The Number Field Sieve

Ronan Bottoms, Maria Gringauze, Zongze Li

June 2023

Contents

1 A Brief History of the Number Field Sieve

1.1 Before the Number Field Sieve

Prior to the invention of the RSA public key cryptosystem in the late 1970s, the problem of factoring large numbers was quite largely ignored. In 1970, it was still almost impossible to factor some 20 digit numbers. It was around the time that RSA was introduced that Richard Schroeppel came up with a method which became known as the linear sieve. Creator of the quadratic sieve Carl Pomerance gives credit to this method as "the forerunner of the quadratic sieve and also its inspiration" (Pomerance 1996). It was in 1981 that Pomerance used the sieve of Eratosthenes, as well as the linear sieve, to create the quadratic sieve. After some testing and convincing, this algorithm turned out to be extremely useful and competitive in the sense that it allowed numbers to be factored that were twice the length of those that previous leading factorization algorithms could factor.

1.2 Emergence of the Number Field Sieve

A few years later in 1988, John Pollard had the idea to factor certain large numbers using algebraic number fields. He took his inspiration from Don Coppersmith, Andrew Odlyzko, and Richard Schroeppel's discrete logarithm algorithm, which utilized quadratic number fields. In 1990, Hendrick and Arjen Lenstra and Mark Manasse used this new algorithm, after some improvements by Hendrick Lentsra, to factor the ninth fermat number $2^{2^9} + 1$. It was "this sensational achievement [that] announced to the world that Pollard's number field sieve had arrived."(Pomerance 1996). By 1990, Joe Buhler, Hendrik Lenstra, and Carl Pomerance finalized the algorithm by addressing any remaining concerns or difficulties, and published a description of it named "The development of the number field sieve". In 1996, the number field sieve finished the factorization of a 130-digit RSA challenge number, beating the 129-digit record that the quadratic sieve had set in 1994. To this day, the number field sieve is the most efficient algorithm we have for factoring integers larger than 10^{100}.

2 Motivation

The motivations behind the Number Field Sieve are similar, if not identical to, the motivations of most modern factorization algorithms including notably the Quadratic Sieve. The crux of the algorithm relies on finding *perfect squares*.

Lemma 2.1. *Let x, y be such that $x \neq \pm y \pmod n$ and $x^2 \equiv y^2 \pmod n$. Then $(x-y), (x+y)$ are divisors of a non-trivial multiple of n.*

Proof. $x^2 \equiv y^2 \pmod n \implies x^2 - y^2 \equiv 0 \pmod n$. By the Difference of Squares identity, $x^2 - y^2 = (x-y)(x+y) \equiv 0 \pmod n$. Then since $x \neq \pm y \pmod n$, $(x-y)$ and $(x+y)$ are both nonzero, and thus $(x+y)(x-y) = kn$ for some $k \neq 0 \in \mathbb{Z}$. □

Suppose we wish to factor some integer n. If we can identify integers x, y as in the above lemma, then we have a non-trivial chance of recovering a factor of n. Indeed, $(x+y)(x-y) \mid kn$ means that there is a chance that $(x+y)$ or $(x-y)$ are non-trivial factors of n.

In the Number Field Sieve, we look for perfect squares in two separate rings: the integers $\mathbb{Z}$ and $\mathbb{Z}[\alpha]$, the integers adjoined with some complex root α of a polynomial f with some particular properties (discussed in detail in (4)). In practice, finding perfect squares is difficult. We increase our odds of finding them by searching for *smooth numbers* which only have prime factors in some finite set and taking a select product them such that the result is a square. In the Number Field Sieve, we require squares in two rings, and thus we sieve for numbers that are smooth in both rings. The algorithm discussed in this paper goes as far as sieving for smooth numbers and defers to linear algebra methods outside the scope of this project for constructing the perfect squares.

Lemma 2.2. *Let ϕ be the reduction map $\mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z}$ such that $\phi(\alpha) = m$ and define $x \coloneqq \phi(w)$. Further let S be a set of pairs of numbers $(a, b) \in \mathbb{Z}^2$ such that*

$$\prod_{(a,b)\in S} a + b\alpha = w^2 \in \mathbb{Z}[\alpha] \qquad \prod_{(a,b)\in S} a + bm = y^2 \in \mathbb{Z} \tag{2.2.1}$$

Then $x^2 \equiv y^2 \pmod n$.

Proof. Let variables be as defined. Since $\phi : \mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z}$, consider the following set of equalities modulo n:

$$\begin{aligned}
x^2 &\coloneqq \phi(w)\phi(w) \\
&= \phi(w^2) && \text{(homomorphism)} \\
&= \phi\Big(\prod_{(a,b)\in S} a + b\alpha\Big) \\
&= \prod_{(a,b)\in S} \phi(a + b\alpha) && \text{(homomorphism)} \\
&= \prod_{(a,b)\in S} a + b\phi(\alpha) && \text{(def. of } \phi) \\
&= \prod_{(a,b)\in S} a + bm && (\phi(\alpha) = m) \\
&= y^2
\end{aligned}$$

Thus $x^2 \equiv y^2 \pmod n$. □

Here the numbers $a + bm$ and $a + b\alpha$ are our desired smooth numbers in both $\mathbb{Z}$ and $\mathbb{Z}[\alpha]$ respectively. If we can find a set S of $(a, b) \in \mathbb{Z}^2$ such that (2.2.1) is true, then by Lemma (2.2) and Lemma (2.1), we have a slim but nontrivial chance of factoring n. By finding numerous such sets S, the chance of successfully factoring n increases. The goal of the Number Field Sieve is then precisely to produce such elements (a, b) for which (2.2.1) holds.

3 Mathematical Background

3.1 Number Rings

We begin by solidifying the concept of $\mathbb{Z}[\alpha]$.

Definition 3.1. *$\alpha \in \mathbb{C}$ is an **algebraic integer** if it a root of a monic polynomial $f \in \mathbb{Z}[x]$.*

Proposition 3.1. *Let $f \in \mathbb{Q}[x]$ be a monic irreducible polynomial of degree d, and $\alpha \in \mathbb{C}$ a root of f. The set of all algebraic integers $\mathcal{O} \subseteq \mathbb{Q}(\alpha)$ forms a subring of the field $\mathbb{Q}(\alpha)$.*

Proposition 3.2. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree d, and $\alpha \in \mathbb{C}$ a root of f. The set of all $\mathbb{Z}$-linear combinations of $\{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$, denoted $\mathbb{Z}[\alpha]$, forms a subring of $\mathcal{O}$ in $\mathbb{Q}(\alpha)$.*

3.2 The Algebraic Factor Base and Smoothness

A rational factor base over $\mathbb{Z}$ is a set of prime integers. A factor base of the ring $\mathbb{Z}[\alpha]$ that turns out to work best for the Number Field Sieve is a set of special prime ideals of $\mathbb{Z}[\alpha]$. Once we have chosen this set of prime ideals, called the **algebraic factor base**, the goal is to find pairs (a, b) such that the element $a + b\alpha$ is **smooth**. That is, the ideal $\langle a + b\alpha \rangle$ factors completely into prime ideals of the algebraic factor base. This will later allow us to find squares in $\mathbb{Z}[\alpha]$.

To be able to determine whether an element is smooth, we must first familiarize ourselves with the norm function and some of its properties.

Definition 3.2. *Let J be an ideal of a ring R. The **norm** of J is $[R : J]$, the number of cosets of J in R.*

Proposition 3.3. *Let N be the norm function* (3.2)*. Then*

1. *N is a multiplicative function that maps ideals of $\mathcal{O}$ (as in Proposition* (3.1)*) to positive integers. In particular, if $\theta \in \mathcal{O}$ then $N(\langle\theta\rangle) = |N(\theta)|$.*
2. *If ρ is an ideal of $\mathcal{O}$ such that $N(\rho) = p$ for some prime p, then ρ is a prime ideal of $\mathcal{O}$. Conversly, if ρ is a prime ideal of $\mathcal{O}$, then $N(\rho) = p^e$ for some prime p and some positive integer e.*

Due to a result beyond the scope of this paper, for any $\beta \in \mathcal{O}$ the principal ideal $\langle\beta\rangle$ of $\mathcal{O}$ factors uniquely as $\langle\beta\rangle = \rho_1^{e_1}\rho_2^{e_2}\cdots\rho_k^{e_k}$ for some distinct prime ideals ρ_i of $\mathcal{O}$ and positive integers e_i. Then by Proposition (3.3) we have that

$$|N(\beta)| = N(\langle\beta\rangle) = N(\rho_1^{e_1}\rho_2^{e_2}\cdots\rho_k^{e_k}) = N(\rho_1^{e_1})N(\rho_2^{e_2})\cdots N(\rho_k^{e_k}) = (p_1^{f_1})^{e_1}(p_2^{f_2})^{e_2}\cdots(p_k^{f_k})^{e_k} \tag{3.3.1}$$

for some primes p_i and positive integers e_i, f_i. Equation (3.3.1) is a key result that allows us to determine the smoothness of an element. Before we can use it, we solidify the definition of an algebraic factor base.

Definition 3.3. *A **first degree prime ideal** ρ of $\mathcal{O}$ is a prime ideal such that $N(\rho) = p$ for some prime integer p. An **algebraic factor base** I over $\mathbb{Z}[\alpha]$ is a finite set of first degree prime ideals in $\mathbb{Z}[\alpha]$.*

The following Theorem gives another representation for first degree prime ideals that we will utilize when determining the smoothness of an element.

Theorem 3.4. *Let $f \in \mathbb{Z}[x]$ be a monic, irreducible polynomial, and $\alpha \in \mathbb{C}$ a root of f. The set of $(r, p) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}$ such that p is prime and $f(r) \equiv 0 \pmod p$ is in bijective correspondence with the set of all first degree prime ideals of $\mathbb{Z}[\alpha]$*

Proof. If ρ is a first degree prime ideal of $\mathbb{Z}[\alpha]$, then $[\mathbb{Z}[\alpha] : \rho] = p$ for some prime p. Due to a result beyond the scope of this paper, there exists a surjective ring homomorphism $\phi : \mathbb{Z}[\alpha] \mapsto \mathbb{Z}/p\mathbb{Z}$ such that $\ker\phi = \rho$ and $\phi(a) \equiv a \pmod p$ for all $a \in \mathbb{Z}$. Then if $f(x) = a_0 + a_1x + ... + x^d \in \mathbb{Z}[\alpha]$, since $f(\alpha) = 0$ we have

$$0 \equiv \phi(f(\alpha)) \equiv \phi(a_0 + a_1\alpha + ... + \alpha^d) \equiv a_0 + a_1\phi(\alpha) + ... + \phi(\alpha)^d \equiv f(\phi(\alpha)) \pmod p.$$

Therefore $\phi(\alpha)$ is a root of $f \pmod p$, and the ideal ρ determines the unique pair $(r,p) = (\phi(\alpha), p)$. Conversely, if p is a prime and $r \in \mathbb{Z}/p\mathbb{Z}$ such that $f(r) \equiv 0 \pmod p$, then (due to a result beyond the scope of this paper) $\phi(a) \equiv a \pmod p$ for all $a \in \mathbb{Z}$ and $\phi(\alpha) = r \pmod p$. Since $\ker \phi = \rho$ is an ideal of $\mathbb{Z}[\alpha]$ and ϕ is surjective, it follows that $\mathbb{Z}[\alpha]/\rho \cong \mathbb{Z}/p\mathbb{Z} \Rightarrow [\mathbb{Z}[\alpha] : \rho] = p$, so ρ is a first degree prime ideal of $\mathbb{Z}[\alpha]$. Therefore the pair (r,p) determines the unique first degree prime ideal ρ. □

Now we can generalize equation (3.3.1) to prime ideals of $\mathbb{Z}[\alpha]$, and then use this generalization to test smoothness of an element $a + b\alpha$ over an algebraic factor base. First we observe that every exponent e_i in (3.3.1) can be represented as a homomorphism $e_{p_i} : \mathbb{Q}(\alpha)^* \mapsto \mathbb{Z}$. Then, using a result beyond the scope of this paper, we can define a homomorphism that has the same properties as the previously mentioned homomorphism but instead is defined on prime ideals of $\mathbb{Z}[\alpha]$:

Proposition 3.5. *Let ρ_i be a prime ideal of $\mathbb{Z}[\alpha]$. Then there exists a group homomorphism $l_{\rho_i} : \mathbb{Q}(\alpha)^* \mapsto \mathbb{Z}$ such that*

1. *$l_{\rho_i} \geq 0$ for all $\beta \in \mathbb{Q}(\alpha)^*$.*
2. *$l_{\rho_i} > 0$ if and only if ρ_i divides the principal ideal $\langle\beta\rangle$.*
3. *$l_{\rho_i} \neq 0$ for a finite number of prime ideals ρ_i of $\mathbb{Z}[\alpha]$, and $|N(\beta)| = \prod N(\rho_i)^{l_{\rho_i}}$ for all prime ideals ρ_i of $\mathbb{Z}[\alpha]$.*

In the Number Field Sieve, we focus on principal ideals of the form $\langle a + b\alpha\rangle$. In the following Theorem we see that this simplifies which prime ideals can be factors of $\langle a + b\alpha\rangle$.

Theorem 3.6. *Let $\beta \in \mathbb{Z}[\alpha]$ be an element of the form $a + b\alpha$ for coprime integers a, b and ρ a prime ideal of $\mathbb{Z}[\alpha]$. If ρ is not a first degree prime ideal then $l_\rho(\beta) = 0$. If ρ a first degree prime ideal of $\mathbb{Z}[\alpha]$ that corresponds to the pair (r,p) as in theorem (3.4), then*

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

where $ord_p(N(\beta))$ is the exponent of p in the prime factorization of $N(\beta)$.

The proof of this result is omitted due to length, but is described in detail in Theorem 3.1.9 of (Briggs 1998).

The importance of this Theorem comes from the following result: the only prime ideals that factor $\langle a+b\alpha\rangle$ are first degree prime ideals, and a first degree prime ideal corresponding to the pair (r,p) is a non-trivial factor of $\langle a + b\alpha\rangle$ if and only if $a \equiv -br \pmod p$.

Let's summarize what we've seen so far. To find an element $a + b\alpha \in \mathbb{Z}[\alpha]$ that is smooth over an algebraic factor base of first degree prime ideals of $\mathbb{Z}[\alpha]$, we find an element $a + b\alpha$ such that the integer $N(a + b\alpha)$ factors completely over the primes occurring in the (r,p) pairs corresponding to the first degree prime ideals in the algebraic factor base.

3.3 Finding Squares

Now that we have a background on the algebraic factor base and smoothness, we can establish the following results which give necessary (but not sufficient) conditions for an element to be a square in $\mathbb{Q}(\alpha)$.

Theorem 3.7. *Let U be a set of $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ such that $\prod_{(a,b)\in U}(a + b\alpha) \in \mathbb{Z}[\alpha]$ is a perfect square $\beta^2 \in \mathbb{Q}(\alpha)$. Then*

$$\sum_{(a,b)\in U} l_{\rho_i}(a + b\alpha) \equiv 0 \pmod 2 \tag{3.7.1}$$

for all prime ideals ρ_i of $\mathbb{Z}[\alpha]$.

Proof. If ρ_i is a prime ideal of $\mathbb{Z}[\alpha]$, by Proposition (3.5) we have

$$\sum_{(a,b)\in U} l_{\rho_i}(a+b\alpha) = l_{\rho_i}\left(\prod_{(a,b)\in U}(a+b\alpha)\right) = l_{\rho_i}(\beta^2) = 2l_{\rho_i}(\beta) \equiv 0 \pmod 2$$

. □

Theorem 3.8. *Let U be a set of pairs (a,b) such that*

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

for some $\theta \in \mathbb{Q}(\alpha)$. Let $\boldsymbol{q}$ be a first degree prime ideal corresponding to the pair (s,q) that does not divide $\langle a+b\alpha\rangle$ for any pair (a,b) and for which $f'(s) \not\equiv 0 \pmod q$. It follows that

$$\prod_{(a,b)\in U}\left(\frac{a+bs}{q}\right) = 1. \tag{3.8.1}$$

Note that $\left(\frac{a+bs}{q}\right)$ is the legendre symbol. The proof of this theorem is beyond the scope of this paper, but it can be seen in Theorem 3.2.1 of (Briggs 1998).

Let I be an algebraic factor base over $\mathbb{Z}[\alpha]$, and Q a set of first degree prime ideals corresponding to pairs (s,q) such that (3.8) is satisfied. Let U be a set of pairs (a,b) for which the elements $a+b\alpha$ are smooth over I and that satisfy (3.7.1) for all $\rho_i \in I$ and (3.8.1) for all $\mathbf{q} \in Q$. Then $\prod_{(a,b)\in U}(a+b\alpha)$ is very likely to be a perfect square in $\mathbb{Q}(\alpha)$. If it is a square in $\mathbb{Q}(\alpha)$ but not in $\mathbb{Z}[\alpha]$, that is $\prod_{(a,b)\in U}(a+b\alpha) = \omega^2$ for some $\omega \in \mathbb{Q}(\alpha)\backslash\mathbb{Z}(\alpha)$, we find that it is still quite simple to produce a difference of squares, as in Lemma (2.1).

Suppose we have the set up in Lemma (2.2), but with $\omega \in \mathbb{Q}(\alpha)\backslash\mathbb{Z}(\alpha)$. Let f be the polynomial in Proposition (3.2), and let $\beta = f'(\alpha)\cdot\omega \in \mathbb{Z}[\alpha]$, $z = f'(m)\cdot y$, and $x = \phi(\beta) \in \mathbb{Z}/n\mathbb{Z}$. Then

$$x^2 \equiv \phi(\beta)^2 \equiv \phi\left(f'(\alpha)^2\cdot\prod_{(a,b)\in U}(a+b\alpha)\right) \equiv \phi(f'(\alpha))^2\cdot\prod_{(a,b)\in U}\phi(a+b\alpha) \equiv f'(m)^2\cdot\prod_{(a,b)\in U}(a+b\alpha) \equiv z^2 \pmod n,$$

so we have once again produced a difference of squares.

4 Algorithm

Let n be a number we wish to factor.

4.1 Setup

In order to construct the ring $\mathbb{Z}[\alpha]$ and the reduction homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}[\alpha]$, we need to generate a polynomial f with several desired properties:

Definition 4.1. *Let $f \in \mathbb{Z}[x]$ be a polynomial such that: 1. is monic, 2. is irreducible, 3. $deg(f) \coloneqq d \geq 1$ and d is moderately small*[1] *, 4. $f(m) \equiv 0 \pmod{n}$ for some $m \in \mathbb{Z}$.*

The perhaps quickest and simplest way to generate such an f and m is by the *Base-m Method*. For this method, choose a relatively small degree $d \in \mathbb{Z}$ and let $m \coloneqq \left\lfloor n^{\frac{1}{d}} \right\rfloor$. Then we can write n in base-m, yielding $n = \sum_{i=0}^{d} c_i m^i$. Then using the $\{c_i\}_{i=0}^{d}$ as coefficients, we define $f(x) \coloneqq \sum_{i=0}^{d} c_i x^i$. We then confirm that $f(m) = \sum_{i=0}^{d} c_i m^i = n \equiv 0 \pmod{n}$ by construction.

Further note that we can take $f(x)$ to be irreducible. If it weren't, then $f(x) = g(x)h(x)$ and notably $f(m) = g(m)h(m) = n$ implies we have found a factorization of n. If this factorization is trivial, i.e. $g(m) = 1$, then we also have $f(m) = h(m) = n$, and we can take $h(x)$ to be our new $f(x)$, repeating as many times as necessary until we arrive at an irreducible. Finally, by construction of n in base-m, the polynomial f will be monic (see (6)). Thus our constructed f satisfies all requirements in (4.1).

The Number Field Sieve also requires a rational and an algebraic factor base to sieve for smooth numbers over. A rational factor base is simply a set of positive prime integers and choosing such a set poses no difficulties. One important detail, however, is that a prime may divide a number multiple times. To account for this, once the set of unique primes is determined, we add additional copies of each prime to $\mathscr{R}$ for all powers of that prime that are less than the greatest prime. For instance, if $\mathscr{R} = \{2, 3, 5, 7, 11\}$, we would add two other copies of 2 as $2^2 = 4, 2^3 = 8 < 11$ and one other copy of 3 as $3^2 = 9 < 11$. Our new $\mathscr{R}$ would then be $\{2, 2, 2, 3, 3, 5, 7, 11\}$.

Finding an algebraic factor base, however, requires more effort. By (3.4), finding first degree prime ideals ("primes" in $\mathbb{Z}[\alpha]$) is equivalent to finding pairs (r, p) such that $f(r) \equiv 0 \pmod{p}$. Put simply, prime ideals are equivalent to roots of our polynomial f viewed modulo primes p. An obvious method to search for these ideals is to loop over the set of primes p in our rational factor base $\mathscr{R}$ and compute the zeros of $f \pmod{p}$. This is taken to be our algebraic factor base $\mathscr{Q}$. Similar to the rational factor base, we account for powers of primes in the same manner.

We also determine a quadratic character base $\mathscr{C}$ to be a subset of prime ideals $\mathfrak{c} \subset \mathbb{Z}[\alpha]$ that satisfy (3.8).

4.2 Sieving

With all the required pieces in place, the actual sieving can begin. In this paper we will detail the simplest implementation, the "Brute Force" equivalent for the Number Field Sieve. Put simply, we fix the b parameter and traverse through all suitable a values in both rings and sieve for smooth numbers.

Let f be as in (4.1), and let our rational factor base be $\mathscr{R}$ and algebraic factor base be $\mathscr{Q}$. We begin by fixing $b > 0$. Commonly b is set to begin with a value of 1. We then initialize two sieving arrays, one for rational and one for algebraic. Each column of the sieving array corresponds to an integer value of a_i, denoted here as the *index*, between our bounds $-l < a_i < l$. We then set the first entry in each column as $a_i + bm$ for the rational array and $a_i + b\alpha$ for the algebraic array.

The process for sieving in each array is the same. In pseudo-code: we loop through all values p_i in our factor base, determine which values $a_j + bm / a_j + b\alpha$ are divisible by p_i, and if possible divide by p_i. After we have done this for every value in our factor base, we scan the final values in the arrays for 1s and return the pairs (a_j, b) for which this is true. The details for each kind of sieving, in particular how to determine when a prime divides an entry, are detailed in the next sections.

[1] In practice we take this to mean $3 \leq d \leq 10$ (Stevenhagen, 2008)

a_0	a_1	a_2	...	a_k
$a_0 + bm$	$a_1 + bm$	$a_2 + bm$	...	$a_k + bm$
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$

Figure 1: Rational sieve array

a_0	a_1	a_2	...	a_k
$a_0 + b\alpha$	$a_1 + b\alpha$	$a_2 + b\alpha$	...	$a_k + b\alpha$
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$

Figure 2: Algebraic sieve array

4.2.1 Rational sieving

Consider now sieving in the rational array. Let $p \in \mathscr{R}$. Since b is fixed, we wish to find elements a such that $p|a + bm$. Note then that

$$p|(a + bm) \iff a + bm \equiv 0 \pmod{p} \iff a \equiv -bm \pmod{p} \iff a = bm + cp \text{ for some } c \in \mathbb{Z}.$$

We can then generate a finite set of a_i such that $|a_i| < l$ and $a_i = bm + c_i p$ for some $c_i \in \mathbb{Z}$. Then for each of the a_i, $p|(a_i + bm)$ by above and since $|a_i| < l$ it occurs as an index in the sieving array. We can then divide the value in the a_i index of the rational sieving array by p. Repeating this process for all elements in $\mathscr{R}$, the only indices $\tilde{a}$ with values that are successfully sieved down to 1 are precisely those for which $\tilde{a} + bm$ is smooth over $\mathscr{R}$.

4.2.2 Algebraic sieving

Algebraic sieving proceeds in a similar fashion. Let prime ideal $\mathfrak{p} \in \mathscr{Q}$ have equivalent pair $(r, p) \in \mathbb{Z}^2$ by (3.4). Then

$$\mathfrak{p} \mid a + b\alpha \overset{(3.3.1)}{\iff} a \equiv -br \pmod{p}.$$

Analogous to (4.2.1), we generate a finite set of a_i such that $a_i = -br + k_i p$ for $k_i \in \mathbb{Z}$ and $|a_i| \leq l$. Then a_i occurs as an index in the algebraic sieving array and we can divide the entry $a_i + b\alpha$ by $\mathfrak{p}$. Apply this procedure for all $\mathfrak{p} \in \mathscr{Q}$, the elements that were sieved down to one are precisely those that are smooth over $\mathscr{Q}$.

†

It is unlikely that after a single value of b we procure enough smooth numbers to generate enough perfect squares to factor n. In practice, after following the above sieving procedure, the value of b is then changed and the process is repeated.

4.3 Exponents and Matrix Construction

Similar to the Quadratic Sieve, now having sieved a set of numbers that are smooth over both factor bases we wish to construct a matrix such that via linear algebra methods we can construct perfect squares in both rings from these smooth numbers. Each row of the matrix must then contain several pieces of information, represented as a binary vector:

1. A column with an entry 0 if $a + bm$ is positive and 1 if negative (as a was allowed to be negative),
2. For each $p \in \mathscr{R}$ a column with the number of times that p divides $a + bm$ modulo 2,
3. For each $\mathfrak{p} \in \mathscr{Q}$ a column with the number of times that $\mathfrak{p}$ divides $a + b\alpha$ modulo 2.
4. For each $\mathfrak{c} \in \mathscr{C}$ a column with whether the results of (3.7) and (3.8) hold for $a + b\alpha$ and $\mathfrak{p}$.

The last piece comes from the added requirements that determine whether a number is a perfect square in $Z[\alpha]$, which is non-trivial. Note that the resulting matrix will have $1 + |\mathscr{R}| + |\mathscr{Q}| + |\mathscr{C}|$ columns, which requires that more than or equal to that many smooth numbers be found in order for this matrix to have a suitable set of solutions. With this matrix now constructed, we defer to the blackbox linear algebra methods used to create squares in the two rings.

5 Running time, Pros & Cons

Again, let n be a number we wish to factor. Fix an integer l as the bound for which to sieve for smooth numbers in the interval $(-l, l)$.

5.1 Running time estimation

By class and homework contents we have: For quadratic sieve, the time complexity is $e^{\sqrt{ln(n)ln(ln(n))}}$.
Since $ln(n) > ln(ln(n))$, we have $e^{\sqrt{ln(n)ln(ln(n))}} < e^{\sqrt{ln(n)ln(n)}} = e^{ln(n)} = n$
We also have $e^{\sqrt{ln(n)ln(ln(n))}} > e^{\sqrt{ln(ln(n))ln(ln(n))}} = e^{ln(ln(n))} = ln(n)$.
So that it can be solved sub-exponential time(it may take longer than polynomial time).
And for number field sieve, the time complexity is $e^{ln(n)^{\frac{1}{3}} ln(ln(n))^{\frac{2}{3}}}$.
And we also have $e^{ln(n)^{\frac{1}{3}} ln(ln(n))^{\frac{2}{3}}} > e^{ln(ln(n))} = ln(n)$, namely it can not be solved in polynomial time.
But we know it is faster than the quadratic sieve method since $e^{ln(n)^{\frac{1}{3}} ln(ln(n))^{\frac{2}{3}}} < e^{\sqrt{ln(n)ln(ln(n))}}$, so that it is also under exponential time, and thus can be solved in sub-exponential time.
As a result, both sievings may not be considered as "easy".
And in fact, as shown in the homework, it is much faster than quadratic sieve method especially when the number is large: a 10^6 difference when $n = 2^{256}$, which has $\lceil log_{10} 2^{256} \rceil = 78$ digits; and a 10^{16} difference when $n = 2^{1024}$, which has $\lceil log_{10} 2^{1024} \rceil = 309$ digits.

5.2 Pros and Cons

As one of the most efficient factoring methods, number field sieve works especially good when there are more than 100 digits, and quadratic field sieve works well for smaller digit numbers like below 100 digits.
The main difficulty for the method lies in finding a monic irreducible polynomial $f(x)$ and a number m with $f(m) \equiv 0 \pmod{n}$. The higher the degree of the polynomial is, the smaller m can be, but the harder to examine whether it is irreducible and whether $f(m) \equiv 0 \pmod{n}$; finding such m sometimes may not be easy.
Compare to quadratic sieve, if for a function $g(x)$ with $g(a_1)$ is not a square after the prime factorization steps, we can pick additionally $g(a_2)$, $g(a_3)$ etc and make the sum of the powers for each prime in the prime factorization to be even, thus finding a square and possibly a nontrivial solution of $u^2 = v^2$ with $u \neq \pm v$.
But for number field sieve and the number m, we tend to only find one of it to simplify our workload.
In general, number field sieve is much more powerful, but requires more delicate techniques. For smaller digits number, we may just use quadratic sieve to find values, which may ended up faster and easier than number field sieve, but then when the number becomes really large, number field sieve can be an efficient way, as long as we find the desired polynomial and corresponding m for which $f(m) \equiv 0 \pmod{n}$.

6 Examples

6.1 Homework example

Considering for: $L_{\frac{1}{2}}(N) = e^{\sqrt{ln(n)ln(ln(n))}}$, $L_{\frac{1}{3}}(N) = e^{ln(n)^{\frac{1}{3}}ln(ln(n))^{\frac{2}{3}}}$, and suppose a computer does one billion operations per second and 1 year = 365.25 days.
For $n_1 = 2^{256}$ and $n_2 = 2^{1024}$, by calculating the values and converting them to hours,
$L_{\frac{1}{2}}(n_1) = 4.0631$ hours, $L_{\frac{1}{3}}(n_1) = 5.6061 \times 10^{-6}$ hours;
$L_{\frac{1}{2}}(n_2) = 1.2289 \times 10^{17}$ hours, $L_{\frac{1}{3}}(n_2) = 1.0622 \times 10^{1}$ hours.
There is a 10^6 difference when $n = 2^{256}$, and a 10^{16} difference when $n = 2^{1024}$.

6.2 Example from Briggs GNFS Thesis

Step 1: background definition
Definition of Prime Ideal: a prime ideal is an ideal I such that if $ab \in I$, then either $a \in I$ or $b \in I$.
For example, in $\mathbb{Z}$, the multiples of prime p, $\langle p \rangle$ is an ideal since for $\forall a, b$ with $ab \in \langle p \rangle$, at least one of a and b is a multiple of p.

Step 2: determining the highest degree of the polynomial.
Now suppose we want to factor the number $n = 45113$.
Say that we have $d = 3$ as the highest degree of a monic irreducible polynomial $f(x)$ (From the thesis, it is suggested that the degree needs to be odd, and we pick a relatively small one here so that we can examine whether it is irreducible easier).

Step 3: finding a satisfied number with 0 modulo.
Now we want to find a number m with $f(m) \equiv 0 \pmod{n}$. One easy way would be just set $f(m) = n$ and find the coefficients of $f(x)$, since the highest degree is 3, and the coefficient is 1 due to it being monic, we can roughly choose $m \approx n^{\frac{1}{d}}$, which gives us $45113^{\frac{1}{3}} \approx 35$, say we choose a prime one of $m = 31$ (The choice of m here also follows (4.1)).

Step 4: finding a corresponding monic irreducible polynomial.
And then we have $45113 = 31^3 + 15 \cdot 31^2 + 29 \cdot 31 + 8$, by choosing the coefficients between 0 and 30, we can find them for degrees of 2, 1 and 0. This gives us $f(x) = x^3 + 15x^2 + 29x + 8$ with $f(m) \equiv 0 \pmod{n}$.
Now examine whether $f(x)$ is irreducible in $\mathbb{Q}$: the only possible roots by Rational Root Theorem are ± 1. ± 2, ± 4 and ± 8. Clearly since all coefficients are chosen to be positive, all positive roots won't make the polynomial equals 0 and thus will not be factored into lower degree polynomials. We can examine each of the negative roots one by one and $f(-1) = -7$, $f(-2) = 2$, $f(-4) = 68$ and $f(-8) = -224$, so that $f(x)$ is irreducible in $\mathbb{Q}$.

Step 5: Finding the rational factor base.
The rational factor base part consists of all primes up to 29(included) as $m = 31$.

$(m \pmod{p}, p)$	$(m \pmod{p}, p)$	$(m \pmod{p}, p)$
$(1, 2)$	$(9, 11)$	$(8, 23)$
$(1, 3)$	$(5, 13)$	$(2, 29)$
$(1, 5)$	$(14, 17)$	
$(3, 7)$	$(12, 19)$	

Table 1: Rational Factor Base for $n = 45113$

Step 6: Finding the algebraic factor base.
The algebraic factor base consists of first degree prime ideals, represented as pairs (r, p) where p is a prime integer and r is a root of $f(x) = x^3 + 15x^2 + 29x + 8$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$.

Say we choose the prime 67. We want to find the roots of $f(x)$ in $\mathbb{Z}/67\mathbb{Z}$. We can use $g(x) = \gcd(f(x), x^{67} - x)$ to isolate the factors of $f(x)$. In this case, $g(x) \equiv f(x) \pmod{67}$. And since $g(x)$ divides $x^{67} - x = x(x^{33}+1)(x^{33}-1)$ and $g(0) = 8 \neq 0$, $g(x)$ divides $(x^{33}+1)(x^{33}-1)$. Trying some numbers and we can have $g(6) \equiv 938 \equiv 0 \pmod{67}$, so $x - 6 = x + 61$ is a factor in $\mathbb{Z}/67\mathbb{Z}$. Using methods like long division gives us the other one $x^2 + 21x + 21$. Trying some numbers again give us $x^2 + 21x + 21 = (x + 23)(x + 65)$, so the three roots are 2, 6 and 44. Notice we can find other roots for other prime selections as well. Below is a table for other pairs of (r, p).

(r,p) pair	(r,p) pair	(r,p) pair	(r,p) pair
$(0, 2)$	$(19, 41)$	$(44, 67)$	$(62, 89)$
$(6, 7)$	$(13, 43)$	$(50, 73)$	$(73, 89)$
$(13, 17)$	$(1, 53)$	$(23, 79)$	$(28, 97)$
$(11, 23)$	$(46, 61)$	$(47, 79)$	$(87, 101)$
$(26, 29)$	$(2, 67)$	$(73, 79)$	$(47, 103)$
$(18, 31)$	$(6, 67)$	$(28, 89)$	

Table 2: Algebraic Factor Base for $n = 45113$

Step 7: Finding the quadratic character base.
We will also have some primes pairs come from quadratic character base sieving, they are modulo primes q with q strictly larger than those used in the algebraic factor base. We compute the following table.

(r,p) pair	(r,p) pair	(r,p) pair
$(4, 107)$	$(80, 107)$	$(99, 109)$
$(8, 107)$	$(52, 109)$	

Table 3: Quadratic Character Base for $n = 45113$

Step 8: Sieving.
Suppose we have $a, b \in \mathbb{Z}$ as in (4.1) and $-1000 < a < 1000$, we find pairs starting with $b = 1$ and then 2, 3, 4, so forth. For example, for prime $p = 5$, from table 1 we have $m \equiv 1 \pmod{5}$, for $a + bm$ divisible by $p = 5$ with $b = 7$, we will have $a = -7m + 5k = -7(1) + 5k$, $k \in \mathbb{Z}$, sieve for $\mathbb{N}(a + b\theta)$ using values from table 2 will find the desired pairs as well. As from (4.3), finding more than $1 + 10 + 23 + 5 = 39$ pairs will guarantee a linear dependence among the binary vectors associated with these pairs, leading to perfect squares. After enough sieving, 40 pairs of (a, b) with $a + bm$ and $a + b\theta$ smooth are found as in the following table.

(a,b) pair	(a,b) pair	(a,b) pair	(a,b) pair	(a,b) pair	(a,b) pair	(a,b) pair
$(-73, 1)$	$(-2, 1)$	$(-1, 1)$	$(2, 1)$	$(3, 1)$	$(4, 1)$	$(8, 1)$
$(13, 1)$	$(14, 1)$	$(15, 1)$	$(32, 1)$	$(56, 1)$	$(61, 1)$	$(104, 1)$
$(116, 1)$	$(-5, 2)$	$(3, 2)$	$(25, 2)$	$(33, 2)$	$(-8, 3)$	$(2, 3)$
$(17, 3)$	$(19, 4)$	$(48, 5)$	$(54, 5)$	$(313, 5)$	$(-43, 6)$	$(-8, 7)$
$(11, 7)$	$(38, 7)$	$(44, 9)$	$(4, 11)$	$(119, 11)$	$(856, 11)$	$(536, 15)$
$(5, 17)$	$(5, 31)$	$(9, 32)$	$(-202, 43)$	$(24, 55)$		

Table 4: (a, b) Pairs Found during Sieving

Bibliography

Carl Pomerance, *A tale of two sieves*, Notices of the American Mathematical Society **43** (1996), no. 12, 1473–1485

Matthew E. Briggs, *An Introduction to the General Number Field Sieve*, Blacksburg, Virginia, 1998

Peter Stevenhagen, *The number field sieve*, Algorithmic Number Theory MSRI Publications Volume 44, 2008