Finding orders with prescribed index in number fields

Alex J. Best
Supervised by Dr. Lassina Dembélé

2014

Abstract

We develop algorithms for performing computations within algebraic number theory. Methods are developed to obtain all orders in a given number field with a specified index. 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 discussed.

We first go through the background material needed to motivate, define and describe the solution of our problems in chapter 2. Then in section 3.1 we move on to 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. 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

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

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.

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

Example 1.

In fact every abelian group can be given a $\mathbf{Z}$-module structure so of course they are ubiquitous in all commutative algebra, nevertheless it is useful to think of the modules used here in terms of $\mathbf{Z}$ rather than as abstract abelian groups.

Definition 2 (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.

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.

Definition 3 (Index)**.** Given two R-modules $M \subset N$ the index of M in N, denoted $[N\colon M]$ is the size of the quotient abelian group, ignoring the module structure.

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

Definition 4 (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 5 (Torsion submodule)**.** The *torsion submodule* M_{tors} of an R-module M is the set

$$\{m \in M \mid \exists r \in R \setminus 0 \text{ s.t. } rm = 0\}.$$

This is the set of elements that can be killed by a 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 6 (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 with submodule

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

The quotient module

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

has torsion submodule equal to $\mathbf{Z}/2\mathbf{Z}$ and is of rank 1.

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].

Definition 7 (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 8 (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 9 (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).

Definition 10 (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 $\mathbf{Q}$.

We can use the notion of index in a variety of situations here, such as considering the index of a module in another, the index of a module in a ring, etc.

Example 4.

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

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 section 4.1 uses these ideas heavily.

Given an elliptic curve E and a field K we let $E(K)$ be the set of points in K^2 satisfying the equation defining E, along with an extra point ∞. This extra point is called the point at infinity, the reasons for its inclusion in the set should become clear later.

Example 5. Let

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

Then we can see for example 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:

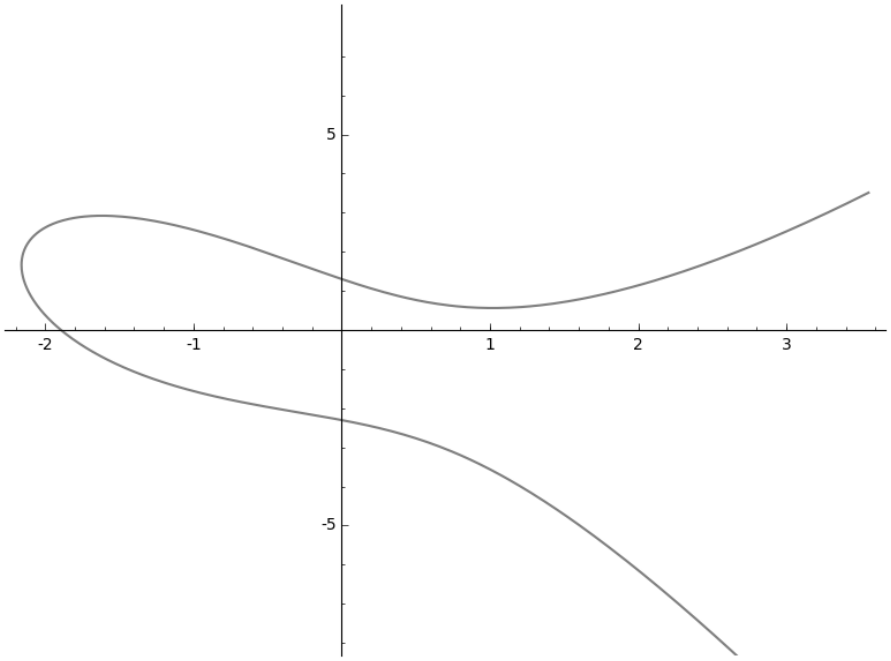

Figure 2.1: $E(\mathbf{R})$

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, and if this is done properly the set of points on the curve becomes a group.

Definition 11 (Group law)**.**

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 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 1 (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 12 (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 by theorem 1 $E(\mathbf{Q})_{\text{tors}}$ cannot be very large it is still useful to consider the n-division points of a curve and we will use this group later.

We are now ready to state in precise terms the project 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

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

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.

Notation 1.

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

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

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

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 $f \in \mathbf{Z}$, α as above.

For a proof see [Cox13, pp. 133–134].

Definition 13. 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). □

3.3 Monogenic orders

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

Definition 14 (Monogenic order)**.** An order of the form $\mathbf{Z}[\alpha]$ for some algebraic integer α is called *monogenic*.

Monogenic orders are easier to work with and are fairly 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 $[K\colon \mathbf{Q}]$).

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

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

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

Example 6. Let $K = \mathbf{Q}[x]/(x^4) = \mathbf{Q}(\alpha)$ be a number field and take

$$\mathcal{O} = \mathbf{Z} + \mathbf{Z}3\alpha + \mathbf{Z}9\alpha^2 + \mathbf{Z}3\alpha^3.$$

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

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

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

The following theorem which is a specialisation of [Bra09, Thm. 4.1] will allow us to find cocyclic orders very easily.

Theorem 2. Let K be a number field and fix some $m \in \mathbf{Z}$ then let

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

and

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

Then there is a bijection between V and W given by

$$\begin{aligned} f\colon W &\to V \\ \mathcal{O} &\mapsto (\mathbf{Z}_K\colon \mathcal{O}) \end{aligned}$$

and

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

Proof. [Bra09, Thm. 4.1, pp.???]

□

The set W above is the set of cocyclic orders of index m and so we can find them by finding the corresponding ideals of V and then simply adding in $\mathbf{Z}$.

However this is not a complete solution of the problem we wish to solve as not all orders of number fields are cocyclic.

Example 7. With $K =$ (as in 6) and $\mathcal{O} = \mathbf{Z} + 9\mathbf{Z}_K$ we have

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

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

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 2) 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.

3.5.1 The Hermite normal form

3.5.2 The basic algorithm

3.5.3 Making use of less general methods

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

3.6 Relative number fields

3.7 Practical speed-ups

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 algorithm 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.

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

$$E_l\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \text{ with } a_i \in \mathbf{Q},$$

we can find an isomorphic curve $E\colon y^2 = x^3+$.

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

Definition 16 (p-division field)**.** For a prime p the p-division field of E, denoted $\mathbf{Q}(E[p])$ is obtained by taking all points $(x, y) \in E(\mathbf{Q})[p] \setminus 0 \subset \mathbf{Q}^2$ and adjoining each of their coordinates x and y to $\mathbf{Q}$.

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 fairly nice.

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

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

Letting α be the image of x in the above quotient, we can see that

$$\mathbf{Z}[\alpha] \subset \mathbf{Q}(\alpha)$$

is an order of $\mathbf{Q}(\alpha)$.

5 Conclusion

5.1 Further work

It seems fairly 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 cases and the general cases could yield 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.

[Bra09] J. Brakenhoff. *Counting problems for number rings*. PhD thesis, Universiteit Leiden, 2009.

[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 New York, 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.

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

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

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

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

[Sut12] A. V. Sutherland. Torsion subgroups of elliptic curves over number fields. 2012.