Finding orders with prescribed index in number fields

Alex J. Best

Supervised by Dr. Lassina Dembélé

2014

Abstract

Orders of number fields are common objects of study in algebraic number theory. Here we develop methods to obtain all orders with a specified index inside another given one. The performance, both theoretically and in implementations of these methods is discussed. We also apply these techniques to problems relating to elliptic curves over the rational numbers.

Keywords. Number theory, algebraic number theory, elliptic curves, number fields, algorithms.

Contents

1 Introduction

In this report we develop algorithmic methods for the solution of a problem arising from algebraic number theory. Specifically we develop methods to find all orders of an algebraic number field with a given index inside another order. We detail some situations in which these algorithms can be applied at the end. Though the problem is a natural one we do not know of any previous work with exactly the same aim as ours. Instead there is some existing work that relates to special cases of our problem, these are discussed in their relevant sections.

The report is organised as follows. We first go through the background material needed to motivate, define and describe the solution of our problems in chapter 2. In section 2.1 we cover some commutative algebra dealing with the basic properties of modules over rings, after this in section 2.2 we move into algebraic number theory defining the key notions needed to study orders and considering the reasons such ideas were introduced. We finish up the background material in section 2.3 with an introduction to the theory of elliptic curves, which will be one of the areas we will apply our methods to.

Chapter 3 is where we consider our main problem and solutions to it. First we define the problems themselves and discuss the interest in studying them. After this in the rest of chapter 3 we detail the techniques used to solve the problems considered, starting with some special cases before moving onto more general results. Next we discuss the advantages of the algorithms developed and their practical timings.

Finally in chapter 4 we move on to some interesting applications of these methods to finding elliptic curves with given properties.

2 Background material

In this section we fix several definitions and important results from algebraic number theory and commutative algebra. We assume only fairly basic knowledge of abstract algebra, such as the notions of groups, rings and fields.

The results given here are well known and are used throughout the rest of the report.

2.1 Commutative algebra

We introduce several notions and results that will be useful to us throughout the report, proofs for those results not proved here can be found in many textbooks on commutative algebra, such as [AM94] or [MR89].

All rings here are commutative with an identity element.

Definition 1 (Module)**.** Given a ring R we define an *R-module* M to be an abelian group under addition, with a scalar multiplication map $\cdot\colon R \times M \to M$ satisfying

$$\begin{aligned} 1 \cdot m &= m && \text{for all } m \in M \\ r_1 \cdot (r_2 \cdot m) &= (r_1 r_2) \cdot m && \text{for all } r_1, r_2 \in R,\ m \in M \\ r \cdot (m_1 + m_2) &= r \cdot m_1 + r \cdot m_2 && \text{for all } r \in R,\ m_1, m_2 \in M \\ (r_1 + r_2) \cdot m &= r_1 \cdot m + r_2 \cdot m && \text{for all } r_1, r_2 \in R,\ m_1 \in M \end{aligned}$$

We often refer to elements of the ring R as *scalars*.

From now on we will omit the notation $\cdot$ for scalar multiplication as it will be clear from context when the multiplication is taking place in the ring R or on a module M. We will also not make explicit the ring R involved if it is not relevant to the discussion at hand, instead referring simply to a *module*.

The most common modules we will use here will be $\mathbf{Z}$-modules such as:

Example 1.

$$\mathbf{Z},\ \{(a,b) \mid a,b \in \mathbf{Z}\},\ \text{or } \{a\sqrt{2} + b\sqrt[3]{2} \mid a,b \in \mathbf{Z}\}.$$

In fact every abelian group can be given a $\mathbf{Z}$-module structure so of course they are ubiquitous in commutative algebra, nevertheless it is useful to think of the modules used here in terms of $\mathbf{Z}$ rather than as abstract abelian groups. We now list some standard definitions that are used to talk about how different modules relate to one another and describe ways of constructing new modules from old.

Definition 2 (Module homomorphism)**.** Given R-modules M_1 and M_2, a function $f\colon M_1 \to M_2$ satisfying

$$\begin{aligned} f(rm) &= rf(m) && \text{for all } r \in R,\ m \in M_1 \\ f(m+m') &= f(m) + f(m') && \text{for all } m, m' \in M_1 \end{aligned}$$

is called an *R-module homomorphism* or simply a *module homomorphism* when the ring is clear. We also use the term map for this concept.

Definition 3 (Isomorphism of modules)**.** Two R-modules M_1 and M_2 are said to be *isomorphic* is there exists a bijective module homomorphism between them. In this case we write $M_1 \cong M_2$.

Module isomorphism is an equivalence relation on the class of all modules and so we often think of two isomorphic modules as being the same, just written in a different manner.

Definition 4 (Submodule)**.** A *submodule* N of a module M is a module whose elements all belong to M and whose operations are the same as those from M on the elements on N.

Definition 5 (Quotient module)**.** The *quotient module* of two R-modules M and N where N is a submodule of M is defined to be the R-module whose additive group quotient abelian group M/N under addition with scalar multiplication given by

$$r \cdot (m+N) = rm + N \text{ for all } r \in R,\ m \in M.$$

This module is denoted by M/N.

Definition 6 (Index)**.** Given a module N that is a submodule of a module m the *index* of N in M, denoted $[M : N]$ is the size of the quotient module M/N.

Definition 7 (Direct sum)**.** Given two R-modules M_1 and M_2 we define their *direct sum* (denoted $\oplus$) to be the module with element set $M_1 \times M_2$ and operations given by the operations of M_1 and M_2 performed elementwise. i.e.

$$r \cdot (m_1, m_2) = (r \cdot m_1, r \cdot m_2)$$
$$(m_1, m_2) + (m_1', m_2') = (m_1 + m_1', m_2 + m_2').$$

Not that this is in general distinct from when we have M_1 and M_2 submodules of some module N and write

$$M_1 + M_2 = \{m_1 + m_2 \mid m_1 \in M_1,\ m_2 \in M_2\}.$$

For example with this elementwise addition we have $M + M = M$ for any module M, whereas $M \oplus M$ is not isomorphic to M unless M is the trivial module (i.e. the module containing only a zero element and no others).

The well known isomorphism theorems also hold for modules, we require only two.

Theorem 1 (First isomorphism theorem for modules)**.** Given a surjective module homomorphism $f\colon M \to N$ the kernel of f is a submodule of M and

$$M/\ker(f) \cong N.$$

Theorem 2 (Third isomorphism theorem for modules)**.** Given a chain of submodules $M_1 \subseteq M_2 \subseteq M_3$ the quotient module M_2/M_1 is a submodule of M_3/M_1 and we have an isomorphism

$$(M_3/M_1)/(M_2/M_1) \cong (M_3/M_2).$$

An easy consequence of this relating the indices of submodules is worth noting.

Corollary 1. Given a chain of submodules $M_1 \subseteq M_2 \subseteq M_3$ where $[M_3 : M_2]$ and $[M_2 : M_1]$ are finite we have

$$[M_3 : M_1] = [M_3 : M_2][M_2 : M_1].$$

We now define a property of modules that makes them easier to work with and, importantly, easier to do computations with.

Definition 8 (Finitely generated)**.** An R-module M is *finitely* generated if there is a

finite set $B \subset M$ such that any $m \in M$ can be written as

$$m = \sum_{b \in B} \alpha_b b$$

for some coefficients $\alpha_b \in R$.

Definition 9 (Torsion submodule)**.** The *torsion submodule* M_{tors} of an R-module M is the set

$$\{m \in M \mid \exists\, r \in R \setminus 0 \text{ such that } rm = 0\}.$$

This is the set of elements that are killed by some non-zero scalar. As implied by the name this is always submodule of M.

A module M is called a torsion module if $M_{\text{tors}} = M$, and torsion-free if $M_{\text{tors}} = 0$.

Definition 10 (Rank of a $\mathbf{Z}$-module)**.** Given a $\mathbf{Z}$-module M we can always write $M = M_{\text{tors}} \oplus \mathbf{Z}^r$ for some unique $r \in \mathbf{Z}_{\geq 0}$. This r is called the *rank* of the $\mathbf{Z}$-module.

Example 2.

$$M = \mathbf{Z}^2 = \{(a, b) \mid a, b \in \mathbf{Z}\}$$

is a torsion free $\mathbf{Z}$ module. Let

$$N = \{(2c, 0) \mid c \in \mathbf{Z}\} \cong \mathbf{Z}$$

be a submodule of M. Then the quotient module

$$M/N \cong (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}$$

has torsion submodule $(M/N)_{\text{tors}}$ equal to $\mathbf{Z}/2\mathbf{Z}$ and is of rank 1.

Definition 11 (Short exact sequence)**.** A *short exact sequence of R-modules* is a sequence of R-modules and maps between them, drawn as

$$0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$$

such that for every occurrence of a triple $N_1 \xrightarrow{g_1} N_2 \xrightarrow{g_2} N_3$ we have $\text{im}(g_1) = \ker(g_2)$.

In any short exact sequence we therefore have f_1 injective and f_2 surjective.

Definition 12 (Split short exact sequence)**.** A short exact sequence $0 \to M_1 \xrightarrow{q} M_2 \xrightarrow{r} M_3 \to 0$ is called *split* if any of the following equivalent conditions hold:

(i) There is a map $t\colon M_2 \to M_1$ such that $t \circ q$ is the identity on M_1.

(ii) There is a map $u\colon M_3 \to M_2$ such that $u \circ r$ is the identity on M_2.

(iii) $M_2 \cong M_1 \oplus M_3$.

We have one more notion to define.

Definition 13 (R-algebra)**.** An R-module which is also a

2.2 Algebraic number theory

Algebraic number began with the study of algebraic numbers and their uses in solving Diophantine equations. The subject has since expanded to encompass a huge amount of mathematics involving the use of algebraic techniques to tackle number theoretic problems. We give a short introduction to the results relevant to us here. As above, more details about anything not proved here can be found in any of the many texts on algebraic number theory, for example [NS10], [Lan94], [Nar04] or [ST02].

Definition 14 (Number field)**.** A *number field* K is a field that is also a finite dimensional $\mathbf{Q}$-vector space.

Example 3. We write $\mathbf{Q}(\sqrt{3})$ for the smallest field containing both $\mathbf{Q}$ and $\sqrt{3}$, it is clear that the set

$$\{a + b\sqrt{3} \mid a, b \in \mathbf{Q}\}$$

must be contained in such a field. But we can also see that this set is closed under addition, subtraction, multiplication and non-zero division, and hence this set is the field $\mathbf{Q}(\sqrt{3})$.

Here we see that $\mathbf{Q}(\sqrt{3})$ has dimension 2 as a vector space over $\mathbf{Q}$.

Definition 15 (Degree of a number field)**.** The dimension of a number field K as a $\mathbf{Q}$ vector space is called the *degree* of K, denoted $[K : \mathbf{Q}]$.

We say that number fields of degree 2, such as in example 3 above are *quadratic*. Similarly degree 3 number fields are called *cubic*.

The following few definitions are central to the whole problem.

A number field will have a large quantity of subrings, only some of which are of real number theoretic interest. So we distinguish some subrings that have desirable properties and single them out for study.

Definition 16 (Order)**.** An *order* of a number field K is a subring of K that is finitely generated as a $\mathbf{Z}$-module, and of rank equal to the degree of K (this is the maximal rank).

By definition orders have finite bases over $\mathbf{Z}$ and so we will often represent orders by writing them as sums

$$\mathcal{O} = \mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2 + \cdots + \mathbf{Z}\alpha_n.$$

We also use the notation $\mathbf{Z}[\alpha]$ to mean the ring of polynomials expressions in α with integer coefficients, provided α is an algebraic integer this will be an order.

Definition 17 (Ring of integers)**.** The *ring of integers*, denoted $\mathbf{Z}_K$, of a number field K is the unique maximal order.

The terminology for this ring comes from the fact that its behaviour is analogous to the way $\mathbf{Z}$ behaves inside $\mathbf{Q}$. As we will see later the maximal order of a quadratic number field is easy to determine but the complexity of such calculations increases with the degree.

The notion of index introduced earlier applies here and as all orders lie inside the ring of integers we can always find the index of an order $\mathcal{O}$ inside $\mathbf{Z}_K$. If we just use the term index of an order, without specifying another containing it, we will mean exactly this, the index inside the maximal order.

Example 4.

$$[\mathbf{Z} \cdot 1 + \mathbf{Z} \cdot \sqrt{2} : \mathbf{Z} \cdot 1 + \mathbf{Z} \cdot 2\sqrt{2}] = 2.$$

In figure 2.1 one embedding into the complex plane of the ring of integers of $\mathbf{Q}[x]/(x^2+19) \cong \mathbf{Q}(\sqrt{-19})$ is shown. Highlighted in bold is a suborder of index 3 in this order.

2.3 Elliptic curves

We now introduce the background material relevant to elliptic curves, one of the intended applications of these methods. This is not required for the main problem discussed in chapter 3, but chapter 4 uses these ideas heavily. As with the above sections everything here can be found in textbooks on elliptic curves (such as [Kna92] or [Cas91]), we offer a rapid summary, moving quickly to the notions relevant to this project.

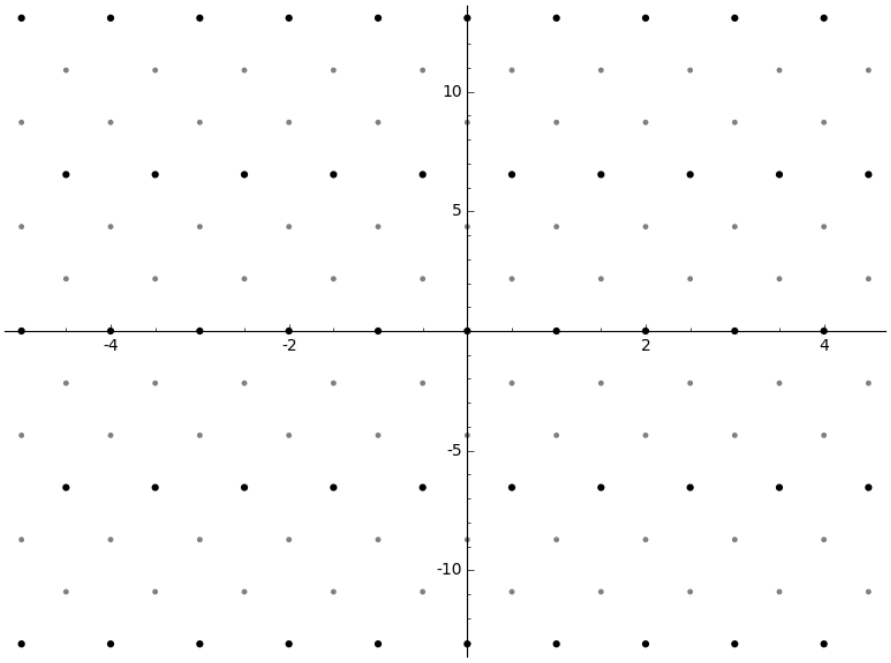

Figure 2.1: An embedding in $\mathbf{C}$ of the ring of integers of $\mathbf{Q}(\sqrt{-19})$ and an index 3 suborder.

Definition 18 (Elliptic curve)**.** For us an *elliptic curve* E defined over a field K will be given by a binary cubic equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ with } a_i \in K.$$

To such a curve we assign several b invariants based on the coefficients in the definition as follows

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

We then also require that the *discriminant* Δ of E, given by

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

is not zero for E to really be an elliptic curve.

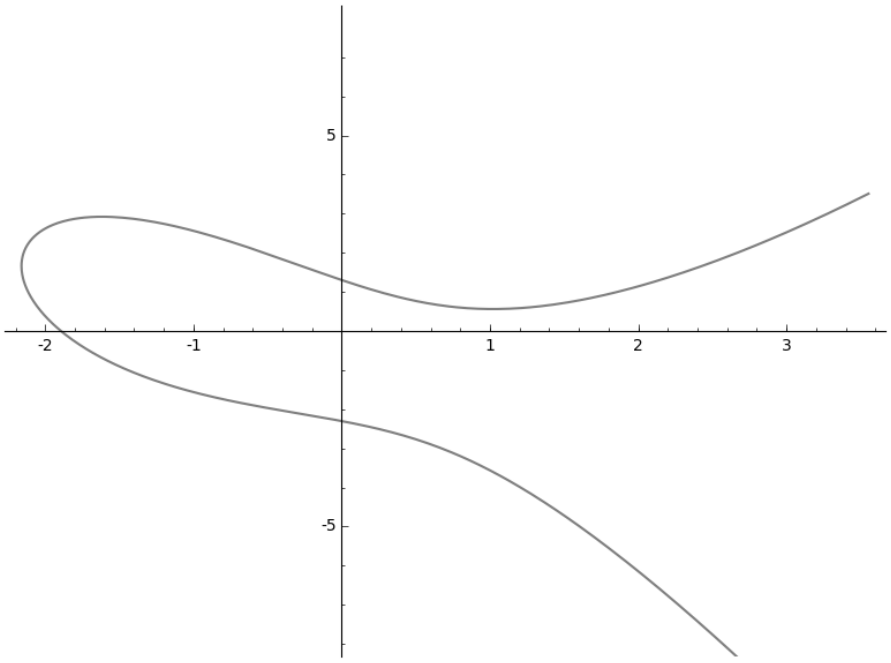

Figure 2.2: The real points of $E\colon y^2 + 2xy + y = x^3 - 2x + 3$.

Given an elliptic curve E defined over a field K with $K \subset K'$ another field, we let $E(K')$ be the set of points in $K' \times K'$ satisfying the equation defining E, along with an extra point ∞. This additional point is called the point at infinity, the reasons for its inclusion in the set should become clear later.

The condition on Δ given above is to ensure that our curve does not have any points where both the derivatives with respect to x and y vanish, such a point is called a singular point and the existence of such a point causes the behaviour of the curve to differ highly from what we would normally expect.

Example 5. Let

$$E\colon y^2 + 2xy + y = x^3 - 2x + 3$$

be an elliptic curve. Then we can see that $(1, (\sqrt{17} - 3)/2) \in E(\mathbf{R}) \subset E(\mathbf{C})$ as the coordinates satisfy the equation defining the curve.

We can plot the real points of this curve, such a plot is shown in figure 2.2. This plot of the real points is typical for an elliptic curve, though there can easily be two connected components rather than one as in this case.

One of the things that makes elliptic curves so interesting to study is the fact that we can define a natural way of adding points of the curve over some field, with this

definition the set of points on the curve becomes a group.

Definition 19 (Group law)**.** We define the sum of two points $P, Q \in E(K)$ for some field K as follows, let L be the line joining P and Q (take L to be the tangent at P if $P = Q$). Then L intersects E in three points (with multiplicity) so there is one point in addition to P and Q on both L and E, call this point R. Now there is at most one other point with the same x coordinate as R that lies on E, this is our sum $P + Q$.

In the above definition we think of the point at infinity as lying infinitely far away in the positive y direction, therefore a line from ∞ to the point P is the line through P perpendicular to the x-axis.

With this definition of addition the set of points of E over some field K is a group, and moreover this group is abelian (as the line through P and Q is the same as the line through Q and P). The identity element of our group is the point at infinity referred to above. From now on we will denote the point $\infty \in E(K)$ as 0, but still refer to it as *at infinity*.

We want to consider some special maps between elliptic curves that respect both the curve and group structure.

Definition 20 (Homomorphism of elliptic curves)**.** Let E be an elliptic curve defined over a field K. A group homomorphism $f\colon E \to E'$ such that there are polynomials $a, b, c, d \in \overline{K}[x, y]$ with

$$f(x, y) = \left(\frac{a(x, y)}{b(x, y)}, \frac{c(x, y)}{d(x, y)} \right) \text{ for } (x, y) \in E \setminus 0$$

is called a *homomorphism of elliptic curves*.

Definition 21 (Isomorphism of elliptic curves)**.** If we have two elliptic curves E and E' such that there exists homomorphisms $f\colon E \to E'$ and $g\colon E' \to E$ with $f \circ g = \mathrm{id}_{E'}$ and $g \circ f = \mathrm{id}_E$ then E and E' are called *isomorphic*. A homomorphism f with an inverse g as in the definition above is called an *isomorphism*.

We can also consider homomorphisms from a given elliptic cuve to itself, these are known as *endomorphisms* and they form a ring.

Definition 22 (Endomorphism ring)**.** The *endomorphism ring* of an elliptic curve is the set

$$\mathrm{End}(E) = \{f\colon E \to E \mid f \text{ is a homomorphism of elliptic curves}\}$$

with a ring structure given by $(f+g)(P) = f(P) + g(P)$ and multiplication is composition.

As remarked above any abelian group can be regarded as a $\mathbf{Z}$-module M in a natural way by letting

$$n \cdot z = \underbrace{z + z + \cdots + z}_{n \text{ times}}, \text{ for } n \in \mathbf{Z}_{\geq 0},\ z \in M$$

and letting $n \cdot z = (-n) \cdot (-z)$ for negative $n \in \mathbf{Z}$. With this idea in mind $E(K)_{\text{tors}}$ is the set of points of E defined over K that can be added to themselves some finite number of times to get the point at infinity. This is often called the *torsion subgroup* of E. It turns out that when $K = \mathbf{Q}$ there are only a finite number of groups that $E(\mathbf{Q})_{\text{tors}}$ can be.

Theorem 3 (Mazur's torsion theorem)**.** Given an elliptic curve E defined over the rationals $E(\mathbf{Q})_{\text{tors}}$ is one of:

$$\mathbf{Z}/i\mathbf{Z}, \text{ for } i \in \{1, 2, \ldots, 9, 10, 12\} \text{ or } \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2i\mathbf{Z}, \text{ for } i \in \{1, 2, 3, 4\}.$$

In fact similar results have been obtained for quadratic fields too, for more detail on what is known about the torsion subgroup of an elliptic curve over a number field see [Sut12].

Sometimes it is necessary to talk about smaller subgroups of this group whose elements have order dividing some fixed n and so we introduce the following definition.

Definition 23 (n-division points)**.** For some $n \in \mathbf{Z}$ the set of *n-division points* (or *n-torsion points*) of E over K is

$$E(K)[n] = \{P \in E(K) \mid nP = 0\}.$$

We are now ready to state in precise terms the problem we aimed to solve and to detail the methods used in its solution.

3 Finding orders with prescribed index

The aim of the project was to find a general method to solve the following problem, and moreover to find efficient algorithms that can solve the problem on any given inputs.

Problem 1. Given an order R of an absolute number field K and an integer I find the set

$$\mathrm{Orders}(R, I) = \{\mathcal{O} \subseteq R \mid \mathcal{O} \text{ is a suborder, } [R : \mathcal{O}] = I\}.$$

To find a suborder we really mean to compute a $\mathbf{Z}$ basis for the suborder in terms of the basis of the larger order. Such a basis defines an order completely.

One very natural extension of the above problem is to consider relative extensions of number fields. More precisely we can generalise the above problem to the following one.

Problem 2. Given an extension of number fields $L|K$, a $\mathbf{Z}_K$-order R of $\mathbf{Z}_L$ and an integer I find the set

$$\{\mathcal{O} \subseteq R \mid \mathcal{O} \text{ is a } \mathbf{Z}_K\text{-suborder, } [R : \mathcal{O}] = I\}.$$

We now detail some methods to solve the problem in the absolute setting in varying generality. Much of what follows should be extendible to relative orders fairly easily, however we do not consider this problem any further.

3.1 Quadratic number fields

Quadratic number fields are the simplest non-trivial number fields and they have a large amount of structure which can often make them easier to work with than more general number fields. As we will see, in this case the solution of our problem is very simple.

It is well known [Lan94] that the ring of integers of a quadratic field $K = \mathbf{Q}(\sqrt{d})$ for d non-square always takes the form

$$\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\alpha, \text{ with } \alpha = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Indeed there is so little room for manoeuvre here that the following result on the structure of an order holds in this case.

Proposition 1. Every order $\mathcal{O}$ of a quadratic number field can be expressed as

$$\mathcal{O} = \mathbf{Z} + \mathbf{Z}f\alpha$$

for some $f \in \mathbf{Z}$, α as above.

For a proof see [Cox13, pp. 133–134].

Definition 24. The f appearing in the above proposition is called the *conductor* of the order $\mathcal{O}$. Later we shall abuse this definition slightly by redefining the conductor to generalise this concept.

Now it is clear that

$$[\mathbf{Z} + \mathbf{Z}\alpha : \mathbf{Z} + \mathbf{Z}f\alpha] = |\mathbf{Z}/f\mathbf{Z}| = |f|.$$

So we have an incredibly simple solution for quadratic number fields, there is exactly one order of a given index in $\mathbf{Z}_K$. Hence in the quadratic case can say the following.

Proposition 2. If $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\alpha$ and $R = \mathbf{Z} + \mathbf{Z}m\alpha$ then

$$\text{Orders}(R, I) = \{\mathbf{Z} + \mathbf{Z}Im\alpha\}.$$

Proof. This follows immediately from the above description of orders of K (proposition 1) and the fact that the index is multiplicative (corollary 1). □

Orders in quadratic fields appear in the theory of elliptic curves with complex multiplication. The endomorphism ring of an elliptic curve is either isomorphic to $\mathbf{Z}$ or an order $\mathcal{O}$ of an imaginary quadratic number field (i.e. a quadratic number field K where $K \cap \mathbf{R} \neq K$). In the second case the curve is said to have *complex multiplication*. The theory of such curves is interesting and has practical applications in the field

of cryptography and other areas, see [Sch10]. A general solution to our problem is of course not particularly useful here as the situation is so simple. However it is maybe conceivable that our methods could find application in generalisations of the theory of complex multiplication (to higher dimensional abelian varieties). This is not a direction we have pursued but it might be worthwhile to do so.

3.2 Monogenic orders

We now look at a special class of orders that have been studied extensively by other authors, though the focus of their methods has been slightly different to ours.

Definition 25 (Monogenic order)**.** An order of the form $\mathbf{Z}[\alpha]$ for some algebraic integer α is called *monogenic*.

Monogenic orders can be easier to work with than more general orders and are common in algebraic number theory. The ease of computing with them comes from the fact that

$$\mathbf{Z}[\alpha] = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\alpha^2 + \cdots + \mathbf{Z}\alpha^{n-1}$$

and so $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $\mathbf{Z}[\alpha]$ as a $\mathbf{Z}$ module (here n is $[K : \mathbf{Q}]$). With this basis computing products of elements with a computer (and by hand) is simpler to do than in general making them natural bases to work with. A basis of this form is known as a *power basis*.

Several authors have studied the problem of finding monogenic orders, mostly with a view to showing that the ring of integers is monogenic and finding elements α such that $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ in this case. This is essentially the problem of finding monogenic orders of index 1 in $\mathbf{Z}_K$. An up-to-date account of the methods known for performing such computations is given in István Gaál's book [Gaá02]. Here we attempt to convey the approach these methods take without going into detail concerning the exact methods of solution.

Given an order $\mathcal{O}$ of a number field K of degree n such that

$$\mathcal{O} = \mathbf{Z} + \mathbf{Z}\omega_2 + \cdots + \mathbf{Z}\omega_n.$$

We can calculate the index of the order $\mathbf{Z}[\alpha]$ where $\alpha = x_1 + x_2\omega_2 + \cdots x_n\omega_n \in \mathcal{O}$ as follows.

First we recall [NS10, pp. 11–15] that the discriminant of an order $\mathcal{O}$ in a number field K is given by

$$d(\mathcal{O}) = \det(\sigma_i(\alpha_j))^2$$

where the σ_i are the embeddings of K into $\mathbf{C}$ and the α_j are a $\mathbf{Z}$-basis for $\mathcal{O}$. Now given two orders $\mathcal{O} \subset \mathcal{O}'$ it is the case that

$$d(\mathcal{O}) = [\mathcal{O}' : \mathcal{O}]^2 d(\mathcal{O}')$$

And so the index is given by

$$[\mathcal{O}' : \mathcal{O}] = \sqrt{\frac{d(\mathcal{O})}{d(\mathcal{O}')}}. \tag{3.1}$$

In the special case where $\mathcal{O} = \mathbf{Z}[\alpha]$ a $\mathbf{Z}$-basis for $\mathcal{O}$ is $1, \alpha, \ldots, \alpha^{n-1}$ and we have that

$$\begin{aligned} d(\mathcal{O}) &= \det \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_{n-1}(\alpha) & \cdots & \sigma_{n-1}(\alpha)^{n-1} \end{pmatrix}^2 \\ &= \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \end{aligned}$$

Now if we take α to be given by $\alpha = x_1 + x_2\omega_2 + \cdots x_n\omega_n$ we have that in fact

$$\prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = \prod_{1 \leq i < j \leq n} (\sigma_i(x_2\omega_2 + \cdots + x_n\omega_n) - \sigma_j(x_2\omega_2 + \cdots + x_n\omega_n))^2$$

as the term x_1 will be fixed under all embeddings σ_i. To simplify things a little we let $\beta = x_2\omega_2 + \cdots + x_n\omega_n$.

We can introduce polynomials $f_{i,j}(x_2, \ldots, x_n)$ for $1 \leq i, j \leq n$ such that

$$\beta^{i-1} = f_{1,i}(x_2, \ldots, x_n) + f_{2,i}(x_2, \ldots, x_n)\omega_2 + \cdots + f_{n,i}(x_2, \ldots, x_n)\omega_n$$

and then we have

$$\begin{aligned}
d(\mathcal{O}) &= \prod_{1\le i<j\le n} (\sigma_i(\beta)-\sigma_j(\beta))^2 \\
&= \det \begin{pmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \sigma_1(\beta) & \cdots & \sigma_1(\beta)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_{n-1}(\beta) & \cdots & \sigma_{n-1}(\beta)^{n-1} \end{pmatrix}^2 \\
&= \det \begin{pmatrix} 1 & \omega & \cdots & \omega^{n-1} \\ 1 & \sigma_1(\omega) & \cdots & \sigma_1(\omega)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_{n-1}(\omega) & \cdots & \sigma_{n-1}(\omega)^{n-1} \end{pmatrix}^2 \cdot \\
&\quad \det \begin{pmatrix} f_{1,1}(x_2,\ldots,x_n) & \cdots & f_{1,n}(x_2,\ldots,x_n) \\ f_{2,1}(x_2,\ldots,x_n) & \cdots & f_{2,n}(x_2,\ldots,x_n) \\ \vdots & \ddots & \vdots \\ f_{n,1}(x_2,\ldots,x_n) & \cdots & f_{n,n}(x_2,\ldots,x_n) \end{pmatrix}^2 \\
&= d(\mathcal{O}')I(x_2,\ldots,x_n)^2.
\end{aligned}$$

Where $I(x_2,\ldots,x_n)$ is the determinant of the last matrix above, this is a homogeneous polynomial of degree $n(n-1)/2$, known as the *index form*.

Substituting this into 3.1 gives that

$$[\mathcal{O}' : \mathcal{O}] = |I(x_2,\ldots,x_n)|$$

and so solving this equation $I(x_2,\ldots,x_n)$ for plus and minus the index we would like to find will give us generators for monogenic orders of the required index.

Example 6. Let $K = \mathbf{Q}(\alpha) = \mathbf{Q}[x]/(x^3+x-1)$ and $\mathcal{O}' = \mathbf{Z} + \mathbf{Z}2\alpha + \mathbf{Z}4\alpha^2$, so in this case $\beta = 2x_2\alpha + 4x_3\alpha^2$. And we find the $f_{i,j}$ as follows

$$\begin{aligned}
\beta^0 &= 1 = 1 + 0\omega_2 + 0\omega_3, \\
\beta^1 &= 0 + x_2\omega_2 + x_3\omega_3, \\
\beta^2 &= (2x_2\alpha + 4x_3\alpha^2)^2 = 4x_2^2\alpha^2 + 16x_2x_3\alpha^3 + 16x_3^2\alpha^4 \\
&= 16x_2x_3 + 8x_3(x_3-x_2)\omega_2 + (x_2^2 - 4x_3^2)\omega_3.
\end{aligned}$$

So the index form is given by

$$I(x_2,\ldots,x_n) = \det \begin{pmatrix} 1 & 0 & 16x_2x_3 \\ 0 & x_2 & 8x_3(x_3-x_2) \\ 0 & x_3 & x_2^2-4x_3^2 \end{pmatrix} = x_2^3+4x_2x_3^2-8x_3^3.$$

To find monogenic orders $\mathcal{O}$ of index n in $\mathcal{O}'$ we can now solve

$$x_2^3+4x_2x_3^2-8x_3^3 = \pm n$$

to find the β generating the order. So for example if wish to find orders of index 3 could observe that $x_2 = x_3 = 1$ is a solution to $x_2^3+4x_2x_3^2-8x_3^3 = -3$ and therefore

$$\mathbf{Z}[\beta] = \mathbf{Z}[1\cdot\omega_2 + 1\cdot\omega_3] = \mathbf{Z}[2\alpha+4\alpha^2]$$

is a suborder of index 3 in $\mathcal{O}'$.

Both Gaál's book and many papers both by him and other authors methods to explicitly solve diophantine equations appearing in the above setting are given. As the degree of the field increases so does the number of variables in the index form and the degree of the form so it becomes difficult to solve such equations for even moderate degree.

Unfortunately not all orders are monogenic and even rings of integers need not be in general. Dedekind was the first to give an example of a ring of integers that is not monogenic. His example lies inside a cubic field and it is easy to see that in the quadratic case all orders are monogenic, especially given the discussion in the above section.

Example 7 (Dedekind, 1878)**.** Let

$$K = \mathbf{Q}(\alpha) = \mathbf{Q}[x]/(x^3-x^2-2x-8)$$

then

$$\mathbf{Z}_K = \mathbf{Z}\left[\alpha, \frac{\alpha+\alpha^2}{2}\right]$$

and there is no $\beta \in \mathbf{Z}_K$ such that $\mathbf{Z}_K = \mathbf{Z}[\beta]$.

While our techniques differ from the ones developed for monogenic orders we originally were inspired to consider this problem after using an implementation of some of these techniques in the Magma computational algebra system [BCP97].

3.3 Cocyclic orders

We recall some definitions and results given by Johannes Brakenhoff in his thesis [Bra09]. These will be helpful when considering the class of cocyclic orders, defined as follows.

Definition 26 (Cocyclic subring)**.** Given two rings R and S the ring R is called a *cocyclic* subring of S if R is a subring of S and

$$S/R \cong \mathbf{Z}/m\mathbf{Z},$$

i.e. the quotient of S by R is a cyclic group.

We will refer to suborders that are cocyclic subrings as cocyclic suborders.

Example 8. Let $K = \mathbf{Q}[x]/(x^4 + 5x + 1) = \mathbf{Q}(\alpha)$ be a number field and take

$$\mathcal{O} = \mathbf{Z} + \mathbf{Z}(\alpha + 2\alpha^3) + \mathbf{Z}\alpha^2 + \mathbf{Z}5\alpha^3.$$

Then as $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ in this case we have

$$\mathbf{Z}_K/\mathcal{O} = \mathbf{Z}[\alpha]/\mathcal{O} \cong \mathbf{Z}/5\mathbf{Z}$$

and so $\mathcal{O}$ is cocyclic suborder of $\mathbf{Z}_K$.

In Brakenhoff's thesis he derives bounds for the number of orders with a given index, along with several other interesting results. Some of the methods used to obtain these bounds are naturally applicable to the problem of actually finding the orders of given index.

The following theorem is given in [Bra09, Thm. 4.1], it will allow us to find cocyclic suborders very easily. We include the proof here as it is quite instructive.

Theorem 4. Let Z be a commutative ring, A a commutative Z-algebra and fix some ideal J of Z. If we let

$$W = \{R \text{ an order of } K \mid \mathbf{Z}_K/R \cong Z/J\}$$

and

$$V = \{I \text{ an ideal of } \mathbf{Z}_K \mid A/I \cong (Z/J)^2\}.$$

then there is a bijection between V and W given by

$$\begin{aligned} f\colon W &\to V \\ R &\mapsto \{a \in A \mid aA \subseteq R\} \end{aligned}$$

and

$$\begin{aligned} g\colon V &\to W \\ I &\mapsto \mathbf{Z} + I. \end{aligned}$$

Proof. [Bra09, Thm. 4.1, pp. 35] We first show the maps are well defined. $f(R) = \mathrm{Ann}_A(A/R)$ which is an ideal of A. As Z/J is generated by 1 as a Z-module $Z/J \cong \mathrm{End}_Z(Z/J) \cong \mathrm{End}_Z(A/R)$ and so

$$\begin{aligned} \phi\colon R &\to \mathrm{End}_Z(A/R) \\ r &\mapsto (a \mapsto ra) \end{aligned}$$

is a surjective map. We therefore have the short exact sequence of Z-modules

$$0 \to f(R) \to R \to \mathrm{End}_Z(A/R) \to 0$$

and so $R/f(R) \cong \mathrm{End}_Z(A/R) \cong Z/J$. As $A/R \cong Z/J$ we have that $JA \subseteq R$ which then gives that $JA \subseteq f(R)$. So we can view $A/f(R)$ as a Z/J-module and we have the following short exact sequence of Z/J-modules

$$0 \to R/f(R) \to A/f(R) \to Z/J \to 0.$$

As Z/J is a free module over itself this sequence splits and we obtain the isomorphism

$$A/f(R) \cong R/f(R) \oplus Z/J \cong (Z/J)^2.$$

So the map f is indeed a map from W to V.

Now for g we note that $Z+I$ is a Z-algebra as it is a ring invariant under multiplication by elements of Z. We have that A/I is a quadratic Z/J algebra

□

The image of f above is still well defined for non-cocyclic orders and this ideal is

known as the *conductor* of $\mathcal{O}$ in R. Earlier we called the order $\mathbf{Z} + f\mathbf{Z}_K$ of a quadratic number field the order of conductor f, note that with our new terminology the conductor of $\mathbf{Z} + f\mathbf{Z}_K$ in $\mathbf{Z}_K$ is the ideal (f).

An equivalent definition for the conductor of an order R in another S is that it is the largest ideal of S that is contained in R. Though it is not actually required for an algorithmic resolution of our problem (we go the other way, via g, in our approach) being able to find the conductor of an order is useful for experimentation. An algorithm for computing the conductor is given in [KP05].

In the situation we are interested in the proposition reads.

Corollary 2. Let K be a number field, R an order of K and fix some $m \in \mathbf{Z}$ then let

$$W = \{\mathcal{O} \text{ an order of } K \mid R/\mathcal{O} \cong \mathbf{Z}/m\mathbf{Z}\}$$

and

$$V = \{I \text{ an ideal of } R \mid R/I \cong (\mathbf{Z}/m\mathbf{Z})^2\}.$$

Then there is a bijection between V and W given by

$$\begin{aligned} f\colon W &\to V \\ \mathcal{O} &\mapsto \{a \in R \mid aR \subseteq \mathcal{O}\} \end{aligned}$$

and

$$\begin{aligned} g\colon V &\to W \\ I &\mapsto \mathbf{Z} + I. \end{aligned}$$

This is as the only cyclic quotient of $\mathbf{Z}$ with order m is $\mathbf{Z}/m\mathbf{Z}$. As the set W above is the set of cocyclic orders of index m we can find them by finding the corresponding ideals of V and then simply adding $\mathbf{Z}$ to each. This gives the following algorithm to find cocyclic suborders with index I in another order.

Algorithm 1.
Input: A natural number I and an order R.
Output: All cocyclic suborders of R of index I in R.

for *For all ideals J of R of index I^2* **do**
  Let $M = \mathbf{Z} + I$.
  if *M is of index I* **then**
    add M to the output.
  end
end

The question of course remains, how do we find *ideals* of a given index? At first glance it might seem that this problem should be somehow equivalent to finding orders with a given index, and we have not gained anything by reducing to it. However algebraic number theory was initially developed to deal with the fact that elements of rings of algebraic integers failing to factorise uniquely in general and the theory of ideals was introduced to remedy this. So for rings of integers $\mathbf{Z}_K$ we can use the following to find ideals with a given index (or *norm* as it is more commonly known).

Algorithm 2.
Input: Integer I.
Output: All ideals in $\mathbf{Z}_K$ of norm I.
  Let L be a list containing $\mathbf{Z}_K$.
  for *All primes p dividing I* **do**
    Factor the ideal $p\mathbf{Z}_K$ into prime ideals $\mathfrak{p}_i$, store them by norm, also add the p-adic order of the norm of each $\mathfrak{p}_i$ to a set S.
    Let L' be an empty list.
    for *All expressions* $\mathrm{ord}_p(I) = s_1 + s_2 + \cdots + s_k$ *where all* $s_i \in S$. **do**
      Add all products of prime ideals $\mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_k$ where $\mathrm{ord}_p(N(\mathfrak{q}_i)) = s_i$ to the list L'.
    end
    Set L to be all possible products of an element of L and an element of L'.
  end
  Output L.

Ideal factorisation is not as nice in non-maximal orders and so finding ideals with a specified norm is more difficult there. However there is another approach to this problem which gener

However this is not a full solution of our problem as not all orders of number fields are cocyclic.

Example 9. With $K = \mathbf{Q}[x]/(x^4 + 5x + 1) = \mathbf{Q}(\alpha)$ (as in example 8) and $\mathcal{O} =$

$\mathbf{Z} + \mathbf{Z}3\alpha + \mathbf{Z}9\alpha^2 + \mathbf{Z}3\alpha^3$ we have

$$\mathbf{Z}_K/\mathcal{O} = \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z}$$

and so $\mathcal{O}$ is not cocyclic.

Indeed if we attempt to apply theorem 4 anyway we find that

$$f(\mathcal{O}) = \{a \in \mathbf{Z}_K \mid a\mathbf{Z}_K \subset \mathcal{O}\} = 9\mathbf{Z}_K.$$

However

$$g(9\mathbf{Z}_K) = \mathbf{Z} + 9\mathbf{Z}_K \neq \mathcal{O} \text{ as } 3\alpha \in \mathcal{O} \setminus (\mathbf{Z} + 9\mathbf{Z}_K)$$

and so the correspondence really does fail in this case.

There is a simple sufficient condition on the index for a suborder to be cocyclic that we can use to our advantage when finding orders.

Proposition 3. If R is a suborder of an order S such that $[S : R]$ is squarefree then R is a cocyclic suborder.

Proof. In this case we have that S/R is a finite abelian group of squarefree order I and hence isomorphic to $\mathbf{Z}/I\mathbf{Z}$. □

So we want to find suborders with some squarefree index we can just search for cocyclic orders as we know no others can occur.

3.4 General orders in absolute number fields

We originally hoped that the correspondence between suborders and their conductors that exists in the quadratic case (theorem 4) could be generalised to higher degree number fields. However the direct generalisations of this result fail to hold even in degree 3 number fields. We now give examples of some results that would be good for our purposes if true and explicit counter examples for each of them.

As noted above in proposition 3 if the index we are looking for is squarefree we know all orders of that index are cocyclic and we can use the conductor method described above. Of course there do exist non-squarefree numbers and so we now give some positive results leading to methods that can be used to find general orders in number fields.

Given a change of basis matrix A from an order R to an order S we can see that as abelian groups $R \cong \mathbf{Z}^d$ for some d and so R/S is isomorphic to $\mathbf{Z}^d/A\mathbf{Z}^d$. In fact the size of this group is the absolute value of the determinant of A.

3.4.1 The Hermite normal form

The Hermite normal form of a matrix is a unique matrix that a given matrix of integers can be brought into by unimodular row operations. Using this form will allow us to find additive subgroups of orders which will provide one approach to finding all suborders. There are varying definitions of the Hermite normal form (HNF) the one we use here is fairly common and is used in the Sage mathematical software system [S+14], though others exist such as the one given in [Coh93], they mostly differ by operations such as transposition and reordering of rows.

Definition 27 (Hermite normal form)**.** A matrix $H \in \mathrm{Mat}_{m\times n}(\mathbf{Z})$ is said to be in *Hermite normal form* if there is a strictly increasing function $f\colon \{1,\ldots,m\} \to \{1,\ldots,n\}$ such that

i) if $n' < f(m)$ then $H_{m,n'} = 0$,

ii) if $n' = f(m)$ then $H_{m,n'} > 0$,

iii) and if $m' < m$ then $0 \leq H_{m',f(m)} < H_{m,f(m)}$.

Given a matrix A, the unique matrix in Hermite normal form that can be obtained from A by unimodular row and column operations is called *the* Hermite normal form of A.

Fast algorithms for computing Hermite normal forms is an interesting and useful area of study, for a practical discussion of some of the most effective ways of doing this see Pernet and Stein [PS10]. Cohen also gives several algorithms for finding the Hermite normal form in [Coh93], these are more classical methods that are conceptually simpler. Many basic operations such as checking equality of orders can be performed quickly using Hermite normal forms [Coh93].

One possible method of finding orders with a prescribed index is therefore to attempt to generate their HNF matrices. These will be all those matrices with absolute value of the determinant equal to the index searched for that define suborders rather than simply submodules. In the next sections we look at the steps needed to do this in detail.

3.4.2 Generating matrices in Hermite normal form

For the remainder of this section we deal only with square matrices of full rank as this is all that is required for our purposes.

For a square $(n \times n)$ matrix of full rank the conditions for a matrix to be in Hermite normal form reduce to the following:

i) if $i < j$ then $H_{i,j} = 0$,

ii) if $i = j$ then $H_{i,j} > 0$,

iii) and if $i < j$ then $0 \leq H_{i,j} < H_{j,j}$.

So the matrix is upper triangular and all entries are positive and bounded above by the last non-zero entry of their column. The determinant of an upper triangular matrix is the product of the elements on the diagonal so we first look at ways of expressing our desired determinant as a product of n positive integers. We can do this with a simple recursive algorithm as follows.

Algorithm 3.
Input: Integers n and D.
Output: A list of all possible factorisations with orderings of D which have length n.

if $n = 1$ **then**
| return $[D]$
end
for *each divisor* d *of* D **do**
| Recurse on $n - 1$ and D/d appending d to the end of each factorisation.
| Add each factorisation obtained to the output.
end

Now given the possible diagonal entries we need to consider ways of filling in the off diagonal elements. As mentioned above the only restriction is that we have each entry above the diagonal in column i positive and strictly bounded by $A_{i,i}$ above. So when the diagonal entries are fixed the set of matrices in the right form can be seen

Hence in order to generate matrices that are already in Hermite normal form we use the following algorithm.

3.4.3 Determining if a module is a ring

Assuming that we are given a change of basis matrix A from the basis of an order R we wish to determine if the module spanned by the new basis is an order.

For a full rank **Z**-submodule to be a subring and hence an order we require that it contain 1 and be multiplicatively closed, determining the first of these properties quickly is relatively easy, whereas the second is a little harder. We'll consider them both below.

To determine if a submodule contains 1 we just have to check that we can represent it by an integer vector in out new basis.

Algorithm 4.

Input: Change of basis matrix H.

Output: Whether or not the submodule defined by H contains 1.

Find the representation $\mathbf{v}$ of 1 in the old basis.

if $H^{-1}\mathbf{v}$ *is an integer matrix* **then**

| Return yes.

else

| Return no.

end

It is clear that with this approach we can determine if other elements lie in the submodule too, but 1 is the only one we care about.

In [Coh93] Cohen gives the general method for determining if a finitely generated submodule of a ring is closed under multiplication. The correctness of the method hinges on the fact that if the products of all pairs of basis elements lie inside the module, then the product of any two linear combinations of these elements lie inside the module too.

Algorithm 5.

Input: Change of basis matrix B.

Output: Whether or not the submodule defined by H is multiplicatively closed.

Find matrix B'.

Compute the Hermite normal forms of B and B' denote them H and H'.

if $H' = H$ *on the first* n *rows* **then**

| Return yes.

else

| Return no.

end

3.4.4 The HNF algorithm

Algorithm 6.

Input: A natural number I and an order R.

Output: All suborders of R of index I in R.

for *all* $n \times n$ *HNF matrices* H *of determinant* I **do**
  Find the submodule M of R corresponding to H.
  if M *is a ring (via algorithm 4 and algorithm 5)* **then**
    add M to the output.
  end
end

In fact using the lemma **??** we can improve this algorithm slightly. As we know that we can always include 1 in the basis of an order we can take a basis of the order we are given that contains 1. Then we can find change of basis matrices that fix this element, this provides a slight improvement over simply looking for all submodules.

Algorithm 7.
Input: Natural number I and an order R.
Output: All suborders of R of index I in R.
  Ensure 1 is the first element of the $\mathbf{Z}$ basis of R.
  for *all* $(n-1) \times (n-1)$ *HNF matrices* H *of determinant* I **do**
    Let

$$H' = \left(\begin{array}{c|c} 1 & 0 \cdots 0 \\ \hline 0 & \\ \vdots & H \\ 0 & \end{array}\right).$$

    Find the submodule M of R corresponding to H'.
    if M *is multiplicatively closed (algorithm 5)* **then**
      add M to the output.
    end
  end

3.5 Practical considerations

Though the methods described above are the best we have been able to obtain so far from a theoretical perspective, when it comes down to computing examples in the real world there are a number of ideas and techniques we can use to reduce the time taken.

Many of the algorithms given above are presented in a manner similar to the way in which they are motivated and can in fact be implemented in a faster manner than as they are written. For example

3.5.1 Parallelisation

Several stages of the algorithms for general orders can be naturally parallelised reducing the total time taken linearly with the number of threads used. For example once the set of potential conductors has been computed the orders to which they correspond can all be computed in parallel. Similarly the set of HNF matrices used can be computed in parallel and whether the modules they generate form rings or not can be checked simultaneously too.

3.5.2 Timings

In order to get an idea for how these algorithms behave in practice we have timed the different methods on several large input sets. The algorithms were run on ...

Input	HNF algorithm	Conductor algorithm	Hybrid
Cubic fields of small discriminant (< 100)	1.0s	1.0s	1.0s
Cubic fields of small discriminant (< 100)	1.0s	1.0s	1.0s
Cubic fields of small discriminant (< 100)	1.0s	1.0s	1.0s
Cubic fields of small discriminant (< 100)	1.0s	1.0s	1.0s

Table 3.1: Timings for different algorithms for several input sets

4 Finding elliptic curves

Though the main problem itself is an interesting one which is worth studying in its own right we were also motivated to look at it by the potential applications to other questions within different areas of mathematics. One problem relating to elliptic curves where the methods developed above can be applied is detailed below. We also give a few examples we have solved using our techniques.

Given an elliptic curve we can define a number field to help us study the torsion points of E.

Definition 28 (n-division field)**.** For a natural number n the *n-division field* (or *n-torsion field*) of E, denoted $\mathbf{Q}(E[n])$ is obtained by taking all points $(x, y) \in E(\overline{\mathbf{Q}})[n] \setminus 0$ and adjoining the collections of each of the coordinates x and y to $\mathbf{Q}$. Here $\overline{\mathbf{Q}}$ denotes the algebraic closure of $\mathbf{Q}$, the algebraic numbers.

As the n-torsion subgroup $E(\overline{\mathbf{Q}})[n]$ is always finite there are at most finitely many elements (all of which are algebraic) that need adjoining to $\mathbf{Q}$. So the n-division field is always a number field.

For an elliptic curve defined over the rationals in long Weierstrass form such as

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ with } a_i \in \mathbf{Q},$$

we can always find an isomorphic curve of the form

$$E'\colon y^2 = x^3 + a_2'x^2 + a_4'x + a_6',$$

such a curve is said to be in *medium Weierstrass form.*

Assuming that the curve E has no rational 2-torsion points we must have no rational solution to $f = x^3 + a_2x^2 + a_4x + a_6$ and hence this polynomial is irreducible over $\mathbf{Q}$ as it is of degree 3. We can then see that we have $\mathbf{Q}[x]/(f)$ isomorphic to a subfield of the two torsion field $\mathbf{Q}(E[2])$, we will let K_E be $\mathbf{Q}[x]/(f)$. Letting α be the image of x in the

above quotient, we can see that $\mathbf{Z}[\alpha]$ is an order of K_E. The index of this order in $\mathbf{Z}_K$ is given, as mentioned in the section on monogenic orders, by the following expression

$$[\mathbf{Z}_K : \mathbf{Z}[\alpha]] = \sqrt{\frac{\text{disc}(f)}{\Delta_K}}.$$

The discriminant of f is then related to Δ_E, the discriminant of E, in a simple manner. We have that

$$\text{disc}(f) = 2^8 \Delta_E,$$

this can be seen from the definition of Δ_E.

We want to reverse this process and look at the following problem.

Problem 3. Given a cubic number field K and an integer Δ find an elliptic curve E of discriminant Δ such that $K_E = K$.

As noted above the polynomial f obtained from the curve will give us an order in the number field K with an index that we can calculate from Δ and Δ_K. So our strategy for finding such curves will be as follows, we first find the possible orders, then try and find a polynomial f that can define the order before reconstructing the curve from that. In order for an order to be of the right form it must be monogenic, so we have two approaches to finding these orders. First we could use the methods discussed in section 3.2 to find monogenic orders by finding their ring generators. We could instead use one of the other more general methods for finding orders, and then afterwards attempt to determine if they are monogenic and find their generators if so.

Once a generator for such a monogenic order has been found the polynomial f is simply the minimal polynomial of the ring generator. While the polynomial does change if a different ring generator is used (i.e using some $\alpha + n$ instead of α, with $n \in \mathbf{Z}$) the different polynomials will give isomorphic curves.

Example 10. The elliptic curve

$$E\colon y^2 + y = x^3 - x$$

has discriminant $\Delta = 37$ and is isomorphic to

$$E'\colon y^2 = x^3 - x + \frac{1}{4}.$$

So the field K_E as defined above is $\mathbf{Q}[x]/(x^3 - 16x + 16)$.

gives the curve E': ... which is isomorphic to E!

In this example we knew the curve we were searching for at the start, but in the next one we perform a more open-ended search.

Example 11. Let us try and find elliptic curves E with discriminant in the set $\{\pm 11^s \mid s = 1, \ldots, 11\}$ and $K_E = \mathbf{Q}[x]/(x^3 - x^2 + x + 1)$.

5 Conclusion

We have found several methods for computing orders with a given index, which work in varying generality and with various speeds.

5.1 Further work

It seems likely that other properties of the orders we are looking for could be used to speed up the algorithms given above and so further investigations into both special and general cases could yield results. Other applications of these methods are definitely possible and it would be interesting to see what other areas these methods can be used in.

There are certainly several different ways of improving the above methods that could be tried and it would likely be worthwhile to do so.

Firstly there may be opportunities to exploit the specific structure of orders in number fields of low degree. For example above we observed that the situation is very simple for orders in quadratic fields as there is a very explicit description for orders in these fields. While there is certainly more variety in the cubic case finding good descriptions for orders in cubic fields might allow one to find these orders far faster than any general method.

There are also possibly some easy to check necessary or sufficient conditions for ideals to have a specified quotient structure, these could speed up computations in the case where cocyclic orders are needed. In a similar vein there may be easier to check conditions to determine whether a change of basis matrix defines a subring as opposed to just a submodule, checking such conditions would be useful in the Hermite normal form based algorithms.

The natural extension to relative number fields given as problem 2 above is not something we have considered in detail however it should be fairly simple to generalise to this case as many of the ideas we use (such as the theory of Hermite normal forms and theorem 4) extend to this more general setting.

Finally of course there may be some methods for finding orders completely different to those considered here!

5.2 Acknowledgements

First and foremost I would like to thank Lassina Dembélé for his excellent guidance while I undertook the project, it was truly a pleasure to work with him. I am also grateful to John Cremona for allowing me access to one of the Warwick number theory group's servers to run computations on.

Bibliography

[AM94] M. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley series in mathematics. Westview Press, 1994.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Bra09] J. Brakenhoff. *Counting problems for number rings*. PhD thesis, Universiteit Leiden, 2009. `https://www.math.leidenuniv.nl/scripties/proefschrift-brakenhoff.pdf`.

[Cas91] J. W. S. Cassels. *Lectures on Elliptic Curves*. London Mathematical Society Student Texts. Cambridge University Press, 1991.

[Coh93] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, 1993.

[Coh00] H. Cohen. *Advanced Topics in Computational Number Theory*. Graduate Texts in Mathematics. Springer, 2000.

[Cox13] D. A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2013.

[Gaá02] I. Gaál. *Diophantine Equations and Power Integral Bases: New Computational Methods*. Diophantine Equations and Power Integral Bases: New Computational Methods. Birkhäuser Boston, 2002.

[Kna92] A. W. Knapp. *Elliptic Curves*. Mathematical Notes - Princeton University Press. Princeton University Press, 1992.

[KP05] J. Klüners and S. Pauli. Computing residue class rings and picard groups of orders. *Journal of Algebra*, 292(1):47 – 64, 2005. Computational Algebra.

[Lan94] S. Lang. *Algebraic Number Theory.* Applied Mathematical Sciences. Springer, 1994.

[Mar45] D. A. Marcus. *Number Fields.* Universitext. Springer, 1945.

[MR89] H. Matsumura and M. Reid. *Commutative Ring Theory.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1989.

[Nar04] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers.* Springer Monographs in Mathematics. Springer, 2004.

[NS10] J. Neukirch and N. Schappacher. *Algebraic Number Theory.* Grundlehren der mathematischen Wissenschaften. Springer, 2010.

[PS10] C. Pernet and W. Stein. Fast computation of hermite normal forms of random integer matrices. *Journal of Number Theory*, 130(7):1675 – 1683, 2010.

[PZ89] M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory.* Cambridge University Press, 1989.

[S+14] W. A. Stein et al. *Sage Mathematics Software (Version 6.1.1).* The Sage Development Team, 2014. `http://www.sagemath.org`.

[Sch10] R. Schertz. *Complex Multiplication.* New Mathematical Monographs. Cambridge University Press, 2010.

[Sil91] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics. Springer, 1991.

[ST92] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Springer Undergraduate Texts in Mathematics and Technology. Springer, 1992.

[ST02] I. Stewart and D. Tall. *Algebraic Number Theory and Fermat's Last Theorem.* A K Peters, 2002.

[Ste08] P. Stevenhagen. The arithmetic of number rings. In J. P. Buhler and P. Stevenhagen, editors, *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, Mathematical Sciences Research Institute Publications. Cambridge University Press, 2008.

[Sut12] A. V. Sutherland. Torsion subgroups of elliptic curves over number fields. 2012. `http://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf`.

[WA04] K. S. Williams and S. Alaca. *Introductory Algebraic Number Theory.* Cambridge University Press, 2004.