considerations about \(\sqrt{z}\) where \(z \in \mathbb{Z}\), and then specifically interest ourselves for quadratic residues.

Let \(z \in \mathbb{Z}\) be non-square such that \(\sqrt{z} \notin \mathbb{Z}\). We can then define the expansion formally (as we did before) as:

\[
x_0 = \sqrt{z}, \ b_i = \lfloor x_i \rfloor, \ x_{i+1} = \frac{1}{x_i - b_i}
\]

Since we know that \(z\) is irrational if it is non-square we can immediately conclude that this expansion is infinite. In fact it can be proven that every continued fraction of an irrational square root, \(\sqrt{N}\), is periodic.

**Theorem 3.10.** Let \(N \in \mathbb{Z}\) be a non-square integer such that \(\sqrt{N}\) is irrational, let \(P_i, Q_i \in \mathbb{Z}^+\) and define as follows

\[
x_i = \frac{Q_{i-1}}{\sqrt{N} - P_i} = \frac{\sqrt{N} + P_i}{Q_i}
\]

\[
b_i = \lfloor x_i \rfloor = \lfloor \frac{\sqrt{N} + P_i}{Q_i} \rfloor, \ P_{i+1} = b_iQ_i - P_i
\]

Then the continued fraction of \(\sqrt{N}\) is periodical.
Proof. We will show that \( P_i < \sqrt{N} \) and \( Q_i < 2\sqrt{N} \) limits the possible combinations in the pair \((P_i, Q_i)\) to at most \(2N\), and therefore must imply that there is periodicity in the sequence \(\{b_i|i \in [N]\}\). First we will prove that

\[
\frac{Q_i - 1}{\sqrt{N} - P_i} = \frac{Q_{i-1}(\sqrt{N} + P_i)}{N - P_i^2} = \frac{\sqrt{N} + P_i}{Q_i}
\]

inducing that \(Q_i = \frac{N - P_i^2}{Q_{i-1}}\) is always an integer. For this we will use induction on \(i\):

\(i = 1:\)
For \(i = 1\) we have that

\[
x_i = \frac{1}{\sqrt{N} - b_0} = \frac{\sqrt{N} + b_0}{N - b_0^2} = \frac{\sqrt{N} - P_1}{Q_1}
\]

Where \(Q_1 = N - P_1^2\). Here the desired form is achieved and since \(N, P \in \mathbb{Z}\) it is clear that \(Q_1 \in \mathbb{Z}\).

\(i = n:\)
Now assume that the theorem holds for all \(i < n\) and consider \(i = n\). Then we can assume that

\[
x_i = \frac{\sqrt{N} - P_i}{Q_i}, \text{ with } Q_i \mid N - P_i^2
\]

then

\[
x_{i-1} = b_{i-1} + \frac{\sqrt{N} - (b_{i-1} Q_{i-1} - P_{i-1})}{Q_i} = b_i + \frac{\sqrt{N} - P_i}{Q_{i-1}}
\]

\[
x_i = \frac{Q_{i-1}}{\sqrt{N} - P_i} = \frac{Q_{i-1}(\sqrt{N} - P_i^2)}{N - P_i^2}
\]

since we know that \(\frac{N - P_i^2}{Q_{i-1}}\) is an integer we can deduce that

\[
\frac{N - P_i^2}{Q_{i-1}} = \frac{N - (b_{i-1} Q_{i-1} - P_{i-1})^2}{Q_{i-1}} = \frac{N - P_i^2}{Q_{i-1}} + 2b_{i-1} P_{i-1} - b_{i-1}^2 Q_{i-1}
\]

is also an integer. Hence we have now shown that \(Q_i\) is an integer for any choice of \(i \in \mathbb{N}\).

Now we consider the periodicity. For this consider \(b_i\) and note that for every choice of \(b_i\), \(P_i < \sqrt{N}\), and since \(P_{i+1} = b_i Q_i - P_i\) we have that

\[
Q_i = \frac{P_{i+1} + P_i}{b_i} \leq 2\sqrt{N}
\]
Thus the total number of different fractions $\frac{\sqrt{N} - P}{Q_i}$ in the expansion is at most $\lfloor \sqrt{N} \rfloor \cdot \lfloor 2\sqrt{N} \rfloor < 2N$. Through combinatorial argument we can now say that after at most $2N$ steps we will find a fraction which has occurred in the expansion before, hence the expansion must be periodic with a period of at most length $2N - 1$.

Now that we know that for any non-square $N$ the continued fraction expansion of $\sqrt{N}$ is periodic we can take a look at the relation between continued fractions and quadratic residues. For this we consider the following formula:

$$A_{n-1}^2 - NB_{n-1} = (-1)^n Q_n$$

Where $\frac{A_n}{B_n}$ is the $n$'th partial quotient and $x_n$ and $Q_n$ defined as in Theorem 3.10. This equation can be shown to be valid for all $n \geq 0$. Reducing this equation modulo $N$ yields that

$$A_{n-2}^2 = (-1)^n Q_n \pmod{N}$$

which immediately yields that $(-1)^n Q_n$ is definitely a quadratic residue mod $N$. This method is used in Morrison-Brillhart’s prime factorization method.

### 3.3 Morrison-Brillhart

Morrison-Brillhart’s continued fraction method ([5],[2] 193-200) is a very efficient general factorization method and is, even in modern days, preferred over the General Number Field Sieve in situations considering relatively small prime numbers as the efficiency of this method on smaller primes is much higher than that of the GNFS. One of the most remarkable things is that this was the first method that had a sub-exponential running time, meaning that for a prime $N$ with a running time $N^\alpha$ for the factorization, then $\alpha$ would decrease as $N$ increases.

The idea behind the algorithm is to use Legendre congruences to find a non-trivial congruence for $x^2 = y^2 \pmod{N}$ and then to compute a factor $p \in \mathbb{N}$ of $N$ by applying Euclid’s algorithm on $(x + y, N)$. To increase the success of their method Morrison and Brillhart took inspiration from a technique that uses known quadratic residues to form new ones, first formulated by Maurice Kraitchik in “Theorie des Nombres” in the late 1920’s. We will now explore the algorithm to further our understanding.

Let $N \in \mathbb{N}$ be an odd, composite integer with $N > 1$. Then the algorithm can be described in three simple steps:
Algorithm 3.11. [5]

1. Expand $\sqrt{N}$, or $\sqrt{kN}$ for some suitably chosen integer $k \geq 1$, into a simple continued fraction.

$$\sqrt{kN} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \cfrac{1}{\ddots \cfrac{1}{q_n}}}}}$$

to some point $n = n_0$. For each value of $n$, $1 \leq n \leq n_0$, the identity

$$A_{n-1}^2 - kNB_{n-1}^2 = (-1)^nQ_n$$

where $A_n/B_n$ is the $n$’th convergent, implies the congruence

$$A_{n-1}^2 \equiv (-1)^nQ_n \mod N$$

We shall call this pairing $(A_{n-1}, Q_n)$ an A-Q pair. Note that we in this step assume that $n_0$ is large enough for us to attain a number of A-Q pairs that are sufficient for this method.

2. Find among the set of A-Q pairs generated in the first step certain subsets, which we will call $S$-sets, such that the signed product $\prod_i (-1)^iQ_i$ of it’s $Q_i$’s is a square. If no such set can be generated we return to the first step and expand $\sqrt{kN}$ further.

3. Each $S$-set found in the second step fives rise to the following congruence:

$$A^2 = \prod_i A_{i-1}^2 = \prod_i (-1)^iQ_i = Q^2 \mod N$$

where $1 \leq A < N$. Compute the $A$ and $Q$ of the congruence and then compute $\gcd(A - Q, N) = D$ for all $S$-sets that were produced. If $1 < D < N$ for some $S$-set the algorithm concludes and $D$ is a non-trivial factor of $N$. Else return to step 1 and expand $\sqrt{kN}$ further.

**Note:** For this to work $Q$ must not be reduced modulo $N$.

The greatest improvement, and that which we are interested in, in this method is the way the combination of quadratic residues is produced. The idea is that we limit the amount of prime factors that we allow, $p_m$, and we search each of the $Q_i$’s for prime factors that are less than $p_m$. The prime factorizations for those $Q_i$’s that are fully factored in this way are retained, meanwhile the $Q_i$’s that are not fully factored in this way are inspected further. If the co-factor of a $Q_i$ when we reached the limit of $p_m$ is larger than $p_m$ but smaller than $p_m^2$ then the cofactor must be a prime, hence we have fully factored $Q_i$. If this is not the case then the $Q_i$ is discarded.
**Definition 3.12.** The $m$ primes, $p_1, p_2, ..., p_m \in \mathbb{N}$ as described above are called the factor base. The prime cofactors of $Q_i$ are called large primes.

In the Morrison-Brillhart method most of the computing time is spent on finding these quadratic residues, especially since most of these residues will not factor completely within the factor base. For example: In the factorization of $F_7$ in [5] the 2059 factored residues were found after 1,330,000 trials. This procedure could be made much more efficient if we could devise a strategy so the trial divisions which end in failure would never be performed. This was discovered by Carl Pomerance in the form of the Quadratic Sieve, with the added benefit that those these residues that end in a full factorization within the factor base could be indicated directly.

**3.4 Quadratic Sieve**

The Quadratic Sieve (QS) was the fastest algorithm of the 1980’s and early 90’s and was developed by Carl Pomerance, and is still the most used factoring algorithm on numbers between 50 and 100 digits. In *Smooth numbers and the Quadratic Sieve* [3] by Carl Pomerance, published in 2008, the mathematician gives a gentle and definite insight in the QS and defines the algorithm very strictly.

We start once more by considering, as in Morrison-Brillhart, with a non-square composite $N \in \mathbb{N}$ of sufficient size, think as mentioned between 50 and 100 digits. We then once more consider $\sqrt{N}$, or $\sqrt{kN}$ if more applicable, and we once more try to find something similar to ”A-Q pairs”, however this time we do not use continued fractions. For this we consider the equation

$$x^2 - N = y^2$$

and we let $x \in \mathbb{N}$ run until we get a result such that $y \in \mathbb{N}$, hence $y^2$ is a perfect square. It is easy to observe that as the numbers become more complex (contain fewer small factors, for example) we need to start considering how many routines we have to run to find the perfect square $y^2$. To achieve this QS uses the term ”smooth numbers”.

**Definition 3.13.** Let $m \in \mathbb{N}$. Then $m$ is called smooth if all of its prime factors $m = p_1p_2...p_n$ are small. Specifically we call $m$ $B$-smooth if all of its prime factors are less than $B$, for $B \in \mathbb{N}$.

$$m = p_1p_2...p_n, \ p_1, p_2, ..., p_n \leq B$$
We are going to use this definition of $B$-smoothness to define our factor base. Imagine for example that there is a large prime $p$ for which $p|m$, then if $m$ is used in a square subsequence, which can be seen as the $S$-set equivalent in Morrison-Brillhart, then there must necessarily be another term $m'$ for which $p|m'$ else $p^2$ can not be part of this decomposition. If we are in luck then $p^2|m$ and we don’t need another element, but $p$ is a large prime and multiples of $p$ are distant, so the chances of finding such an $m'$ are limited.

Now we can define a ”maximum factor” cut-off, $B$, and discard every number less than $\sqrt{N}$, that is not $B$-smooth. We now introduce a very important lemma:

**Lemma 3.14.** If $m_1, m_2, ..., m_k$ are positive $B$-smooth integers, and if $k > \pi(B)$, where $\pi(x)$ is the prime-counting function for the interval $[1, x]$, then some non-empty subsequence of $(m_i)$ has a square.

**Proof.** For a $B$-smooth number $m$, look at its exponent vector $v(m)$. For this let

$$m = \Pi_{i} p_i^{v_i}$$

where $p_i$ is the $i$’th prime factor of $m$ and the exponent $v_i$ is a non-negative integer. Then $v(m) = (v_1, v_2, ..., v_{\pi(B)})$. Then a subsequence $m_{i_1}, ..., m_{i_t}$ has a product of squares if and only if $v(m_{i_1}) + ... + v(m_{i_t})$ has all even entries. Equivalently if and only if this sum of vectors is the 0-vector mod 2. Now the vectorspace $\mathbb{F}^{\pi(B)}_2$, where $\mathbb{F}_2$ is the finite field with two elements, has dimension $\pi(B)$, and we have $k > \pi(B)$ vectors. So this sequence of vectors is linearly dependent in this vector space, however a linear dependency when the field of scalars is $\mathbb{F}_2$ is the same as saying that a subsequence sum being the 0-vector.

It is this concept of smooth numbers and how well behaved they are that make the QS so much more efficient than the Morrison-Brillhart method. Let us now make a description of the full algorithm to follow to execute the QS on a specific given number $N$.

**Algorithm 3.15.** [3]

1. Choose a $B \in \mathbb{N}$ and fix a factor base $F = p_1, p_2, ..., p_{\pi(B)}$

2. Examine all the numbers $x^2 - N$ for $B$-smooth values where $x$ runs through the integers starting at $\lceil \sqrt{N} \rceil$

3. When you have more than $\pi(B)$ numbers $x$ with $x^2 - N$ $B$-smooth, then form the exponent vectors and use linear algebra to find the subsequence $x_1^2 - N, ..., x_t^2 - N$ which produces a square, say $A^2$. 

Page 25 of 73
4. From the exponent vectors of the number \(x_i^2 - N\) we can produce the prime factorization \(A\), and thus find the least non-negative residue of \(A\) modulo \(N\), call this \(a\). Moreover, find the least non-negative residue of the product \(x_1...x_t\) modulo \(N\), call this \(b\).

5. We have \(a^2 = b^2 \mod n\). If \(a \not\equiv \pm b \mod n\), then compute \(\gcd(a - b, N)\). Otherwise return to step 1, find additional smooth values of \(x^2 - N\) and repeat.

In the algorithm there are two clear questions that arise: ”How do we define \(B\)?” and ”How do we recognize a number is \(B\) smooth?”. We will take a brief look at how we recognize a smooth number when we see it, as this will help us when we consider the GNFS.

For this consider the Sieve of Eratosthenes, the earliest effective prime number sieve. In this sieve you start with a list of numbers in an interval \([2, n] \in \mathbb{N}\) and then you mark the 2 as being prime. Following this you start crossing out all multiples of 2, which in your table is every second number. Then you do the same for the next unmarked number, in this case 3, etc. etc. When you have done this for all unmarked numbers up to \(\sqrt{N}\) then you are finished and all unmarked numbers up to \(N\) are prime. In our case we are not extremely interested the numbers that are unmarked, but we are interested in the numbers that are marked repeatedly. We are looking for numbers that highly composite, for then they have many prime divisors and making this completely rigorous we can outright detect smooth numbers. Interpret making a mark as taking the number and replacing it with its quotient by the prime, \(n \rightarrow \frac{n}{p_i}\), and then sieve it by the higher powers of the primes as well, again dividing by the underlying prime. Then we get that a number is smooth if
\[
\frac{n}{p_1^{v_1} \cdots p_{\pi(B)}^{v_{\pi(B)}}} = 1
\]
Now consider expanding this to the equation \(x^2 - N\). For this we consider the equation
\[
x^2 - N = 0 \mod p
\]
where \(p\) is prime. Finding the solutions to this equation always results in one of three cases: 0, 1, or 2 solutions. If there are no solutions then there is no sieving at all. If there is 1 solution then the situation must be that \(p|n\), and the sieving is a simple exercise. In the case of 2 solutions, say \(a_1\) and \(a_2\) where \(a_i^2 - N = 0 \mod p\), then we find the multiples of the prime \(p\) in the sequence \(x \equiv a_i \mod p\), where \(i = 1, 2\) and sieve them out. You can even include higher powers of \(p\) and this would have a similar effect.
Now that we have an idea on how to recognize smooth numbers and we know what smooth numbers are we will now progress onto the main topic: The General Number Field Sieve.
4 General Number Field Sieve

To understand the General Number Field Sieve (GNFS) we will be using our understanding of the Quadratic Sieve and see the GNFS as a development upon that sieve. In the GNFS, just like in the Quadratic Sieve, we try to factor a composite number \( n \) by producing congruent squares modulo \( n \) as we have seen multiple times in Chapter 3. To do this we can assume that \( n \) is odd as if \( n \) is even, then \( n = 2^k m \) where \( k, m \in \mathbb{N} \) and \( m \) odd. We may also assume that \( n \neq p^k \) for some prime \( p \in \mathbb{N} \). As per normal we then require \( x, y \in \mathbb{Z} \) such that \( x \neq \pm y \) and

\[
x^2 \equiv y^2 \mod n
\]

As we have shown in the continued fraction method in Chapter 3 then \( (x - y, n) \) is a non-trivial factor of \( n \). We then expanded this in the Quadratic Sieve to observing the polynomial

\[
x^2 - n = y^2
\]

where we looked for smooth numbers such that each prime factor of \( y \) is smaller than a predefined \( B \in \mathbb{N} \). This way we hoped to obtain a non-trivial factor of \( n \).

In the GNFS we will attempt to expand it beyond the confines of the rings \( \mathbb{Z} \) and \( \mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z} \). For this we will want to expand the concept to the algebraic number field \( \mathbb{Q}(\alpha) \) and the ring of integers over the algebraic number field \( \mathbb{Q}(\alpha) : \mathbb{O}_{\mathbb{Q}(\alpha)} \). For this we will start by attempting to expand the ideas of smoothness and factor bases.

Our theory will build upon [4] and [8], while the direct application the GNFS is based on [6], [10], and [7]. More detail will be provided in the separate sections of this section.

4.1 Factor bases and smoothness in Algebraic Number Fields

4.1.1 Field Extensions and Algebraicity

We will begin by introducing the concept of algebraic number fields by exploring how they are defined and some of the properties that belong to them. For this we will define field extensions and algebraicity ([4], Chapter 5-6) before specifying some characteristics of field extensions.
**Definition 4.1.** Let $K, L$ be two fields, then $K$ is said to be a subfield of $L$, or equivalently $L$ is an extension of $K$, if $K \subset L$. The pair of fields fulfilling this relation is called a field extension and is denoted $L/K$.

It is common to use the following notation: $K(\alpha)$ is the smallest field extension of $K$ that contains $\alpha$, and $K[x]$ is the smallest polynomial extension of $K$. Hence elements in $K[x]$ are of the form $k_nx^n + \ldots + k_1x + k_0$ where $\forall i : k_i \in K$.

In a field extension it is also common to consider the larger field as a vector-space over the smaller field, i.e. $L$ is a $K$-vector space. It is therefore not a surprise that we can consider the degree of an extension.

**Definition 4.2.** Let $L/K$ be a field extension, then the degree of this extension is the dimension of the extension as a vector space:

$$[L : K] = \dim_K(L)$$

If $[L : K] < \infty$ then the extension is called finite, else the extension is called infinite.

There is one fundamental theorem about degrees which has to be observed:

**Theorem 4.3. (Tower Law)** - Let $K \subset L \subset M$ be fields. Then

$$[M : K] = [M : L][L : K]$$

To fully understand the next concept we are introducing, algebraicity, we need to formulate the following theorem:

**Theorem 4.4.** Let $K$ be a field, let $f(x) = a_nx^n + \ldots + a_3x^3 + a_2x^2 + a_1x + a_0$ be an irreducible polynomial of degree $n > 0$, and let $\alpha$ be the image of $x$ under $\pi : K[x] \rightarrow K[x]/(f)$ such that $\pi$ is a homomorphism, then we have that:

1. $L = K[x]/(f)$ is a field.
2. $f(\alpha) = 0$, or $\alpha$ is a root of $f$ in $L$
3. $[L : K] = n$ and $1, \alpha, \ldots, \alpha^{n-1}$ is a basis for $L/K$

**Proof.**

1. Since $K$ is a field $K[x]$ is a PID, hence since $f$ is irreducible $(f)$ must be maximal. This implies that $K[x]/(f)$ is a field.
2. Under $\pi : K[x] \to K[x]/(f)$ we have that $x \to a$ and $f(x) \to f(a)$ since $\pi$ is a homomorphism. But $\ker(\pi) = (f)$ so $f(x) \to 0$ for all $x$, so $f(\alpha) = 0$.

3. Take any element of $L = K[x]/(f)$, say $g + (f)$, where $g \in K[x]$ is some representative of the coset. Since $K$ is a field $K[x]$ is Euclidean, hence we can write

$$g = qf + r$$

with the remainder of the form $r = \sum_{i=0}^{n-1} b_i x^i$. Since we have that $\pi(f) = 0$, we have that $g + (f) = \pi(g) = \pi(r)$. This means that every element of $L$ is a $K$-linear combination of $1, \alpha, ..., \alpha^{n-1}$.

We will now show that these are linearly independent in $L$. For this suppose that $g(x)$ is a polynomial of degree $n - 1$ which fulfills that $g(\alpha) = 0$, then $g(\alpha) \in \ker(\pi) = (f)$ hence $f$ divides a polynomial of degree $\leq n - 1$. This is impossible unless $g(x) = 0$, so $c_i = 0$ for all $i$, as desired.

These field extensions can be made with arbitrary numbers, but what we will be interested in are the finite field extensions, such that $[L : K] < \infty$, and for this we need the following:

**Definition 4.5.** Let $A$ and $B$ be integral domains such that $A \subseteq B$. Then an element $\beta \in B$ is said to be integral over $A$ if it satisfies the monic polynomial equation

$$x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$$

where $a_0, a_1, ..., a_{n-1} \in A$.

Note that even with this definition every $a \in A$ is integral as $x - a \in A[x]$.

**Definition 4.6.** A complex number, $\alpha \in \mathbb{C}$, that is integral over $\mathbb{Z}$ is called an algebraic integer.

A complex number, $\alpha \in \mathbb{C}$, that is integral over $\mathbb{Q}$ is called an algebraic number.

**Theorem 4.7.** Every algebraic number is of the form $\frac{\alpha}{b}$, where $\alpha$ is an algebraic integer and $b$ is a nonzero ordinary integer.

**Proof.** Let $\alpha$ be an algebraic number. Then there exist $a_1, ..., a_{n-1} \in \mathbb{Q}$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0$$
Let $b$ be the least common multiple of the denominators of $a_0, a_1, ..., a_{n-1}$. Thus $b \in \mathbb{N}$ and $ba_i \in \mathbb{Q}$ for $i = 0, 1, 2, ..., n - 1$. Hence the polynomial equation

$$(ba)^n + (ba_{n-1})(ba)^{n-1} + \ldots + (ba_1)(ba) + (ba_0) = 0$$

shows that $ba$ is a root of a monic polynomial in $\mathbb{Z}$. This $ba$ is an algebraic integer, say $\beta$. Then $\alpha = \frac{\beta}{b}$, where $\beta$ is an algebraic number and $b \in \mathbb{Z}$.

Now that we have defined what an algebraic number is we can define when a field extension is finite. It turns out that a field extension is finite if the extending element is algebraic ([1]):

**Theorem 4.8.** Let $L/K$ be a field extension. For any $\alpha \in L$ there are two distinct possibilities:

- There exists a unique monic irreducible polynomial $f \in K[x]$ with $f(\alpha) = 0$, called the minimal polynomial of $\alpha$ over $K$ and is denoted $\text{irr}_K(\alpha)$; In this case $\alpha$ is algebraic over $K$ and it holds that $K[\alpha] = K(\alpha) \cong K[x]/(f)$ and we have that $[K(\alpha) : K] = n < \infty$. Or:

- $\alpha$ is not a root of any polynomial $f \in K[x], f \neq 0$. In this case $K[\alpha] \cong K[x], K(\alpha) \cong K(x), [K(\alpha) : K] = \infty$

Such an $\alpha$ is called transcendental over $K$.

**Proof.** The ideal $I = g \in K[x] : g(\alpha) = 0$ is the kernel of $\Psi : K[x] \to L, g \to g(\alpha)$. Note that $I \subseteq K[x]$ as $g(x) = 1$, for example, does not have anything as a root. As $K[x]$ is a PID, I must be principal, so either $I = (0)$ or $I = (f)$; where $f$ is unique up to units in $K[x]$, which can be made monic by dividing $f$ by the leading coefficient.

First suppose that $I = (0)$. Then $g(\alpha) \neq 0$ for all $g \neq 0$, so $\Psi$ is injective and $\text{im}(\Psi) = K[\alpha] \cong K[x]$. Since $\ker(\Psi) = (0)$. And therefore the field of fractions gives us $K(x) \cong K(\alpha)$

Now assume that $I = (f)$. As before $\text{im}(\Psi)$ is an integral domain, so $(f)$ is prime, and so $(f)$ is irreducible. By Theorem 4.4 we now get that

$$K[\alpha] \cong \text{im}(\Psi) \cong \frac{K[x]}{\ker \Psi} = \frac{K[x]}{f}$$

which is a field. So $K(\alpha) = K[\alpha]$ and it has degree $n = \deg(f)$ over $K$, with basis $1, \alpha, ..., \alpha^{n-1}$. \qed
Before we can start talking about algebraic number fields there is one last concept we have to grasp and that is the concept of conjugate elements:

**Definition 4.9.** Let $\alpha \in \mathbb{C}$ be algebraic over a subfield $K$ of $\mathbb{C}$. The conjugates of $\alpha$ over $K$ are the roots of the minimal polynomial of $\alpha$.

The conjugates of $\alpha$ have some interesting properties which will often have a direct relation to $\alpha$. One of these properties is the following:

**Theorem 4.10.** Let $K$ be a subfield of $\mathbb{C}$. Let $\alpha \in \mathbb{C}$ be algebraic over $K$. Then the conjugates of $\alpha$ over $K$ are distinct.

**Proof.** Suppose that $\alpha$ has two conjugates over $K$ that are the same. Then $\text{irr}_K(\alpha)$ has a root of order at least 2. Let $\beta \in \mathbb{C}$ be such a multiple root. Then

$$\text{irr}_K(\alpha) = (x - \beta)^2 r(x)$$

where $r(x) \in \mathbb{C}[x]$. Differentiating the minimal polynomial with respect to $x$ we obtain that

$$\text{irr}_K(\alpha) = (x - \beta)^2 r'(x) + 2(x - \beta)r(x)$$

This $\beta$ is a root of the derivative $\text{irr}_K(\alpha)'$ of $\text{irr}_K(\alpha)$. As $\text{irr}_K(\alpha)' \in K[x]$ we have

$$\text{irr}_K(\alpha) \in I_K(\alpha) = \langle \text{irr}_K(\alpha) \rangle$$

so that $\text{irr}_K(\alpha)|\text{irr}_K(\alpha)'$ and this $\deg(\text{irr}_K(\alpha)) \leq \deg(\text{irr}_K(\alpha)')$ which is impossible. Hence the conjugates of $\alpha$ over $K$ are distinct.

In fact: Not only are they distinct, they are algebraic integers.

**Theorem 4.11.** If $\alpha$ is an algebraic integer then its conjugates over $\mathbb{Q}$ are also algebraic integers.

**Proof.** If $\alpha$ is an algebraic integer then it is a root of a polynomial

$$h(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{Z}[x]$$

Since $h(x) \in \mathbb{Q}[x]$ and $h(\alpha) = 0$ we have that $h(x) \in \langle \text{irr}_Q(\alpha) \rangle$ so that

$$h(x) = \text{irr}_Q(\alpha)q(x)$$

for some $q(x) \in \mathbb{Q}[x]$. Let $\beta$ be a conjugate of $\alpha$ over $\mathbb{Q}$. Then $\beta$ is also a root of $\text{irr}_Q(\alpha)$. Hence $h(\beta) = 0$ and so $\beta$ is an algebraic integer. \hfill $\Box$
In fact a rather important conclusion that can be drawn from this is the following, which we will accept as a fact⁶.

**Theorem 4.12.** If $\alpha$ is an algebraic integer then

$$\text{irr}_Q(\alpha) \in \mathbb{Z}[x]$$

As a final thought exercise we consider what would happen if we find two algebraic integers $\alpha, \beta$ in a field $K$, and we attempt to extend the field extension $K(\alpha)$ with $\beta$. It turns out that this is an interesting concept but does not require much mathematical thought:

**Theorem 4.13.** Let $K$ be a subfield of $\mathbb{C}$. Let $\alpha \in \mathbb{C}$ and $\beta \in \mathbb{C}$ be algebraic over $K$. Then there exists $\gamma \in \mathbb{C}$ algebraic over $K$ such that

$$K(\alpha, \beta) = K(\gamma)$$

**Proof.** Let

$$p(x) = \text{irr}_K(\alpha), q(x) = \text{irr}_K(\beta)$$

then

$$p(x) = (x - \alpha_1)(x - \alpha_m) \in K[x]$$

where $\alpha_1, \alpha_2, ..., \alpha_m$ are the conjugates of $\alpha$ over $K$, and

$$q(x) = (x - \beta_1)(x - \beta_n)$$

where $\beta_1, \beta_2, ..., \beta_n$ are the conjugates of $\beta$ over $K$. By Theorem 4.10 we know that the $\alpha_i$ are distinct, as are the $\beta_j$. The set

$$S = \left\{ \frac{\alpha_r - \alpha_s}{\beta_t - \beta_u} | r, s = 1, ..., m; t, u = 1, ..., n; t \neq u \right\}$$

consists of a finite number of complex numbers. We choose a rational number $c$ different from all the members of $S$. With this choice the $mn$ elements

$$\alpha_i + c\beta_j$$

for $i \in \{1, 2, ..., m\}$ and $j \in \{1, 2, ..., n\}$ are all distinct. Let

$$\gamma = \alpha_1 + c\beta_1 = \alpha + c\beta$$

and let $K_1 = K(\gamma)$. We also let

$$p_1(x) = p(\gamma - cx) \in K_1[x]$$

⁶Proof can be found in [4], p. 92
so
\[ p_q(\beta) = p(\gamma - c\beta) = p(\alpha) = 0, \quad q(\beta) = 0 \]
we see that \( \beta \) is a common root of \( p_1(x) \) and \( q(x) \). Now we show that these polynomials have no other common roots. Let \( \lambda \in \mathbb{C} \) be a common root of \( p_1(x) \) and \( q(x) \) with \( \lambda \neq \beta \). As \( \lambda \) is a root of \( q(x) \) different from \( \beta \) we have \( \lambda = \beta_j \) for some \( j \in \{2, \ldots, n\} \). Then as
\[
p(\gamma - c\beta_j) = p_1(\beta_j) = 0
\]
we must have that \( \gamma - c\beta_j = \alpha_i \) for one \( i \in \{1, \ldots, \} \). Hence
\[
\alpha_k + c\beta_j = \gamma = \alpha_1 + c\beta_1
\]
so that
\[
ce = \frac{\alpha_1 - \alpha_k}{\beta_1 - \beta_j}
\]
contradicting the choice of \( c \). Now let \( h(x) = \text{irr}_{K_1}(\beta) \). Then \( h(x)|p_1(x) \) and \( h(x)|q(x) \). Since \( p_1(x) \) and \( q(x) \) have exactly one common root in \( \mathbb{C} \), we must have \( \deg(h) = 1 \). Thus \( h(x) = x + \delta \) for some \( \delta \in K_1 \). Now \( 0 = h(\beta) = \beta + \delta \) so that \( \beta = -\delta \in K_1 \). Then \( \alpha = \gamma - c\beta \in K_1 \). Hence
\[
K(\alpha, \beta) \subseteq K_1 = K(\gamma)
\]
Since \( \gamma = \alpha + c\beta \in K(\alpha, \beta) \) we have
\[
K(\gamma) \subseteq K(\alpha, \beta)
\]
Hence \( K(\alpha, \beta) = K(\gamma) \).

This leads us to the final theorem of this section:

**Theorem 4.14.** Let \( K \) be a subfield of \( \mathbb{C} \). Let \( \alpha_1, \ldots, \alpha_n \) be algebraic over \( K \). Then there exists \( \alpha \in \mathbb{C} \) algebraic over \( K \) such that
\[
K(\alpha_1, ..., \alpha_n) = K(\alpha)
\]

**Proof.** Repeated application of Theorem 4.13

4.1.2 Algebraic Number Fields

Now that we understand how algebraic field extensions behave we can finally define what an algebraic number field is, as described in ([4], Chapter 6):

**Definition 4.15.** An algebraic number field is a subfield of \( \mathbb{C} \) of the form \( \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n) \), where \( \forall i : \alpha_i \) is an algebraic number.
From the definition we can immediately extrapolate that this field is of finite dimension, since each $\alpha_i$ is an algebraic number, hence the dimension of the algebraic number field as a vectorfield over $\mathbb{Q}$ is finite.

**Theorem 4.16.** If $K$ is an algebraic number field then there exists an algebraic number $\alpha$ such that $K = \mathbb{Q}(\alpha)$. Moreover, there exists an algebraic integer $\phi$ such that $K = \mathbb{Q}(\phi)$

**Proof.** The first part of this theorem is simply a special case $K = \mathbb{Q}$ from Theorem 4.13 above. Now we show that an algebraic integer can be used instead of an algebraic number. For this let $K$ be an algebraic number field. Then it is known that $K = \mathbb{Q}(\alpha)$ where $\alpha$ is an algebraic number. From theorem 4.7 we have that $\alpha = \frac{\phi}{b}$, where $\phi$ is an algebraic integer and $b$ is a non-zero integer. Hence:

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}(\phi/b) = \mathbb{Q}(\phi)$$

We will now dive into some of the properties that will prove useful when we start to discuss the GNFS. For the GNFS we are going to have to deal with rings, so we will craft the ring of algebraic integers over a field.

**Definition 4.17.** The set of all algebraic integers that lie in the algebraic number field $K$ is denoted by $O_K$. Moreover $O_K$ is called the ring of integers of the algebraic number field $K$.

**Theorem 4.18.** Let $K$ be an algebraic number field. Then $O_K$ is an integral domain.

**Proof.** Let $\Omega$ be the set of all algebraic integers. Since $\Omega$ is an integral domain and $K$ is a field, the set of algebraic integers within $K$, which can be expressed as $O_K = \Omega \cap K$ is an integral domain.

There is one more important quality of the ring $O_K$ that it possesses: $O_K$ is integrally closed, that is $O_K$ is an integral domain for which the only elements that are integral over $O_K$ are the elements of $O_K$.

**Theorem 4.19.** If $K$ is an algebraic number field then the quotient field of $O_K$ is $K$.

**Proof.** Let $F$ denote the quotient field of $O_K$, and let $\alpha \in F$. Then $\alpha = \frac{b}{c}$, where $b, c \in O_K$ and $c \neq 0$. As $O_K \subseteq K$ we have $b, c \in K$ so that, as $K$ is a field, $\alpha \in K$. Hence $F \subseteq K$. Now let $\alpha \in K$. Since $\alpha$ is an algebraic number we have that $\alpha = \frac{b}{c}$ where $b$ is an algebraic integer and $c$ is a non-zero rational integer. Then $b = \alpha c \in K$ so $b \in O_K$. Thus $\alpha \in F$ hence $K \subseteq F$. Since we now have $F \subseteq K \subseteq F$ we can conclude that $F = K$. 

Page 35 of 73
**Theorem 4.20.** If $K$ is an algebraic number field then $O_K$ is integrally closed.

**Proof.** By Theorem 4.19 $K$ is $O_K$’s quotient field. Let $\beta \in K$ be integral over $O_K$. As $O_K$ is integral over $\mathbb{Z}$, we have that $\beta$ is integral over $\mathbb{Z}$ by the transitive property of integrity. Hence $\beta$ is an algebraic integer in $K$, which means $\beta \in O_K$, so $O_K$ is integrally closed.

We have shown in Theorem 4.16 that there exists an algebraic integer $\xi$ such that $K = \mathbb{Q}(\phi)$. Since $\phi \in K$ and $\phi \in \Omega$ we can immediately conclude that $\phi \in O_K$. We now want to show that for any ideal $I \in O_K$ we can find an $\alpha \in I$ such that $K = \mathbb{Q}(\alpha)$. We will first have to make an observation upon the minimal polynomial describing an algebraic number in general.

**Theorem 4.21.** Let $K$ be a subfield of $\mathbb{C}$. Let $\alpha \in \mathbb{C}$ be algebraic over $K$. Then $\text{irr}_K(\alpha)$ is irreducible in $K[x]$.

**Proof.** Suppose that $\text{irr}_K(\alpha)$ is reducible in $K[x]$. Then there exist non-zero polynomials $r(x) \in K[x]$ and $s(x) \in K[x]$ such that

$$\text{irr}_K(\alpha) = r(x)s(x)$$

with $r(x), s(x) \notin K[x]^*$. Hence $r(x), s(x) \notin K$ such that $\deg(r(x)) \geq 1, \deg(s(x)) \geq 1$. Thus

$$\deg(\text{irr}_K(\alpha)) = \deg(r(x)) + \deg(s(x)) > \max(\deg(r(x)), \deg(s(x)))$$

As $\alpha$ is a root of $\text{irr}_K(\alpha)$ per definition, we have that $r(\alpha)s(\alpha) = 0$, so that either $r(\alpha) = 0$ or $s(\alpha) = 0$. WLOG we assume that $r(\alpha) = 0$. Hence

$$r(x) \in \langle \text{irr}_K(\alpha) \rangle$$

so that

$$\text{irr}_K(\alpha)|r(x)$$

but then

$$\deg(\text{irr}_K(\alpha)) \leq \deg(r(x))$$

which is a contradiction. Hence $\text{irr}_K(\alpha)$ is irreducible in $K[x]$. □

Note that we have proved that $\text{irr}_K(\alpha)$ is irreducible, not that it preserves minimality (if a minimal polynomial exists). We will now observe the following preliminary theorem, which asserts that if $I \in O_K$ is a non-zero ideal then $I \cap \mathbb{Z}$ is non-empty, hence contains a non-zero integer.
**Theorem 4.22.** Let $K$ be an algebraic number field. Then every non-zero ideal in $O_K$ contains a nonzero rational integer.

**Proof.** Let $I \neq 0$ be an ideal in $O_K$. Choose $\alpha \in I$ with $\alpha \neq 0$. As $\alpha \in I \subseteq O_K$, $\alpha$ is an algebraic integer. Now let $\text{irr}_Q(\alpha) = x^n + b_1x^{n-1} + \ldots + b_n$ be the irreducible polynomial representing $\alpha$. We will now show that $b_n \neq 0$ by induction.

If $n = 1$ then $\text{irr}_Q(\alpha) - x + b_1$ such that $\alpha = b_1 - \alpha \neq 0$.

If $n \geq 2$ then $b_n \neq 0$ since $\text{irr}_Q(\alpha)$ is irreducible in $\mathbb{Q}[x]$. By Theorem 4.12 we know that $\text{irr}_Q(\alpha) \in \mathbb{Z}[x]$ as $\alpha$ is an algebraic integer. Hence $b_1, \ldots, b_n \in \mathbb{Z}$. Thus we can conclude that $b_n = -\alpha^n - b_1\alpha^{n-1} - \ldots - b_1\alpha \in I$. Hence $b_n$ is a nonzero rational integer in $I$.

Recall that a function $f$ is a monomorphism if $f$ is an injective homomorphism. Then the following holds:

**Theorem 4.23.** Let $K$ be an algebraic number field of degree $n$ over $\mathbb{Q}$. Then there are exactly $n$ distinct monomorphisms $\sigma_k : K \rightarrow \mathbb{C}$, where $k \in \{1, 2, \ldots, n\}$

**Proof.** By Theorem 4.16 there exists an algebraic number $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. Let $p(x) = \text{irr}_Q(\theta)$. Then

$$\deg(p(x)) = \deg(\text{irr}_Q(\theta)) = [\mathbb{Q}(\theta) : \mathbb{Q}] = n$$

so that $\theta$ has $n$ distinct conjugates over $\mathbb{Q}$ by Theorem 4.10, say $\theta = \theta_1, \theta_2, \ldots, \theta_n$, and

$$p(x) = (x - \theta_1)(x - \theta_2)\ldots(x - \theta_n)$$

Since every conjugate is distinct and $K$ is a vectorspace over $\mathbb{Q}$ each element of $\alpha$ of $K$ can be expressed uniquely in the form $\alpha = a_{n-1}\theta^{n-1} + \ldots + a_1\theta + a_0$, where $a_i \in \mathbb{Q}$ for $i \in \{1, 2, \ldots, n-1\}$, so, for $k = 1, 2, \ldots, n$ we can define

$$\sigma_k : K \rightarrow \mathbb{C}$$

by

$$\sigma_k(a_{n-1}\theta^{n-1} + a_1\theta + a_0) = a_{n-1}\theta_k^{n-1} + \ldots + a_1\theta_k + a_0$$

We show that $\sigma_k$ is now a field homomorphism for all $k \in \{1, 2, \ldots, n\}$. We start by showing that $\sigma_k$ is additive. Let $\alpha, \beta \in K$. Then

$$\alpha = a_{n-1}\theta^{n-1} + \ldots + a_1\theta + a_0$$

and

$$\beta = b_{n-1}\theta^{n-1} + \ldots + b_1\theta + b_0$$

Page 37 of 73
and
\[ \beta = b_{n-1} \theta^{n-1} + b_1 \theta + b_0 \]
where \( a_1, \ldots, a_{n-1}, b_1, \ldots, b_{n-1} \in \mathbb{Q} \). Hence
\[ \alpha + \beta = (a_{n-1} + b_{n-1}) \theta^{n-1} + \ldots + (a_1 + b_1) \theta + (a_0 + b_0) \]
and so
\[
\sigma_k(\alpha + \beta) = (a_{n-1} + b_{n-1}) \theta^{n-1} + \ldots + (a_1 + b_1) \theta + (a_0 + b_0)
\]
\[
= (a_{n-1} \theta^{n-1} + \ldots + a_1 \theta + a_0) + (b_{n-1} \theta^{n-1} + \ldots + b_1 \theta + b_0)
\]
\[
= \sigma_k(\alpha) + \sigma_k(\beta)
\]
Thus \( \sigma_k \) is additive. Next we show that \( \sigma_k \) is multiplicative. With the same notation we let
\[
f(x) = a_{n-1} x^{n-1} + \ldots + a_1 x + a_0
\]
\[
g(x) = b_{n-1} x^{n-1} + \ldots + b_1 x + b_0
\]
such that
\[
f(\theta) = \alpha, \ g(\theta) = \beta
\]
Dividing \( f(x)g(x) \) by some polynomial \( p(x) \in \mathbb{Q}[x] \), we obtain a quotient \( q(x) \) and remainder \( r(x) \) which both lie in \( \mathbb{Q}[x] \), such that
\[
f(x)g(x) = q(x)p(x) + r(x), \ \deg (r(x)) < \deg (p(x))
\]
Hence, as \( p(\theta) = 0 \), we have that
\[
\alpha \beta = f(\theta)g(\theta) = p(\theta)q(\theta) + r(\theta) = r(\theta)
\]
Thus as \( p(\theta_k) = 0 \), we have
\[
\sigma_k(\alpha \beta) = \sigma_k(r(x)) = r(\theta_k) = f(\theta_k)g(\theta_k) = \sigma_k(\alpha) \sigma_k(\beta)
\]
So we have that \( \sigma_k \) is multiplicative. So we have now shown that \( \sigma_k \) is a homomorphism. We now just have to show that \( \sigma_k \) is injective so that it is a monomorphism. Suppose \( \alpha = a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in K \) and \( \beta = b_{n-1} x^{n-1} + \ldots + b_1 x + b_0 \in K \) are such that \( \sigma_k(\alpha) = \sigma_k(\beta) \). Then we have that
\[
a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = b_{n-1} x^{n-1} + \ldots + b_1 x + b_0
\]
so that \( \theta_k \) is a root of the polynomial
\[
(a_{n-1} - b_{n-1} x^{n-1} + \ldots + (a_1 - b_1 x) + (a_0 - b_0)
\]
of degree < n. As the deg\(\text{irr}_Q(\theta_k)\) = deg\(p(x)\) = n, this polynomial must be the zero polynomial:

\[\forall i \in \{1, ..., n - 1\} : a_i - b_i = 0\]

So

\[\forall i \in \{1, ..., n - 1\} : a_i = b_i\]

and so \(\alpha = \beta\) proving that \(\sigma_k\) is injective. Finally, let \(\lambda : K \to \mathbb{C}\) be a monomorphism. Then

\[p(\lambda(\theta)) = \lambda(p(\theta)) = \lambda(0) = 0\]

so that

\[\lambda(\theta) = \theta_k\]

and so

\[\lambda(a_{n-1}\theta^{n-1} + a_1\theta + a_0) = a_{n-1}\theta_k^{n-1} + a_1\theta_k + a_0 = \sigma_k(a_{n-1}\theta^{n-1} + a_1\theta + a_0)\]

for all \(a_i \in \mathbb{Q}\), proving that \(\lambda = \sigma_k\) Hence \(\{\sigma_k | k = 1, 2, ..., n\}\) comprise all the monomorphisms from \(K\) to \(\mathbb{C}\). \(\square\)

When we consider an algebraic number field we know that an element \(\alpha\) has conjugates. Each of these conjugates can describe a different algebraic number field which is called a conjugate field. We will formally define a conjugate field and a property which will be prove interesting for us:

**Definition 4.24.** Let \(K\) be an algebraic number field, and let \(\alpha\) be an algebraic number such that \(K = \mathbb{Q}(\alpha)\). Let

\[\alpha = \alpha_1, \alpha_2, ..., \alpha_n\]

be the conjugates of \(\alpha\) over \(\mathbb{Q}\). Then the fields

\[\mathbb{Q}(\alpha) = K, \mathbb{Q}(\alpha_2), ..., \mathbb{Q}(\alpha_n)\]

are called the conjugate fields of \(K\).

The following theorem will be left unproven although proofs are available.\(^7\)

**Theorem 4.25.** Let \(K\) be an algebraic number field. Let \(\alpha \in K\). Then all the \(K\)-conjugates of \(\alpha\) are distinct if and only if \(K = \mathbb{Q}(\alpha)\)

\(^7\)See [4] P.121-122
In fact we can define algebraic extensions using an algebraic number in an ideal as well:

**Theorem 4.26.** Let $K$ be an algebraic number field. Let $I$ be a non-zero ideal of $O_K$. Then there exists $\gamma \in I$ such that $K = \mathbb{Q}(\gamma)$

**Proof.** By Theorem 4.15 there exists $\alpha \in O_K$ such that $K = \mathbb{Q}(\alpha)$. By Theorem 4.22 there exists $c \in \mathbb{Z} \cap I$ with $c \neq 0$. Set $\gamma = c\alpha$. As $\alpha \in O_K$ and $c \in I$ we have $\gamma \in I$. Moreover as $c \in \mathbb{Z}\{0\}$, we have $K = \mathbb{Q}(\alpha) = \mathbb{Q}(c\alpha) = \mathbb{Q}(\gamma)$, where $\gamma \in I$. \qed

There is one last consideration we have to make regarding ideals, and that is the function of prime and maximal ideals in the ring of algebraic integers $O_K$ of an Algebraic Number Field $K$. It turns out that there is no distinction between the two, which reinforces the idea that the Quadratic Sieve indeed can be expanded to the GNFS.

**Proposition 4.27.** Let $K$ be an algebraic number field, then $O_K$ is a Noetherian domain.$^8$

**Theorem 4.28.** Let $P$ be a prime ideal of the ring of integers $O_K$ of an algebraic number field $K$. Then $P$ is a maximal ideal of $O_K$

**Proof.** Suppose, for contradiction, that $P_1$ is a prime ideal of $O_K$ such that $P_1$ is not maximal. Let $S$ be the set of all proper ideals of $O_K$ that strictly contain $P_1$. As $P_1$ is not a maximal ideal $S$ is a non-empty set. Since $O_K$ is a Noetherian domain, $S$ must contain a maximal element. Hence there exists $P_2 \supset P_1$ such that

$$P_1 \subset P_2 \subset O_K$$

Since $P_2$ is maximal $P_2$ is a prime ideal. Since every non-zero ideal in $O_K$ contains a non-zero rational integer we see that $P_1 \cap \mathbb{Z} \neq 0$. Hence, $P_1 \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, but $\mathbb{Z}$ is a PID, hence $P_1 \cap \mathbb{Z} = \langle p \rangle$ for some $p \in \mathbb{Z}$, where $p$ is prime. Thus

$$\langle p \rangle = P_1 \cap \mathbb{Z} \subseteq P_2 \cap \mathbb{Z} \subseteq \mathbb{Z}$$

Now $P_2 \cap \mathbb{Z} \neq \mathbb{Z}$ as $1 \notin P_2$, so as $\langle p \rangle$ is a maximal ideal of $\mathbb{Z}$, we have that

$$P_1 \cap \mathbb{Z} = P_2 \cap \mathbb{Z} = \langle p \rangle$$

As $P_1 \subset P_2$ there exists $\alpha \in P_2$ with $\alpha \notin P_1$. Since $\alpha \in O_K$ there exists a minimal polynomial such that $f(\alpha) = 0$ with integer coefficients $a_0, \ldots, a_{k-1}$. Hence $f(\alpha) \in P_1$.

$^8$Proof can be found in [4], p. 137
Let \( l \) be the least positive integer for which there exist \( b_0, \ldots, b_{l-1} \in \mathbb{Z} \) such that
\[
g(\alpha) = \alpha^l + b_{l-1}\alpha^{l-1} + \ldots + b_1\alpha + b_0 \in P_1
\]
Now, as \( \alpha \in P_2 \), we have that
\[
g(\alpha) - b_0 = \alpha(\alpha^{l-1} + b_{l-1}\alpha^{l-2} + \ldots + b_1) \in P_2
\]
Hence, as \( P_1 \subset P_2 \) and \( P_2 \) is an ideal,
\[
b_0 \in P_2
\]
But \( b_0 \in \mathbb{Z} \), so
\[
b_0 \in P_2 \cap \mathbb{Z} = P_1 \cap \mathbb{Z}
\]
and thus \( b_0 \in P_1 \). Hence we can deduce that
\[
g(\alpha) - b_0 \in P_1
\]
Now, let \( l = 1 \). Then \( \alpha \in P_1 \) which is a contradiction the assumption that \( \alpha \notin P_1 \). Hence, \( l \geq 2 \) and
\[
g(\alpha) - b_0 = \alpha(\alpha^{l-1} + b_{l-1}\alpha^{l-2} + \ldots + b_1) \in P_1
\]
Since \( P_1 \) is a prime ideal and \( \alpha \notin P_1 \) we conclude
\[
(\alpha^{l-1} + b_{l-1}\alpha^{l-2} + \ldots + b_1) \in P_1
\]
contradicting the minimality of \( l \) since \( l - 1 \) is a positive integer as \( l \geq 2 \).

We will define the algebraic extension \( \mathbb{Q}[\alpha] \) which is an extension of \( \mathbb{Q} \subset \mathbb{C} \) hence it is an algebraic number field. By Theorem 4.16 we can assume that \( \alpha \) is an algebraic integer. We then observe that \( O_{\mathbb{Q}[\alpha]} \) is the ring of algebraic integers in \( \mathbb{Q}[\alpha] \). We will now find that \( O_{\mathbb{Q}[\alpha]} \) has some particular properties. For this we introduce the following domain.

### 4.1.3 Dedekind domains

A Dedekind domain ([4], Chapter 8) is a particular kind of domain, which is hallmarked to have certain properties which will prove to be vital as we go into depth with the GNFS Algorithm, and these are Dedekind domains, named after German mathematician Richard Dedekind (1931-1916). We will start by defining what a Dedekind domain is.
**Definition 4.29.** An integral domain $D$ that satisfied the following properties:

- $D$ is a Noetherian domain
- $D$ is integrally closed
- Each prime ideal of $D$ is a maximal ideal

is called a Dedekind Domain.

Reading this definition immediately leads us to the following theorem:

**Theorem 4.30.** Let $K$ be an algebraic number field. Let $O_K$ be the ring of integers of $K$. Then $O_K$ is a Dedekind domain.

**Proof.** Let $K$ and $O_K$ be as defined. The three properties are fulfilled by Proposition 4.27, Theorem 4.20, and Theorem 4.28 respectively. Hence $O_K$ is a Dedekind domain.

In Theorem 4.28 we proved that every prime ideal in the ring of algebraic integers $O_K$ is maximal. This is an important first step, but now that we have the concept of a Dedekind domain we can make it much stronger. We will now set out to show that every proper ideal, i.e. any ideal $I$ where $I \neq \langle 0 \rangle, I \neq \langle 1 \rangle$, is a product of prime ideals. To do this we start by showing that every such ideal contains a product of prime ideals.

**Theorem 4.31.** Let $D$ be a Dedekind domain. Then every non-zero ideal $I \in O_K$ contains a product of one or more prime ideals.

**Proof.** Let $D$ be a Dedekind domain, then by Definition 4.29 it is Noetherian. If $D$ has no non-zero ideals that do not contain a product of one or more prime ideals then we are done, so we can WLOG assume that $D$ has at least one such non-zero ideal.

Let $S$ be the set of all non-zero ideals, then by assumption $S \neq \emptyset$. Since $D$ is Noetherian it fulfills the maximal condition, so every non-empty set $S$ of ideals of $D$ contains an ideal that is not properly contained in any other ideal of the set $S$. Hence $S$ contains a non-zero ideal $A$ maximal with respect to the property of not containing a product of one or more prime ideals. Clearly $A$ itself is not a prime ideal. By Proposition 2.9, there exist ideals $B$ and $C$ such that

$$BC \subseteq A, B \nsubseteq A, C \nsubseteq A$$
Now define $B_1$ and $C_1$ of $D$ by

$$B_1 = A + B, C_1 = A + C$$

Clearly $A \subseteq B_1, A \subseteq C_1$ so that $B_1, C_1 \notin S$. Hence there exist prime ideals $P_1, \ldots, P_k$ such that

$$B_1 \supseteq P_1 \ldots P_h, C_1 \supseteq P_{h+1} \ldots P_k$$

But

$$B_1 C_1 = (A + B)(A + C) \subseteq A$$

so then $A \supseteq P_1 \ldots P_k$ which contradicts the statement that $A \subseteq S$. Hence such an $S$ does not exist, which concludes the proof.

So now we know that every non-zero ideal contains a product of one or more prime ideals, since $\mathcal{O}_K$ is a Dedekind domain if $K$ is an algebraic number field. Our next step is that we have to conceptualize the opposite of a prime ideal $P$ in a Dedekind domain. For this we introduce fractional ideals as they are defined in [4]:

**Definition 4.32.** Let $D$ be an integral domain. Let $K$ be the quotient field of $D$. A non-empty subset $A$ of $K$ such that:

1. $\alpha \in A, \beta \in A \Rightarrow \alpha\beta \in A$
2. $\alpha \in A, r \in D \Rightarrow r\alpha \in A$
3. there exists $\gamma \in D$ with $\gamma \neq 0$ such that $\gamma A \subseteq D$

is called a fractional ideal of $D$

The first two requirements are the same as we would require from any ideal $I \in D$, hence any fractional ideal of $D$ that is a subset of $D$ is an ideal of $D$. However the third requirement is what offsets the fractional ideal from the regular, integral, ideal: It means that the elements of a fractional ideal have $\gamma$ as a shared factor or "common denominator".

From this we can immediately deduce that if $A$ is an fractional ideal of $D$ with the common denominator $\gamma$ then $\gamma A$ is an integral ideal of $D$. Hence we get that

$$A = \frac{1}{\gamma} I$$

up to units.
It is important to see that if $D$ is Noetherian then each integral ideal of $D$ is finitely generated hence any fractional ideal will also be finitely generated:

$$I = \langle a_1, a_2, ..., a_k \rangle \Rightarrow A = \frac{I}{\gamma} = \langle \frac{a_1}{\gamma}, ..., \frac{a_k}{\gamma} \rangle$$

Now we will continue to show that, in a Dedekind domain, every ideal is a product of prime ideals. For this we need a definition:

**Definition 4.33.** Let $D$ be an integral domain and let $K$ be the quotient field of $D$. For each prime ideal $P$ of $D$ we define the set $\hat{P}$ by

$$\hat{P} = \{ \alpha \in K : \alpha P \subseteq D \}$$

**Lemma 4.34.** Let $D$ be an integral domain, and let $P$ be a prime ideal of $D$. Then $\hat{P}$ is a fractional ideal of $D$.

Now we will prove that every non-trivial ideal in a Dedekind Domain is the product of prime ideals, but to do this we need the following theorem which we will assume to be correct:

**Theorem 4.35.** Let $D$ be a Dedekind domain. Let $P$ be a prime ideal of $D$. Then $PP = D$.

**Theorem 4.36.** If $D$ is a Dedekind domain every non-trivial integral ideal is a product of prime ideals and this factorization is unique up to order, such that if

$$P_1P_2...P_k = Q_1Q_2...Q_l$$

where $P_i$ and $Q_j$ are prime ideals, then $k = l$ and after reordering $\forall i : P_i = Q_i$

**Proof.** This proof will come in two parts: Existence and Uniqueness. Let $D$ be a Dedekind domain such that there exists a non-trivial ideal of $D$ that is not a product of prime ideals.

**Existence:** As $D$ is a Dedekind domain, it is Noetherian, and so by the maximal principle there is a non-trivial ideal $A$ of $D$ that is maximal with respect to the property of not being a product of prime ideals. Then by Theorem 4.31 there exist prime ideals $P_1, ..., P_k$ of $D$ such that

$$P_1...P_k \subseteq A$$

Now let $k$ be the smallest positive integer for which such a product exists. If $k = 1$ then $P_1 \subseteq A \subset D$. As $P_1$ is a prime ideal it is maximal, since $D$ is

---

9Proof can be found in [4]
a Dedekind domain. This $A = P_1$. This contradicts our assumption that $A$ was not a product of prime ideals. Hence $k \geq 2$. By Theorem 4.35 we have that $P_1P_1 = D$ so that

$$\hat{P}_1 P_1 P_2 \ldots P_k = DP_2 \ldots P_k$$

Hence we have that

$$\hat{P}_1 A \supseteq \hat{P}_1 P_1 \ldots P_k = P_2 \ldots P_k$$

As a consequence of Theorem 4.35 we also have that $D \subseteq \hat{P}_1$ so that $A \subseteq \hat{P}_1 A$. If $A = PA$ then

$$A \supseteq P_2 \ldots P_k$$

which contradicts the minimality of $k$ as $k - 1 \geq 1$. Hence $A \subseteq \hat{P}_1 A$. Since $\hat{P}_1 A$ is an ideal of $D$, by the maximality property of $A$, we have

$$\hat{P}_1 A = Q_2 \ldots Q_h$$

for prime ideals $Q_2 \ldots Q_h$. Then

$$A = AD = A\hat{P}_1 P_1 = P_1 Q_2 \ldots Q_h$$

is also a product of prime ideals, which contradicts the way $A$ was chosen. Hence every ideal of $D$ is a product of prime ideals.

Uniqueness: Suppose now that factorization of ideals as products of prime ideals is not always unique. By the maximal principle we may choose $B$ to be an ideal that is maximal with respect to the property of having at least two distinct factorizations as the product of prime ideals, say,

$$B = P_1 \ldots P_k = Q_1 \ldots Q_k$$

where $P_1, \ldots, P_k, Q_1, \ldots, Q_l$ are prime ideals. Then, as

$$P_1 \ldots P_k \subseteq Q_1$$

and $Q_1$ is a prime ideal, by Proposition 2.9 we have

$$P_i \subseteq Q_1$$

for some $i \in 1, 2, \ldots, k$. Relabeling $P_1$ as $P_i$ and vice versa, we may suppose that

$$P_1 \subseteq Q_1$$

Page 45 of 73
Since $P_1$ is a prime ideal and $D$ is a Dedekind domain we know that $P_1$ is maximal, hence

$$ P_1 = Q_1 $$

Therefore

$$ B \hat{P}_1 = \hat{P}_1 P_1 P_2 ... P_k = P_2 ... P_k $$

$$ B \hat{P}_1 = B \hat{Q}_1 = \hat{Q}_1 Q_1 ... Q_h $$

If $B \hat{P}_1 = B$ then $B \hat{P}_1 P_1 = BP_1$ so $B = BP_1$. Now define the fractional ideal $B$ of $D$ by

$$ \hat{B} = \hat{P}_1 ... \hat{P}_k $$

Then

$$ B \hat{B} = P_1 ... P_k \hat{P}_1 \hat{P}_k = P_1 \hat{P}_1 ... P_k \hat{P}_k $$

So that

$$ D = B \hat{B} = B \hat{P}_1 \hat{B} = P_1 $$

which is a contradiction, as $P_1$ is a prime ideal, hence a proper ideal of $D$. This means $B \hat{P}_1 \neq B$.

As $D \subset P_1$ we have that $B \subset B \hat{P}_1$. But $B \hat{P}_1 \neq B$, so we must have that

$$ B \subset B \hat{P}_1 $$

Since $B \hat{P}_1$ is an ideal of $D$ strictly containing $B$, by the maximality of $B$, $B \hat{P}_1$ has exactly one factorization as a product of prime ideals. Thus from $BP_1 = P_2 ... P_k$ we deduce that $k - 1 = h - 1$, hence $k = h$, and after relabeling we obtain $P_i = Q_i$ for all $i \in \{2, 3, 4, 5, ..., k\}$. Hence these factorizations of $B$ in prime ideals are the same, which is a contradiction to our assumption that the factorizations were distinct.

This is a very important theorem and will be something we use extensively once we get to the algorithm of the general number field sieve. Just to clarify we state the following lemma:

**Lemma 4.37.** Let $K$ be an algebraic number field. Then every proper integral ideal of $O_k$ can be expressed uniquely up to order as a product of prime ideals.

**Proof.** This follows directly from Definition 4.29 of the Dedekind Domain and Theorem 4.36 above.

As we now have that $O_{\mathbb{Q}[\alpha]}$ is a Dedekind domain we have a fairly important property, namely that any ideal $I \in \mathbb{Z}[\alpha]$ can be factored into prime ideals $I = P_1 P_2 P_3 ... P_{\alpha}$. This property will be how we translate the role of prime numbers in the Quadratic Sieve to the General Number Field Sieve.

Page 46 of 73
The idea for this is that we will define a set $I$ of prime ideals of $\mathcal{O}_{\mathbb{Q}[\alpha]}$ to define the algebraic factor base. We do still have to find a way to relate these prime ideals in $\mathcal{O}_{\mathbb{Q}[\alpha]}$ to prime elements of $\mathbb{Z}$. This will be addressed in the next section.

4.1.4 Norms of Ideals

We now have an understanding of Dedekind domains, and in particular we have that if $K$ is an algebraic number field then $\mathcal{O}_K$ is a Dedekind domain, which means that every proper ideal of $\mathcal{O}_K$ can be decomposed into prime ideals. This might have seemed a little odd for us to invest our time in, but it turns out that prime ideals behave very nicely under the norm, as described in ([4], Chapter 9-10). To understand this we will now go in depth with the definition and properties of a norm-function and norms on ideals, specifically prime ideals.

We start by considering the norm on an element. For this recall the definition of the conjugate elements of an element, Definition 4.9, and recalling the following quantity associated with an element $\alpha \in K$, where $K$ is an algebraic number field of degree $n$. Namely:

$$\sigma_1(\alpha)\ldots\sigma_n(\alpha)$$

where

$$\sigma_k : K \to \mathbb{C}, k = 1, 2, \ldots, n$$

are the $n$ distinct monomorphisms from $K$ to $\mathbb{C}$. We now define what the norm of an element in an algebraic number field $K$ is:

**Definition 4.38.** Let $K$ be an algebraic number field of degree $n$. Let $\alpha \in K$ be an element in $K$. Let $\alpha_1 = \alpha, \alpha_2, \alpha_3, \ldots, \alpha_n$ be the $K$-conjugates of $\alpha$. Then the norm of $\alpha$ is denoted $N(\alpha)$ and is defined by

$$N(\alpha) = \alpha_1\alpha_2\ldots\alpha_n$$

From Theorem 4.12 and the definition of the $K$-conjugates, Definition 4.9, it is easy to deduce that for $\alpha \in \mathcal{O}_K$ we have that $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ are algebraic integers, hence $\text{fld}(\alpha) \in \mathbb{Z}[x]$ such that

$$N(\alpha) \in \mathbb{Z}$$

We will now show that the norm as defined above is actually multiplicative (as we expect of a norm):
Theorem 4.39. Let $K$ be an algebraic number field of degree $n$. Let $\alpha, \beta \in K$. Then

$$N(\alpha \beta) = N(\alpha)N(\beta)$$

Proof. Let $\sigma_k : K \to \mathbb{C}$ be the $n$ distinct monomorphisms from $K$ to $\mathbb{C}$. Then

$$N(\alpha \beta) = \prod_{k=1}^n \sigma_k(\alpha \beta) = \prod_{k=1}^n (\sigma_k(\alpha)\sigma_k(\beta))$$

$$= \left( \prod_{k=1}^n \sigma_k(\alpha) \right) \left( \prod_{k=1}^n \sigma_k(\beta) \right) = N(\alpha)N(\beta)$$

We will now take a closer look at some of the properties that the norm of an element submits to, starting with a simple observation on units in $O_K$:

Theorem 4.40. Let $K$ be an algebraic number field of degree $n$ and let $\alpha \in O_K$, then

$$\alpha \in (O_K)^* \iff N(\alpha) = \pm 1$$

Proof. Let $K$ be an algebraic number field, and let $\alpha \in O_K$. Then we need to prove each implication separately.

$\Rightarrow$: Assume $\alpha \in (O_K)^*$, so that $\alpha$ is a unite of $O_K$. Then there exists $\beta \in O_K$ such that $\alpha \beta = 1$. Taking norms we obtain

$$N(\alpha)N(\beta) = N(\alpha \beta) = N(1) = 1$$

As $N(\alpha) \in \mathbb{Z}$ and $N(\beta) \in \mathbb{Z}$ we deduce that $N(\alpha) = \pm 1$.

$\Leftarrow$: Let $\alpha \in O_K$ be such that $N(\alpha) = \pm 1$ Let $\sigma_k : K \to \mathbb{C}$, $(k = 1, 2, 3, \ldots, n)$ be the $n$ distinct monomorphisms from $K$ to $\mathbb{C}$ with $\sigma_1 = 1$. Then

$$\prod_{k=1}^n \sigma_k(\alpha) = N(\alpha) = \pm 1$$

Set

$$\beta = \pm \prod_{k=2}^n \sigma_k(\alpha)$$

so that

$$\alpha \beta = 1$$

As $\alpha \in O_K$, we have that for each $k = 1, 2, 3, \ldots, n$: $\sigma_k(\alpha) \in O_K$ by Theorem 4.23, so that $\beta \in O_K$. Hence $\alpha \in (O_K)^*$.  

Page 48 of 73
We now have a way of checking that an algebraic integer $\alpha$ is a unit of $O_K$. The next theorem will show a way how we can check if an algebraic integer is irreducible (hence $\alpha \neq \beta \gamma$ for $\beta, \gamma \in O_K, \beta, \gamma \notin O_K^*$), which will prove quite useful:

**Theorem 4.41.** Let $K$ be an algebraic number field. If $\alpha \in O_K$ is such that

$$N(\alpha) = \pm p$$

where $p$ is a rational prime, then $\alpha$ is irreducible.

**Proof.** Suppose that $\alpha \in O_K$ is such that $N(\alpha) = \pm p$, where $p$ is a rational prime. Clearly $\alpha \neq 0$ as $N(0) = 0$ by definition. Moreover, $\alpha \notin O_K^*$ as then $N(\alpha) = \pm 1$ by Theorem 4.40. Thus if $\alpha$ is not irreducible then there exist nonzero, nonunit elements $\beta, \gamma \in O_K$ such that

$$\alpha = \beta \gamma$$

Then by Theorem 4.39 we have that

$$\pm p = N(\alpha) = N(\beta \gamma) = N(\beta)N(\gamma)$$

As $N(\beta), N(\gamma) \in \mathbb{Z}$, and $p$ is prime we conclude that

$$N(\beta) = 1 \lor N(\gamma) = 1$$

Hence by Theorem 4.40 $\beta$ or $\gamma$ is a unit which is a contradiction. So $\alpha$ is irreducible. $\square$

We will now start our endeavour to classify the norms of ideals and for this we need a proposition which relates an ideal generated by an element to the norm of the element.

**Proposition 4.42.** Let $K$ be an algebraic number field of degree $n$. Let $O_K$ be the ring of integers of $K$. Let $\alpha \in O_K$. Then

$$N(\langle a \rangle) = |N(\alpha)|$$

Note that this means that if $\alpha$ is irreducible, then the norm of the ideal generated by $\alpha$ is a prime. This becomes increasingly handy as we now show that the norm of a product of ideals is, in fact, just the product of the norm of the ideals. You can imagine that this is an important observation, as we, for a Dedekind domain, have that each ideal can be factored into prime ideals. To do this however we first need to build up some knowledge, beginning with the following definitions:
**Definition 4.43.** Let $D$ be a Dedekind domain. Let $A$ and $B$ be nonzero ideals of $D$. We say that $A$ divides $B$, written $A|B$, if there exists an integral ideal $C$ of $D$ such that $B = AC$.

Now we consider an ideal (fractional or integral) $A$ of a Dedekind Domain $D$. Since $A$ can be uniquely factored into prime ideals we can write it as

$$A = \prod_{i=1}^{n} P_i^{a_i}$$

where $P_i^{a_i}$ are the distinct prime ideals that factorize $A$. We can use this to define the order of an ideal with respect to a prime ideal:

**Definition 4.44.** With the notation above: The order of the non-zero ideal $A$ of the Dedekind domain $D$, with respect to the prime ideal $P_i$ for $i = 1, 2, \ldots n$, is defined by

$$ord_{P_i}(A) = a_i$$

For any prime ideal $P \neq P_i$ for all $i = 1, 2, \ldots, n$ we define

$$ord_P(A) = 0$$

Using this we can now give a notion of divisibility of ideals:

**Definition 4.45.** Let $D$ be a Dedekind domain. Let $A$ and $B$ be non-zero fractional ideals of $D$. We say that $A$ divides $B$, $A|B$, if there exists an integral ideal $C$ of $D$ such that $B = AC$.

This gives rise to the following properties which are useful, which can all be proven. We however omit the proofs:

**Proposition 4.46.**

1. $A|B \iff B \subseteq A$

2. $ord_P(AB) = ord_P(A) + ord_P(B)$

3. $ord_P(A + B) = \min(ord_P(A), ord_P(B))$

Having this definition of the order of an ideal in relation to a prime ideal gives rise to the following definition in which we define the order of a non-zero element with respect to a prime ideal:

**Definition 4.47.** Let $D$ be a Dedekind domain with quotient field $K$. For $\alpha \in K, \alpha \neq 0$, we define

$$ord_P(\alpha) = ord_P(\langle \alpha \rangle)$$

for any prime ideal $P$ in $D$. 

Page 50 of 73
Finally we need the following theorem to be able to show what we set out to do: Showing that the norm of a product of ideals is in fact the product of the norm of ideals.

**Theorem 4.48.** Let $D$ be a Dedekind domain with quotient field $K$. Given any finite set of prime ideals $P_1,...,P_k$ of $D$ and a corresponding set of integers $a_1,...,a_k$ then there exists $\alpha \in K$ such that

$$ord_{P_i}(\alpha) = a_i, \; i = 1,2,...,k$$

and

$$ord_P(\alpha) \geq 0$$

for any prime ideal $P \neq P_1,...,P_k$.

We can now show the following theorem, which shows that there is a generating element for an ideal $A$ in the product of ideals $AB$.

**Theorem 4.49.** Let $D$ be a Dedekind domain. Let $A$ be a fractional or integral ideal of $D$ with $A \neq \langle 0 \rangle$ and let $B$ be an integral ideal of $D$ with $B \neq \langle 0 \rangle, \langle 1 \rangle$. Then there exists $\gamma \in A$ such that

$$A = \langle \gamma \rangle + AB$$

**Proof.** Let $P_1,...,P_n$ be the set of distinct prime ideals for which either

$$ord_{P_i}(A) \neq 0 \lor ord_{P_i}(AB) \neq 0$$

This set is nonempty as $A \neq D$. By Proposition 4.46 and Theorem 4.48 we can find an element $\gamma$ of the quotient field of $D$ such that

$$ord_{P_i}(\gamma) = ord_{P_i}(A), \; i = 1,2,...,n$$

$$ord_P(\gamma) \geq 0, \; P \neq P_i$$

Thus for all prime ideals $P$

$$ord_P(\gamma) \geq ord_P(A)$$

and so

$$\gamma \in A$$

Now for $i = 1,2,...,n$ we have

$$ord_{P_i}(\gamma + AB) = \min(ord_{P_i}(\langle \gamma \rangle), ord_{P_i}(AB))$$
\[= \min(\text{ord}_{P_i}(\gamma), \text{ord}_{P_i}(AB))\]
\[= \min(\text{ord}_{P_i}(A), \text{ord}_{P_i}(AB))\]
\[= \text{ord}_{P_i}(A)\]

as \(B\) is an integral ideal. For a prime ideal \(P \neq P_i\) for \(i = 1, 2, \ldots, n\) we have \(\text{ord}_P(A) = \text{ord}_P(AB) = 0\) such that
\[\text{ord}_P(\langle \gamma \rangle + AB) = \min(\text{ord}_P(\langle \gamma \rangle), \text{ord}_P(AB))\]
\[= \min(\text{ord}_P(\gamma), 0) = 0 = \text{ord}_P(\alpha)\]

Hence
\[\text{ord}_P(\langle \gamma \rangle + AB) = \text{ord}_P(A)\]

for all prime ideals \(P\), and so
\[A = \langle \gamma \rangle + AB\]

Now we can show the crucial theorem of this whole section:

**Theorem 4.50.** Let \(K\) be an algebraic number field. Let \(A\) and \(B\) be nonzero integral ideals in \(D = \mathcal{O}_K\). Then
\[\text{N}(AB) = \text{N}(A)\text{N}(B)\]

**Proof.** If \(A = D\) or \(B = D\) then the result is trivially true as \(\text{N}(D) = \text{card}(D/D) = 1\). Hence we may assume that \(A \neq D\) and \(B \neq D\). Let \(k = \text{N}(A)\) and \(l = \text{N}(B)\). Then by the cardinality of rings, the ring \(D/A\) has \(k\) elements, say,
\[\alpha_1 + A, \ldots, \alpha_k + A\]

Also, \(D/B\) has \(l\) elements, say
\[\beta_1 + B, \ldots, \beta_l + B\]

By Theorem 4.49 there is an element \(\gamma\) of \(A\) such that
\[A = \langle \gamma \rangle + AB\]

If \(\gamma = -\) then \(A = AB\) so that \(B = D\), which contradicts our assumption that \(B \neq D\). Hence \(\gamma \neq 0\). Let \(\delta \in D\). Then there is a unique integer \(i \in \{1, 2, \ldots, k\}\) such that
\[\delta \equiv \alpha_i \mod A\]

Page 52 of 73
Clearly, 
\[ \delta - \alpha_i \in A = \langle \gamma \rangle + AB \]
so there exists \( \sigma \in D \) and \( \tau \in AB \) such that
\[ \delta - \alpha_i = \sigma \gamma + \tau \]
Similarly, there is a unique integer \( j \in \{1, 2, ..., l\} \) such that
\[ \sigma \equiv \beta_j \mod B \]
that is,
\[ \sigma - \beta_j \in B \]
As \( \gamma \in A \) we have that
\[ \sigma - \beta_j \gamma \in AB \]
Hence we have that
\[ \delta = \alpha_i + \sigma \gamma + \tau = \alpha_i + \beta_j \gamma + (\sigma - \beta_j) \gamma + \tau \equiv \alpha_i + \beta_j \gamma \mod AB \]
This shows that the set of \( kl \) elements \( \alpha_i + \beta_j \gamma + AB \) is a complete set of representatives in \( D/AB \) for \( i \in \{1, 2, ..., k\} \) and \( j \in \{1, 2, ..., l\} \). We must still show that they are distinct. For this suppose that
\[ \alpha_i + \beta_j \gamma + AB = \alpha_p + \beta_q \gamma AB \]
Then
\[ \alpha_i + \beta_j \gamma = \alpha_p + \beta_q \gamma \mod AB \]
and this
\[ \alpha_i - \alpha_p = (\beta_q - \beta_j) \gamma \mod AB \]
But since \( \gamma \in A \) so is \( \alpha_i - \alpha_p \), Thus \( i = p \) and
\[ \beta_j \gamma = \beta_q \gamma \mod AB \]
Hence
\[ \beta_j - \beta_q) \gamma \in AB \]
Now let \( B = \prod_{i=1}^{h} P_i^{b_i} \) be the prime ideal composition of \( B \). Then
\[ ord_{P_i}(A) = ord_{P_i}(\langle \gamma \rangle + AB) \]
\[ = \min(ord_{P_i}(\langle \gamma \rangle), ord_{P_i}(AB)) \]
\[ = \min(ord_{P_i}(\gamma), ord_{P_i}(A) + ord_{P_i}(B)) \]
Page 53 of 73
and it follows that

\[ \text{ord}_{P_i}(A) = \text{ord}_{P_i}(\gamma) \]

If \( \beta_j - \beta_q \neq 0 \) then \((\beta_j - \beta_q)\gamma\) is a nonzero element of \( AB \) so that for \( i \in \{1, 2, \ldots, h\} \) we have

\[ \text{ord}_{P_i}((\beta_j - \beta_q)\gamma) \geq \text{ord}_{P_i}(AB) \]

and thus

\[ \text{ord}_{P_i}(\beta_j - \beta_q) + \text{ord}_{P_i}(\gamma) \geq \text{ord}_{P_i}(A) + \text{ord}_{P_i}(B) \]

Then we can appeal to Proposition 4.46, and we can deduce that

\[ \text{ord}_{P_i}(\beta_j - \beta_q) \geq \text{ord}_{P_i}(B), i \in \{1, 2, \ldots, h\} \]

which shows that \((\beta_j - \beta_q) \in B\) hence \( j = q \), contradicting that \( \beta_j - \beta_q \neq 0 \). This proves that \( \beta_j - \beta_q = 0 \) so that \( j = q \). Hence

\[ \{\alpha_i + \beta_j \gamma AB|i \in \{1, 2, \ldots, k\}, j \in \{1, 2, \ldots l\}\} \]

is a complete set of distinct representatives of \( D/AB \) and so

\[ N(AB) = \text{card}(D/AB) = kl = N(A)N(B) \]

An identical result can be attained for the fractional ideals of \( O_K \) where \( K \) is an algebraic number field.¶ Now that we have all these indications for norms of ideals we want to take a short detour and check some special features of the norms of prime ideals.

**Proposition 4.51.** Let \( K \) be an algebraic number field. Let \( P \) be a prime ideal of \( O_K \). Then there exists a unique rational prime \( p \) such that

\[ P \supset \langle p \rangle \]

Such a prime \( p \) for which \( P \langle p \rangle \) is called the prime lying below \( P \) as \( P \supset \langle p \rangle \). Conversely given a rational prime we can say that \( P \) is the prime ideal lying over \( p \). The importance for us is that we can define the norm of \( P \) using this number:

**Theorem 4.52.** Let \( K \) be an algebraic number field with \([K : Q] = n\). Let \( P \) be a prime ideal of \( O_K \) and let \( p \) be the rational prime below \( P \). Then

\[ N(P) = p^f \]

for some \( f \in \{1, 2, \ldots n\} \)

\[ \text{[4], Theorem 9.4.1, p. 232} \]
Proof. As $p$ lies below $P$, therefore we have $P|\langle p \rangle$. Hence $\langle p \rangle = PQ$ for some integral $Q$ of $O_K$. By Theorem 4.50 we have that

$$N(\langle p \rangle) = N(PQ) = N(P)N(Q)$$

As the $K$-conjugates of $p$ comprise $p$ repeated $n$ times by Theorem 4.25, we have

$$N(P) = p^n$$

Hence we have

$$p^n = N(P)N(Q)$$

so that

$$N(P) = p^f$$

for some $f \in \{1, 2, ..., n\}$.

There are three more properties that we want to list for prime ideals:

**Theorem 4.53.** Let $K$ be an algebraic number field with $[K : Q] = n$. Let $p$ be a rational prime. Suppose that the principal ideal $\langle p \rangle$ factors in $O_K$ in the form

$$\langle p \rangle = P_1^{\alpha_1}P_g^{\alpha_g}$$

where $P_1, ..., P_g$ are distinct prime ideals of $O_K$ and $\alpha_1, ..., \alpha_g$ are positive integers.

**Theorem 4.54.** Let $K$ be an algebraic number field. Let $I(\neq \langle 0 \rangle)$ be an ideal of $O_K$.

1. If $N(I) = p$, where $p$ is prime, then $I$ is a prime ideal.

2. $N(I) \in I$

Now we let $\mathbb{Q}[\alpha]$ be an algebraic number field and we let $O_{\mathbb{Q}[\alpha]}$ be the ring of algebraic integers of $\mathbb{Q}[\alpha]$. Then we let $P$ be a set of prime ideals of $O_{\mathbb{Q}[\alpha]}$ which will be the algebraic factor base (equivalent to the factor base in the Quadratic Sieve). We will then consider pairs of elements $(x, y)$ for which the element $x + y\alpha$ has a principal ideal $\langle x + y\alpha \rangle$. If this principal ideal completely factors into prime ideals then we will define that element as smooth. A more detailed argument can be found in ([7], 57-60). Note that $O_{\mathbb{Q}[\alpha]}$ is a Dedekind domain, so we know that any such ideal can be factored into prime ideals by Theorem 4.36. Using this we will be able to find perfect squares in $\mathbb{Q}[\alpha]$, just like we would in the Quadratic Sieve.

Now with the norm function the real benefit that the GNFS will have is
that of multiplicativity. Given any ideal \( I \) of \( \mathbb{O}_Q[\alpha] \) we can decompose it into prime ideals \( P_1, P_2, \ldots, P_k \) of \( \mathbb{O}_Q[\alpha] \) such that
\[
N(I) = N(P_1 P_2 \ldots P_k) = N(P_1)N(P_2)\ldots N(P_k)
\]
and from the norm of a prime ideal, Theorem 4.52, we can now see that
\[
N(I) = (p_1^{d_1})^{e_1}(p_2^{d_2})^{e_2}(p_k^{d_k})^{e_k}
\]
But by Theorem 4.53 we can now make the following relation
\[
|N(a)| = N(\langle a \rangle) = (p_1^{d_1})^{e_1}(p_2^{d_2})^{e_2}(p_k^{d_k})^{e_k}
\]
for any \( a \in \mathbb{O}_Q[\alpha] \). It is this observation that is the key to show when an ideal \( \langle a + b\alpha \rangle \) is smooth over the algebraic factor base.

4.2 Sieving for smooth elements

As we are interested in how we can factor a composite number, \( n \in \mathbb{N} \), into prime factors we will now be limiting ourselves to this, instead the more general theory we have had above. This is extensively discussed in ([6] p.88-92), ([4] chapter 10), and ([7] p. 10,56-60). To be able to sieve for smooth elements we need to understand the Base-M method which we will now introduce.

It is important to note that \( \mathbb{Z}[\alpha] \subseteq \mathbb{O}_Q[\alpha] \) and as we will discuss later that even if \( \mathbb{Z}[\alpha] \neq \mathbb{O}_Q[\alpha] \) that we can use \( \mathbb{Z}[\alpha] \) freely as if it is equal to \( \mathbb{O}_Q[\alpha] \). In fact we will show that any square root in \( \mathbb{O}_Q[\alpha] \) can be made to be inside \( \mathbb{Z}[\alpha] \) with a very simple trick. Hence we will from now on work with \( \mathbb{Z}[\alpha] \) instead of the much less concrete \( \mathbb{O}_Q[\alpha] \).

4.2.1 Base-M Method

The Base-M method is a very simple method originating in Number Theory. Assume for an integer \( z \in \mathbb{Z} \) that we wish to decompose it, then we know that this can be done by decomposing it into a prime factorization. There is however also a semi-additive way of doing this, and this is called the Base-M polynomial:

**Definition 4.55.** Let \( z \in \mathbb{Z} \) and let \( a_i \in \mathbb{Z} \) for any \( i \in \{1, 2, \ldots, n\} \), then the Base-M polynomial decomposition is
\[
z = a_{n-1}m^{n-1} + a_{n-2}m^{n-2} + \ldots + a_0
\]
where \( m \in \mathbb{N} \) is fixed. We call this \( m \) the base.
It is clear that such a polynomial can be made for any integer in \( \mathbb{Z} \) and that the manner in which such a number decomposes depends on the base we pick for it. What is more interesting for us is that we can define a polynomial
\[
f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0
\]
such that \( f(m) = n \) by definition from this we get that \( f(m) = 0 \mod n \). Note that we from this automatically get that \( \deg(f) > 1 \) and that for any realistic situation \( f \) will be monic. There is one last thing we need from \( f \) and that is that it is irreducible, for then it is minimal:

**Proposition 4.56.** Let \( f(x) \) be a polynomial for which \( \deg(f) > 1 \), such that for \( m, n \in \mathbb{N} : f(m) = 0 \mod n \). If \( f \) is reducible, hence \( f(x) = a(x)b(x) \) then \( a(m)|n \) or \( b(m)|n \).

**Proof.** Assume for a contradiction that \( f \) is not irreducible. Then there exist two polynomials \( a(x), b(x) \) such that
\[
f(x) = a(x)b(x)
\]
Then by the definition of \( f \) we must have that
\[
f(m) = a(m)b(m) = 0 \mod n
\]
Hence
\[
a(m)|n \lor b(m)|n
\]
By definition we have that \( f(m) = a(m)b(m) \) is the Base-M decomposition of some integer, hence \( a(m) \) and \( b(m) \) are the Base-M decompositions of some \( c, d \in \mathbb{N} \) respectively. So
\[
c|n \lor d|n
\]
which are both non-trivial as \( a(x) \) and \( b(x) \) are non-trivial factors of \( f(x) \).

Hence we now have a minimal polynomial \( f \) such that \( f(x) = a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \) such that \( f(m) = 0 \mod n \).

### 4.2.2 Homomorphism and Smooth elements

Now that we have the definition for such an irreducible polynomial in place we can start thinking on how we can relate \( \mathbb{Z}[\alpha] \) to \( \mathbb{Z}/n\mathbb{Z} \). We will do this by observing prime ideals in \( \mathbb{Z}[\alpha] \) starting with the following definition:
**Definition 4.57.** Let $K$ be an algebraic number field such that $[K : \mathbb{Q}] = n$. Let $p$ be the rational prime lying below the prime ideal $P$. Then the positive integer $f$ such that

$$N(P) = p^f$$

is called the inertial degree of $P$ in $O_K$.

We will be especially interested in prime ideals with inertial degree $f = 1$.

**Definition 4.58.** A first degree prime ideal is a prime ideal for which its inertial degree is 1.

This induces an isomorphism

$$\mathbb{Z}[\alpha]/P \cong \mathbb{Z}/p\mathbb{Z}$$

Since $[\mathbb{Z}[\alpha] : P] = p$ and every $P$ such that the index of $P$ over the field is prime is maximal $P$ is maximal in $\mathbb{Z}[\alpha]$. However we know that every maximal ideal in a PID is a prime ideal, by Theorem 2.16, and we had already noted that $\mathbb{Z}[\alpha]$ is a PID. The set of first degree primes has a very interesting property:

**Theorem 4.59.** Let $f(x)$ be a monic irreducible polynomial with coefficients in $\mathbb{Z}$. Let $\alpha$ be a root of $f(x)$. Then there is a bijective correspondence between the set of first degree prime ideals and the pairs $(p,m)$, where $p \in \mathbb{Z}$ prime and $m \in \mathbb{Z}/p\mathbb{Z}$ such that $f(m) = 0 \mod n$.

This bijective correspondence has given us a relation between $\mathbb{Z}[\alpha]$ and $\mathbb{Z}/p\mathbb{Z}$ which will be very important for us. In particular we can define a function $\phi^* : \mathbb{Z}[\alpha] \to \mathbb{Z}/p\mathbb{Z}$ which maps $\alpha$ to $m \mod p$. Moreover, the prime ideal $P$ is generated by the elements $p$ and $m - \alpha$. This function is not only unique, but we can obtain a ring-homomorphism using $\phi^*$:

**Theorem 4.60.** Let $f(x), m, n$ be defined as above, such that $f(m) = 0 \mod n$. Let $d = \deg(f)$ Then the map

$$\phi : \mathbb{Z} \times \mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$\left(x, \sum_{i=0}^{d-1} a_i \alpha^i\right) \to \left(x \mod n, \sum_{i=0}^{d-1} a_i m^i \mod n\right)$$

is a homomorphism.
Proof. Let \( \phi(x) \) be as stated, let \( x_1, x_2 \in \mathbb{Z} \) and let \( y_1, y_2 \in \mathbb{Z}[\alpha] \). For \( \phi \) to be a homomorphism it suffices to show the following three things

\[
\phi(e) = e \\
\phi((x_1, y_1)(x_2, y_2)) = \phi(x_1, y_1)\phi(x_2, y_2) \\
\phi(x_1, y_1) + (x_2, y_2)) = \phi(x_1, y_1) + \phi(x_2, y_2)
\]

where \( e \) is the neutral element. Note that in all \( \mathbb{Z}, \mathbb{Z}[\alpha], \) and \( \mathbb{Z}/n\mathbb{Z} \) the neutral element is 0. So we see if \( \phi((0,0)) = e \):

\[
\phi((0,0)) = (0 \mod n, 0 \mod n) = e
\]

Now we let \( (x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z}[\alpha], \) such that

\[
y_1 = \sum_{i=0}^{d-1} a_i \alpha^i \\
y_2 = \sum_{i=0}^{d-1} b_i \alpha^i
\]

then

\[
\phi((x_1, y_1)(x_2, y_2)) = \phi((x_1 x_2, y_1 y_2)) = (x_1 x_2 \mod n, y_1 y_2 \mod n)
\]

Since \( x_1 x_2 \mod n = (x_1 \mod n)(x_2 \mod n) \) we have that the first coordinate is easily splittable, now we check if the same is true for \( y_1 \) and \( y_2 \). Note that \( d, m, \) and \( \alpha \) are given hence

\[
\sum_{i=0}^{d-1} a_i \alpha^i \cdot b_i \alpha^i = \sum_{i=0}^{d-1} (a_i b_i) \alpha^i
\]

So the \( y \)-coordinates of the function above becomes

\[
\sum_{i=0}^{d-1} (a_i b_i) m^i \mod n = \sum_{i=0}^{d-1} a_i m^i \mod n \sum_{i=0}^{d-1} b_i m^i \mod n
\]

So indeed we have that

\[
\phi((x_1 x_2, y_1 y_2)) = \phi(x_1, y_1)\phi(x_2, y_2)
\]

An identical argument can be formulated for the +-condition, hence \( \phi \) is a homomorphism. \( \square \)
This means that we can use this homomorphism to obtain sets $S$ such that $S = \{(a, b) | a, b \in \mathbb{Z}, \gcd(a, b) = 1\}$ for which it holds that

$$\prod_{(a, b) \in S} (a - bm) = c^2$$

$$\prod_{(a, b) \in S} (a - b\alpha) = \beta^2$$

where $c \in \mathbb{Z}$ and $\beta \in \mathbb{Z}[\alpha]$. To be able to do this we will be looking for smooth elements. As we have defined before: A $B$-smooth element is a number whose prime factors are all less than $B$. Since we are working in a Dedekind domain, $\mathbb{Z}[\alpha]$, finding these smooth elements is a lot easier than in general rings. For this we take a look at an ideal $I \in \mathbb{Z}[\alpha]$. We observed that $\mathbb{Z}[\alpha]$ is a PID so we can simply say that $I = \langle \beta \rangle$. Since $\mathbb{Z}[\alpha]$ is assumed to be equivalent to a Dedekind domain we know that this ideal factors completely into prime ideals:

$$I = \prod_{i=1}^{n} P_i^{e_i}$$

Such that

$$N(I) = N\left(\prod_{i=1}^{n} P_i^{e_i}\right) = \prod_{i=1}^{n} (p_i^{d_i})^{e_i}$$

We will now seek to construct such a set $S$ that the above products hold for both $(a - bm)$ and $(a - b\alpha)$.

### 4.2.3 Finding the set of solutions, $S$:

To be able to tackle this section we let $f$, $m$, and $d = \deg(f)$, be defined as above. Let $a, b, c \in \mathbb{Z}$. To find the pair $(a, b)$ such that $(a - bm) = c^2$ we want to sieve to find elements of a set $T = \{(a, b) | a + bm \text{ smooth}, a + b\alpha \text{ smooth}\}$. When we have found the set $T$ we will use linear algebra over $\mathbb{F}_2$ to find a subset $S \subset T$. This section closely follows ([6], with additional information from [7], p.56-60).

We start this process by defining a universe $U$ such that

$$U = \{(a, b) | a, b \in \mathbb{Z}, \gcd(a, b) = 1, |a| \leq q, 0 < b < u\}$$

for some large integer $u$. The exact definition of this $u$ will depend in full on the choice of the number $n$ we attempt to factorize, as it will have to be able to contain a set $S$ such that the above products hold. To efficiently tackle
this problem we will treat the cases of \( \mathbb{Z} \) and \( \mathbb{Z}[\alpha] \) seperately.

In the case of finding a square in \( \mathbb{Z} \) the procedure is nearly standardized. Choose a factor base \( B_1 \), and by sieving we can find a subset such that

\[
T_1 = \{(a, b) \in U | a + bm \text{ is } B_1 \text{ smooth}\}
\]

The sieving proceeds as follows:

**Algorithm 4.61.**

1. For each fixed integer \( b \) with \( 0 < b \leq u \) initialize an array with the integers \( a + bm \) for \( -u \leq a \leq u \).

2. For each \( p \) prime in the array corresponding to values of \( a \) such that \( a \equiv -bm \mod p \) are retrieved one at a time.

3. Divide \( a \) such that \( a \equiv -bm \mod p \) by the highest power of \( p \) that divides it, and replace the quotient in the same array at the same location.

4. At the end of this procedure the number in the \( a \)'th location is, up to sign, the largest divisor of \( a + bm \) that is coprime to the primes in \( B_1 \).

5. Any location in the array that contains a \( \pm 1 \) at the end of the procedure corresponds to a number \( a + bm \) such that \( a + bm \) is \( B_1 \) smooth.

6. If \( \gcd(a, b) = 1 \) add the pair \((a, b)\) to \( T_1 \)

We will not spend time on exploring the functionality or efficiency of this algorithm and merely accept it as a fact that this algorithm spits out a number of pairs \((a, b)\) such that \( T_1 \neq \emptyset \). If, however, after using this algorithm no \((a, b)\) pairs have been found then one can choose to enlarge \( B_1 \) and attempt again.

Now consider the situation such that \(|T_1| > B_1 + 1\), we will accept that this is possible by letting \( B_1 \) be large enough. Then we can use linear algebra over the field \( \mathbb{F}_2 \) to find a non-empty subset \( S \) of \( T_1 \) for which

\[
\prod_{(a,b) \in S} a - bm = c^2
\]

holds. We will choose to leave this to the reader to explore as it is fairly simple and to not distract from the more theoretical approach. For more information on how to implement this linear algebra on \( \mathbb{F}_2 \) refer to ([7], p.56, p. 69-70)

Now that we have found $T_1$ we will now focus on finding $T_2$ which will be defined as follows:

$$T_2 = \{(a, b) \in U | a + b\alpha \text{ is } B_2 \text{ smooth}\}$$

where we will define $B_2$ in just a second. First we let $\mathbb{Q}[\alpha]$ be the field of fractions of $\mathbb{Z}[\alpha]$ and we let $O_{\mathbb{Q}[\alpha]}$ be the ring of algebraic integers of $\mathbb{Q}[\alpha]$. That we can do this is clear as $\mathbb{Q}[\alpha]$ is a algebraic number field as we have seen in section 5.1.1. Now from our considerations regarding norms of ideals we know that for an algebraic integer $\alpha \in O_{\mathbb{Q}[\alpha]}$ the following holds:

$$N(\alpha) = N(\langle \alpha \rangle)$$

so we can speak of the norm of an element without running into problems. To find a square in $\mathbb{Z}[\alpha]$ we take a look at the algorithm above and ponder if we can make this work for us in the algebraic situation. With the above notion of a norm we can make the immediate consideration that we can link smoothness in $\mathbb{Z}[\alpha]$ to smoothness in $\mathbb{Z}$:

**Definition 4.62.** Let $\beta$ be an arbitrary algebraic integer in $\mathbb{Z}[\alpha]$ and let $y \in \mathbb{Z}$, then we say that $\beta$ is $y$-smooth in $\mathbb{Z}[\alpha]$ if and only if $N(\beta)$ is $y$-smooth in $\mathbb{Z}$.

Now we simply define $B_2$ to be some number in $\mathbb{Z}$ and the set $T_2$ is well-defined as a set of smooth pairs. Now we can explicitly describe the algorithm for the algebraic case:

**Algorithm 4.63.**

1. For each prime $p$ let the set of zeroes $f \mod p$ be denoted by $R(p)$, such that

$$R(p) = \{r \in \{0, 1, ..., p - 1\} | f(r) = 0 \mod p\}$$

2. For any fixed integer $b$ with $0 < b \leq u$ and $b \neq 0 \mod p$, the integers $a$ with $N(a + b\alpha) \equiv 0 \mod p$ are those with $a \equiv -br \mod p$ for some $r \in R(p)$.

3. For each fixed $b$ initialize an array with the numbers $N(a + b\alpha)$ for $-u \leq a \leq u$.

4. For each prime $p \leq B_2$ that does not divide $b$ and each choice $r \in R(p)$ the positions corresponding to $a$ that are congruent to $-br \mod p$ are identified.
5. Retrieve the numbers in the theses positions and divide them by $p^e$ where $e$ is maximal, and then replace the quotient in the array.

6. When this process is finished the locations containing ±1 correspond to $B_2$-smooth values of $a + b\alpha$ with $\gcd(a, b) = 1$, hence are elements of $T_2$.

Note that if $b = 0 \mod p$ in step 2 then there are no integers $a$ with $(a, b) \in U$ and $N(a + b\alpha) \equiv 0 \mod p$.

If we were to follow the same procedure as above we would now apply linear algebra over $\mathbb{F}_2$, but here some complications arise. Note that for $a + b\alpha$ we have that

$$N(a + b\alpha) = N(\langle a + b\alpha \rangle) = p_1^{e_1} \cdots p_k^{e_k}$$

Now consider the exponents $e_i$ of the numbers $a + b\alpha$ for which $(a, b) \in T_2$. This leads to a subset $S \subset T_2$ such that only the norm of the product $\prod_{(a,b) \in S}(a + b\alpha)$ is a square in $\mathbb{Z}$. It is clear that this is a neccessary condition for $\prod_{(a,b) \in S}(a + b\alpha)$ to be a square in $\mathbb{Z}[\alpha]$ but it is in no way sufficient. To counter this problem however we can observe the pair $(p, R(p))$, where $p|N(a + b\alpha)$.

For this let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$, and let $p \in \mathbb{Z}$ be a prime and $r \in R(p)$. Then we can define the function $e_{(p,r)}(a + b\alpha)$ as follows:

$$e_{(p,r)}(a + b\alpha) = \begin{cases} \text{ord}_p(N(a + b\alpha)) & a + br \equiv 0 \mod p \\ 0 & \text{otherwise} \end{cases}$$

where $\text{ord}_p(k)$ is the number of factors $p$ in $k$. It is a trivial observation that

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

This definition leads us to consider properties of this function, but to be able to talk about them we must define the following proposition and a correlating lemma:

**Proposition 4.64.** For each prime ideal $P \in \mathbb{Z}[\alpha]$ there is a group homomorphism $\phi_P : \mathbb{Q}[\alpha]^* \to \mathbb{Z}$, such that the following hold:

1. $\phi_P(\beta) \geq 0$ for all $\beta \in \mathbb{Z}[\alpha], \beta \neq 0$.

2. if $\beta \in \mathbb{Z}[\alpha], \beta \neq 0$, then $\phi_P(\beta) > 0$ if and only if $\beta \in P$.
3. for each $\beta \in \mathbb{Q}[\alpha]^*$ one has $\phi_P(\beta) = 0$ for all but finitely many $P$, and

$$|N(\beta)| = \prod_P N(P)^{\phi_P(\beta)}$$

where $P$ ranges over the set of all prime ideals of $\mathbb{Z}[\alpha]$.

This leads to a direct lemma which will prove useful:

**Lemma 4.65.** Let $a$ and $b$ be coprime integers and let $P$ be a prime ideal of $\mathbb{Z}[\alpha]$. If $P$ is not a first degree prime then $\phi_P(a + b\alpha) = 0$. If $P$ is a first degree prime corresponding to a pair $(p, r)$ then $\phi_P(a + b\alpha) = e_{p,r}(a + b\alpha)$.

**Proof.** Let $P$ be a prime ideal of $\mathbb{Z}[\alpha]$ with $\phi_P(a + b\alpha) > 0$, and let $p$ be the prime number lying below $P$ as in Proposition 4.51. Then by Proposition 4.64 the element $a + b\alpha$ maps to 0 under the map $\mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]/P$. If $p | b$, then $b\alpha$ also maps to 0, so the same is true for $a$. Hence $p | a$, which contradicts the assumption that $\gcd(a, b) = 1$.

It follows that $b$ maps to a non-zero element of $\mathbb{Z}[\alpha]/P$. Denote by $b'$ the inverse of the image of $b$, this belongs to the prime field $\mathbb{F}_p$ of $\mathbb{Z}[\alpha]$. Since $a + b\alpha$ maps to 0 the element $\alpha$ maps to $-ab'$, which belong to $\mathbb{F}_p$. Therefore all of $\mathbb{Z}[\alpha]$ must map to $\mathbb{F}_p$, which proves that $P$ is a first degree prime ideal. This implies the first assertion: If $P$ is not a first degree prime then $\phi_P(a + b\alpha) = 0$.

If $P$ corresponds to $(p, r)$, then $r$ is determined by $a + br \equiv 0 \mod p$. This shows that $P$ is the unique prime ideal of $\mathbb{Z}[\alpha]$ containing $p$ and $a + b\alpha$. Now the last statement of the lemma follows if one compares the power of $p$ on both sides of Proposition 4.64 (3) $\square$

This leads us to a very important property of the function $e_{(p, r)}$:

**Theorem 4.66.** Let $S$ be a finite set of coprime integer pairs $(a, b)$ with the property that $\prod_{(a, b) \in S}(a + b\alpha)$ is the square of an element in $K$. Then for each prime number $p$ and each $r \in R(p)$ we have

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

**Proof.** Let $P_i$ be a first degree prime ideal of $\mathbb{Z}[\alpha]$ and let $\prod_{(a, b) \in S}(a + b\alpha) = \gamma^2$. Then by Proposition 4.64 $\phi_P : \mathbb{Q}[\alpha]^* \to \mathbb{Z}$ is a homomorphism and

$$\sum_{(a, b) \in S} e_{(p, r)}(a + b\alpha) \sum_{(a, b) \in S} \phi_P(a + b\alpha) = \phi_P \left( \prod_{(a, b) \in S}(a + b\alpha) \right)$$

Page 64 of 73
\[ = \phi_P(\gamma^2) = 2\phi_P(\gamma) = 0 \mod 2 \]

There are however still a few considerations we have to make before we can use the outcome that \( \prod_{(a,b) \in S} (a + b\alpha) \) has even exponents at all prime ideals \( P \subset \mathbb{Z}[\alpha] \) to imply that \( \prod_{(a,b) \in S} (a - b\alpha) \) is a square in \( \mathbb{Z}[\alpha] \).

### 4.3 Hunting for Perfect Squares

#### 4.3.1 Resolving obstructions: Quadratic Characters:

The obstructions we might see in this are limited to four vital considerations we have to make. To do this efficiently let \( \omega = \prod_{(a,b) \in S} (a + b\alpha) \), then the obstructions are as follows:

1. We have never shown that \( \mathbb{Z}[\alpha] = \mathbb{O}_{\mathbb{Q}[\alpha]} \), hence we do not know if \( \mathbb{Z}[\alpha] \) is a UFD as we have assumed so far. Hence we do not know if \( \omega \mathbb{O}_{\mathbb{Q}[\alpha]} \) is the square of an ideal.

2. If \( \omega \mathbb{O}_{\mathbb{Q}[\alpha]} \) is a square of some ideal \( I \), then \( I \) does not have to be a principal \( \mathbb{O}_{\mathbb{Q}[\alpha]} \)-ideal.

3. If \( \omega \mathbb{O}_{\mathbb{Q}[\alpha]} \) is the square of some principal ideal \( \gamma \mathbb{O}_{\mathbb{Q}[\alpha]} \), we only have \( \omega = \gamma^2 \) up to units of \( \mathbb{O}_{\mathbb{Q}[\alpha]} \).

4. If we do obtain \( \omega = \gamma^2 \) in \( \mathbb{O}_{\mathbb{Q}[\alpha]} \), then we may still have that \( \gamma \notin \mathbb{Z}[\alpha] \). At which point the map \( \mathbb{Z} \times \mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \) is not defined for \( \gamma \) and we do not obtain the congruence of squares we are looking for.

These are the general obstructions that need to be fixed for the general number field sieve to work. (See [6] p. 93-97, or [7] p.61-70 for an in depth analysis.) First we note that the fourth obstruction is nothing more than a formality. To show that we need a quick proposition:

**Proposition 4.67.** Suppose \( f \in \mathbb{Z}[x] \) is a monic and irreducible polynomial of degree \( d = \deg(f) > 1 \). Let \( \alpha \in \mathbb{C} \) be a root of \( f \), and let \( m \in \mathbb{Z}/n\mathbb{Z} \) be an integer for which \( f(m) \mod n \), then the mapping \( \phi : \mathbb{Z}[\theta] \to \mathbb{Z}/n\mathbb{Z} \) with \( \phi(1) = 1 \mod p \) and which sends \( \alpha \) to \( m \) is a ring epimorphism.

If

\[ \prod_{(a,b) \in S} (a + b\alpha) = \gamma^2 \]
with \( \gamma \in \mathbb{Q}[\alpha] \) then \( \gamma \in O_{\mathbb{Q}[\alpha]} \) and \( \gamma f'(\alpha) \in \mathbb{Z}[\alpha] \) by the above proposition as the condition that restricts us to \( a + b\alpha \in \mathbb{Z}[\alpha] \) is self-imposed. This can easily be extrapolated to \( a + b\alpha \in \mathbb{Q}[\alpha] \). Hence

\[
f'(\alpha)^2 \cdot \prod_{(a,b) \in S} (a + b\alpha)
\]

is the square of an element of \( \mathbb{Z}[\alpha] \). For more information on how to deduce this exactly can be found in ([7], p. 60-61).

To combat the second and third obstruction Leonard Adleman (Yes, the same Adleman as the one from RSA Cryptography) came with the idea to use quadratic characters to greatly simplify the algebra on the algebraic side, \( a + b\alpha \), by doing it over \( \mathbb{F}_2 \). In order to explain the idea behind, what is now called, "character columns" we consider a simpler situation using Legendre symbols as defined in Section 2. To do this consider \( x, y \in \mathbb{Z} \) and let \( x = y^2 \).

Then it is easily verified that \( x = y^2 \mod p \) for any \( p \in \mathbb{Z} \). By the Legendre symbol

\[
\left( \frac{x}{p} \right) = x^{\frac{p-1}{2}} = (y^2)^{\frac{p-1}{2}} = y^{p-1} = 1 \mod p
\]

by Euler’s criterion, Theorem 2.30 in section 2, for any odd prime \( p \in \mathbb{Z} \). Note that for \( p = 2 \) any number is either congruent to 0 \mod 2 or 1 \mod 2 hence a perfect square, so in fact this holds for all primes \( p \). Conversely we can argue that if

\[
\left( \frac{x}{p} \right) = -1
\]

for some \( p \in \mathbb{Z} \) prime, then \( x \) must not be a perfect square. Now if we had a method to expand Legendre characters from \( \mathbb{Z} \) to \( \mathbb{Z}[\alpha] \) then we would have mitigated much that obstruction 2 and 3 had to offer. This induces the following theorem which show how Legendre symbols give us a necessary condition for a product of elements \( a + b\alpha \) to be a square.

**Theorem 4.68.** Let \( S \) be a finite set of integer pairs \( (a,b) \) such that \( \gcd(a,b) = 1 \) with the property that

\[
\prod_{(a,b) \in S} (a + b\alpha) = \omega
\]

is the square of an element of \( K \). Moreover let \( q \) be an odd prime number and \( r \in R(q) \), such that

\[
a + br \equiv 0 \mod q \text{ for each } (a,b) \in S
\]
Then we have
\[
\prod_{(a,b) \in S} \left( \frac{a + br}{q} \right) = 1
\]

Proof. Let \( \phi : \mathbb{Z}[\alpha] \to \mathbb{Z}/q\mathbb{Z} \) be the ring homomorphism given by \( \phi(\alpha) = r \mod q \), and let \( \ker(\phi) = Q \). Then \( Q \) is the first degree prime ideal corresponding to the pair \( (q, r) \). Define the map \( \chi_Q : \mathbb{Z}[\alpha] \to \{ \pm 1 \} \) and let \( \psi_Q : \mathbb{Z}[\alpha]/Q \to \mathbb{Z}/q\mathbb{Z}\{0\} \) with the Legendre symbol \( L_Q : \mathbb{Z}/q\mathbb{Z} \to \{ \pm 1 \} \) such that \( \chi_Q = L_Q \circ \psi_Q \). Then
\[
\chi_Q(a + b\alpha) = \left( \frac{a + br}{q} \right)
\]
As we saw with Obstruction 4 above we have that
\[
f'(\alpha)^2 \cdot \prod_{(a,b) \in S} (a + b\alpha) = \delta^2
\]
for some \( \delta \in \mathbb{Z}[\alpha] \). By hypothesis the factors on the left are not in \( Q \), so we have that \( \delta \notin Q \). Now we can apply \( \chi_Q \) to the equation:
\[
\chi_Q(\delta^2) = \left( \frac{\phi(\delta^2)}{q} \right) = \left( \frac{\phi(\delta)}{q} \right)^2 = 1
\]
and similarly
\[
\chi_Q(f'(\alpha)^2) = 1
\]
But then
\[
\prod_{(a,b) \in S} \left( \frac{a + br}{q} \right) = 1
\]
which completes this proof.

We however will choose to focus on the converse to this theorem: If an element \( \beta \in \mathbb{Z}[\alpha]/\{0\} \) satisfies that \( \chi_Q(\beta) = 1 \) for all first degree primes \( Q \) with \( 2\beta \notin Q \), then \( \beta \) is in fact a square in \( \mathbb{Q}[\alpha] \). In fact this converse is so powerful it can be shown that if \( \chi_Q(\beta) = 1 \) for all first degree primes \( Q \) with \( 2\beta \notin Q \) except for finitely many exceptions, then \( \beta \) is a square in \( \mathbb{Q}[\alpha] \).

In the GNFS Algorithm we use Legendre symbols and \( e_{(p,r)} \) to produce the square we need. We will not go into details as to why this seems to work as we will need a very strong version of the Chebotarev Density Theorem, which
is far beyond the scope of this project. In essence "The Chebotarev Density Theorem is a complicated theorem in Algebraic number theory which yields an asymptotic formula for the density of prime ideals of a number field $K$ that split in a certain way in an algebraic extension $L$ of $K."^ {11} One thing that can be said is that the product $\omega = \prod_{(a,b) \in S} a + b\alpha$ corresponding to the $(a,b)$ pairs in $\mathbb{Z}$ being a perfect square in $\mathbb{Q}(\theta)$ becomes more and more likely as we increase the number of prime ideals we observe. Now let us finish with the following definition:

**Definition 4.69.** Let $P = \{P_1, \ldots, P_n\}$ be a set of first degree prime ideals in $\mathbb{Z}[\alpha]$ such that Theorem 4.59 is satisfied. Then $P$ is called the quadratic character base, and the maps $\chi_P$ are called the quadratic characters.

We now observe that in our discussion we have in fact also mitigated Ob-struction 1, as we have multiplied our prospected squares by $(f'(m)^2, f'(\alpha)^2)$ which puts the square roots in $\mathbb{Z} \times \mathbb{Z}[\alpha]$, which means that we can progress to the next point. Now that we have found the smooth elements and they are in fact a square we will see how we can in fact extract the square roots.

### 4.3.2 Extracting Square Roots

To find the square roots of the pairs of squares in $\mathbb{Z}$ and $\mathbb{Z}[\alpha]$ we will tackle each of the found squares seperately. It is quite clear that for $\mathbb{Z}$ this is quite an easy practice: If $f'(m)^2 \prod_{(a,b) \in S} a + bm$ is a square, then computing the square root is going to be quite simple as we have the prime factorization of $a + bm$ known. To reduce the size of the integers we work with we can make the problem more efficient by simply considering all arithmetic mod $n$.

In the case of $\mathbb{Z}[\alpha]$ the question will be substantially more difficult, since just because we can easily find the prime ideal factorization of

$$\prod_{(a,b) \in S} a - b\alpha$$

does not immediately mean we can find a root as some of these prime ideals may not have any generators. We could of course simply compute the root of the polynomial $x^2 - \gamma^2$ for $\gamma = f'(\alpha)^2 \prod_{(a,b) \in S} (a + b\alpha)$ in $\mathbb{Q}[\alpha]$ but this is a long and arduous task which can cost a lot of time. There are however theoretical approaches which make the finding of the square root a lot easier.

For this let $\gamma = f'(\alpha)^2 \prod_{(a,b) \in S} (a + b\alpha)$ be a square in $\mathbb{Z}[\alpha]$. From this

---

let \( q \in \mathbb{Z} \) be a prime number such that \( f \mod q \) is irreducible in the field \( \mathbb{F}_q[x] \), then it is clear that \( \mathbb{Z} \alpha/q \mathbb{Z}[\alpha] \) is isomorphic to the field \( \mathbb{F}_q[x]/f \mod q \). This leads us to the following theorem:

**Theorem 4.70.** Let \( I = q \mathbb{Z}[\alpha] \) be an ideal of \( \mathbb{Z}[\alpha]/q \mathbb{Z}[\alpha] \). Then there exists a \( \delta \) such that \( \delta^2 \gamma \equiv 1 \mod I \).

**Proof.** Since \( \mathbb{Z} \alpha/q \mathbb{Z}[\alpha] \) is isomorphic to the field \( \mathbb{F}_q[x]/f \mod q \) we know that it has cardinality \( q^d \) where \( d = \deg(f) \). Hence the ideal \( I = q \mathbb{Z}[\alpha] \), consisting wholly of elements of the form \( \sum_{i=1}^{d-1} a_i \alpha_i \) such that \( q | a_i \) for all \( i \in \{1, \ldots, d-1\} \), is a prime in \( \mathbb{Z}[\alpha] \) of degree \( d \). From the irreducibility of \( f \mod q \) it follows that \( f'(\alpha) \notin I \), and for each \((a, b) \in S\) we have that \( a + b \alpha \notin I \) since \( \gcd(a, b) = 1 \). Therefore the product \( \gamma \) of all these elements does not lie in \( I \) either:

\[
\gamma \notin I
\]

Taking the coefficients of \( \gamma \mod q \), and applying a square root algorithm on polynomials \(^{12}\) we find an element \( \delta \pmod{I} \) such that \( \delta^2 \gamma \equiv 1 \mod I \)

Note that this means that \( \delta \) is the inverse of a square modulo \( I \). We will now apply Newton-Rhapson’s method ([7],[10]) of finding approximations to the root of a polynomial to find \( \delta_1, \delta_2, \ldots \) such that

\[
\delta_j \equiv \delta_{j-1}(3 - \delta_{j-1}^2 \gamma) \mod (q \mathbb{Z}[\alpha])^2
\]

Continuing the Newton-Rhapson iteration we will eventually find a \( \beta \) such that

\[
\beta \equiv \delta \gamma \mod (q \mathbb{Z}[\alpha])^2
\]

such that \( \beta \) is a true square root of \( \gamma \) in \( \mathbb{Z}[\alpha] \).

Now there is only one assumption which we still have to validate for this whole technique to work. Earlier in this section we assumed that there exists an odd prime number \( q \) such that \( f \mod q \) is irreducible. This is something that is not always possible, but this claim can be validated. For this we need to show that the Galois group of \( f \) is a full symmetric \( S_d \) group of order \( d! \), which goes beyond the scope of this project hence we will accept that this can be done.

---

\(^{12}\)Berlekamp’s Algorithm, [10], Algorithm 4.1
4.4 Statement of the Algorithm

Now with everything in place we can finally state the Algorithm as it is presented:\(^{13}\)

**Algorithm 4.71.** Let \( n \) be the composite number we wish to factor.

1. Choose \( m \in \mathbb{Z} \) and find a corresponding polynomial \( f(z) = a_n z^n + ... + a_1 z + a_0 \) such that \( f(m) \equiv 0 \mod n \) using the Base-M expansion method.

2. Define a rational factor base \( \mathbb{B} \) such that \( |\mathbb{B}| = k \) for some \( k \in \mathbb{N} \), and such that \( \forall x \in \mathbb{B}, x \) is prime.

3. Define an algebraic factor base \( \mathbb{A} \) such that \( |\mathbb{A}| = l \) for some \( l \in \mathbb{N} \), and such that \( \forall (r, p) \in \mathbb{A}, p \) is prime and \( f(r) \equiv 0 \mod p \).

4. Define a quadratic character base \( \mathbb{P} \) such that \( |\mathbb{P}| = t \) for some \( t \in \mathbb{N} \), and such that \( \forall (s, q) \in \mathbb{P}, q \) is prime and \( f(s) \equiv 0 \mod q \). Noting that \( \forall (s, q) \in \mathbb{P}, (s, q) \) may not be an element in \( \mathbb{A} \).

5. Use the sieving techniques discussed to find sufficient \((a, b)\) pairs such that \( a + bm \) is smooth in \( \mathbb{B} \) and \( a + b\theta \) is smooth in \( \mathbb{A} \) and record the divisors \( q_i \in \mathbb{B} \) and \((r_i, p_i)\mathbb{A}\) for each \((a, b)\) pair.

6. Use Linear Algebra on \( \mathbb{F}_2 \) to find a set find a set \( S \) such that for \((a, b) \in S:\)

\[ \prod_{(a, b) \in S} a - b\alpha, \prod_{(a, b) \in S} a - bm \]

are perfect squares in \( \mathbb{Z}[\alpha] \) and \( \mathbb{Z} \) respectively.

7. Use Newton-Rhapson iteration to find \( \zeta \) such that \( \zeta \) is a true square root of \( f'(\alpha)^2 \prod_{(a, b) \in S} a - ba \) in \( \mathbb{Z}[\alpha] \).

8. Use the prime factorization of \( z^2 = f'(m)^2 \prod_{(a, b) \in S} a - bm \) to find the square root \( z \).

9. Compute \( \gcd(z - \zeta, n) \). If this is non-trivial, then output the result. Else conclude failure and return to step (2) and repeat.

---

\(^{13}\)This is an adaptation of ([7], p. 80) so it fits with the progression we made through the GNFS.
5 Conclusion

With the intricacy of the internet and the encryption that is required to keep our information safe the research that goes into factorizing primes has taken the spotlight where it once was only considered a puzzle to solve.

In this the General Number Field Sieve is a very complex but effective method with the ability to factor primes over 100 digits long and with an conjectured running time of

\[
\exp(((64/3)^{1/3} + o(1))(\log(n))^{2/3}(\log(\log(n)))^{2/3})
\]

it is still considerably faster than the in [3] conjectured running time of the quadratic sieve for large enough \( n \):

\[
\exp((1 + o(1))\sqrt{\log(\log(n))})
\]

while elliptic curves have a similar running time.

Finally, despite the considerable background in algebra and number theory that is required to fully understand this method, the author hopes to have given a sincere indication to the reader about the existence and workings of the General Number Field Sieve, and perhaps even awoken some interest in further research in, if not this specific sieve, prime factorization as a whole.

\[14[6], \text{Section 2}\]
Acknowledgements

Despite it being highly unusual for a project I want to thank my partner, Sarah Wyard, for all her support. This is the project that signifies the end of my Bachelor in Mathematics so I found the location and timing appropriate. Not only was she there to support me mentally and linguistically during the project, but she was there throughout my education to ensure that I had the mental and physical capacity to push on, even if I lost the drive.

Barry van Leeuwen,
University of Bristol, February 1, 2019
References


