# Finding orders with prescribed index in number fields

Alex J. Best

Supervised by Dr. Lassina Dembélé

2014

**Abstract**

Orders in 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

This report deals with the algorithmic solution of a problem arising from algebraic number theory. Other interesting situations to which this algorithm can be applied are also looked at.

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 interesting areas we will apply our methods to.

Chapter 3 is where we consider our main problem and solutions to it. In section 3.1 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 practial timings.

Finally in section 4.1 we move on to some interesting applications of these methods to the study of elliptic curves.

# 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 $\cdot : R \times M \to M$ 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 **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 **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

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

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 $N$ with $M$ a submodule of $N$ is defined to be the quotient abelian group under addition $N/M$ with scalar multiplication given by

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

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

**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 $M_1 \subseteq M_2 \subseteq M_3$ 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* $M_{\text{tors}}$ 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 **Z**-module). Given a **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 **Z**-module.

**Example 2.**

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

is a torsion free **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.

## 2.2 Algebraic number theory

Algebraic number began with the study of algebraic numbers and their uses in solving Diophantine equations but has since expanded to encompass a huge amount of mathematics involving the use of algebraic techniques to tackle number theoretic problems.

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] or [Nar04].

**Definition 12** (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 13** (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 often have a large number of subrings, which may be of interest to us, however not all subrings are as nice as we would like them to be. So we distinguish some subrings that have desirable properties and single them out for study.

**Definition 14** (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 $\alpha$ with integer coefficients, provided $\alpha$ is an algebraic integer this will be an order.

**Definition 15** (Ring of integers)**.** The *ring of integers*, denoted $\mathbf{Z}_K$, of a number field $K$ is the unique maximal order.
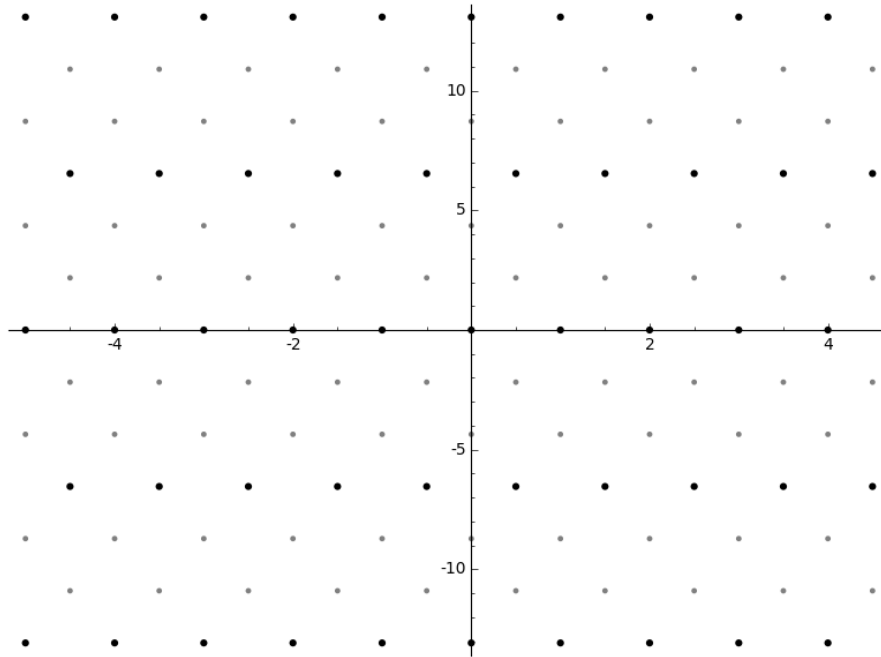
Figure 2.1: An embedding in $\mathbf{C}$ of the ring of integers of $\mathbf{Q}(\sqrt{-19})$ and an index 3 suborder.

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

11

chapter 3, but section 4.1 uses these ideas heavily. As with the above sections everything here can be found in textbooks on elliptic curves (such as [Kna92]), we offer a rapid summary moving quickly to the notions relevant to the project in this overview.

**Definition 16** (Elliptic curve). For us an *elliptic curve E* defined over a field $K$ will be given by a binary cubic equation of the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \text{ with } a_i \in K.$$

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

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

We then also require that the *discriminant* $\Delta$ of $E$, given by

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

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

Given an elliptic curve $E$ defined over a field $K \subset K'$ 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 $\infty$. This additional point is called the point at infinity, the reasons for its inclusion in the set should become clear later.

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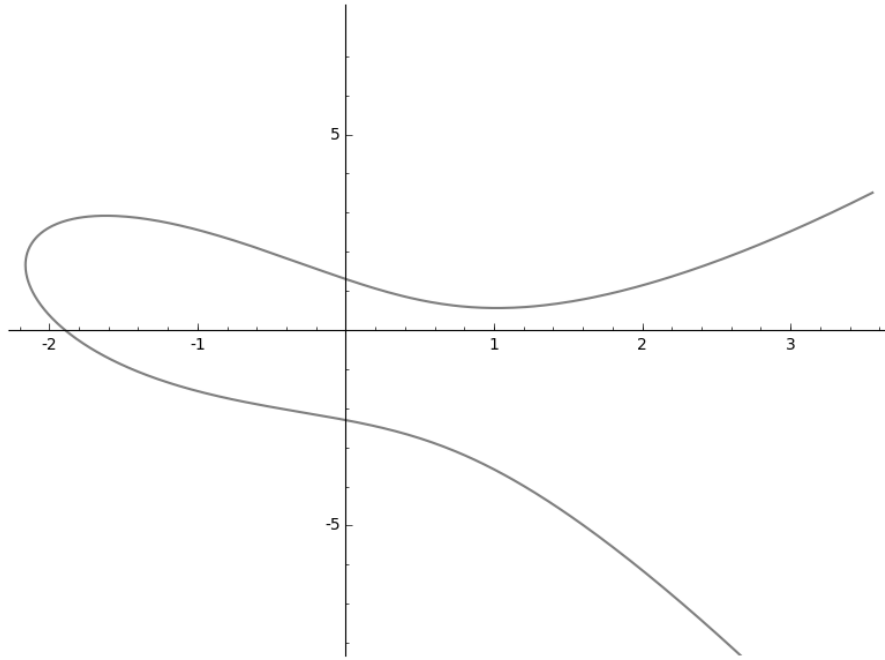
Figure 2.2: The real points of $E\colon y^2 + 2xy + y = x^3 - 2x + 3$.

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 17** (Group law)**.** We define the sum of two points $P, Q \in E(K)$ 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 $P + Q$.

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 $P$). From now on we will denote the point $\infty \in E(K)$ as $0$, but still refer to it as *at infinity.*

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

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

13

and letting $n \cdot z = (-n) \cdot (-z)$ for negative $n \in \mathbf{Z}$. With this idea in mind $E(K)_{\mathrm{tors}}$ 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 $E(\mathbf{Q})_{\mathrm{tors}}$ can be.

**Theorem 3** (Mazur's torsion theorem)**.** Given an elliptic curve $E$ defined over the rationals $E(\mathbf{Q})_{\mathrm{tors}}$ 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 18** ($n$-division points)**.** For some $n \in \mathbf{Z}$ the set of *$n$-division points* of $E$ over $K$ is

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

Although $E(\mathbf{Q})_{\mathrm{tors}}$ cannot be large by theorem 3 it is still useful to consider the $n$-division points of a curve over the rationals and we will use this group later.

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 The problem

## 3.1 Statement

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

To find a suborder we really mean compute a $\mathbf{Z}$ basis for the order, as such a basis defines an order completely. With $R$ and $I$ as in the proposition we introduce the following notation to refer to the set we are looking for.

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

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

**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 this problem in varying generality.

## 3.2 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 $f \in \mathbf{Z}$, $\alpha$ as above.

For a proof see [Cox13, pp. 133–134].

**Definition 19.** 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). $\qquad\square$

Orders in quadratic fields appear in the theory of elliptic curves with complex multiplication. While the solution to our problem in this special case is not useful here as the theory is so simple, it is maybe conceivable that our methods could find application in generalisations of the theory of complex multiplication (to higher dimensional abelian varieties).

## 3.3 Monogenic orders

We now look at a special class of orders that have, in effect, been studied extensively by other authors.

**Definition 20** (Monogenic order). An order of the form $\mathbf{Z}[\alpha]$ for some algebraic integer $\alpha$ is called *monogenic*.

Monogenic orders are easier to work with 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.

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 6** (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 $\mathbf{Z}_K = \mathbf{Z}[\beta]$.

## 3.4 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 21** (Cocyclic order). An order $\mathcal{O}$ of a number field $K$ is called *cocyclic* if

$$\mathbf{Z}_K/\mathcal{O} \cong \mathbf{Z}/m\mathbf{Z},$$

i.e. the quotient of the maximal order of the $K$ by $\mathcal{O}$ is a cyclic group.

**Example 7.** 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 $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ we have

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

and so $\mathcal{O}$ is cocyclic.

The following theorem is given in [Bra09, Thm. 4.1], it will allow us to find cocyclic orders 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

$$f : W \to V$$
$$R \mapsto \{a \in A \mid aA \subseteq R\}$$

and

$$g : V \to W$$
$$I \mapsto \mathbf{Z} + I.$$

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

$\operatorname{End}_Z(Z/J) \cong \operatorname{End}_Z(A/R)$ and so

$$\phi \colon R \to \operatorname{End}_Z(A/R)$$
$$r \mapsto (a \mapsto ra)$$

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

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

$\square$

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 $(f)$. 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

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

and

$$g \colon V \to W$$
$$I \mapsto \mathbf{Z} + I.$$

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.**

> **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 rings of algebraic integers failing to have unique factorisation 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: Norm $I$
>
> **for** *All primes $p$ dividing $I$* **do**
> > Factor the ideal $p\mathbf{Z}_K$ into prime ideals $\mathfrak{p}_i$, store them by norm.
> >
> > Find all ideals in $\mathbf{Z}_K$ of index $I^2$.
>
> **end**

Ideal factorisation is not as nice in non-maximal orders and so finding ideals with a specified norm is more difficult there.

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

**Example 8.** With $K = \mathbf{Q}[x]/(x^4 + 5x + 1) = \mathbf{Q}(\alpha)$ (as in example 7) and $\mathcal{O} = \mathbf{Z} + \mathbf{Z}3\alpha + \mathbf{Z}9\alpha^2 + \mathbf{Z}3\alpha^3$ we have

$$\mathbf{Z}_K/\mathcal{O} =$$

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.

## 3.5 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.

Here we now give some positive results leading to methods that can be used to find general orders in number fields.

### 3.5.1 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 22** (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 an 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. In the next sections we look at the steps needed to do this in detail.

### 3.5.2 Generating matrices in Hermite normal form

### 3.5.3 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.

In [Coh93] Cohen gives the basic .

|                 |                         |
|-----------------|-------------------------|
|                 | Input: $H$.             |
|                 | Check if $1 \in M$.     |
| **Algorithm 3.** | Find matrix.            |
|                 | Compute HNF.            |
|                 | Check equality.         |

### 3.5.4 The HNF algorithm

**Algorithm 4.**

> **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 3)* **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 and of course as all orders necessarily contain 1 we

**Algorithm 5.**

    **for** *all $(n-1) \times (n-1)$ HNF matrices $H$ of determinant $I$* **do**

        Let
$$H' = \begin{pmatrix} 1 & 0\cdots0 \\ \hline \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} & H \end{pmatrix}.$$

        Find the submodule $M$ of $R$ corresponding to $H'$.

        **if** *$M$ is multiplicatively closed* **then**

          |  add $M$ to the output.

        **end**

    **end**

### 3.5.5 Making use of less general methods

Given the results discussed in 3.4 we can improve the performance of the above algorithm as follows.

**Algorithm 6.**

    Find cocyclic orders of index $I$ in $\mathcal{O}$ using algorithm 1.

    **for** *all HNF matrices $H$ of determinant $I$* **do**

        **if** *$H$ is the matrix of a cocyclic order already found* **then**

          |  Move to the next matrix.

        **end**

        Find the submodule $M$ of $\mathcal{O}$ corresponding to $H$.

        **if** *$M$ is a subring* **then**

          |  add $M$ to the output.

        **end**

    **end**

## 3.6 Relative number fields

## 3.7 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.

### 3.7.1 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.

### 3.7.2 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 |

Table 3.1: Timings for different algorithms for several input sets

# 4 Applications

Through 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 the same areas of mathematics. One of the most prominent areas in which a solution to the problem can be used is to answer questions about elliptic curves. How a solution to the problem considered above can be applied in this case is detailed below, along with results obtained from the application of our methods there.

## 4.1 Elliptic curves

Given an elliptic curve defined over the rationals in long Weierstrass form, for example

$$E_l \colon y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \text{ with } a_i \in \mathbf{Q},$$

we can find an isomorphic curve $E \colon y^2 = x^3 + a_2' x^2 + a_4' x + a_6'$, such a curve is said to be in *medium Weierstrass form*.

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

**Definition 23** (*p*-division field). For a prime $p$ the *p*-division field of $E$, denoted $\mathbf{Q}(E[p])$ is obtained by taking all points $(x, y) \in E(\overline{\mathbf{Q}})[p] \setminus 0 \subset \mathbf{Q}^2$ and adjoining the collection of each of their coordinates $x$ and $y$ to $\mathbf{Q}$. Here $\overline{\mathbf{Q}}$ denotes the algebraic closure of $\mathbf{Q}$, the algebraic numbers.

As the torsion subgroup $E(\mathbf{Q})_{\text{tors}}$ is always finite there are at most finitely many elements that need adjoining to $\mathbf{Q}$, so this field is always a number field.

Assuming that the curve $E$ has no rational 2-torsion points we must have no rational solution to $f = x^3 + a_2 x^2 + a_4 x + a_6$ and hence this polynomial is irreducible over $\mathbf{Q}$. We can then see that we have

$$\mathbf{Q}(E[2]) \cong \mathbf{Q}[x]/(f)$$

as $\mathbf{Q}(E[2])$ is the splitting field of $f$ and $f$ is irreducible. Letting $\alpha$ be the image of $x$ in the above quotient, we can see that $\mathbf{Z}[\alpha]$ is an order of $\mathbf{Q}(\alpha) \cong \mathbf{Q}(E[2])$.

**Example 9.**

**Example 10.**

# 5 Conclusion

## 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 interesting results. Further applications of these methods are certainly possible and it would be interesting to see what other areas these methods can be used in.

## 5.2 Acknowledgements

First and foremost I would like to thank Lassina Dembélé for his excellent guidance while I undertook the project. 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]  Wieb Bosma, John Cannon, and Catherine 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`.

[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.

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

[KP05]   Jürgen Klüners and Sebastian 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]    Clément Pernet and William 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`.

[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.

[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.