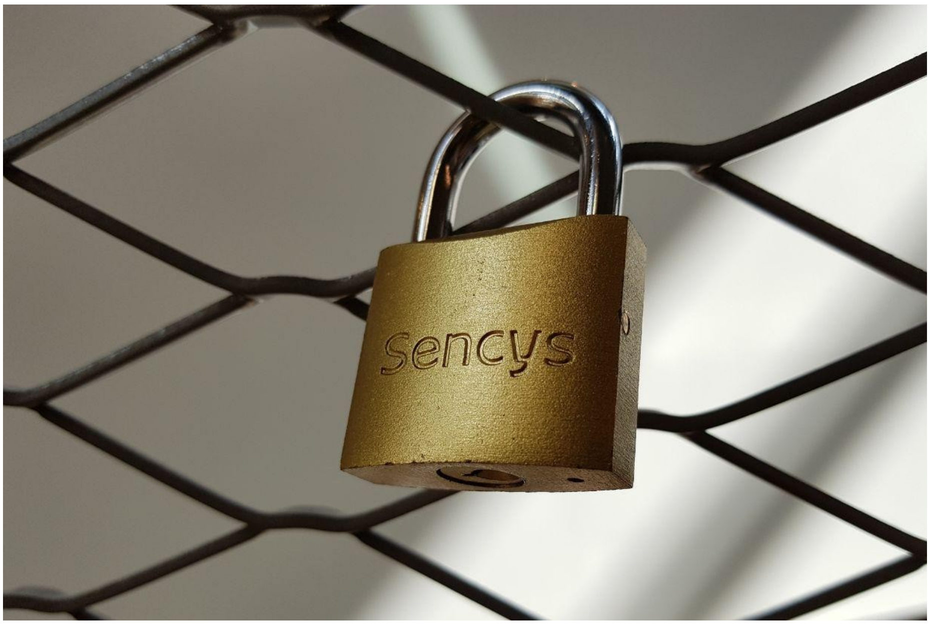
Dirichlet L-series and transforming generators of principal ideals in lattice-based cryptography

Thijs Blom

July 13, 2018

Bachelor thesis Mathematics and Computer Science

Supervisor: dr. Christian Schaffner, dr. Steffen Löbrich



Institute for Logic, Language and Computation
Korteweg-de Vries Institute for Mathematics
Informatics Institute
Faculty of Sciences
University of Amsterdam

Abstract

This thesis discusses an algorithm [1] to transform an arbitrary generator of a principal fractional ideal to a short generator. This algorithm contributes to a key-recovery attack on Soliloquy [2]. Both Soliloquy and the key-recovery attack are discussed in this thesis. Lattices in cryptography and algebraic number theory are connected using the log-unit lattice by embedding number fields in $\mathbb{R}^n$. Furthermore, Dirichlet L-series are explored, including its analytical continuation and the special values $L(1, \chi)$. Finally, Dirichlet L-series are linked to the class number of a number field.

Title: Dirichlet L-series and transforming generators of principal ideals in lattice-based cryptography
Authors: Thijs Blom, thijs.blom@student.uva.nl, 11051523
Supervisors: dr. Christian Schaffner, dr. Steffen Löbrich
First grader: dr. Christian Schaffner, dr. Lenny Taelman
End date: July 13, 2018

Institute for Logic, Language and Computation
University of Amsterdam
Science Park 107, 1098 XG Amsterdam
`http://www.illc.uva.nl`

Korteweg-de Vries Institute for Mathematics
University of Amsterdam
Science Park 105–107, 1098 XG Amsterdam
`http://www.kdvi.uva.nl`

Informatics Institute
University of Amsterdam
Science Park 904, 1098 XH Amsterdam
`http://www.ivi.uva.nl`

Contents

1. Introduction

Cryptography has been around in some form for thousands of years. Perhaps one of the more commonly known examples is the *Caesar cipher* named after Julius Caesar, who is said to have used this scheme to protect military information. He would take each letter of the message and shift it by 3 positions in the alphabet, wrapping around when reaching the end. Instead of the letter A, the letter D would be written down, and so forth. To anyone unfamiliar with the encryption scheme, the resulting text would seem nonsense, keeping the original message confidential.

With knowledge of current techniques, such a scheme could easily be broken, even for unknown shifts. In our current alphabet, there are only 26 different shift values, making it trivial to break. Even if we consider some larger set of characters to use (such as ASCII) it still barely provides security. Each letter in the alphabet is always replaced by a unique fixed letter, allowing one to calculate the relative frequency of each letter in the encrypted text and compare this frequency to the frequency distribution for the corresponding language. For example, the letter 'e' is the most frequently used letter in the English language. Matching the distributions would quickly reveal the shift value.

Over time, cryptography became more sophisticated and prevalent, and it is ubiquitous in modern life. Although still useful for military communication, cryptography is now commonly used to message securely using services such as Whatsapp, complete online banking transactions, and browse the web securely. These applications have also required many new techniques to construct such schemes. One of the schemes used often today is RSA, which relies on the hardness of factorisation of integers into prime numbers. Using computers currently available, it is not known how to solve the factorisation problem efficiently, making it difficult for adversaries to break the encryption. However, a new threat to cryptography looms on the horizon: quantum computers are able to break some prevalent current cryptography with relative ease. This sparked new developments in cryptography to ensure efficient security in the era of the quantum computer, leading to a field known as post-quantum cryptography.

One possible solution comes in the form of lattices, a structure previously known in algebraic number theory, a subfield of mathematics. Essentially, a lattice is a regular grid, which may be skewed and stretched. Some lattice problems seem to be algorithmically hard, allowing the construction of cryptography. Numerous proposals have used more tools from algebraic number theory to provide these lattices with more structure. Additional structure can be a powerful tool, but may also lead to unforeseen consequences. This thesis will explore an article by Cramer et al. [1], which exploits such additional structure. They provide a classical algorithm, which can efficiently break certain cryptographic schemes when combined with another quantum step. We will show an implementation of the classical part of the algorithm, and examine the results. Furthermore, we shall dive further into algebraic number theory. It is useful for cryptography, but also a field in its own right. Areas of study include zeta functions and L-series, somewhat mysterious objects that are powerful tools in number theory. A famous example is the Riemann-zeta function, which may be written as a product over all primes, revealing its first connection to number theory. In particular, we will show the class number formula: a formula linking together these functions with another quantity associated to number fields, the class number.

Acknowledgements

I wish to thank my supervisors dr. Christian Schaffner and dr. Steffen Löbrich for their time, help and guidance. I would also like to thank Koen de Boer for helping me understand Soliloquy.

2. Preliminaries

2.1. Cryptography

As mentioned in the introduction, cryptography has come a long way since the primitive constructions used in the Roman Empire and earlier. Modern cryptography is based on solid principles and mathematical approaches to ensure security, and perhaps just as important, to know when it fails to do so. These principles will be discussed briefly in this section. For further reading on these principles and foundations of modern cryptography, we refer to [3].

Consider the situation where two individuals wish to securely communicate over a public channel. Messages sent between these individuals have to be encrypted, and the parties must agree on the method, called an encryption scheme.

It is important to note that the scheme itself does not need to be kept secret. In fact, the scheme should be secure when everything except the key is public, which is known as *Kerckhoffs' principle* [3, p. 7]. Not only is it easier to keep just the key secret, public schemes may be reused and standardised too.

2.1.1. Principles of modern cryptography

What distinguishes modern cryptography from classical cryptography is the focus on formal reasoning and analysis to provide proofs of security. Specifically, three principles form the basis of modern cryptography [3].

Principle one: *formal definitions.* Security needs to be formally defined. This has many advantages: one can precisely know what type of attacks they are protected against, one may prove that a proposed scheme actually satisfies such a definition, and it allows for easy comparison of different schemes.

Principle two: *precise assumptions.* Often encryption schemes rely on the assumption that some underlying problem is hard to solve. Precisely specifying these assumptions allows them to be studied carefully, resulting in trust that the assumptions hold, or showing that they do not. Both cases are of vital importance for security.

Principle three: *proofs of security.* In the past, cryptography used to be a back-and-forth battle between those making and those breaking schemes. A rigorous proof provides certainty that no attacker can break the scheme, as long as the assumptions hold.

Before we can apply these principles, we need to formally define what a cryptographic scheme is. Although many different types of schemes exist, we shall only define a public-key encryption scheme, which is often used in practice and the most relevant for this thesis. First of all, we need the notion of *negligible* functions.

Definition 2.1 (Negligible function)**.** Consider a function $f\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$. If for every polynomial p that is positive on $\mathbb{N}$ there exists an integer $N_p \in \mathbb{N}$ such that $n > N$ implies

$$f(n) < \frac{1}{p(n)},$$

we call f *negligible.*

We may now define public-key encryption schemes.

Definition 2.2 (Public-key encryption scheme, Definition 11.1 of [3])**.** A public-key encryption scheme is a set of algorithms $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ such that:

- The *key-generation algorithm* Gen takes a security parameter 1^n as input, and outputs a keypair (pk, sk) called the *public key* and the *private key* respectively.
- The *encryption algorithm* Enc takes a public key pk and a message m as input, and outputs a ciphertext $c \leftarrow \mathrm{Enc}_{pk}(m)$, where $\leftarrow$ means (randomised) assignment.
- The *decryption algorithm* Dec takes a private key sk and a ciphertext c, producing a message m or $\perp$ in case of failure, denoted by $\mathrm{Dec}_{sk}(c)$.

For correctness, it is required that the probability $\mathrm{Dec}_{sk}(\mathrm{Enc}_{pk}(m)) \neq m$ is 'small' for all messages m. Formally, it must be negligible in the security parameter n, see [3, Definition 3.4].

In public-key encryption schemes, only the private key must be kept secret, and the public key may be shared. As only the public key is required to encrypt a message, two individuals may communicate without exchanging keys beforehand. This feature is very important in the context of online communication with other people and websites, as there may be no opportunity to exchange keys before secure communication is necessary. Further encryption schemes in this thesis will be public-key encryption schemes, unless specifically mentioned otherwise. Before proceeding, let us consider an example of public-key cryptography: RSA.

Example 2.3 (RSA)**.** The key-generation algorithm Gen takes the security parameter 1^n, and calculates $N = pq$, where p and q are random n-bit primes. It then chooses $e > 1$ such that $\gcd(e, \phi(N)) = 1$, where ϕ is the Euler totient function. Finally, it computes $e^{-1} \mod \phi(N)$ and outputs (N, e, d). The public key is (N, e) and the private key is (N, d).

Encryption and decryption for a message $m \in \{0, \dots, N-1\}$ are defined respectively by $\mathrm{Enc}_{pk}(m) = m^e \mod N$ and $\mathrm{Dec}_{sk}(c) = c^d \mod N$.

Correctness follows from $c^d = (m^e)^d = m^{ed} = m \mod N$ as $d = e^{-1} \mod \phi(N)$.

Note that even though RSA is indeed a public-key encryption scheme, it is not actually secure in this form [3, p. 411–415] as will be shown in Section 2.1.2. Another example of a public-key encryption scheme can be found in Section 4.4.

2.1.2. Defining security

As mentioned in the principles of modern cryptography [3], it is necessary to define what we mean by security if we want to have a chance at designing secure schemes. Multiple different security definitions exist, usually influenced by the *threat model*, that specifies which capabilities the attacker is assumed to have. One such definition is known as EAV-security, where encryptions are indistinguishable to a passive eavesdropper. To formally define EAV-security of a scheme Π against an attacker $\mathcal{A}$, we define an experiment $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)$.

Definition 2.4 (EAV-security)**.** Let the experiment $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)$ be defined as follows.

1. Run $\mathrm{Gen}(1^n)$ to obtain (pk, sk).

2. Adversary $\mathcal{A}$ is given pk and outputs two messages m_0, m_1 of equal length.

3. A uniform bit $b \in \{0, 1\}$ is chosen, and then m_b is encrypted and given to $\mathcal{A}$. The ciphertext c is called the *challenge ciphertext.*

4. $\mathcal{A}$ outputs a bit b', guessing which message was encrypted. If $\mathcal{A}$ succeeds, i.e. $b = b'$, the experiment outputs 1. Otherwise, the experiment outputs 0.

If for any probabilistic polynomial time adversary $\mathcal{A}$ the inequality $\mathbb{P}[\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \varepsilon(n)$ holds for a negligible function ε, we refer to the scheme Π as EAV-secure.

Example 2.5. We show that RSA as defined in Example 2.3 does not satisfy this definition of security. Note that the encryption algorithm is deterministic. An attacker may choose two messages m_0, m_1 of equal length, and encrypt both messages using the public key to get c_0, c_1 respectively. Upon receiving the challenge ciphertext c, the attacker outputs 0 if $c = c_0$ and 1 if $c = c_1$. The success chance is 1, and therefore Example 2.3 does not satisfy EAV-security.

Remark 2.6. *As illustrated by Example 2.5, any public-key encryption scheme satisfying EAV-security must have a non-deterministic encryption algorithm.*

Note that to satisfy EAV-security — and any other meaningful definition of security — the adversary must be unable to efficiently derive the private key from the public key. To illustrate this, assume that an adversary $\mathcal{A}$ can efficiently obtain the private key from the public key. It may then use the private key to decrypt the challenge ciphertext and succeed at the experiment with overwhelming probability. The algorithm presented by Cramer et al. leads to such a key-recovery attack for Soliloquy [1], discussed in Section 4.4. This fact immediately highlights why such an algorithm is important in cryptography, as key-recovery attacks are devastating to the security of encryption schemes.

2.2. Lattices

As certain current encryption schemes such as RSA will no longer be secure after the advent of the quantum computer, new foundations have to be found to build new cryptography upon. One candidate is a structure called a lattice. In this section, we will define a lattice, show some properties and give some examples.

Definition 2.7 (Lattice)**.** Consider the $\mathbb{R}$-vector space $\mathbb{R}^n$ with the standard inner product denoted $\langle \cdot, \cdot \rangle$. A *lattice* is a subgroup of the form

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

with linearly independent vectors $v_1, \ldots, v_m \in \mathbb{R}^n$, called a basis of Γ. If $m = n$, the lattice is called *complete.*

Essentially, a lattice can be thought of as a regular m-dimensional grid in n-dimensional space. Consider for example the 2-dimensional lattice in $\mathbb{R}^2$ spanned by $\{(2,1)^T, (0,1)^T\}$. It consists of all points $(2a, a+b)$, where $a, b \in \mathbb{Z}$. It is a complete lattice, as both dimensions equal two. Note that this does not always have to be the case. In fact, some lattices we will come across in the setting of cryptography will *never* be complete. Let us define the volume of a lattice, which can be thought of as the size of the fundamental parallelogram in the lattice, or more mathematically:

$$\{\alpha_1 v_1 + \cdots + \alpha_m v_m \mid 0 \leq \alpha_i < 1\}.$$

Definition 2.8 (Volume)**.** Let Γ be a lattice spanned by $v_1, \ldots, v_n$ and define the matrix A by $A_{ij} = \langle v_i, v_j \rangle$. We then define

$$\operatorname{vol}(\Gamma) = |\det A|^{1/2}.$$

Remark 2.9. *The volume of a lattice is independent of the chosen basis. Let* $\mathbf{v} = \{v_1, \ldots, v_n\}$ *and* $\mathbf{v}' = \{v_1', \ldots, v_n'\}$ *be bases of the same lattice. We may then write* $v_i = \sum a_{ij} v_j'$ *for integer coefficients,* $0 \leq i \leq n$*, and construct the matrix* $T' = (a_{ij})$ *to transform the basis* $\mathbf{v}'$ *to the basis* $\mathbf{v}$*. Similarly, we can create a square matrix that transforms the basis* $\mathbf{v}$ *to the basis* $\mathbf{v}'$*. The matrices* T *and* T' *are inverses of each other, and have integer entries. It follows that* $|\det(T)| = |\det(T')| = 1$*, showing that choice of basis does not affect the volume of the lattice.*

Again referring to the example above with basis $\{(2,1)^T, (0,1)^T\}$, we find that the matrix $(\langle v_i, v_j \rangle)$ is $\begin{pmatrix} 5 & 1 \\ 1 & 1 \end{pmatrix}$, yielding a volume of 2. We shall now use this volume, to illustrate a property of a lattice: the shortest nonzero vector. To do this, we need the notions of *centrally symmetric* and *convex* sets. A set $X \subseteq \mathbb{R}^n$ is called *centrally symmetric* if for any $x \in X$ we have $-x \in X$. A set $X \subseteq \mathbb{R}^n$ is called *convex* if for any points $x, y \in X$ the line between x and y is contained in X, or formally:

$$\{tx + (1-t)y \mid 0 \leq t \leq 1\} \subseteq X.$$

We may now continue to the theorem.

Theorem 2.10 (Minkowski's Lattice Point Theorem [4, Theorem 4.4])**.** *let Γ be a complete lattice in the Euclidean vector space $\mathbb{R}^n$ and X a centrally symmetric, convex subset of $\mathbb{R}^n$. Suppose that*

$$\mathrm{vol}(X) > 2^n \, \mathrm{vol}(\Gamma).$$

Then X contains at least one nonzero point $\gamma \in \Gamma$.

Note that any nonempty convex centrally symmetric subset of $\mathbb{R}^n$ contains the lattice vector 0. In certain cases it is important to find the shortest nonzero vector of lattice. Theorem 2.10 gives an upper bound on the norm of this vector by considering a large enough ball X around the origin, such that the condition is satisfied.

2.2.1. Building cryptography with lattices

In public-key cryptography, we have a public key and a private key. As mentioned in Section 2.1, it is crucial that the private key cannot be derived from its public counterpart. To achieve this property, some algorithmic problem is required that is hard to solve in general, but is greatly simplified by knowledge of some secret structure. In the case of RSA in Example 2.3, this secret structure is the prime factorisation of the modulus N. If the primes p, q such that $N = pq$ are known, then $\phi(N)$ and $d = e^{-1} \mod \phi(N)$ may be easily calculated, revealing the private key.

We shall dive into some problems that might qualify as being hard. First of all, we define the *shortest vector problem* abbreviated SVP as follows: given a basis of a lattice $\mathcal{L} \subseteq \mathbb{R}^n$, find a vector with norm $\min_{0 \neq x \in \mathcal{L}} \|x\|$.

Example 2.11. Consider the lattice $\mathcal{L} = \mathbb{Z}b_1 + \mathbb{Z}b_2$, where

$$b_1 = \begin{pmatrix} 2 \\ 5 \\ 6 \end{pmatrix}, \quad b_2 = \begin{pmatrix} 1 \\ 3 \\ 3 \end{pmatrix}.$$

Note that the vector $(0, 1, 0)^T = 2b_2 - b_1$ is in the lattice and has norm one. Any nonzero vector in this lattice has norm at least one, as all coefficients are integers. We may conclude that we have found a vector satisfying SVP.

For low dimensions n, this problem is not particularly difficult. In two dimensions, one may use a basis reduction due to Lagrange and Gauss, given by Algorithm 1 below. However, difficulty increases rapidly as n grows, and low dimensions are generally not used for cryptographic purposes. A slightly easier problem related to SVP is approximated-SVP with factor γ. In this case any solution v with $\|v\| \leq \gamma \min_{0 \neq x \in \mathcal{L}} \|x\|$ is accepted, providing a trade-off between accuracy and speed.

Another common lattice-based problem is CVP, short for the *closest vector problem.* It is defined similarly to SVP: given a basis of a lattice $\mathcal{L}$, and a target $t \in \mathbb{R}^n$, find a vector $v \in \mathcal{L}$ such that $\|v - t\| = \min_{x \in \mathcal{L}} \|x - t\|$. An approach to solving this problem is known as Babai's rounding algorithm, which will also be used in Chapter 4.

```
Data: A basis $b_1, b_2$
Result: A lattice basis $\widetilde{b_1}, \widetilde{b_2}$ such that $\widetilde{b_1}$ is the shortest non-zero lattice vector,
        and $\widetilde{b_2}$ is the shortest linearly independent vector after $\widetilde{b_1}$
while $b_1$ or $b_2$ can be reduced do
    if $\|b_1\| > \|b_2\|$ then
        Swap $b_1$ and $b_2$
    end
    while $\|b_2 \pm b_1\| < \|b_2\|$ do
        Replace $b_2$ with $b_2 \pm b_1$
    end
end
```

Algorithm 1: Lagrange-Gauss reduction

2.3. Number fields

In this section, we define some of the building blocks of algebraic number theory. This area of mathematics is concerned with number fields: finite field extensions of $\mathbb{Q}$. Concepts such as integers, prime numbers and factorisation as known in $\mathbb{Z}$ and $\mathbb{Q}$ are generalised to arbitrary number fields. These are useful and fundamental constructs in algebraic number theory, and also find applications in cryptography. For the rest of this thesis, we will implicitly assume that any ring mentioned is commutative.

2.3.1. Integrality

First of all, we shall concern ourselves with defining integers in a more general setting.

Definition 2.12. Let $A \subseteq B$ be an extension of rings. An element $b \in B$ is called *integral* over A, if there exists a monic, non-constant polynomial $f \in A[X]$ such that $f(b) = 0$. The ring B is called integral over A if all elements of B are integral over A.

A natural question to ask is whether integrality is preserved under multiplication and addition of integral elements. This is especially important as we wish to define the ring of all integral elements in a ring extension $A \subseteq B$. Note however, that this set must be closed under the usual ring operations to actually be a ring.

Theorem 2.13 (Proposition 2.2 of [4])**.** *Finitely many elements $b_1, \ldots, b_n \in B$ are all integral over A if and only if the ring $A[b_1, \ldots, b_n]$ viewed as an A-module is finitely generated.*

As mentioned in [4], it follows that any element $b \in A[b_1, \ldots, b_n]$ is integral, as $A[b_1, \ldots, b_n, b] = A[b_1, \ldots b_n]$ is finitely generated. Clearly, $b_1 + b_2, b_1 b_2 \in A[b_1, b_2]$, showing that the product and sum of integral elements b_1 and b_2 are again integral. We may now define the ring of all integral elements as intended.

Definition 2.14 (Integral closure)**.** Define the *integral closure* of A in B as the set $\overline{A} = \{b \in B \mid b \text{ integral over } A\}$. If $\overline{A} = A$, we say A is integrally closed in B.

In algebraic number theory, specific ring extensions are of particular interest: *number fields*, which are defined as finite field extensions of $\mathbb{Q}$. Let K be a number field. We consider the subring $\mathbb{Z}$ of K and define the *ring of integers* $\mathcal{O}_K$ as the integral closure of $\mathbb{Z}$ in K. These are the generalised integers that we will be working with in number fields. Consider for example the field $\mathbb{Q}(i)$, such that $i^2 + 1 = 0$. Then its *ring of integers* is $\mathbb{Z}[i]$, which is a ring extension of $\mathbb{Z}$.

Next, we turn our attention to the notion of a basis.

Definition 2.15 (Integral basis)**.** A tuple of elements $\omega_1, \dots, \omega_n \in B$ such that each $b \in B$ can be written uniquely as a linear combination

$$b = a_1\omega_1 + \cdots + a_n\omega_n$$

with $a_i \in A$ is called an *integral basis* of B over A.

Note that such a basis does not necessarily exist.

Often we consider the number field K as subset of $\mathbb{C}$. However, there is no unique way to do this whenever $K \neq \mathbb{Q}$. Formally, this is solved by the definition of an *embedding.*

Definition 2.16 (Embedding)**.** Consider rings A, B and let $\sigma\colon A \to B$ be a ring-homomorphism. If σ is injective, it is called an *embedding* of A into B.

In number fields, an integral basis always exists [4, Ch.1 Proposition 2.10]. Existence of an integral basis allows us to define the following.

Definition 2.17 (Discriminant)**.** Let $\omega_1, \dots, \omega_n$ be an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$ and define the matrix A by $A_{ij} = \sigma_i(\omega_j)$, where σ_i goes through all embeddings of K in $\mathbb{C}$. We define the *discriminant* of K as

$$d_K := \det(A)^2.$$

It is important to note that the discriminant is well-defined. Any other integral basis gives the same discriminant [4, p. 15]. Furthermore, note that the matrix A in Definition 2.17 is a square matrix. Any element of K may be written as b/a with $b \in \mathcal{O}_K$, $a \in \mathbb{Z}$ [4, p. 8]. This means that an integral basis is also a $\mathbb{Q}$-basis of K, by writing out the linear combination of b, and dividing all coefficients $a_i \in \mathbb{Z}$ by $a \in \mathbb{Z}$, and remarking that $a_i/a \in \mathbb{Q}$. This shows that the length of the integral basis equals the degree of the number field. As the number of embeddings of K in $\mathbb{C}$ also equals the degree of the number field, we find that the matrix A is a square matrix.

In this thesis, one family of number fields will often reappear: *cyclotomic fields.*

Definition 2.18 (Cyclotomic field)**.** Let $n \in \mathbb{N}$, $n > 2$ and let ζ be a primitive n-th root of unity, i.e. $\zeta^n = 1$ and $\zeta^m \neq 1$ for $m < n$. Then $\mathbb{Q}(\zeta)$ is called the n-th *cyclotomic field.*

Note that $\mathbb{Q}(\zeta)$ is an extension of $\mathbb{Q}$ of degree $\phi(n) < \infty$, and is therefore a number field. Its ring of integers is determined in the following lemma.

Lemma 2.19 (Proposition 10.2 of [4])**.** *A $\mathbb{Z}$-basis of the ring $\mathcal{O}$ of integers of $\mathbb{Q}(\zeta)$ is given by $1, \zeta, \dots, \zeta^{d-1}$, with $d = \phi(n)$, in other words,*

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{d-1} = \mathbb{Z}[\zeta].$$

2.3.2. Ideals

Having considered integers of number fields, we shall now turn our attention to generalising prime numbers. An important notion used in this generalisation is that of an ideal: an additive subgroup of a ring, closed under multiplication by elements from that ring. Ideals generated by one element, denoted $(a) := a\mathcal{O}_K$ for some $a \in K$ are called *principal ideals*. In general number fields, unique factorisation of numbers into prime factors is lost.

Example 2.20. Consider $K = \mathbb{Q}(\sqrt{-5})$ with ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}\,]$. We then have

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

We can equip this number field with the norm $N(a+b\sqrt{-5}) = a^2+5b^2$. If the element 2 would admit a decomposition $2 = \alpha\beta$ for α, β non-units in $\mathcal{O}_K$, we would get the equation

$$4 = N(2) = N(\alpha)N(\beta),$$

and thus $N(\alpha) = \pm 2$. However, the equation $a^2+5b^2 = 2$ has no integer solutions. The same reasoning shows that the elements $3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducible. Furthermore, the elements $2, 3$ generate the ideals $(2) := 2\mathbb{Z} + 2\mathbb{Z}\sqrt{-5}$ and $(3) := 3\mathbb{Z} + 3\mathbb{Z}\sqrt{-5}$ respectively. Clearly, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are not elements of (2) or (3), showing that the generated ideals and therefore the factorisations are truly different. We conclude that the element $6 \in \mathcal{O}_K$ has no unique factorisation.

To combat this issue, the notion of an ideal was introduced, which do keep this property (under certain conditions) when going from $\mathbb{Q}$ to an arbitrary number field. We define *prime ideals*, which shall take the place of prime numbers. To consider factorisations into prime ideals, we must define what the product of two ideals is. For any ring R, and ideals I, J of R, we define the product of I and J to be

$$IJ := \Big\{ \sum_{k=1}^{n} i_k j_k \mid i_k \in I,\ j_k \in J,\ n \in \mathbb{N} \Big\}.$$

Definition 2.21 (Prime ideal)**.** Let I be an ideal of a ring R. If for all $a, b \in R$ the condition $ab \in I$ implies $a \in I$ or $b \in I$, we say I is *prime.*

It is important to note that in general, ideals of arbitrary rings do not factorise uniquely into prime ideals. However, ideals of the ring of integers do satisfy this property.

Theorem 2.22 (Theorem 3.3 of [4])**.** *Every ideal $\mathfrak{a}$ of $\mathcal{O}_K$ different from $\{0\}$ and $\mathcal{O}_K$ admits a factorisation*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

into nonzero prime ideals $\mathfrak{p}_i$ of $\mathcal{O}_K$ which is unique up to the order of the factors.

Remark 2.23. *Rings that have such unique factorisation of ideals are called* Dedekind domains.

Having discussed integrals of $\mathcal{O}_K$, we turn our attention to another notion of ideals.

Definition 2.24 (Fractional ideal)**.** A *fractional ideal* of K is a finitely generated $\mathcal{O}_K$-submodule of K.

Remark 2.25. *An equivalent characterisation is as follows: a $\mathcal{O}_K$-submodule $\mathfrak{a}$ of K is a fractional ideal if and only if there exists $c \in \mathcal{O}_K \setminus \{0\}$ such that $c\mathfrak{a} \subseteq \mathcal{O}_K$ [4, p.21].*

As an example, consider the number field $\mathbb{Q}(i)$, where $i^2 + 1 = 0$, with $\mathcal{O}_K = \mathbb{Z}[i]$. Then $2\mathbb{Z}[i]$ and $i\mathbb{Z}[i]$ are ideals of $\mathcal{O}_K$. However, $\frac{1}{2}\mathbb{Z}[i]$ and $\frac{i}{2}\mathbb{Z}[i]$ are not ideals of $\mathcal{O}_K$, but are finitely generated $\mathbb{Z}[i]$-submodules of K and therefore *fractional* ideals. In fact, both these fractional ideals are generated by a single element from K.

Theorem 2.26 (Proposition 3.8 of [4])**.** *The nonzero fractional ideals form an abelian group under multiplication, the* ideal group J_K *of K. The identity element is* $(1) = \mathcal{O}_K$, *and the inverse of $\mathfrak{a}$ is*

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}_K\}.$$

Remark 2.27. *Note that $\mathfrak{a}^{-1}$ is in fact a non-zero fractional ideal. We may write each element $x \in K$ as $x = b/a$ with $b \in \mathcal{O}_K$ and $a \in \mathbb{Z}$ [4, p.8]. Let $b_1/a_1, \ldots, b_n/a_n$ be an integral basis of $\mathfrak{a}$ over $\mathbb{Z}$ and define $c = \operatorname{lcm}(a_1, \ldots, a_n)$. Then we have $c\mathfrak{a} \subseteq \mathcal{O}_K$ as all denominators cancel. It follows that $c \in \mathfrak{a}^{-1}$, so $\mathfrak{a}^{-1}$ is non-zero.*

Next, we show that $\mathfrak{a}^{-1}$ is a $\mathcal{O}_K$-submodule of K and that there exists $d \in \mathcal{O}_K$ such that $d\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. It then follows from Remark 2.25 that $\mathfrak{a}^{-1}$ is a fractional ideal. Let $x, y \in \mathfrak{a}^{-1}$. By definition, we have $\mathfrak{a}^{-1} \subseteq K$ and $xm, ym \in \mathcal{O}_K$ for all $m \in M$. Therefore we also have $(x + y)m = xm + ym \in \mathcal{O}_K$. As $xm \in \mathcal{O}_K$, we also have $rxm \in \mathcal{O}_K$ for all $r \in \mathcal{O}_K$. It follows that $\mathfrak{a}^{-1}$ is a $\mathcal{O}_K$-submodule of K.

As $\mathfrak{a}$ is non-zero, we can choose $y \in \mathfrak{a}$, $y \neq 0$. By definition of $\mathfrak{a}^{-1}$ we have $y\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. We also have $cy \in \mathcal{O}_K$ by definition of c. Then $cy\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. We conclude $\mathfrak{a}^{-1}$ is a non-zero fractional ideal.

In particular, we are interested in a specific subgroup and its index in the ideal group.

Definition 2.28 (Class group)**.** The nonzero fractional principal ideals $(a) = a\mathcal{O}_K$ for $a \in K^*$ are a subgroup of J_K denoted P_K. We define the *class group* as $Cl_K = J_K/P_K$. The order of this group is called the *class number*.

An interesting fact is that the class number is finite when considering number fields and the corresponding rings of integers [4, Ch.1 Theorem 6.3]. The class number will reappear when looking at L-series in Section 3.2.4, where we find a way to compute it. It will also be discussed in Chapter 4.

3. Algebraic number theory

3.1. General theory

In this section, we return to a number field K with ring of integers $\mathcal{O}_K$. Recall that $\mathcal{O}_K$ is defined as the integral closure of $\mathbb{Z}$ in K. First of all, we briefly recall the concept of units, as they play an important role in Chapter 4. For a ring R, we call $a \in R$ a *unit* if there exists $b \in R$ such that $ab = ba = 1$, and we write $b = a^{-1}$. The group of all units in a ring R is denoted by R^*. In this section, we show a result on the structure of $\mathcal{O}_K^*$ and use this structure to define the *log-unit lattice*.

3.1.1. Mapping the number field to $\mathbb{R}^n$

We show how to map non-zero elements of a number field K to vectors in $\mathbb{R}^n$, using *Minkowski Theory* [4, Ch.1 §5]. To do this, we consider embeddings $\sigma\colon K \to \mathbb{C}$ (see Definition 2.16). We split the embeddings into *real* and *complex* embeddings. An embedding σ is called *real* if $\operatorname{Im}\sigma \subseteq \mathbb{R}$, and called *complex* otherwise. The complex embeddings come in pairs: if σ is an embedding, so is $\overline{\sigma}$ defined by $\overline{\sigma}(a) = \overline{\sigma(a)}$ for $a \in K$. Suppose we have r real embeddings $\rho_1, \ldots \rho_r$ and s pairs of complex embeddings $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s}$. We choose order the embeddings and choose one from each pair to define the map $\lambda\colon K^* \to \mathbb{R}^{r+s}$ given by

$$\lambda(a) = \begin{pmatrix} \log|\rho_1(a)| \\ \vdots \\ \log|\rho_r(a)| \\ 2\log|\sigma_1(a)| \\ \vdots \\ 2\log|\sigma_s(a)| \end{pmatrix}. \tag{3.1}$$

Note that $|x| = |\overline{x}|$ for each $x \in \mathbb{C}$, and therefore the choice of embedding from a complex pair is arbitrary. Furthermore, only 0 is mapped to 0 by any embedding, and $0 \notin K^*$, so the logarithm in the definition is always defined. It follows that λ is well-defined.

Example 3.1. Consider the number field $K = \mathbb{Q}(\zeta)$ where $\zeta \in \mathbb{C}$ is a primitive fifth root of unity. There are no real embeddings, and two pairs of complex embeddings of K in $\mathbb{C}$: σ_1 defined by $\zeta \mapsto \zeta$ and σ_2 defined by $\zeta \mapsto \zeta^2$ (and their conjugate counterparts). We then have

$$\lambda(a + b\zeta + c\zeta^2 + d\zeta^3) = \begin{pmatrix} 2\log|a + b\zeta + c\zeta^2 + d\zeta^3| \\ 2\log|a + b\zeta^2 + c\zeta^4 + d\zeta| \end{pmatrix}$$

as $\zeta^6 = \zeta$.

3.1.2. Dirichlet's unit theorem and the log-unit lattice

We shall now explore the structure of $\mathcal{O}_K^*$. The following theorem gives an explicit description.

Theorem 3.2 (Dirichlet's Unit Theorem [4, Ch.1 Theorem 7.4])**.** *Let r be the number of real embeddings, and $2s$ the number of complex embeddings from K to $\mathbb{C}$. There exist units $\varepsilon_1, \dots \varepsilon_t \in \mathcal{O}_K^*$, $t = r + s - 1$, called fundamental units, such that any unit $\varepsilon \in \mathcal{O}_K^*$ can be written uniquely as a product*

$$\varepsilon = \zeta \varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t}$$

with a root of unity $\zeta \in \mathcal{O}_K^*$ and integers ν_i.

Remark 3.3. *According to Theorem 3.2, any $\varepsilon \in \mathcal{O}_K^*$ may be written uniquely as $\zeta \varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t}$. Note that all factors in the product are also elements of $\mathcal{O}_K^*$. It follows that for all integers $\nu_1, \dots, \nu_t$ and any root of unity $\zeta \in \mathcal{O}_K^*$, we have $\zeta \varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t} \in \mathcal{O}_K^*$.*

We now consider $\varepsilon \in \mathcal{O}_K^*$ and apply λ from Section 3.1.1. This yields

$$\begin{aligned}\lambda(\varepsilon) &= \begin{pmatrix} \log|\rho_1(\zeta\varepsilon_1^{\nu_1}\cdots\varepsilon_t^{\nu_t})| \\ \vdots \\ \log|\rho_r(\zeta\varepsilon_1^{\nu_1}\cdots\varepsilon_t^{\nu_t})| \\ 2\log|\sigma_1(\zeta\varepsilon_1^{\nu_1}\cdots\varepsilon_t^{\nu_t})| \\ \vdots \\ 2\log|\sigma_s(\zeta\varepsilon_1^{\nu_1}\cdots\varepsilon_t^{\nu_t})| \end{pmatrix} = \begin{pmatrix} \log\left(|\rho_1(\zeta)|\cdot|\rho_1(\varepsilon_1^{\nu_1})|\cdots|\rho_1(\varepsilon_t^{\nu_t})|\right) \\ \vdots \\ \log\left(|\rho_r(\zeta)|\cdot|\rho_r(\varepsilon_1^{\nu_1})|\cdots|\rho_r(\varepsilon_t^{\nu_t})|\right) \\ 2\log\left(|\sigma_1(\zeta)|\cdot|\sigma_1(\varepsilon_1^{\nu_1})|\cdots|\sigma_1(\varepsilon_t^{\nu_t})|\right) \\ \vdots \\ 2\log\left(|\sigma_s(\zeta)|\cdot|\sigma_s(\varepsilon_1^{\nu_1})|\cdots|\sigma_n(\varepsilon_t^{\nu_t})|\right) \end{pmatrix} \\ &= \nu_1\lambda(\varepsilon_1) + \cdots + \nu_t\lambda(\varepsilon_t). \end{aligned} \tag{3.2}$$

Here we used the properties $\log(ab) = \log(a) + \log(b)$, $\log(a^b) = b\log(a)$, $\log 1 = 0$ and that for any embedding τ and any root of unity ζ we have $\tau(a^b) = \tau(a)^b$ and $|\tau(\zeta)| = 1$.

Definition 3.4 (Log-unit lattice)**.** The group $\lambda(\mathcal{O}_K^*)$ is called the *log-unit lattice.*

By Theorem 3.2, any element in the log-unit lattice can be written as in (3.2). Remark 3.3 shows that any element of the form (3.2) is a point in the log-unit lattice. The log-unit lattice is therefore a lattice with basis $\{\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t)\}$.

Lemma 3.5. *The log-unit lattice is orthogonal to the all-ones vector* $\mathbf{1}$.

Proof. For arbitrary $a \in \mathcal{O}_K^*$, consider the vector $\lambda(a)$ in the log-unit lattice. We show that $\langle \lambda(a), \mathbf{1} \rangle = 0$ where $\langle \cdot, \cdot \rangle$ denotes the standard inner product on $\mathbb{R}^n$. First of all, note that $\log|\sigma(a)|^2 = 2\log|\sigma(a)|$ and $\log|\sigma(a)| = \log|\overline{\sigma}(a)|$. We may therefore rewrite

$$\langle \lambda(a), \mathbf{a} \rangle = \sum_{\rho \text{ real}} \log|\rho(a)| + \sum_{\substack{(\sigma,\overline{\sigma}) \\ \text{complex pair}}} \log|\sigma(a)|^2 = \sum_{\rho \text{ real}} \log|\rho(a)| + 2 \sum_{\substack{(\sigma,\overline{\sigma}) \\ \text{complex pair}}} \log|\sigma(a)|,$$

where we only consider one from each embedding from each complex pair to

$$\sum_{\tau} \log |\tau(a)|$$

over all embeddings τ from K into $\mathbb{C}$. This may be further manipulated to get

$$\sum_{\tau} \log |\tau(a)| = \log \big| \prod_{\tau} \tau(a) \big|$$

For a unit $a \in \mathcal{O}_K^*$, we have $|N(a)| \coloneqq |\prod_\tau \tau(a)| = 1$ as N is multiplicative, giving $N(a)N(a^{-1}) = N(aa^{-1}) = N(1) = 1$ for integers $N(a)$ and $N(a^{-1})$. We conclude that $\langle \lambda(a), \mathbf{1} \rangle = 0$, thus the log-unit lattice is orthogonal to the all-ones vector. □

Finally, we introduce the regulator of a number field K, which can be used to determine the volume of the log-unit lattice. It will also be important in Section 3.3.

Definition 3.6 (Regulator)**.** Write $\lambda^{(i)}(a)$ for the i-th component of $\lambda(a)$ and consider the matrix

$$\begin{pmatrix} \lambda^{(1)}(\varepsilon_1) & \cdots & \lambda^{(1)}(\varepsilon_t) \\ \vdots & & \vdots \\ \lambda^{(t+1)}(\varepsilon_1) & \cdots & \lambda^{(t+1)}(\varepsilon_t) \end{pmatrix}.$$

Remove any row from this matrix, and call the result M. We define the regulator of a number field to be $R = |\det(M)|$.

We show that the regulator is well-defined, by proving that it is independent of choice of fundamental units and choice of row to delete. First of all, we discuss the choice of row to delete. Define

$$\lambda_0 = \frac{1}{\sqrt{r+s}}(1, \ldots, 1) \in \mathbb{R}^{r+s}. \tag{3.3}$$

By Lemma 3.5, the vector λ_0 is orthogonal to the log-unit lattice. Clearly, it also has Euclidian length 1. Write $\lambda_0^{(i)}$ for the i-th component of λ_0 and $\lambda^{(i)}(a)$ for the i-th component of $\lambda(a)$. Note that $r + s = t + 1$ by definition. Consider the matrix

$$A = \begin{pmatrix} \lambda_0^{(1)} & \lambda^{(1)}(\varepsilon_1) & \cdots & \lambda^{(1)}(\varepsilon_t) \\ \vdots & \vdots & & \vdots \\ \lambda_0^{(t+1)} & \lambda^{(t+1)}(\varepsilon_1) & \cdots & \lambda^{(t+1)}(\varepsilon_t) \end{pmatrix}. \tag{3.4}$$

Now choose some row $i \in \{1, \ldots, r+s\}$ of A, and add all other rows to row i. We then get the matrix B, where the i-th row is $(\sqrt{r+s}, 0, \ldots, 0)$.

$$B = \begin{pmatrix} \lambda_0^{(1)} & \lambda^{(1)}(\varepsilon_1) & \cdots & \lambda^{(1)}(\varepsilon_t) \\ \vdots & \vdots & & \vdots \\ \sqrt{r+s} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ \lambda_0^{(t+1)} & \lambda^{(t+1)}(\varepsilon_1) & \cdots & \lambda^{(t+1)}(\varepsilon_t) \end{pmatrix} \tag{3.5}$$

The zeroes appear due to Lemma 3.5, and clearly the components of λ_0 sum to $\sqrt{r+s}$. Note that the determinant of a matrix remains unchanged when adding rows to other rows, thus $\det(A) = \det(B)$. We compute $\det(B)$ by developing along row i. As the zeroes do not contribute, this gives $\pm\sqrt{r+s}\,\det(M)$, where M is the submatrix of B with row i and column 1 removed. This matrix M is then given by removing row i from the matrix

$$\begin{pmatrix} \lambda^{(1)}(\varepsilon_1) & \cdots & \lambda^{(1)}(\varepsilon_t) \\ \vdots & & \vdots \\ \lambda^{(t+1)}(\varepsilon_1) & \cdots & \lambda^{(t+1)}(\varepsilon_t) \end{pmatrix}, \tag{3.6}$$

which matches the matrix from Definition 3.6. We now have $\det(A) = \det(B) = \sqrt{r+s}\,\det(M)$ for arbitrary i, showing that $\det(M)$ is independent of the row we delete.

Secondly, we discuss choice of fundamental units. Using Lemma 3.7, we connect the regulator to the volume of the log-unit lattice. As stated in Remark 2.9, the volume of a lattice does not depend on choice of basis. It follows that the regulator is independent of choice of fundamental units.

Finally, we use the regulator to calculate the volume of $\lambda(\mathcal{O}_K^*)$, following [4, p.43–44].

Lemma 3.7 (Proposition 7.5 of [4])**.** *The volume of the log-unit lattice is given by $\sqrt{r+s}\,R$, where R is the regulator, r is the number of real embeddings, and s is the number of complex pairs of embeddings.*

Proof. By Lemma 3.5, the vector λ_0 (see (3.3)) is orthogonal to the log-unit lattice. As the length of λ_0 is 1, the t-dimensional volume of the log-unit lattice equals the $(t+1)$-dimensional volume of the log-unit lattice with λ_0 added as basis vector. Consider the matrix A from (3.4). Then A^TA is the matrix of inner products from Definition 2.8. We then have $|\det(A)| = |\det(A^TA)|^{1/2} = \mathrm{vol}(\lambda(\mathcal{O}_K^*))$. As seen when developing (3.5), we have $|\det(A)| = |\det(B)| = \sqrt{r+s}\,R$. □

3.2. L-series and zeta functions

One of the most well known functions in mathematics is the Riemann zeta function. It has interesting connections to number theory, which are not immediately apparent. In this section, we discuss some properties of the Riemann zeta function and a generalisation, the Dirichlet L-series. Many of the results derived for the Riemann zeta function hold for more general series too. This section will follow Chapter 7 of [4].

3.2.1. The Riemann zeta function

Riemann's zeta function is defined for the complex variable s by the series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Clearly, we must ask whether this series converges.

Lemma 3.8 (Ch.7 Proposition 1.1 of [4]). *The series $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ is absolutely and uniformly convergent in the domain $\Re(s) \geq 1 + \delta$, for every $\delta > 0$. It therefore represents an analytic function in the half-plane $\Re(s) > 1$.*

Proof. Let $\sigma = \Re(s) \geq 1 + \delta$ and note that $|1/n^s| = 1/n^\sigma$ as $n^{i\alpha}$ has norm one for every $\alpha \in \mathbb{R}$. We then find

$$\sum_{n=1}^{\infty} \left| \frac{1}{n^s} \right| = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} \leq \sum_{n=1}^{\infty} \frac{1}{n^{1+\delta}},$$

in which the last term converges by the integral test. The Weierstrass M-test implies that $\zeta(s)$ converges absolutely and uniformly. □

Its connection with number theory however, has not yet been revealed. It turns out that the series may be rewritten as a product over all primes. As the set of all prime numbers if infinite, we must first define infinite products. An infinite product $\prod_{n=1}^{\infty} a_n$ is defined to converge if the partial products $p_n = a_1 \cdots a_n$ have a nonzero limit, which is the case if and only if $\sum_{n=1}^{\infty} \log a_n$ converges, with log the principal branch of the logarithm. The product is called absolutely convergent if the series converges absolutely.

Lemma 3.9 (Proposition 1.1 of [4]). *The identity*

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

holds for $\Re(s) > 1$, and is referred to as Euler's identity.

Proof. Let $M \in \mathbb{N}$. We take the logarithm of $E(s) := \prod_{p \leq M} 1/(1 - p^{-s})$ and use $\log(1 - z) = -\sum_{n=1}^{\infty} z^n/n$ to get

$$\log E(s) = \sum_{p \leq M} -\log(1 - p^{-s}) = \sum_{p \leq M} \sum_{n=1}^{\infty} \frac{1}{np^{-ns}}.$$

As remarked in the proof of Lemma 3.8, we have $|p^{ns}| = p^{n\sigma} \geq p^{(1+\delta)n}$, for $\Re(s) = \sigma \geq 1 + \delta$. Using a geometric series and the fact that $a/2 \leq a - 1$ for $a \geq 2$, we find that

$$\sum_{p \leq M} \sum_{n=1}^{\infty} \frac{1}{np^{-ns}} \leq \sum_{p \leq M} \sum_{n=1}^{\infty} \frac{1}{np^{(1+\delta)n}} \leq \sum_{p \leq M} \sum_{n=1}^{\infty} \left(\frac{1}{p^{1+\delta}} \right)^n = \sum_{p \leq M} \frac{1}{p^{1+\delta} - 1} \leq 2 \sum_{p \leq M} \frac{1}{p^{1+\delta}}.$$

For any $M \in \mathbb{N}$, the sum $\sum_{p \leq M} 1/p^{1+\delta}$ is smaller than $\sum_{n=1}^{\infty} 1/n^{1+\delta}$, which is convergent as mentioned in Lemma 3.8. Taking the limit $M \to \infty$ shows that the series $\log E(s)$ converges absolutely for $\Re(s) \geq 1 + \delta$. This allows us to redefine $E(s)$ as the infinite product

$$E(s) := \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

Once more we write out the geometric series, obtaining

$$\frac{1}{1-p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots ,$$

which we use to expand $\prod_{p \le N} 1/(1-p^{-s})$ by multiplying all terms. For all prime numbers $p_1, \ldots, p_r \le N$ this yields

$$\prod_{p \le N} \frac{1}{1-p^{-s}} = \sum_{\nu_1, \ldots, \nu_r = 0}^{\infty} \frac{1}{(p_1^{\nu_1} \cdots p_r^{\nu_r})^s} = \sum_n{}' \frac{1}{n^s}$$

where $\sum'$ is the sum over all n for which all prime divisors are smaller than N. Clearly, for $n \le N$ all prime divisors are smaller than N, so we get

$$\prod_{p \le N} \frac{1}{1-p^{-s}} = \sum_n{}' \frac{1}{n^s} = \sum_{n \le N} \frac{1}{n^s} + \sum_{n > N}{}' \frac{1}{n^s}.$$

Finally, comparing with $\zeta(s)$ we get

$$\begin{aligned} |\prod_{p \le N} \frac{1}{1-p^{-s}} - \zeta(s)| &= |\sum_{n \le N} \frac{1}{n^s} + \sum_{n > N}{}' \frac{1}{n^s} - \sum_n \frac{1}{n^s}| \\ &\le \sum_{n > N} \frac{1}{n^s} \to 0, \end{aligned}$$

as it is the remainder of a convergent series. □

We consider the behaviour of the function. Specifically, we concern ourselves with *poles.*

Definition 3.10 (Pole, Residue)**.** If a complex function f is analytic on the set $G = \{x \in \mathbb{C} \mid 0 < |c - x| < R\}$ for some $c \in \mathbb{C}$ and $R \in \mathbb{R}$, we may write

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z-c)^n$$

for the *Laurent* series around $c \in \mathbb{C}$ [5, Theorem 9.9, Corollary 9.11]. If for some $n < 0$ we have $a_n \neq 0$, we say f has a *pole* at c with *residue* a_{-1}. If $a_{-1} \neq 0$ and $a_n = 0$ for $n < -1$, the pole is called *simple.*

Remark 3.11. *Lemma 3.9 shows the Riemann zeta function may be written as a product over all primes. It is well known that the $\zeta(s)$ has a pole at $s = 1$. It follows that the product*

$$\prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

cannot be bounded as $s \to 1$. As any finite product is bounded, there are infinitely many prime numbers.

3.2.2. Dirichlet L-series

One generalisation of the Riemann zeta function comes in the form of the Dirichlet L-series. To define it, we first need to discuss the notion of a *Dirichlet character.*

Definition 3.12 (Dirichlet character)**.** Let $m \in \mathbb{N}$. A *Dirichlet character* mod m is a multiplicative homomorphism

$$\chi\colon (\mathbb{Z}/m\mathbb{Z})^* \to S^1 = \{z \in \mathbb{C} \mid |z| = 1\}.$$

A Dirichlet character is called *primitive* if there is no proper divisor $m' \mid m$ such that $a \equiv b \pmod{m'}$ implies $\chi(a) = \chi(b)$. The smallest of such divisors is called the conductor f_χ of χ.

We extend a Dirichlet character χ to all integers, by defining

$$\chi(n) = \begin{cases} \chi(n \bmod m) & \text{for } \gcd(n,m) = 1, \\ 0 & \text{for } \gcd(n,m) \neq 1. \end{cases}$$

Example 3.13. A basic, but important character is the *trivial character* χ^0 mod m. It is the homomorphism $(\mathbb{Z}/m\mathbb{Z})^* \to S^1$ mapping all elements of $(\mathbb{Z}/m\mathbb{Z})^*$ to 1. Extending χ^0 to all integers, we have $\chi^0(n) = 1$ if $\gcd(n,m) = 1$ and $\chi^0(n) = 0$ if $\gcd(n,m) \neq 1$. A special case of the *trivial character* is the *principal character*, where we choose $m = 1$. Therefore the principal character ψ extended to all integers gives the function $\psi(n) = 1$ for all $n \in \mathbb{N}$.

Secondly, consider the following non-trivial example. Define $\chi\colon (\mathbb{Z}/8\mathbb{Z})^* \to S^1$ by $\chi(1) = 1$, $\chi(3) = -1$, $\chi(5) = 1$, $\chi(7) = -1$. Note that χ is a character mod 8. We see that $\chi(a+4) = \chi(a)$, so we may also define χ' as $\chi'(1) = 1$, $\chi(3) = -1$ and consider this character mod 4. By definition, it follows that χ is not a primitive character. As $\chi'(1) \neq \chi'(3)$ and 2 is the only prime divisor of 4, we conclude that χ' is in fact primitive. Consequently $f_\chi = f_{\chi'} = 4$.

Often, we only consider a character mod f_χ for simplicity. Having defined Dirichlet characters, we turn our attention to the Dirichlet L-series.

Definition 3.14 (Dirichlet L-series)**.** Let χ be a Dirichlet character. The Dirichlet L-series corresponding with χ is defined as

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

for complex variable s.

Note that for the principal character $\chi(n) = 1$ for all $n \in \mathbb{N}$, we have $L(s,\chi) = \zeta(s)$. Alternatively, consider the Dirichlet character mod 2 given by $\chi(1) = 1$. Then $L(s,\chi) = \sum_{n \text{ odd}} 1/n^s$.

Like in the case of the Riemann zeta function (see Lemmas 3.8 and 3.9), the Dirichlet L-series can be related to prime numbers.

Lemma 3.15 (Ch.7 Proposition 2.1 of [4])**.** *The series $L(s, \chi)$ converges absolutely and uniformly in the domain $\Re(s) \geq 1 + \delta$, for any $\delta > 0$. It therefore represents an analytic function on the half-plane $\Re(s) > 1$. We have an Euler product expansion*

$$L(\chi, s) = \prod_{p\ prime} \frac{1}{1 - \chi(p)p^{-s}}.$$

3.2.3. Continuing the L-series

This section will follow Chapter 4 of [6]. As seen in Lemma 3.15, the Dirichlet L-series converges on the half-plane $\Re(s) > 1$. However, it may be analytically continued to the entire complex plane if χ is not the principal character. First, we need to introduce another function: the *Gamma function.*

Definition 3.16 (Gamma function)**.** For $\Re(s) > 0$, the *Gamma function* is defined as

$$\Gamma(s) = \int_0^\infty e^{-y} y^{s-1} \, \mathrm{d}y$$

The Gamma function may be continued to a large part of $\mathbb{C}$, but not the entire complex plane. To describe this, we define a function to be *meromorphic* on $\mathbb{C}$ if it is holomorphic on $\mathbb{C}$, except for a set of isolated poles. We may now state the following lemma.

Lemma 3.17 (Ch.7 Proposition 1.2 of [4])**.** *The Gamma function is analytic and admits a meromorphic continuation to $\mathbb{C}$. These poles are located at $s = -n$, for non-negative integers n with corresponding residues $(-1)^n/n!$. It has no poles elsewhere, and it is nowhere zero.*

We now split the L-series into a finite sum of 'shifted zeta functions'. Define the Hurwitz zeta functions as

$$\zeta(s, b) = \sum_{n=0}^{\infty} \frac{1}{(b+n)^s} \qquad \text{for } \Re(s) > 1, \quad 0 < b \leq 1.$$

Let χ be a Dirichlet character with conductor f. Then

$$f^{-s}\zeta(s, a/f) = f^{-s} \sum_{n=0}^{\infty} \frac{1}{(a/f + n)^s} = \sum_{n=0}^{\infty} \frac{1}{(a + nf)^s} = \sum_{n = a \bmod f} \frac{1}{n^s}.$$

By considering classes mod f, we partition $\mathbb{N}$. Furthermore, if $n \equiv m \mod f$, we have $\chi(n) = \chi(m)$, allowing us to extract the factor $\chi(n)$ from the L-series. This means we can write

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{a=1}^{f} \chi(a) f^{-s} \zeta\Big(s, \frac{a}{f}\Big). \tag{3.7}$$

Continuing the L-series now reduces to continuing the Hurwitz zeta function.

Theorem 3.18 (Theorem 4.2 of [6]). *The Hurwitz zeta function, and therefore the Dirichlet L-series, may be analytically continued to $\mathbb{C} \setminus \{1\}$.*

Proof. Let

$$F(t) := \frac{te^{(1-b)t}}{e^t - 1}$$

and define $H(s) := \int_\gamma F(z)z^{s-2}\mathrm{d}z$, where γ is the continuous the path in Figure 3.1, consisting of three parts:

1. The horizontal line $y = \varepsilon/2$ from infinity towards the circle $C(0, \varepsilon)$,
2. Part of the circle $C(0, \varepsilon)$, connecting to both horizontal lines, say from angle φ_ε to $2\pi - \varphi_\varepsilon$ with $\varphi_\varepsilon \to 0$ as $\varepsilon \to 0$,
3. The horizontal line $y = -\varepsilon/2$ from $C(0, \varepsilon)$ towards infinity.

These parts will be referred to as γ_1, γ_2, and γ_3 respectively.

In the definition of $H(s)$, z^s means $e^{s \log z}$, where we define the complex logarithm in terms of the real logarithm as follows: $\log(z) := \log |z| + i \arg(z)$ with $\arg(z) \in (0, 2\pi)$. This choice ensures continuity. For $\Re(s) > 1$ we know that $\zeta(s, b)$ converges by Lemma 3.8.

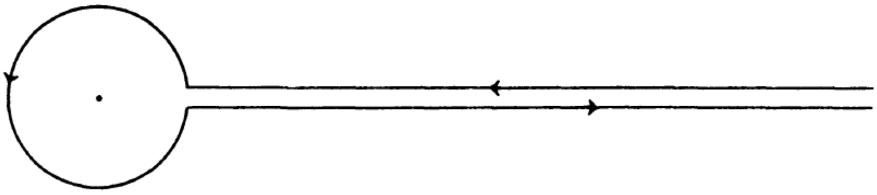


Figure 3.1.: The path of the integral, from [6, p. 33]

We will show that $\zeta(s, b) = H(s)/\big((e^{2\pi is} - 1)\Gamma(s)\big)$ for $\Re(s) > 1$. Furthermore we will show that $H(s)/\big((e^{2\pi is} - 1)\Gamma(s)\big)$ converges for all $s \neq 1$ and therefore provides an analytic continuation to $\mathbb{C} \setminus \{1\}$ of $\zeta(s, b)$.

First of all, note that $F(z)z^{s-2}$ has no poles on γ. Furthermore, $F(t)$ decays exponentially as $t \to \infty$. It follows that $H(s)$ is defined, and analytic for all $s \in \mathbb{C}$. Secondly, consider $s \neq 1$ such that $\Re(s) \leq 1$. The function $\Gamma(s)$ is nowhere zero, and has (simple) poles only at $-n$ for *non-positive* integers n (see Lemma 3.17). However, $e^{2\pi is} - 1$ is zero at $-n$ for integers n and has no poles. The simple poles and zeroes cancel, showing that the denominator of $(e^{2\pi is} - 1)\Gamma(s)$ is analytic and nonzero for $\Re(s) \leq 1$, $s \neq 1$. It follows that $H(s)/((e^{2\pi is} - 1)\Gamma(s))$ is an analytic function on $\mathbb{C} \setminus \{1\}$.

Finally, we show that $\zeta(s, b)$ and the suggested continuation agree for s such that $\Re(s) > 1$. We return to the function $H(s)$ and rewrite it. Let $\Re(s) > 1$. We show that $\int_{\gamma_2} F(z)z^{s-2}\mathrm{d}z \to 0$ as $\varepsilon \to 0$. Note that $F(z)$ is analytic near $z = 0$ as the zero and simple pole cancel. It follows that $F(z)$ is bounded near $z = 0$, say $|F(z)| \leq A \in \mathbb{R}$. We then have

$$\left| \int_{\gamma_2} F(z)z^{s-2}\mathrm{d}s \right| = \left| \int_{\varphi_\varepsilon}^{2\pi - \varphi_\varepsilon} F(\varepsilon e^{i\varphi})(\varepsilon e^{i\varphi})^{s-2}\varepsilon \mathrm{d}\varphi \right| \leq \int_0^{2\pi} A\varepsilon^{s-1}\mathrm{d}\varphi = 2\pi A\varepsilon^{s-1},$$

which goes to 0 as $\varepsilon \to 0$. Now we take the limit $\varepsilon \to 0$, and rewrite the integrals over γ_1 and γ_3, considering their different limits due to the cut in the domain of log at the positive real numbers. This yields

$$H(s) = (e^{2\pi i s} - 1) \int_0^\infty F(t) t^{s-2} \mathrm{d}t, \tag{3.8}$$

as only the parts of γ along the positive real axis remain. Using a geometric series, we may write

$$\sum_{m=0}^{\infty} e^{-(b+m)t} = e^{-bt} \sum_{m=0}^{\infty} e^{-mt} = \frac{e^{-bt}}{1-e^{-t}} = \frac{e^{1-bt}}{e^t - 1} = F(t)/t.$$

Substituting this in (3.8) gives

$$H(s) = (e^{2\pi i s} - 1) \int_0^\infty t^{s-1} \sum_{m=0}^{\infty} e^{-(b+m)t} = (e^{2\pi i s} - 1) \sum_{m=0}^{\infty} \int_0^\infty t^{s-1} e^{-(b+m)t} \mathrm{d}t,$$

where the last equality follows from Fubini's theorem. Applying the substitution $t \mapsto t/(m+b)$, we get

$$(e^{2\pi i s} - 1) \sum_{m=0}^{\infty} \frac{1}{(m+b)^s} \int_0^\infty e^{-t} t^{s-1} \mathrm{d}t,$$

which equals $(e^{2\pi i s} - 1)\Gamma(s)\zeta(s,b)$ by definition. It follows that

$$\zeta(s,b) = \frac{H(s)}{(e^{2\pi i s} - 1)\Gamma(s)}. \tag{3.9}$$

As $H(s)/((e^{2\pi i s} - 1)\Gamma(s))$ is analytic on $\mathbb{C} \setminus \{1\}$, we conclude $\zeta(s,b)$ may be analytically continued to $\mathbb{C} \setminus \{1\}$. Combining (3.7) and the analytic continuation of $\zeta(s,b)$ results in an analytic continuation of $L(s,\chi)$. □

3.2.4. The special values $L(1,\chi)$

Theorem 3.18 shows that the Dirichlet L-series can be analytically continued to $\mathbb{C} \setminus \{1\}$. Naturally, one may ask how the L-series behaves around the point 1. For $\chi = 1$, the trivial character, we have $L(s,\chi) = \zeta(s)$. It is known that $\zeta(s)$ has a pole at $s = 1$, and therefore so does $L(s,\chi)$. For non-trivial characters χ however, the Dirichlet L-series $L(s,\chi)$ may be analytically continued to the entire complex plane [4, Ch.8 Theorem 2.8]. As it turns out, the value $L(1,\chi)$ has some interesting applications. It is used in [1] to derive bounds required for the algorithm described in Section 4.1. Some of those results will be discussed in this section. The value $L(1,\chi)$ can also be used to calculate the class number of a number field, to which we will return in Section 3.3.

First of all, we discuss a two-sided bound on $L(1,\chi)$, which we need in Chapter 4. Before stating the theorem, let us define the following: a character is called *quadratic* if it is non-trivial and real-valued. Note that Dirichlet characters map to roots of unity, and $\{-1,1\}$ are the only real roots of unity.

Theorem 3.19 (Theorem 2.6 of [1])**.** *There exists a universal constant $C > 0$ such that, for any non-quadratic character χ of conductor $f > 1$,*

$$\frac{1}{C \log f} \leq |L(1, \chi)| \leq C \log f.$$

Moreover, for any quadratic character χ,

$$|L(1, \chi)| \geq \frac{1}{C\sqrt{f}}$$

Theorem 3.19 does not extend to the principal character χ^0, as $L(s, \chi^0)$ has a pole at $s = 1$. Improving the constant C is an active field of research [1]. For $\lambda \approx 9.27628$ we have the bound

$$|L(1, \chi)| \geq \frac{1 + o(1)}{\lambda \log(f/\pi)}$$

for non-quadratic primitive Dirichlet characters, where $o(1)$ tends to 0 as the conductor f of χ tends to infinity [7]. It is also possible to express $L(1, \chi)$ directly.

Theorem 3.20 (Theorem 4.9 of [6])**.** *We have*

$$L(1, \chi) = \begin{cases} \pi i \frac{\tau(\chi)}{f^2} \sum_{a=1}^{f} \overline{\chi}(a) a & \text{if } \chi(-1) = -1, \\ -\frac{\tau(\chi)}{f} \sum_{a=1}^{f} \overline{\chi}(a) \log |1 - \zeta_f^a| & \text{if } \chi(-1) = 1, \chi \neq 1, \end{cases}$$

where

$$\tau(\chi) = \sum_{a=1}^{f} \chi(a) e^{2\pi i a/f}.$$

The function τ is called a Gauss sum*.*

If one only wishes to calculate $|L(1, \chi)|$, the expression may be simplified by using the fact that $|\tau(\chi)| = \sqrt{f}$ [6, Lemma 4.8].

3.3. The class number formula

In Section 2.3 we defined the class group (see Definition 2.28). Recall that a fractional ideal of K is a finitely generated $\mathcal{O}_K$-submodule of K (see Definition 2.24). The nonzero fractional ideals form an abelian group, denoted J_K. The class group is defined as $Cl_K = J_K/P_K$ (see Definition 2.28). The order of this group is finite, and is referred to as the *class number* [4, Ch.1 Theorem 6.3]. Even though many class numbers have been calculated, they still appear mostly unpredictable [4, p. 37]. In this section we concern ourselves with calculating class numbers.

First of all, we introduce some notation.

Definition 3.21 (Absolute norm)**.** Let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{O}_K$. We define the *absolute norm* as

$$\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}),$$

the index of $\mathfrak{a}$ in $\mathcal{O}_K$.

The absolute norm is finite [4, Proposition 2.12]. We use the absolute norm to define a function similar to the Riemann zeta function and the Dirichlet L-series: the *Dedekind zeta function.*

Definition 3.22 (Definition 5.1 of [4])**.** The *Dedekind zeta function* of the number field K is defined by the series

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s},$$

where $\mathfrak{a}$ varies over the non-zero ideals of $\mathcal{O}_K$.

Example 3.23. Consider $K = \mathbb{Q}(i)$ with $\mathcal{O}_K = \mathbb{Z}[i]$. Note that $\mathbb{Z}[i]$ is a principal ideal domain. By [4, p. 35], we have $\mathfrak{N}((a+bi)) = N(a+bi) = a^2 + b^2$, where $(a+bi)$ is defined as the principal ideal $(a+bi)\mathbb{Z}[i]$. The sum over all non-zero ideals of $\mathcal{O}_K$ then becomes a sum over all ideals $(a+bi)$ for $a > 0$ or $b > 0$. Therefore we find the Dedekind zeta function

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s} = \sum_{\substack{a,b \geq 0 \\ a>0 \text{ or } b>0}} \frac{1}{(a^2+b^2)^s}.$$

We now return to an arbitrary number field K. The Dedekind zeta function converges absolutely and uniformly for $\Re(s) \geq 1 + \delta$ for every $\delta > 0$ [4, Proposition 5.2], and may be analytically continued to $\mathbb{C} \setminus \{1\}$ [4, Corollary 5.11]. The Dedekind zeta function can be related to the class number using the following formula.

Theorem 3.24 (Class number formula [4, Corollary 5.11])**.** *We have*

$$\operatorname{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|d|}},$$

where r_1 and r_2 are the number of real and complex embeddings of K respectively, h is the class number, R is the regulator, w is the number of roots of unity in K, and d is the discriminant.

The value $\operatorname{Res}_{s=1} \zeta_K(s)$ is related to the special values $L(1, \chi)$ of the Dirichlet L-series. To do this, we first need to associate Dirichlet characters with number fields.

Definition 3.25 (Associated field)**.** Let X be a finite group of Dirichlet characters under multiplication. Let n be the least common multiple of the conductors of the characters in X, and consider each character mod n. Then $\cap_{\chi \in X} \ker \chi$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^* \cong \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. The fundamental theorem of Galois theory guarantees that this subgroup corresponds to a number field K [8, Theorem 2.8.8]. We call K the field *associated with* X.

The following theorem uses the associated field to connect ζ_K and the Dirichlet L-series.

Theorem 3.26 (Theorem 4.3 of [6])**.** *Let X be a group of Dirichlet characters, K the associated field, and $\zeta_K(s)$ the Dedekind zeta function of K. Then*

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi).$$

We can connect the special values $L(1, \chi)$ to the class number formula using Theorem 3.26 [6, p.38]. For χ^0 the principal character, $L(1, \chi^0) = \zeta(s)$ has a simple pole at $s = 1$ with residue 1. Combined with Theorem 3.26 and Theorem 3.24, this gives

$$\prod_{\chi \in X \setminus \{\chi^0\}} L(1, \chi) = \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|d|}},$$

We may also consider the special case where the number field K is a cyclotomic field. In that case we have the following result.

Theorem 3.27 (Ch.1 Proposition 5.12 of [4])**.** *Let $K = \mathbb{Q}(\zeta)$ where ζ is a primitive n-th root of unity. We have*

$$\zeta_K(s) = G(s) \prod_{\chi} L(s, \chi)$$

where χ varies over all characters mod m and

$$G(s) := \prod_{\mathfrak{p} | m} \left(1 - \mathfrak{N}(\mathfrak{p})^{-s}\right)^{-1}$$

where $\mathfrak{p} \mid m$ if and only if $m\mathcal{O}_K \subseteq \mathfrak{p}$.

4. Transforming generators to short generators

Cramer et al. have examined a specific lattice problem, and propose an algorithm designed to solve this problem efficiently on a quantum computer. The algorithm is used to find short generators of principal ideals in certain cyclotomic rings. To define shortness, we need some notion of length in the number field. For this reason, the elements will be embedded in $\mathbb{R}^n$ in a way similar to Section 3.1.1, and use the (Euclidian) norm on this space. Furthermore, it should be noted that principal ideals are understood as principal *fractional* ideals (see Section 2.3) of the form $g\mathcal{O}_K$ for a generator $g \in K$. In this chapter, the number field K will be a cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive m-th root of unity for prime-power $m = p^k$.

4.1. The algorithm

Cramer et al. put forth an algorithm meant for efficiently finding the short generator of a principal ideal, *given that one exists* [1]. This last part is rather important, and distinguishes the problem from its more general counterpart. Formally, the *Short Generator of a Principal Ideal Problem*, abbreviated SG-PIP is described as follows: given a $\mathbb{Z}$-basis of an ideal guaranteed to have a short generator, find any shortest generator of that ideal. As mentioned in [1], this problem is usually broken down in two parts: finding any generator of the ideal — usually named the Principal Ideal Problem (PIP) — and transforming this generator to a short generator. Cramer et al. take on the latter.

First of all, we give a more precise definition to the length of a generator. We represent elements of K by real vectors by considering complex embeddings of K (see Definition 2.16). As K is a cyclotomic field, it has no real embeddings. The complex embeddings come in pairs: if τ is an embedding, so is $\overline{\tau}$, defined by $\overline{\tau}(a) = \overline{\tau(a)}$ for $a \in K$. For this reason we define $G = (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}$, considering only one conjugate embedding from each pair. We identify G with $\{1, \ldots, \phi(m)/2\}$. The number field K is now embedded in $\mathbb{R}^{\phi(m)/2}$ using the map

$$\mathrm{Log}\colon K^* \to \mathbb{R}^{\phi(m)/2}, \quad a \mapsto (\log|\sigma_i(a)|)_{i \in G}. \tag{4.1}$$

Restricting this map to $\mathcal{O}_K^*$ and applying Dirichlet's Unit Theorem (see Theorem 3.2), we find that $\Lambda = \mathrm{Log}(\mathcal{O}_K^*)$ is a lattice in $\mathbb{R}^{\phi(m)/2}$ of rank $\phi(m)/2 - 1$.

Remark 4.1. *As a cyclotomic field has no real embeddings, we have* $\mathrm{Log} = \frac{1}{2}\lambda$*, where* λ *is defined as in (3.1). It then follows from Lemma 3.5 that* Λ *is orthogonal to the all-ones* *vector. We shall refer to Λ as the log-unit lattice. It is nearly equal to the previously defined log-unit lattice (see Definition 3.4), just scaled with factor* $1/2$.

We need the notion of cyclotomic units to properly state the algorithm. Recall we identified G with $\{1, \ldots, \phi(m)/2\}$.

Definition 4.2 (Cyclotomic units)**.** Define the *cyclotomic generators* by

$$b_j := \frac{\zeta^j - 1}{\zeta - 1}, \quad j \in G \setminus \{1\}.$$

Elements of the group generated by the cyclotomic generators and $\pm\zeta$ are called *cyclotomic units.* The group of cyclotomic units is denoted by C.

We now generally describe the algorithm presented by Cramer et al.

Theorem 4.3. *Consider a generator $g' = gu$ for a short generator $g \in K$ and a cyclotomic unit u. There exists an efficient algorithm that given g' finds g with some probability at least $\alpha > 0$, where α is independent of the input generator and unit.*

Before discussing the details of the algorithm, we elaborate on the requirement $g' = gu$. When transforming a generator g to another generator g', we need to make sure they produce the same ideal, i.e. $g\mathcal{O}_K = g'\mathcal{O}_K$. If $g\mathcal{O}_K = g'\mathcal{O}_K$, we may write $g = g'a$ and $g' = gb$ for some $a, b \in \mathcal{O}_K$. Substituting these equations yields $g = gba$ and $g' = g'ab$. As there are no zero divisors in a (cyclotomic) field, we find that $g = g' = 0$ or that a, b are units of $\mathcal{O}_K$. The ideal (0) has only one element, and therefore only one generator, allowing us to claim the following.

Lemma 4.4. *If g and g' are generators of the same principal ideal, then $g' = gu$ for some unit $u \in \mathcal{O}_K^*$.*

Remark 4.5. *Lemma 4.4 shows that $g' = gu$ for a unit $u \in \mathcal{O}_K^*$, while Theorem 4.3 considers a cyclotomic unit $u \in C \subseteq \mathcal{O}_K^*$. However, the algorithm can be extended to cover the general case $u \in \mathcal{O}_K^*$ [1, p.11].*

Applying Log to both sides of the equation $g' = gu$, we get $\mathrm{Log}(g') = \mathrm{Log}(g) + \mathrm{Log}(u)$. We define $\mathbf{b}_j := \mathrm{Log}(b_j)$ for $j \in G \setminus \{1\}$. The vectors $\mathbf{b}_j$ form a basis of the sublattice $\mathrm{Log}(C)$ of the log-unit lattice. To find $\mathrm{Log}(u)$ and reconstruct g, we can use CVP (see Section 2.2). By definition of CVP (see Section 2.2), we have a target $t \in \mathbb{R}^n$, and a lattice $\mathcal{L} \subseteq \mathbb{R}^n$ with basis B. We must find the vector v such that

$$\|v - t\| = \min_{x \in \mathcal{L}} \|x - t\|.$$

In this case we have $t = \mathrm{Log}(g')$, $\mathcal{L} = \mathrm{Log}(C)$, $v = \mathrm{Log}(u)$ and the basis $B = \{\mathbf{b}_2, \ldots, \mathbf{b}_{\phi(m)/2}\}$. An approach to solving CVP is Babai's rounding algorithm, of which we will provide a proof of correctness. To describe it, we must first define *dual* bases.

Definition 4.6. Let $B = \{\alpha_1, \dots, \alpha_n\}$ be a basis of $\mathbb{R}^n$. Then the basis $B^\vee = \{\alpha_1^\vee, \dots, \alpha_n^\vee\}$ satisfying $\langle \alpha_i^\vee, \alpha_j \rangle = \delta_{ij}$ is called the dual basis of B, where δ is the Kronecker delta function and $\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbb{R}^n$. By abuse of notation, we also write $B^\vee$ for the matrix $[\alpha_1^\vee \mid \cdots \mid \alpha_n^\vee]$ where we consider the dual basis vectors as column vectors in $\mathbb{R}^n$.

We will describe Babai's rounding algorithm to solve CVP under certain conditions.

Definition 4.7 (Babai's rounding algorithm)**.** Given a lattice basis $B \subset \mathbb{R}^n$ and a target $t \in \mathbb{R}^n$, return $B \cdot \lfloor (B^\vee)^T \cdot t \rceil$, where $\lfloor \cdot \rceil$ denotes element-wise rounding to the nearest integer.

The algorithm does not necessarily output the right vector for any target and basis. We specify a set of conditions such that Babai's rounding algorithm outputs the right vector, and prove correctness of the algorithm under these conditions.

Lemma 4.8 (Claim 2.1 of [1])**.** *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice with basis $B = \{\alpha_1, \dots, \alpha_m\}$, and let $t = v + e \in \mathbb{R}^n$ for some $v \in \mathcal{L}, e \in \mathbb{R}^n$. If $-\frac{1}{2} \leq \langle \alpha_j^\vee, e \rangle < \frac{1}{2}$ for all j, then on input t and basis B, Babai's rounding algorithm outputs v.*

Proof. As $v \in \mathcal{L}$, we know $v = Bz$ for an integer vector z. Then $(B^\vee)^T \cdot t = z + (B^\vee)^T \cdot e$ as $(B^\vee)^T B = I$. Note that

$$(B^\vee)^T \cdot e = \begin{pmatrix} \langle \alpha_1^\vee, e \rangle \\ \vdots \\ \langle \alpha_m^\vee, e \rangle \end{pmatrix},$$

so $\lfloor (B^\vee)^T \cdot t \rceil = z$ as the assumption on $\langle \alpha_j^\vee, e \rangle$ ensures correct rounding. Then

$$v = Bz = B \cdot \lfloor (B^\vee)^T \cdot t \rceil$$

shows that Babai's rounding algorithm outputs v. □

In our specific case, we must have $|\langle \mathbf{b}_j^\vee, \mathrm{Log}(g) \rangle| < \frac{1}{2}$. Clearly this bound depends on the norm of the dual basis vectors $\mathbf{b}_j^\vee$. For the next theorem, recall that we are working in the number field $\mathbb{Q}(\zeta)$, where m is the order of ζ.

Theorem 4.9 (Theorem 3.1 of [1])**.** *Let $m = p^k$ for a prime p, and let $\{\mathbf{b}_j^\vee\}_{j \in G \setminus \{1\}}$ denote the basis dual to $\{\mathbf{b}_j\}_{j \in G \setminus \{1\}}$. Then all $\|\mathbf{b}_j^\vee\|$ are equal, and*

$$\|\mathbf{b}_j^\vee\|^2 = O(m^{-1} \cdot \log^3 m).$$

We can now state the algorithm in full.

```
Data: A generator $g' = gu$ for some short generator $g$ and cyclotomic unit $u$
Result: A short generator of $g\mathcal{O}_K$ of the form $\pm\zeta^j g$
Apply Babai's rounding algorithm to $\mathrm{Log}(g')$ with basis $\mathbf{b}_j$ for $j \in G \setminus \{1\}$ and
  name the output $v$.
Find integer coefficients such that $v = \sum a_j \mathbf{b}_j$.
Compute $u' = \prod b_j^{a_j}$.
Output $g'/u'$.
```

Algorithm 2: An algorithm to transform an arbitrary generator to a short generator [1, Theorem 4.1].

An implementation of Algorithm 2 in Python can be found in Appendix A. It is important to note that the output of the algorithm is not necessarily correct for any input $g' = gu$. However, sampling g using a certain probability measure ensures the algorithm succeeds with some non-zero probability, as stated in the following theorem.

Theorem 4.10 (Theorem 4.1 of [1])**.** *There exists a constant $c > 0$ such that the following property holds. Let D be a probability measure over $\mathbb{Q}(\zeta)$ such that for any tuple of vectors $v_1, \ldots, v_{\phi(m)/2-1} \in \mathbb{R}^{\phi(m)/2}$ of Euclidean norm 1 that are orthogonal to the all-ones vector, the probability that $|\langle \mathrm{Log}(g), v_i \rangle| < c\sqrt{m} \cdot (\log m)^{-3/2}$ holds for all i is at least some $\alpha > 0$. If we choose g from D and let u be a cyclotomic unit, Algorithm 2 succeeds with probability at least α.*

Proof. The algorithm applies the rounding algorithm from Definition 4.7 to $\mathrm{Log}(g') = \mathrm{Log}(g) + \mathrm{Log}(u)$, using the vectors $\mathbf{b}_j$ as the basis. By the assumption on D and Theorem 4.9, with probability at least α the output is $\mathrm{Log}(u) \in \mathrm{Log}(C)$. We next find integer coefficients a_j such that $\mathrm{Log}(u) = \sum a_j \mathbf{b}_j$, and compute $u' = \prod b_j^{a_j}$. Since $\mathrm{Log}(u') = \mathrm{Log}(u)$ it follows that u' must be of the form $\pm\zeta^j u$ for some sign and some j. Therefore, g'/u' is the desired element. □

4.2. Implementing the algorithm

Algorithm 2 can be used to find a short generator of a principal ideal, when an arbitrary generator is known. In this section, an implementation of the algorithm is discussed. The corresponding code can be found in Appendix A. Any references to line numbers refer to Appendix A too.

Recall that we are working in the number field $\mathbb{Q}(\zeta)$, where ζ is a primitive m-th root of unity. Note that we must be able to calculate the embedding of number field elements as described in (4.1) To do this computation, all embeddings of an element are kept track of during the entire execution. For example, consider line 21, where ζ is defined. In the code, it is an array of embeddings of the form $(\sigma_i(\zeta))_{i \in G}$, similar to (4.1). The function *log_embed* in line 14–15 then computes the map

$$(\sigma_i(a))_{i \in G} \to (\log |\sigma_i(a)|)_{i \in G} = \mathrm{Log}(a).$$

As σ_i is a homomorphism, we can first embed an element, and then perform computations on it. This order of operations ensures that we only need to know the image of the embedding for a select number of elements — in our case just the image of ζ.

Let us now turn our attention to the constants defined in line 17–26. First of all, note that m in line 17 is the order of ζ. In line 18–20, $(\mathbb{Z}/m\mathbb{Z})^*$, $\phi(m)$ and $G = (\mathbb{Z}/m\mathbb{Z})^* \cap \{1, \ldots, \phi(m)/2 - 1\}$ are calculated. We define the generators of the cyclotomic units, variable b in line 23. Mathematically, these generators are defined as

$$b_j = \frac{\zeta^j - 1}{\zeta - 1} \quad \text{for } j \in G \setminus \{1\}.$$

Note that as we are keeping track of embeddings using arrays, the variable b is a two-dimensional array. Lemma 4.4 shows that generators of the same principal ideal differ by a unit. In this program, this unit is fixed and defined as $u = b_2$ in line 24. Finally, we embed the cyclotomic generators, yielding the basis B in line 25, and compute its dual basis $B^\vee$, the variable D in line 26.

The main loop of the program consists of randomly drawing a generator g from $\mathbb{Q}(\zeta)$, calculating $g' = gu$, and trying to retrieve a short generator by running the algorithm. It runs 10000 times, and the frequency of success is output on termination. The generator g is drawn by calculating

$$g = \sum_{i=0}^{\phi(m)-1} a_i \zeta^i,$$

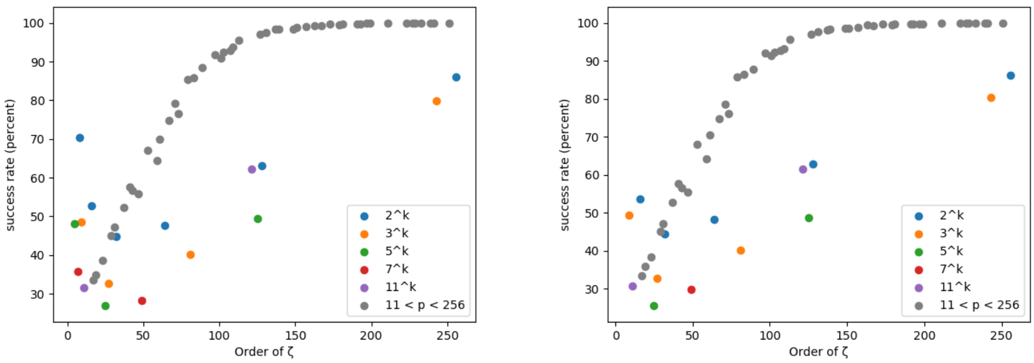
where a_i is randomly sampled from a standard Gaussian distribution ($\mu = 0$, $\sigma = 1$). This calculation is performed in line 28–30, and called in line 39. Sampling is done in line 38. Algorithm 2 runs in line 42–45. Babai's algorithm can be found in line 42 of the program, calculating

$$u_{\text{guess}} = B \cdot \lfloor (B^\vee)^T \cdot g' \rceil.$$

Line 43 is used to find integer coefficients such that $u_{\text{guess}} = \sum_{j \in G} a_j b_j$. Finally, we calculate $u' = \prod_{j \in G} b_j^{a_j}$ and $g_{\text{guess}} = g'/u'$. The resulting element g' is the output of the algorithm, and according to Theorem 4.10, a short generator with some probability. Note that u' is a cyclotomic unit, and thus g'/u' and g generate the same ideal. Therefore we only need to verify that g_{guess} is indeed short.

4.3. Numerical results

In this section, we share some numerical results from Algorithm 2 as implemented in Appendix A. Recall that we are working in the cyclotomic field $K = \mathbb{Q}(\zeta)$, where ζ is a primitive m-th root of unity for $m = p^k$ for p prime and $k \in \mathbb{N}$. For a fixed cyclotomic unit, we consider every prime-power m such that $5 \leq m < 256$, and retrieve the percentage of cases where the algorithm successfully finds a short generator. A scatter plot showing the resulting data can be found in Figure 4.1. The data does not appear to change when considering either $u = b_2$ or $u = b_3$. It is interesting to note that the success rate rapidly goes to 100% for prime m. Even for non-prime m, the success rate appears to rise for larger m. The precise relation between m and the success rate may be interesting for further research.



(a) Fixed cyclotomic unit $u = b_2$. Raw data can be found in Table B.1.

(b) Fixed cyclotomic unit $u = b_3$. Raw data can be found in Table B.2.

Figure 4.1.: The success rate of Algorithm 2 implemented as in Appendix A when varying the order $m = p^k$ of the root of unity ζ.

4.4. Soliloquy

Soliloquy is a key-encapsulation mechanism, developed as a possibly quantum-resistant protocol [2]. A key-encapsulation mechanism is similar to a public-key encryption scheme (see Definition 2.2). Instead of encrypting messages, a key is encrypted using the scheme and sent to the other party. This shared secret key may then be used for further secure communication. Soliloquy has since been shown [2, 9] to be insecure. In particular, the scheme is vulnerable to a key-recovery attack using a quantum algorithm and Algorithm 2. In this section, we shall first define what the scheme is, and show how it may be used to encrypt and decrypt messages. Similar to Chapter 4, we consider the number field $K = \mathbb{Q}(\zeta)$, where ζ is a primitive n-th root of unity for prime n. Recall that $K = \mathbb{Q}(\zeta)$ has ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

The description of Soliloquy in this section follows [2]. First of all, we define the key generation algorithm. For $i \in \{1, \ldots, n\}$, let a_i be sampled independently from a discrete Gaussian distribution of mean 0 and width σ. We construct

$$\alpha := \sum_{i=1}^{n} a_i \zeta^i \in \mathcal{O}_K. \tag{4.2}$$

and define

$$p := \prod_{\sigma} \sigma(\alpha),$$

where σ ranges over all embeddings $K \to \mathbb{C}$. To be a valid Soliloquy key, p must be prime and satisfy

$$c := 2^{(p-1)/n} \neq 1 \mod p. \tag{4.3}$$

If these conditions are not satisfied, the coefficients are resampled. Condition (4.3) ensures that c is a non-trivial n-th root of unity. Most importantly, the Dedekind–Kummer theorem [10, Theorem B] states that we have the equation

$$\alpha\mathcal{O} = p\mathcal{O} + (\zeta - c)\mathcal{O}.$$

The private and public key are given by the element α and p respectively. Having defined the key, we turn our attention to encapsulating message. We generate a small element

$$\varepsilon := \sum_{i=1}^{n} e_i \zeta^i \in \mathcal{O}_K$$

by sampling the coefficients e_i from a discrete Gaussian of mean 0 and width σ'. This element ε is then encapsulated by computing

$$z := \sum_{i=1}^{n} e_i c^i \mod p$$

and considering it as an integer $0 \leq z < p$ in $\mathcal{O}_K$. Essentially, we compute $z := \varepsilon \mod \alpha\mathcal{O}_K$. This means that $z - \varepsilon = 0 \mod \alpha\mathcal{O}_K$. We may actually view finding ε as an instance of CVP (see Section 2.2), as non-zero ideals form lattices when embedded [4, Ch.1 Proposition 5.2] The receiver knows a relatively short generator α for the ideal, and may use the basis defined by the cyclic matrix

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & a_3 & \cdots & a_0 & a_1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{pmatrix},$$

where the a_i denote the coefficients from (4.2). As α is relatively small, this is a good enough basis to use Babai's rounding algorithm to solve CVP, revealing ε.

Next, we shall discuss the key-recovery attack on Soliloquy. Note that p, n, ζ and c are public, allowing an attacker to compute the ideal $\alpha\mathcal{O} = p\mathcal{O} + (\zeta - c)\mathcal{O}$. As the ideal $\alpha\mathcal{O}$ is known to the attacker, recovering the private key α has been reduced to solving SG-PIP for the ideal $\alpha\mathcal{O}$. There exists a technique to efficiently find an arbitrary generator using a quantum computer [9]. Finally, Algorithm 2 may be used to efficiently transform the arbitrary generator to a short generator, revealing the private key.

5. Conclusion

Cryptography is an important part of secure communication, and our current methods are threatened by the advent of the quantum computer. This thesis looks into an attack on cryptographic schemes relying on the SG-PIP problem (see Section 4.1). Furthermore, interesting results in algebraic number theory are explored.

In Chapter 2, we define public-key encryption schemes and one notion of security for such schemes. We note that schemes cannot be considered secure when vulnerable to key-recovery attacks, as is the case with Soliloquy, which is discussed in Section 4.4. We define lattices, which are considered as a possible foundation for post-quantum cryptography. In particular, the shortest vector problem (SVP) and the closest vector problem (CVP) are described. Furthermore we outline some basic algebraic number theory, which is required for analysis of the algorithm and further mathematical results.

We discuss mathematical results from algebraic number theory in Chapter 3. First of all, we define how number fields may be embedded into $\mathbb{R}^n$. Using this embedding, we define the log-unit lattice, which explicitly connects number fields and cryptography on lattices. Furthermore, the Riemann zeta function and the more general Dirichlet L-series are discussed. Convergence and analytic continuations are discussed in Section 3.2.4. We show the Riemann zeta function may be written in terms of all primes numbers, and note that a similar result holds for the Dirichlet L-series. Lastly, we discuss the class number formula and its relation to the special values $L(1, \chi)$.

In Chapter 4, we discuss an algorithm presented by Cramer et al. for transforming generators of fractional principal ideals. The details of the algorithm are explained in Section 4.1 We implement the algorithm and show the results in Sections 4.2 and 4.3. Our results show that the success rate grows quickly as the order of the cyclotomic field increases. An analysis showing why this is the case could be a topic for further research. Finally we discuss Soliloquy, a particular cryptographic scheme which is vulnerable to a key-recovery attack as it relies on SG-PIP.

Bibliography

[1] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. *Recovering Short Generators of Principal Ideals in Cyclotomic Rings.* Cryptology ePrint Archive, Report 2015/313. `https://eprint.iacr.org/2015/313`. 2015.

[2] Peter Campbell, Michael Groves, and Dan J. Shepherd. *Soliloquy: a Cautionary Tale.* `https://docbox.etsi.org/workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf`. 2014.

[3] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography.* 2nd ed. Chapman and Hall/CRC, 2014. ISBN: 978-1-4665-7026-9.

[4] Jürgen Neukirch. *Algebraic Number Theory.* Springer-Verlag Berlin Heidelberg, 1999. ISBN: 978-3-540-65399-8. DOI: `10.1007/978-3-662-03983-0`.

[5] Joseph Bak and Donald J. Newman. *Complex Analysis.* Springer-Verlag New York, 2010. ISBN: 978-1-4419-7287-3. DOI: `10.1007/978-1-4419-7288-0`.

[6] Lawrence C. Washington. *Introduction to Cyclotomic Fields.* Springer-Verlag New York, 1997. ISBN: 978-0-387-94762-4. DOI: `10.1007/978-1-4612-1934-7`.

[7] Stéphane R. Louboutin. „An explicit lower bound on moduli of Dirichlet L-functions at $s = 1$". In: *J. Ramanujan Math. Soc.* 30.1 (2015), pp. 101–113. ISSN: 0970-1249.

[8] Steven Weintraub. *Galois Theory.* Springer-Verlag New York, 2006. ISBN: 978-0-387-28917-5. DOI: `10.1007/0-387-28917-8`.

[9] Jean-François Biasse and Fang Song. *On the quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in $\mathbb{Q}(\zeta_{p^n})$.* Tech. rep. Technical report, Tech Report CACR 2015-12, 2015.

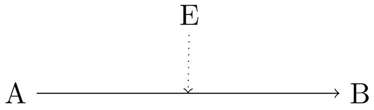
[10] Sudesh K. Khanduja and Munish Kumar. „On a Theorem of Dedekind". In: *International Journal of Number Theory* 04.06 (2008), pp. 1019–1025. DOI: `10.1142/S1793042108001833`. eprint: `https://doi.org/10.1142/S1793042108001833`.

Populaire samenvatting

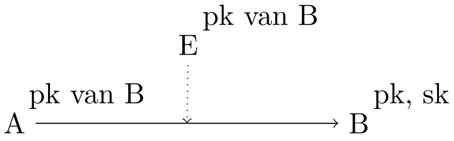
Cryptografie is zeer belangrijk in onze moderne wereld, maar toch vaak onzichtbaar. Dagelijks gebruikt iedereen vele malen toepassingen van cryptografie voor verschillende vormen van veilige en confidentiële communicatie. Berichten die via bijvoorbeeld Whatsapp of Signal verstuurd worden, zijn versleuteld en dus onleesbaar voor iedereen behalve zender en ontvanger. Ook zorgt cryptografie ervoor dat we veilig kunnen internetbankieren en helpt het computers te beschermen tegen bepaalde aanvallen door de identiteit van de andere partij te verifiëren. Kortom, zonder cryptografie zou onze communicatie een stuk minder veilig verlopen.

Public-key cryptografie

We zullen hier kort het principe van *public-key* cryptografie weergeven, wat bijvoorbeeld gebruikt wordt bij het surfen op het internet. In dit geval hebben we een persoon A die een bericht probeert te sturen naar persoon B. Er is echter een derde persoon E, die de communicatie afluistert. Deze situatie is geschetst in Figuur P1. Van tevoren heeft persoon B al een paar sleutels gegenereerd: de *public key* pk en de *secret key* sk. Alleen persoon B heeft de secret key, maar iedereen heeft de public key. Persoon A versleutelt een bericht met de public key, en stuurt het versleutelde bericht naar B. Dit versleutelde bericht kan nu alleen met de secret key ontsleuteld worden, dus persoon E kan de inhoud van het bericht niet zien. Als het bericht bij B is aangekomen, kan deze het bericht met de secret key ontsleutelen.



Figuur P1.: De setting van public-key cryptografie. Persoon A stuurt een bericht naar persoon B, terwijl E de communicatie onderschept.



Figuur P2.: De setting van public-key cryptografie (zie Figuur P1) waar de sleutels zijn aangegeven.

RSA

Een concreet voorbeeld van een dergelijk schema is RSA, waarvan we een versimpeld voorbeeld zullen laten zien. Hiervoor hebben we het concept van modulo rekenen nodig, wat we kunnen vergelijken met uren op de klok. Om 14:00 is het twee uur, en om 15:00 is het drie uur. Wat we hier wiskundig doen, is 12 aftrekken van het getal totdat we een getal tussen 0 en 11 krijgen. We schrijven $14 \mod 12 = 2$ en $15 \mod 12 = 3$. Natuurlijk kunnen we dit ook voor andere getallen dan 12 doen, bijvoorbeeld $11 \mod 7 = 4$ en $17 \mod 7 = 3$.

We beschrijven vervolgens de werking van RSA. persoon B genereert getallen N, e, d die aan bepaalde voorwaarden voldoen. De public key bestaat uit de getallen N en e, dus deze zijn bij iedereen bekend. Alleen persoon B heeft naast N en e ook de secret key d.

Als een voorbeeld nemen we $N = 77$, $e = 13$, $d = 37$. We kunnen op deze manier alleen getallen versturen, maar met uitgebreidere technieken kunnen we ook tekst versturen. Persoon A versleutelt het bericht $m = 5$ door $c = m^e \mod N = 5^{13} \mod 77 = 1220703125 \mod 77 = 26$ uit te rekenen. Vervolgens stuurt A het versleutelde bericht $c = 26$ naar B. Tenslotte ontsleutelt B het bericht door $m = c^d \mod N = 26^{37} \mod 77 = 5$ uit te rekenen. Op deze manier ontvangt B het bericht van A, zonder dat E het heeft kunnen lezen.

De scriptie

Quantumcomputers kunnen RSA en soortgelijke constructies eenvoudig kraken. Hoewel er op dit moment nog geen voldoende grote quantumcomputers zijn om dit daadwerkelijk te doen, is het wel van belang nieuwe cryptografie te ontwikkelen die toekomstbestendig is. Een van de mogelijkheden is de zogenaamde *lattice-based* cryptografie. In deze scriptie laten we een algoritme zien dat ook bepaalde lattice-based cryptografie kan kraken door de secret key te berekenen. Zo kan iedereen de versleutelde berichten weer ontsleutelen, dus is het systeem niet veilig. Verder wordt de wiskundige achtergrond van deze cryptografie besproken, de algebraïsche getaltheorie. Ook worden een aantal andere resultaten uit de algebraïsche getaltheorie besproken.

A. Code

```python
#! /usr/bin/env python3
from fractions import gcd
from random import gauss
import numpy as np
import numpy.linalg

def naiveEuler(n):
    elements = np.empty(0)
    for x in range(1,n):
        if gcd(x,n) == 1:
            elements = np.append(elements, x)
    return elements

def log_embed(el):
    return np.log(np.abs(el))

m = 125 #The order of the primitive root of unity
elements = naiveEuler(m)
phi_m = len(elements)
G = elements[:int(phi_m/2)]
zeta = np.power(np.exp(2j * np.pi / m), G)
# generators cyclotomic units, first coordinate is j, second is embedding
b = (np.power(zeta, G[1:].reshape((len(G)-1,1))) - 1)/(zeta - 1)
u = b[0] # b[0] = b_2, b[1] = b_3
B = log_embed(b.T)
D = np.matmul(B, np.linalg.inv(np.matmul(B.T, B))) #Dual basis

def coef_to_el(coef_list):
    return np.matmul(coef_list,
                         np.power(zeta, np.arange(0,phi_m).reshape((phi_m,1))))

count = 0
num_it = 10000
for iteration in range(num_it):
    if iteration % (num_it/10) == 0:
        print(iteration)
    #Calculate a linear combination with random coefficients
    rand = [gauss(0,1) for _ in range(phi_m)]
    g = coef_to_el(rand)
    gprime = g * u
    #Use Babai's algorithm to find Log(u) and construct short generator
    log_u = np.matmul(B, np.around(np.matmul(D.T, log_embed(gprime))))
    a = np.round(np.linalg.lstsq(B, log_u)[0])
    uprime = np.prod(np.power(b, a.reshape((len(a),1))), axis=0)
    g_guess = gprime / uprime
    if np.linalg.norm(log_embed(g) - log_embed(g_guess)) < 1e-12:
        count += 1
print('Success rate: {}%'.format(count / num_it * 100))
```

B. Data

Order of ζ	Success (%)
8	70.37
16	52.74
32	44.76
64	47.69
128	63.20
256	86.13
9	48.45
27	32.74
81	40.22
243	79.87
5	48.02
25	26.90
125	49.53
7	35.83
49	28.25
11	31.47
121	62.19
17	33.50
19	34.89
23	38.64
29	44.94
31	47.32
37	52.35
41	57.65
43	56.63
47	55.75
53	67.16
59	64.38
61	69.88
67	74.77
71	79.25
73	76.66
79	85.44
83	85.83
89	88.48
97	91.87
101	90.82
103	92.49
107	92.86
109	93.87
113	95.42
127	97.15
131	97.60
137	98.29
139	98.30
149	98.50
151	98.84
157	99.03
163	99.38
167	99.31
173	99.68
179	99.49
181	99.62
191	99.78
193	99.78
197	99.85
199	99.86
211	99.93
223	99.94
227	99.94
229	99.95
233	99.98
239	99.97
241	99.98
251	99.98

Table B.1.: Data retrieved as explained in Section 4.3, using the fixed cyclotomic unit b_2.

Order of ζ	Success (%)
16	53.74
32	44.42
64	48.29
128	62.80
256	86.21
9	49.33
27	32.64
81	40.20
243	80.35
25	25.49
125	48.75
49	29.91
11	30.61
121	61.63
17	33.52
19	35.81
23	38.45
29	45.12
31	47.20
37	52.69
41	57.72
43	56.53
47	55.50
53	68.07
59	64.19
61	70.52
67	74.72
71	78.61
73	76.06
79	85.75
83	86.51
89	87.74
97	92.03
101	91.35
103	92.35
107	92.81
109	93.18
113	95.77
127	97.15
131	97.82
137	98.17
139	98.31
149	98.54
151	98.60
157	98.93
163	99.44
167	99.23
173	99.67
179	99.57
181	99.71
191	99.80
193	99.80
197	99.81
199	99.84
211	99.92
223	99.95
227	99.96
229	99.97
233	99.96
239	99.99
241	99.95
251	100.0

Table B.2.: Data retrieved as explained in Section 4.3, using the fixed cyclotomic unit b_3.