ANALYSIS OF ALGORITHMS IN NUMBER THEORY PROBLEM SESSION

ASIMINA S. HAMAKIOTES

These are exercises written for the 2026 Arizona Winter School on Computational Aspects of Arithmetic Geometry and Cryptography. This problem set does not belong to any of the 2026 AWS lecture series in particular; however, the goal of these exercises is to familiarize the reader with analysis of algorithms in number theory, which is an important topic of the 2026 AWS.

The reader is not expected to complete the entire problem set in the duration of five days. The exercises cover a broad range of difficulty, so the reader should feel free to jump around and do whichever exercises that are helpful. Some problems are meant to help the reader learn a concept, while other problems are meant to challenge the reader who already knows the topic. In each section, the exercises are loosely in ascending order of difficulty.

Most of these questions appeared in the problem sets for the 2025 Preliminary Arizona Winter School (PAWS) on Mathematical cryptography and algorithms in number theory. The problems accompanied Juanita Duque-Rosero's lectures on the analysis and implementation of algorithms in number theory. You can find videos and notes from those lectures on the PAWS website.

1. Computational Problems

In this section, there are two long exercises designed to introduce the reader to using Magma. Magma is a software package designed for computations in algebra, number theory, algebraic geometry, and algebraic combinatorics. It is a great tool for implementing number theoretic algorithms. A free online calculator for short computations is available here. You are welcome to use Magma or your favorite computer algebra system for the problem set.

Exercise 1.1. This first exercise (designed by Duque-Rosero) is a short scavenger hunt to get you started as a new Magma user. Some resources are: first steps in Magma, general examples, and handbook. Duque-Rosero has also compiled a list of random Magma tricks she likes to use.

(a) Start with $A := 55489564$.
(b) Let B be the largest prime factor of A.
(c) Define C as the discriminant of the polynomial $x^3 + x + B \in \mathbb{Q}[x]$.
(d) The number D is the class number of the quadratic field $\mathbb{Q}(\sqrt{C})$.
(e) Construct the elliptic curve $E\colon y^2 + xy + y = x^3 - x^2 - 96x + D$ over $\mathbb{Q}$.
(*Hint:* you can define an elliptic curve in Magma using `EllipticCurve([a,b,c,d,e]);`. Find out what the appropriate values of the elements in the list are.)
(f) Let F be the rank of E.
(g) Define G as the conductor of E.
(h) By adding one digit of G at a time from right to left, how many of the intermediate numbers you form are a prime numbers? Let H be this quantity. For example, 103 gives 3 prime numbers: 3, 03, and 103.
(i) Define $I := \mathbb{Q}(\zeta_H)$ as the cyclotomic field where ζ_H is a primitive H-th root of unity.
(j) Find the trace of $\zeta_H + 2 \in I$ and call it J.
(k) Let K be the number of elements $\zeta_H + x \in I$ have norm at most 700 for $x \in [1, \ldots, 100]$.

(l) Find L, the list of prime numbers up to 100 (ordered in increasing order) that split in the field $I = \mathbb{Q}(\zeta_H)$.
(m) The number M is the third element of L.
(n) Now change the base field of the elliptic curve E from $\mathbb{Q}$ to $I = \mathbb{Q}(\zeta_H)$. Let N denote the number of points on E up to naive height bound of 20 whose coordinates lie in $\mathbb{Q}(\zeta_H)$ but not in $\mathbb{Q}$.

Where does Magma live?

M - K - F - N - J - K

Exercise 1.2. Using Magma, complete the following:

(a) Factor the polynomial $x^6 - 1$ over $\mathbb{Q}$, and then over $\mathbb{F}_7$. Over which field does it have more irreducible factors? Can you explain why?
(b) How many monic irreducible univariate polynomials of degree 4 are there over $\mathbb{F}_5$?
(c) Up to isomorphism, how many subfields does $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ have? Can you check that the strict subfields among these are isomorphic to $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{6})$, and $\mathbb{Q}(\sqrt{3})$?
(c) Create the ring $L = \mathbb{Z}[x]/(x^2 + 1)$. What is the value of x in L? Of x^4?
(d) Consider the matrix $M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ over $\mathbb{F}_5$. What are its rank, trace, and determinant? What are its minimal and characteristic polynomials? What is its order in $\mathrm{GL}_2(\mathbb{F}_5)$?

2. Background Material

In this section, we will see exercises related to complexity, field extensions, and Galois groups, which serve as background for understanding exercises in later sections.

Definition 2.1. Let $f(n)$ and $g(n)$ be functions defined on the natural numbers. We say that $f(n)$ *is big-O of* $g(n)$, and write

$$f(n) = O(g(n)),$$

if there exist constants $C > 0$ and $n_0 \in \mathbb{N}$ such that, for all $n \geq n_0$,

$$|f(n)| \leq C\,|g(n)|.$$

Exercise 2.1. Prove that for all $x \in \mathbb{R}_{>0}$, we have $\ln(x) \leq x$. (*Hint:* you can differentiate)

Exercise 2.2. Prove that

$$\frac{x}{\ln(x)} \to +\infty \quad \text{as} \quad x \to +\infty.$$

(*Hint:* you can use Exercise 2.1 and the equality $\ln(x) = 2\ln(\sqrt{x})$.)

Exercise 2.3. Using a change of variables, compute the following limit:

$$\lim_{x \to +\infty} \frac{x \ln(x)}{x \ln(\ln(x))}.$$

Exercise 2.4. Select the dominant term(s) having the steepest increase in n to simplify the following expressions. For example: $O(10n + n^2) = O(n^2)$.

(a) $O(100n + 0.01n^2)$
(b) $O(0.01n + 100n^2)$
(c) $O(n^2 \ln(\ln(n)) + n \ln(n))$
(d) $O(n^2 + n\sqrt{n})$
(e) $O(100n \log_3 n + n^3 + 100n)$
(f) $O(0.003 \log_4 n + \log_2 \log_2 n)$

Definition 2.2. Let L/K be a field extension. We denote by $[L : K] = \dim_K(L)$ the *degree* of the extension L/K. When $[L : K]$ is finite, we say that L/K is a *finite field extension*. In that case, for any $\alpha \in L$, we call *minimal polynomial* of α the unique monic polynomial $m_\alpha \in K[x]$ of smallest degree such that $m_\alpha(\alpha) = 0$.

Exercise 2.5. Determine the minimal polynomial of the following:

(a) $1 + i$ over $\mathbb{Q}$.
(b) $1 + i$ over $\mathbb{Q}(i)$.

Exercise 2.6. Consider the field extensions $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

(a) Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Conclude that $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$.
(*Hint:* one inclusion is obvious, for the other consider $(\sqrt{2} + \sqrt{3})^2$, etc.)
(b) Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.
(c) Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$.

Definition 2.3. Let K be a field. A *splitting field* of $f \in K[x]$ is a field extension L/K of smallest degree such that f factors as linear in L as a product of linear factors.

Exercise 2.7. Determine the splitting field and its degree over $\mathbb{Q}$ for:

(a) $x^4 - 2$.
(b) $x^4 + x^2 + 1$.

Exercise 2.8. Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$.

Exercise 2.9. Determine the Galois group of the splitting field of $f \in \mathbb{Q}[x]$ over $\mathbb{Q}$ of the following polynomials:

(a) $f(x) = x^8 - 3$.
(b) $f(x) = x^4 - 14x^2 + 9$.
(c) $f(x) = x^4 - 7$.

Exercise 2.10. Let $n \in \mathbb{Z}_{>0}$.

(a) Prove that $\cos(\frac{2\pi}{n})$ and $\sin(\frac{2\pi}{n})$ are algebraic over $\mathbb{Q}$.
(b) Compute $[\mathbb{Q}(\cos(\frac{2\pi}{9}) : \mathbb{Q}]$.
(c) Show that $\mathbb{Q}(\cos(\frac{2\pi}{n}))/\mathbb{Q}$ is Galois.
(d) Is $\mathbb{Q}(\sin(\frac{2\pi}{n}))/\mathbb{Q}$ a Galois extension in general?

3. Arithmetic and Linear Algebra

In this section, we will get more comfortable with $O(n)$ notation and practice systematically thinking about algorithms. We will also review and use some linear algebra and Magma! Lecture 1 from the 2025 PAWS course on analysis and implementation of algorithms in number theory will serve as a good reference for working on these exercises.

Lemma 3.1. *Let $f(n)$, $g(n)$, $a(n)$, and $b(n)$ be functions satisfying $f(n) = O(g(n))$ and $a(n) = O(b(n))$. Then*

$$f(n) + a(n) = O\big(\max(|g(n)|, |b(n)|)\big)$$

and

$$f(n)a(n) = O\big(g(n)b(n)\big).$$

Exercise 3.1. Prove Lemma 3.1.

Algorithm 1 Euclidean Algorithm for gcd

Given integers $a \geq b > 0$, compute $g := \gcd(a, b)$.

1. Set $r_0 := a$ and $r_1 := b$.
2. Set $i := 1$ and while $r_i \neq 0$, do the following
   (a) Set $r_{i+1} := \mathrm{rem}(r_{i-1}, r_i)$ and $i := i + 1$.

Return r_{i-1}.

Exercise 3.2. Explain why Algorithm 1 terminates and correctly computes the greatest common divisor.

Exercise 3.3. Write and analyze an algorithm that implements naive multiplication for integers. What is the complexity of your algorithm, in terms of the number of bits m and n of the integers you are multiplying?

Exercise 3.4. Let $M = \begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 4 & 16 \end{pmatrix}$. Using Gaussian elimination-like algorithms, compute (first by hand and then with Magma to check your results):

(a) all possible solutions to $MX = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$,
(b) its determinant,
(c) its inverse if it exists.

Exercise 3.5. Describe the classical long division algorithm for binary integers. Prove that the complexity of your algorithm is $O((n - m)m)$, where m and n are the number of bits of the integers.

Exercise 3.6. Use Exercise 3.3 and 3.5 to prove that the Euclidean Algorithm (Algorithm 1) for positive integers a, b with n, m bits, respectively, has complexity $O(mn)$.

Exercise 3.7. Compute a function $f(n)$ such that $O(f(n))$ represents the number of field multiplications needed to compute the product of two square $n \times n$ matrices. Why do we not care about the number of addition operations?

Exercise 3.8. Implement Gaussian elimination & inverse for square matrices in Magma. Compare the speed of your implementation with Magma built-in intrinsics on big inputs (big matrices and/or big entries).

A nice way to compute the complexity of divide-and-conquer algorithms is to use the Master theorem, of which we present a simpler version, tailored to our needs.

Theorem 3.1. *We suppose given a recurrence relation of the form*

$$T(n) = aT(n/b) + O(n^c),$$

where $a \geq 1$, $b > 1$, and $c < \log_a(b)$. Then we have

$$T(n) = O(n^{\log_a(b)}).$$

Exercise 3.9. In this problem, we study Karatsuba's algorithm for the multiplication of integers, which relies on a divide-and-conquer approach.

Let x and y be two integers with even length $n \in \mathbb{Z}_{>}0$ in a base $B \in \mathbb{Z}_{>1}$. Further, let us write $x = x_0 B^{n/2} + x_1$, and $y = y_0 B^{n/2} + y_1$, where $0 \leq x_0, x_1, y_0, y_1 < B^n$. The goal of this exercise

is to reduce the multiplication of two integers of length n to a few multiplications of integers of lengths $n/2$.

(a) Show that
$$xy = x_1y_1B^n + (x_0y_1 + x_1y_0)B^{n/2} + x_0y_0.$$
How many $n/2$-digits integers multiplications do you need to perform to compute xy?

(b) We denote by $T(n)$ the complexity of the multiplication of two n-digits integers using this approach. Show that T satisfies
$$T(n) = 4T\left(\frac{n}{2}\right) + O(n).$$

(c) Using Theorem 3.1, can you solve this recursion formula for T? Is this approach asymptotically better than the naive approach?

(d) Karatsuba noticed that we can compute $(x_0B^{n/2} + x_1)(y_0B^{n/2} + y_1)$ using only 3 multiplications, instead of the four naive $x_0y_0, x_0y_1, x_1y_0, x_1y_1$.

More precisely, we let
$$\begin{aligned} z_0 &= x_0y_0 \\ z_2 &= x_1y_1 \\ z_1 &= (x_1 + x_0)(y_1 + y_0) - z_0 - z_2 \end{aligned}$$
Show that
$$xy = z_2B^n + z_1B^{n/2} + z_2.$$

(e) Write the recursion formula for the complexity $T(n)$ in terms of $T(n/2)$ with this new approach.

(f) Using Theorem 3.1, solve this recursion formula for T.

(g) Implement a recursive algorithm that uses Karatsuba's trick to compute the multiplication of any two integers in Magma. How does this algorithm compare to Magma's built-in multiplication for 2048-bit integers?

4. Algebraic Numbers and Number Fields

In this section, we will explore problems involving the basics of number fields and algebraic numbers from a computational perspective. We will also continue to use Magma. Lecture 2 from the 2025 PAWS course on analysis and implementation of algorithms in number theory will serve as a good reference for working on these exercises.

Exercise 4.1. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. Show that $f(x)$ is squarefree in $\mathbb{Z}[x]$ if and only if $\gcd(f(x), f'(x)) = 1$.

Exercise 4.2. Recall that an algebraic extension can be written as a quotient $\mathbb{Q}[x]/(f)$, where $f(x)$ is irreducible. Also, recall that the ring of integers of an extension is the ring of all algebraic integers (roots of monic polynomials whose coefficients are in $\mathbb{Z}$) contained in said extension.

(a) Show that the ring of integers for $\mathbb{Q}(\sqrt{5})$ is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

(b) For d a squarefree integer, describe a generator of the ring of integers for $\mathbb{Q}(\sqrt{d})$.

Exercise 4.3. Show that $\mathrm{Res}_y(y^m m_\alpha(x/y), m_\beta(y))$ has $\alpha\beta$ as a root, so factoring this polynomial will result in finding the minimal polynomial of $\alpha\beta$. Similarly, show that you can recover the minimal polynomial of α/β from $\mathrm{Res}_y(m_\alpha(xy), m_\beta(y))$.

Exercise 4.4. Consider the quadratic number field $K = \mathbb{Q}(\sqrt{-7})$. Note that $\sqrt{-7} + 1$ is an element of K.

(a) Can you find the minimal polynomial of $\sqrt{-7} + 1$?

(b) How is it related to the minimal polynomial of $\sqrt{-7}$?
(c) Can you now find an algorithm to compute the minimal polynomial of any element $a + b\sqrt{-7} \in K$?
(d) Can you generalize this to any quadratic number field?

Exercise 4.5. Consider a large monic polynomial over $\mathbb{Z}[x]$ that one wants to factor. One way you could create it in Magma is with:

```
R<t,y> := PolynomialRing(Integers(),2);
S<x> := PolynomialRing(Integers());
degree := 4;
f := x^degree + Evaluate(Random(degree-1,R,100),[x,1]);
```

This polynomial is almost surely irreducible. We can approximate one of the roots by:

```
r := Roots(PolynomialRing(ComplexField())!f)[1][1];
```

Find the minimal polynomial of the root by checking what algebraic (integer) relations $1, r, r^2, r^3, r^4, r^5$ hold. If you find an algebraic relation of degree smaller than 5, the polynomial is reducible. Otherwise, does it show that it is irreducible?

Lemma 4.1 (Hensel's Lemma for integers)**.** *Let p be a prime and $f(x) \in \mathbb{Z}[x]$. Suppose there exists $a_0 \in \mathbb{Z}$ such that*

$$f(a_0) \equiv 0 \bmod p \quad \textit{and} \quad f'(a_0) \not\equiv 0 \bmod p.$$

Then for every $k \geq 1$, there exists an integer a_k such that

$$f(a_k) \equiv 0 \bmod p^k \quad \textit{and} \quad a_k \equiv a_0 \bmod p.$$

There is a similar version of the lemma for polynomials:

Lemma 4.2 (Hensel's Lemma for polynomials)**.** *Let p be a prime and $f(x) \in \mathbb{Z}[x]$. Suppose $f(x) \equiv g_0(x)h_0(x) \bmod p$, where $g_0(x), h_0(x) \in \mathbb{Z}[x]$ are monic and coprime modulo p. Then, for each $k \geq 1$, there exist monic polynomials $g_k(x), h_k(x) \in \mathbb{Z}[x]$ such that*

$$f(x) \equiv g_k(x)h_k(x) \mod p^k, \quad g_k(x) \equiv g_0(x) \mod p, \quad h_k(x) \equiv h_0(x) \mod p,$$

and $g_k(x), h_k(x)$ remain coprime modulo p.

Exercise 4.6. Let $f(x) = x^3 - x - 2$.

(a) Find all roots of $f(x)$ mod 2 in $\mathbb{Z}/2\mathbb{Z}$.
(b) Recall Hensel's Lemma for integers (Lemma 4.1). Which of the roots of $f(x)$ in $\mathbb{Z}/2\mathbb{Z}$ lift to a root in $\mathbb{Z}/2^k\mathbb{Z}$ for every $k \geq 1$?
(c) For each root of $f(x)$ in $\mathbb{Z}/2\mathbb{Z}$ that lifts to a root in in $\mathbb{Z}/2^k\mathbb{Z}$ for every $k \geq 1$, find its approximation modulo 2^5.

Exercise 4.7. Prove that a number field is an algebraic extension of $\mathbb{Q}$.

Exercise 4.8. Prove that $\mathbb{Q}(\sqrt{d})$ is the smallest field containing $\sqrt{d}$.

Exercise 4.9. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial and α be a root of f. Recall $\mathbb{Q}(\alpha)$ denotes the smallest field that contains both $\mathbb{Q}$ and α. Explain why

$$\mathbb{Q}[\alpha] = \{p(\alpha) : p \in \mathbb{Q}[x]\} = \mathbb{Q}(\alpha).$$

Note that it is enough to write the inverse of α as a polynomial (over $\mathbb{Q}$) in α. What is the degree of $\mathbb{Q}(\alpha)$ in terms of the degree of $f(x)$?

Theorem 4.1 (Primitive Element Theorem)**.** *Let K be a number field, then there exists an element $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. We say that θ is a primitive element.*

Sketch of the proof. Let $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_m)$ be a number field generated over $\mathbb{Q}$ by algebraic numbers α_i. We will show that there is $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. It suffices to show this for $K = \mathbb{Q}(\alpha, \beta)$ (by induction on the number of generators). If α and β are both in $\mathbb{Q}$, then $K = \mathbb{Q}$. Otherwise, consider the elements $\theta = \alpha + c\beta$ for $c \in \mathbb{Q}$. It turns out that $K = \mathbb{Q}(\theta)$ for all but finitely many c (proving this fact requires using automorphisms of K, so we skip it for brevity). Pick one of the infinitely many c so $K = \mathbb{Q}(\theta)$[1]. □

Exercise 4.10. Consider the biquadratic number field $\mathbb{Q}(\sqrt{a}, \sqrt{b})$. Follow the proof of Theorem 4.1 to find a primitive element θ such that $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\theta)$. Can you find a way to compute the minimal polynomial of θ? Can you write $\sqrt{a}$ and $\sqrt{b}$ as polynomials in θ? If you want, you can pick specific values for a and b.

Exercise 4.11. Recall the following discussion of multiplication in number fields: To make multiplication more efficient, we can precompute and store those reductions. Suppose $\theta^n = -t_{n-1}\theta^{n-1} - \cdots - t_0$. Then for $k \geq n$, we have

$$\theta^{n+k} = \sum_{i=0}^{n-1} r_{i,k}\theta^i, \tag{1}$$

where $r_{i,0} = -t_i$ and

$$r_{k+1,i} = \begin{cases} r_{k,i-1} - t_i r_{k,n-1} & \text{if } i \geq 1, \\ -t_0 r_{k,n-1} & \text{if } i = 0. \end{cases}$$

Show that pre-computing the constants $r_{i,k}$ as in (1) takes $O(kn)$ field operations.

Proposition 4.1. *Let $\overline{f}(x) \in \mathbb{F}_p[x]$ be squarefree and assume that its decomposition into irreducibles is $\overline{f}(x) = \prod_{1 \leq i \leq r} f_i(x)$. The polynomials $T(x) \in \mathbb{F}_p[x]$ with $\deg(T(x)) < \deg(\overline{f}(x))$ for which for each i with $q \leq i \leq r$ there exists $s_i \in \mathbb{F}_p$ with $T(x) \equiv s_i \pmod{f_i(x)}$, are exactly the p^r polynomials $T(x)$ such that $\deg(T(x)) < \deg(\overline{f}(x))$ and $T(x)^p \equiv T(x) \pmod{\overline{f}(x)}$.*

Exercise 4.12. Show that the Berlekamp algorithm for small p terminates and correctly computes the factorization of $\overline{f}$ into irreducibles. You can follow the following steps.

(a) As a warm-up, let $\overline{f}(x) \in \mathbb{F}_p(x)$ be a polynomial of degree n. Show that $\overline{f}(x)$ is irreducible if and only if
   (i) $x^{p^n} \equiv x \pmod{\overline{f}(x)}$; and
   (ii) for each prime $q|n$, $\gcd(x^{p^{n/q}} - x, \overline{f}(x)) = 1$.

(b) Prove Proposition 4.1.

(c) Using the notation of Step 2 of the algorithm, show that any polynomial $T(x)$ in the kernel of $Q - I$ holds that $T(x)^p \equiv T(x) \pmod{\overline{f}(x)}$.

(d) Explain why the dimension of $\ker(Q - I)$ is exactly r and why the column vector $(1, 0, \ldots, 0)^t$ belongs to the kernel.

(e) Let $T(x)$ be a polynomial corresponding to a V_j. Explain why the polynomials F from Step 4 of the algorithm correspond to irreducible factors once we have $k = r$.

Exercise 4.13. You can generate random integer polynomials of degree d with coefficients in $[-b, b]$ in Magma by running the script

```
R<t,y> := PolynomialRing(Integers(),2);
S<x> := PolynomialRing(Integers());
f := Evaluate(Random(d,R,b),[x,1]);
```

[1] In practice, trying $\alpha + \beta$ is always a good choice.

Create a polynomial that has 10 random divisors of degree 3. Run the steps of the Berlekamp algorithm with at least two primes and compare results.

5. Trace, Norm, and Discriminant

In this section, we will get our hands dirty with other information that we can gather on algebraic numbers and compute: the trace, norm, and characteristic polynomial. Feel free to use Magma to check any of your work and to practice computing these as well. Lecture 3 from the 2025 PAWS course on analysis and implementation of algorithms in number theory will serve as a good reference for working on these exercises.

Definition 5.1. Let K be a number field of degree n over $\mathbb{Q}$ and let σ_i denote the n distinct embeddings of K in $\mathbb{C}$.

- The *trace of α in K*, denoted $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$, is the sum of all its conjugates, i.e.,
$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$
- The *norm of α in K*, denoted $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$, is the product of all its conjugates, i.e.,
$$\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$
- The *characteristic polynomial* $C_\alpha(x)$ of $\alpha \in K$ is
$$C_\alpha(x) := \prod_{i=1}^{n} (x - \sigma_i(\alpha)).$$

Exercise 5.1. Let α be an algebraic number with minimal polynomial $\sum_{i=0}^{n} a_i x^i$. Show that
$$\mathrm{Tr}(\alpha) = -a_{n-1} \quad \text{and} \quad \mathrm{Nm}(\alpha) = (-1)^n a_0.$$

Proposition 5.1 ([Coh93, Proposition 4.4.1])**.** *Let K be a number field of degree n with embeddings of K into $\mathbb{C}$ given by $\{\sigma_1, \ldots, \sigma_n\}$, and $\{\alpha_1, \ldots, \alpha_n\}$ be a set of n elements of K. Then*
$$\det([\sigma_i(\alpha_j)]_{i,j})^2 = \det([\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)]_{i,j}) \tag{2}$$
and this quantity is a rational number.

Definition 5.2. With the notation of Proposition 5.1, the *discriminant* of $\{\alpha_1, \ldots, \alpha_n\}$, denoted $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$, is the rational number in (2).

Exercise 5.2. Let K be the cyclotomic field $\mathbb{Q}(\zeta_5)$, where ζ_5 is a primitive 5th root of unity. Compute

(a) $\mathrm{disc}(1, \zeta_5, \zeta_5^2, 1 + \zeta_5 + \zeta_5^2)$.
(b) $\mathrm{disc}(1, \zeta_5, \zeta_5^2, \zeta_5^3)$.
(c) $\mathrm{disc}\left(1, \zeta_5, \frac{\zeta_5^2}{5}, \zeta_5^3\right)$.

Exercise 5.3. Let $f(x) = x^3 - x - 1$, and let $\alpha \in \overline{\mathbb{Q}}$ such that $f(\alpha) = 0$. Show that $\{1, \alpha, \alpha^2\}$ is an integral basis of $\mathcal{O}_{\mathbb{Q}(\alpha)}$.

Exercise 5.4. Let K be a number field of degree n over $\mathbb{Q}$ and let $\alpha \in K$ be an algebraic number with minimal polynomial of degree m. Show that the following hold.

(a) m divides n.

(b) $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \frac{n}{m}\mathrm{Tr}(\alpha)$.

(c) $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = (\mathrm{Nm}(\alpha))^{n/m}$.

Lemma 5.1. *Let K be a number field. For all $\alpha \in K$, there exists a nonzero $d \in \mathbb{Z}$ such that $d\alpha \in \mathcal{O}_K$.*

Exercise 5.5. Prove Lemma 5.1.

Exercise 5.6. Consider $K = \mathbb{Q}(\sqrt{d})$ for a squarefree integer d.

(a) Compute the discriminant of the polynomial $x^2 - d$.

(b) Calculate the discriminant of $\{1, \sqrt{d}\}$, in two different ways.

(c) What is the discriminant of K?

Exercise 5.7. Verify using `Magma` that the number of quadratic fields of absolute discriminant x is asymptotic to $\frac{6}{\pi^2}x$, i.e. the number

$$Z(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}; x) = \#\{L/\mathbb{Q} : [L : \mathbb{Q}] = 2, |\operatorname{disc}(L)| \leq x\}$$

approaches $\frac{6}{\pi^2}x$ as x grows.

Lemma 5.2. *If $\{\omega_1, \ldots, \omega_n\}$ and $\{\omega_1', \ldots, \omega_n'\}$ are two integral bases for the ring of integers $\mathcal{O}_K$ of a number field K, then*

$$\operatorname{disc}(\omega_1, \ldots, \omega_n) = \operatorname{disc}(\omega_1', \ldots, \omega_n').$$

Exercise 5.8. Prove Lemma 5.2.

Exercise 5.9. Let $K = \mathbb{Q}(\theta)$, where θ is an algebraic integer with minimal polynomial $m_\theta(x) \in \mathbb{Z}[x]$ of degree n. Show that the following hold:

(a) $\operatorname{disc}(1, \theta, \ldots, \theta^{n-1}) = \operatorname{disc}(m_\theta(x))$;

(b) if $f = [\mathcal{O}_K : \mathbb{Z}[\theta]]$, then

$$\operatorname{disc}(m_\theta(x)) = \operatorname{disc}(K) f^2,$$

where $\operatorname{disc}(m_\theta(x))$ denotes the discriminant of the polynomial $m_\theta(x)$: if $\theta_1, \ldots, \theta_n$ are the roots of $m_\theta(x)$, then

$$\operatorname{disc}(m_\theta(x)) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Hint: You may find the Vandermonde determinant helpful for part (1). Please also feel free to check out the hint in Exercise 3.38 in the Lecture Notes.

Exercise 5.10. Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field. Show that $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. First consider the case when n is prime.

Exercise 5.11. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $X^3 - X - 1$. Let us fix $\alpha_1, \alpha_2, \alpha_3$ the complex roots of $X^3 - X - 1$. The different embeddings of K into $\mathbb{C}$ are the $\sigma_i : \alpha \mapsto \alpha_i$.

We know that the map $\sigma : K \to \mathbb{C}^3$, which sends $x \in K$ to $\sigma(x) = (\sigma_1(x), \sigma_2(x), \sigma_3(x))$, is injective. In this exercise, we use this injectivity to represent elements of K as 3-tuples of complex numbers, and simplify operations. We use the fact that integers are easily recognizable as complex numbers (given that we have enough precision to begin with).

(a) Let L be a number field. Show that if $\beta \in L$ there exists $N \in \mathbb{Z}$ such that $N \cdot \beta \in \mathcal{O}_L$.

(b) Let L be a number field. Show that if $\beta \in \mathcal{O}_L$, then $\frac{\mathcal{N}(\beta)}{\beta} \in \mathcal{O}_L$.

(c) Now, we go back to our case $K = \mathbb{Q}(\alpha)$, where α is a root of $X^3 - X - 1$. Show that any element in $\mathcal{O}_K$ can be written as $a + b\alpha + c\alpha^2$, for $a, b, c \in \mathbb{Z}$.

(d) We introduce the matrix $M = \begin{pmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha)^2 \\ 1 & \sigma_3(\alpha) & \sigma_3(\alpha)^2 \end{pmatrix}$. Show that for any $x = a + b\alpha + c\alpha^2 \in K$,

$$(\sigma_1(x), \sigma_2(x), \sigma_3(x))^T = M \cdot (a, b, c)^T.$$

Note that one can also retrieve (a, b, c) in terms of $(\sigma_1(x), \sigma_2(x), \sigma_3(x))$.

(e) Let $x = 201\alpha^2 - 6458\alpha + 11$ and $y = 519\alpha^2 - 457\alpha + 326$ be elements of $\mathcal{O}_K$.
   (a) Using `Magma`, Compute $\sigma(x)$ and $\sigma(y)$. You can use the built-in function `Conjugates`.
   (b) Compute the component-wise product of $\sigma(x)$ and $\sigma(y)$, and the component-wise division of $\sigma(x)$ by $\sigma(y)$.
   (c) Using (4), retrieve the decomposition of $x \cdot y$ in the base $\{1, \alpha, \alpha^2\}$.
   (d) Can we do the same for the division? Fix that problem using (2), and find the decomposition of x/y in the base $\{1, \alpha, \alpha^2\}$.

(f) Can you give a few pros and cons of that method compared to the algebraic computation?

6. LLL and the Subfield Problem

In this section, we will study a powerful algorithm in linear algebra (the LLL algorithm) and the subfield problem. We will review some linear algebra problems. Feel free to use Magma to check your work. Lecture 4 from the 2025 PAWS course on analysis and implementation of algorithms in number theory will serve as a good reference for working on these exercises.

Definition 6.1. Let K and L be two number fields. The subfield problem consists of determining whether or not K is isomorphic to a subfield of L.

Exercise 6.1. Apply the Gram-Schmidt orthogonalization process to the following sequence of vectors in $\mathbb{R}^3$:

$$\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 8 \\ 1 \\ -6 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Definition 6.2. Let q be a quadratic form on an $\mathbb{R}$-vector space V. We say that q is *positive-definite* if for all $\mathbf{x} \in V$ we have $q(\mathbf{x}) > 0$.

Exercise 6.2. Find a 3×3 matrix representing the quadratic form

$$q(x_1, x_2, x_3) = x_1^2 + 5x_2^2 - 3x_3^2 + 6x_1x_2 - 4x_1x_3 + 8x_2x_3$$

for all $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{R}^3$. Is it positive definite?

Definition 6.3. A *lattice* is a free $\mathbb{Z}$-module of finite rank together with a positive definite quadratic form q on $L \otimes \mathbb{R}$.

Exercise 6.3. Let L be a lattice with associated quadratic form $q\colon V \to K$ and $\mathbb{Z}$-basis $\{b_1, \ldots, b_n\}$. Then, we can recover q from the matrix

$$Q = [q_{i,j}]_{i,j}, \qquad \text{where } q_{i,j} = b(b_i, b_j), \tag{3}$$

with $b(b_i, b_j)$ denoting the bilinear form $b(x, y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$. Indeed, for all $x \in \mathbb{R}^n$, we have $q(x) = x^{\mathsf{t}}Qx$. Show that the determinant of the matrix Q is independent of the choice of $\mathbb{Z}$-basis for L.

Exercise 6.4. Let $A = \begin{pmatrix} a & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & a \end{pmatrix}$. For what range of values a is A positive definite?

Exercise 6.5. Let $x = 0.30901699437494742410229341718 + 0.95105651629515357211643933338\,0\,i$ be a numerical approximation of an algebraic integer. Can you find that algebraic integer?

Let L be a lattice in a number field K with a $\mathbb{Z}$-basis $\mathcal{B} := \{b_1, \ldots, b_n\}$ and an orthogonal basis $\{b_1^*, \ldots, b_n^*\}$ obtained from Gram-Schmidt. We are interested in *reducing* the basis $\mathcal{B}$ as much as possible. The following is the idea that Arjen Lenstra, Hendrik Lenstra, and László Lovász had in [LLL82].

Definition 6.4. The basis $\mathcal{B}$ is *LLL-reduced* if

$$|\mu_{i,j}| \leq \frac{1}{2} \qquad \text{for } 1 \leq j < i \leq n$$

and

$$|b_i^*|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) |b_{i-1}^*|^2 \qquad \text{for } 1 < i \leq n,$$

where $\mu_{i,j} := \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*}$.

Theorem 6.1. *Let $\{b_1, \ldots, b_n\}$ be an LLL-reduced basis of a lattice L. Then*

$$d(L) \leq \prod_{i=1}^{n} |b_i| \leq 2^{n(n-1)/4} d(L); \tag{4}$$

$$|b_j| \leq 2^{(i-1)/2} |b_i^*|, \qquad \text{if } 1 \leq j \leq i \leq n; \tag{5}$$

$$|b_1| \leq 2^{(n-1)/4} d(L)^{1/n}; \tag{6}$$

for every $x \in L$ with $x \neq 0$, we have

$$|b_1| \leq 2^{(n-1)/2} |x|; \tag{7}$$

and for linearly independent vectors $x_1, \ldots, x_t \in L$, we have

$$|b_j| \leq 2^{(n-1)/2} \max(|x_1|, \ldots, |x_t|) \qquad \text{for } 1 \leq j \leq t. \tag{8}$$

Some examples of applications of LLL are computing integer kernel and images of matrices and finding small vectors in lattices. Hopefully, we have enough justification for wanting to write an algorithm to compute an LLL-reduced basis.

Algorithm 2 LLL Algorithm [Coh93, Algorithm 2.6.3]

The input is a basis $b_1, \ldots, b_n$ of a lattice L with quadratic form q. This algorithm transforms the vectors b_i so that when the algorithm terminates, they form an LLL-reduced basis. In addition, the algorithm gives a change of basis matrix H that writes the new basis in terms of the old one.

1. Set $k := 2$, $k_{\max} := 1$, $b_1^* = b_1$, $B_1 := b_1 \cdot b_1$, and $H := I_n$.
2. If $k \leq k_{\max}$ go to Step 3. Otherwise, set $k_{\max} := k$ and $b_k^* := b_k$. Then, for $j = 1, \ldots, k-1$, set $\mu_{k,j} := b_k \cdot b_j^* / B_j$ and $b_k^* := b_k^* - \mu_{k,j} b_j^*$. Finally, set $B_k := b_k^* \cdot B_k^*$.
3. Execute RED$(k, k-1)$ (Algorithm 3). If $B_k < (0.75 - \mu_{k,k-1}^2) B_{k-1}$, execute SWAP$(k)$ (Algorithm 4). Set $k := \max(2, k-1)$ and go to Step 3. Otherwise, for $l = k-2, k-3, \ldots, 1$ execute RED(k, l), then set $k := k+1$.
4. If $k \leq n$, then go to Step 2. Otherwise, output $b_1, \ldots, b_n$ and the transformation H, and terminate.

The two subalgorithms are the following.

Algorithm 3 Subalgorithm RED(k, l)

1. If $|\mu_{k,l}| < 0.5$, terminate.
2. Set $r := \lfloor \mu_{k,l} \rceil = \lfloor 0.5 + \mu_{k,l} \rfloor$, the integer nearest to $\mu_{k,l}$.
3. Set $b_k := b_k - rb_l$, $H_k := H_k - rH_l$, and $\mu_{k,l} := \mu_{k,l} - r$. For all i such that $1 \leq i \leq l-1$, set $\mu_{k,i} := \mu_{k,i} - r\mu_{l,i}$ and terminate.

Algorithm 4 Subalgorithm SWAP(k)

1. Exchange the vectors b_k and b_{k-1}, H_k and H_{k-1}, and if $k > 2$, for all j such that $1 \leq j \leq k-2$ exchange $\mu_{k,j}$ with $\mu_{k-1,j}$. Then set (in this order) $\mu := \mu_{k,k-1}$, $B := B_k + \mu^2 B_{k-1}$, $\mu_{k,k-1} := \mu B_{k-1}/B$, $b := b^*_{k-1}$, $b^*_{k-1} := b^*_k + \mu b$, $b^*_k := -\mu_{k,k-1} b^*_k + (B_k/B)b$, $B_k := B_{k-1}B_k/B$, and $B_{k-1} := B$. Finally, for $i = k+2, \ldots, k_{\max}$ set $t := \mu_{i,k}$, $\mu_{i,k} := \mu_{i,k-1} - \mu t$, $\mu_{i,k-1} := t + \mu_{k,k-1}\mu_{i,k}$, and terminate the subalgorithm.

Remark 6.1. Note that the algorithm does not require an orthogonal basis as an input. Instead, we perform Gram-Schmidt as needed.

Exercise 6.6. Implement the subalgorithm RED(k, l) in Magma.

Exercise 6.7. Implement the subalgorithm SWAP(k) in Magma.

Exercise 6.8. In this question, we show that $K = \mathbb{Q}(\sqrt{-3})$ is a subfield of $L = \mathbb{Q}(\zeta_9)$, where ζ_9 is a primitive 9-th root of unity.

(1) First, choose an embedding of K and L into $\mathbb{C}$. You can use the command `Roots()` on each of the minimal polynomials of K and L (denoted by m_K and m_L respectively).
(2) Then, ask for an integral linear combination between the numerical approximations of $\sqrt{-3}$, and $1, \zeta_9, \ldots, \zeta_9^5$. You can use the command `IntegerRelation()` to do that.
(3) Using the previous item, find a polynomial P such that we have, at least heuristically, $\sqrt{-3} = P(\zeta_9)$. Check that $m_K(P(x))$ is divisible by m_L, and conclude that K is a subfield of L.

Exercise 6.9. Show that the running time of the LLL algorithm is at most $O(n^6 \ln^3 B)$ field multiplications/divisions, if $|b_i|^2 \leq B$ for all i.

Exercise 6.10. Prove Theorem 6.1 about LLL-reduced bases.

Exercise 6.11. Try writing your own implementation of LLL and comparing running times for small examples. Use the subalgorithms from previous problems.

7. Class and Unit Groups

In this section, we will focus on the structure of the ring of integers of a number field, describing and computing ideals, class groups, regulators, and fundamental units. The reader can find more information than is provided in this problem set in any algebra textbook. Feel free to use Magma to check your answers. Lecture 5 from the 2025 PAWS course on analysis and implementation of algorithms in number theory will serve as a good reference for working on these exercises.

Definition 7.1. Let K be a number field with ring of integers $\mathcal{O}_K$. An *ideal* I of $\mathcal{O}_K$ is a sub-$\mathbb{Z}$-module of $\mathcal{O}_K$ such that for every $r \in \mathcal{O}_K$ and $i \in I$ we have $ri \in I$.

Definition 7.2. A *fractional ideal* I in $\mathcal{O}_K$ is a nonzero submodule of K such that there exists a nonzero integer d with dI ideal of $\mathcal{O}_K$. The smallest positive integer d for which this is possible is called the *denominator* of I.

Exercise 7.1. Show that the set of fractional ideals of $\mathcal{O}_K$ forms a group under multiplication.

Exercise 7.2. Find a $\mathbb{Z}$-basis for the ideal generated by $\{3, 2+\theta, 1-\theta^2, 1+\theta+\theta^3\}$ in the number field $K = \mathbb{Q}(\theta)$, where θ has minimal polynomial $x^4 - x^3 + x^2 - 2x + 2$.

Exercise 7.3. Prove that $\mathbb{Z}[i]$ is a Euclidean domain.

Definition 7.3. Let K be a number field. The set of units in $\mathcal{O}_K$ forms a multiplicative group, denoted by $U(K)$, and called the *unit group* of K.

We can describe the structure of the unit group as follows.

Theorem 7.1 (Dirichlet's Unit Theorem)**.** *Let K be a number field and let r and $2s$ be the number of real and complex embeddings, respectively. Then*

$$U(K) \cong \mu(K) \times \mathbb{Z}^{r+s-1},$$

where $\mu(K)$ denotes the set of roots of unity in $U(K)$.

Exercise 7.4. Show that the unit group of a number field K is finite if and only if K is either $\mathbb{Q}$ or an imaginary quadratic field.

Definition 7.4. With the notation of Theorem 7.1, a set $u_1, u_2, \ldots, u_{r+s-1}$ of units of K that generates the free part of $U(K)$ is called a system of fundamental units in K.

Exercise 7.5. Compute a fundamental unit for $\mathbb{Q}(\sqrt{5})$.

Definition 7.5. An $m \times n$ matrix $M = (m_{i,j})$ with integer coefficients is in Hermite normal form if there exists $r \leq n$ and a strictly increasing map f from $[r+1, n]$ to $[1, m]$ satisfying:

(1) For $r+1 \leq j \leq n$, $m_{f(j),j} \geq 1$; $m_{i,j} = 0$ if $i > f(j)$; and $0 \leq m_{f(k),j} < m_{f(k),k}$ if $k < j$.
(2) The first r columns of M are equal zero.

Theorem 7.2. *Let A be an $m \times n$ matrix with coefficients in $\mathbb{Z}$. Then there exists a unique $m \times n$ matrix B in Hermite normal form of the form AU with $U \in \mathrm{GL}_n(\mathbb{Z})$.*

Definition 7.6. With the notation from Theorem 7.2, the matrix W corresponding to the nonzero columns of B is called the *Hermite normal form* of the matrix A.

The key point of this definition is that, if the columns of A represent a set of generators for a $\mathbb{Z}$-module, then the columns of its Hermite normal form represent the unique basis for the $\mathbb{Z}$-module whose matrix is in Hermite normal form. Such a basis is called the *Hermite normal form basis*.

Exercise 7.6. Use Hermite normal forms to implement an algorithm to compute the sum of two ideals of $\mathcal{O}_K$.

Exercise 7.7. Compute the regulators of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5})$.

Exercise 7.8. A ring R is an Euclidean domain if it admits an Euclidean algorithm.

(a) Show that every Euclidean domain is a principal ideal domain.
(b) Prove that $\mathbb{Z}[\sqrt{-3}]$ is not a principal ideal domain.

Exercise 7.9. Prove that the class group of $\mathbb{Q}(i)$ is trivial by showing that the quadratic form $x^2 + y^2$ composed with itself is equivalent to $x^2 + y^2$.

Exercise 7.10. Consider the ring $\mathbb{Z}[x]$.

(a) Compute the norm of the ideal $(2, x^2)$ in $\mathbb{Z}[x]$ and determine the maximal ideal that contains $(2, x^2)$.

(b) In the ring $\mathbb{Z}[\sqrt{5}]$, show that the principal ideal (3) is prime.

Theorem 7.3 (Minkowski's bound)**.** *Let K be a number field of degree n over $\mathbb{Q}$ and discriminant* $\operatorname{disc}(K)$*. Let $2s$ be the number of complex embeddings of K. Then every class in* $\mathrm{Cl}(K)$ *contains an ideal I (not fractional) of norm*

$$\mathcal{N}(I) \leq \sqrt{|\operatorname{disc}(K)|}\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}.$$

Exercise 7.11. In the number field $K = \mathbb{Q}(\sqrt{-5})$, compute Minkowski's bound and list all ideals with norm bounded by it. Use this to determine the structure of the class group of K.

Exercise 7.12. Implement an algorithm to compute a system of fundamental units in `Magma`. For the LLL reduction, you can use the native command `LLL`. Use the online documentation for this command at this link.

Exercise 7.13. Compute a system of fundamental units and the class group for the number field defined by $f(x) = x^4 - 3x - 5$.

Theorem 7.4 (Stark, 1967)**.** *If the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ has class number 1 for a prime number p, then $p < 200$.*

Exercise 7.14. List all imaginary quadratic fields with class number 1, for p prime and $p < 200$, and conclude that your list includes all imaginary quadratic fields with class number 1 using Theorem 7.4.

References

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.