Tables of elliptic curves over number fields

John Cremona

University of Warwick

10 March 2014

EPSRC
Engineering and Physical Sciences Research Council

THE UNIVERSITY OF WARWICK

Overview

1. Why make tables? What is a table?
2. Simple enumeration
3. Using modularity
4. Curves with prescribed primes of bad reduction, or known conductor or L-function

Why make tables of elliptic curves?

Since the early days of using computers in number theory, computations and tables have played an important part in experimentation, for the purpose of formulating, proving (and disproving) conjectures. This is particularly true in the study of elliptic curves.

Why make tables of elliptic curves?

Since the early days of using computers in number theory, computations and tables have played an important part in experimentation, for the purpose of formulating, proving (and disproving) conjectures. This is particularly true in the study of elliptic curves.

Originally the tables were relatively hard to use (let alone to make) as they were available in printed form, or on microfiche! Example: the Antwerp IV tables (1976).

Why make tables of elliptic curves?

Since the early days of using computers in number theory, computations and tables have played an important part in experimentation, for the purpose of formulating, proving (and disproving) conjectures. This is particularly true in the study of elliptic curves.

Originally the tables were relatively hard to use (let alone to make) as they were available in printed form, or on microfiche! Example: the Antwerp IV tables (1976). Now life is much easier! Packages such as SAGE, MAGMA and PARI/GP contain elliptic curve databases (sometimes as optional add-ons as they are large); the internet makes accessing even “printed” tables much easier; and we have the **LMFDB**.

Why make tables of elliptic curves?

Since the early days of using computers in number theory, computations and tables have played an important part in experimentation, for the purpose of formulating, proving (and disproving) conjectures. This is particularly true in the study of elliptic curves.
Originally the tables were relatively hard to use (let alone to make) as they were available in printed form, or on microfiche! Example: the Antwerp IV tables (1976). Now life is much easier! Packages such as SAGE, MAGMA and PARI/GP contain elliptic curve databases (sometimes as optional add-ons as they are large); the internet makes accessing even "printed" tables much easier; and we have the **LMFDB**.
These tables / databases are for **elliptic curves over** $\mathbb{Q}$ only!

Early tables over number fields

What tables exist for elliptic curves over number fields (other than $\mathbb{Q}$)?

Early tables over number fields

What tables exist for elliptic curves over number fields (other than $\mathbb{Q}$)?
My PhD thesis (1981) contains 184 elliptic curves (in 138 isogeny classes) defined over five imaginary quadratic fields:

Field	norm $\leq$	#classes	#curves
$\mathbb{Q}(\sqrt{-1})$	500	$40+2=42$	$55+2=57$
$\mathbb{Q}(\sqrt{-2})$	300	$36+4=40$	$51+4=55$
$\mathbb{Q}(\sqrt{-3})$	500	$30+2=32$	$33+2=35$
$\mathbb{Q}(\sqrt{-7})$	200	$18+1=19$	$30+1=31$
$\mathbb{Q}(\sqrt{-11})$	200	$14+3=17$	$15+3=18$

These appeared in my first paper (Compositio 1984) with some additional (previously “missing”) curves added in 1987.

Why these fields and ranges?

For these five fields I had developed a theory of modular symbols and hence had computed, for levels $\mathfrak{n}$ whose norm is bounded as above, all rational cuspidal newforms of weight 2 for the Bianchi congruence subgroups $\Gamma_0(\mathfrak{n})$.

Why these fields and ranges?

For these five fields I had developed a theory of modular symbols and hence had computed, for levels $\mathfrak{n}$ whose norm is bounded as above, all rational cuspidal newforms of weight 2 for the Bianchi congruence subgroups $\Gamma_0(\mathfrak{n})$.

This explains the small norm bound! The computations were mostly done in 1980-81. The elliptic curves were mostly found by a simple search, and I could detect isogenies but not compute them, so these tables are not complete under isogeny.

Why these fields and ranges?

For these five fields I had developed a theory of modular symbols and hence had computed, for levels $\mathfrak{n}$ whose norm is bounded as above, all rational cuspidal newforms of weight 2 for the Bianchi congruence subgroups $\Gamma_0(\mathfrak{n})$.

This explains the small norm bound! The computations were mostly done in 1980-81. The elliptic curves were mostly found by a simple search, and I could detect isogenies but not compute them, so these tables are not complete under isogeny.

The combination of

1. modular form computations: which curves do we expect? and
2. targeted searching: which curves can we find?

will be an underlying theme of this talk.

Which curve models?

How do we specify an elliptic curve defined over a number field K? By a Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

or $[a_1, a_2, a_3, a_4, a_6]$ for short.

Which curve models?

How do we specify an elliptic curve defined over a number field K? By a Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

or $[a_1, a_2, a_3, a_4, a_6]$ for short. We can insist on **integral models** (with all $a_j \in \mathcal{O}_K$) and if the class number $h_K = 1$ on **global minimal models** (minimal at all primes of K).

Which curve models?

How do we specify an elliptic curve defined over a number field K? By a Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

or $[a_1, a_2, a_3, a_4, a_6]$ for short. We can insist on **integral models** (with all $a_j \in \mathcal{O}_K$) and if the class number $h_K = 1$ on **global minimal models** (minimal at all primes of K).

We still have to deal with scaling by units ($a_j \mapsto u^j a_j$), not a big issue for imaginary quadratic K, and by coordinate shifts we can assume that a_1, a_2, a_3 are reduced modulo $2, 3, 2$ (respectively).

Which curve models?

How do we specify an elliptic curve defined over a number field K? By a Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

or $[a_1, a_2, a_3, a_4, a_6]$ for short. We can insist on **integral models** (with all $a_j \in \mathcal{O}_K$) and if the class number $h_K = 1$ on **global minimal models** (minimal at all primes of K).

We still have to deal with scaling by units ($a_j \mapsto u^j a_j$), not a big issue for imaginary quadratic K, and by coordinate shifts we can assume that a_1, a_2, a_3 are reduced modulo $2, 3, 2$ (respectively).

Over $\mathbb{Q}$ this gives **unique** "reduced minimal models", but not over any other number fields except for the 7 imaginary quadratic fields K with $h_K = 1$ and $\mathcal{O}_K^* = \{\pm 1\}$.

How do we order curves?

There are several possibilities:

How do we order curves?

There are several possibilities:

- By height: say by $\max\{|a_1|, |a_2|, |a_3|, |a_4|, |a_6|\}$, or $\max\{|c_4|, |c_6|\}$, or $\max\{|c_4|^3, |c_6|^2\}$: that is, by some suitably weighted height of the coefficient vector;
- By discriminant norm $N(\Delta_E)$;
- By conductor norm $N(\mathfrak{n})$.

How do we order curves?

There are several possibilities:

- By height: say by $\max\{|a_1|, |a_2|, |a_3|, |a_4|, |a_6|\}$, or $\max\{|c_4|, |c_6|\}$, or $\max\{|c_4|^3, |c_6|^2\}$: that is, by some suitably weighted height of the coefficient vector;
- By discriminant norm $N(\Delta_E)$;
- By conductor norm $N(\mathfrak{n})$.

I will normally go for the last possibility, listing curves by conductor with conductors in order of norm. (Note that the number of isomorphism classes of curves with fixed conductor is finite.)

How do we order curves?

There are several possibilities:

- By height: say by $\max\{|a_1|, |a_2|, |a_3|, |a_4|, |a_6|\}$, or $\max\{|c_4|, |c_6|\}$, or $\max\{|c_4|^3, |c_6|^2\}$: that is, by some suitably weighted height of the coefficient vector;
- By discriminant norm $N(\Delta_E)$;
- By conductor norm $N(\mathfrak{n})$.

I will normally go for the last possibility, listing curves by conductor with conductors in order of norm. (Note that the number of isomorphism classes of curves with fixed conductor is finite.)

Otherwise we might fix a set of primes $\mathcal{S}$ and list all curves with good reduction outside $\mathcal{S}$, again a finite set.

Enumeration methods

This is the simplest approach:

- For each triple $(a_1, a_2, a_3) \in \mathcal{O}_K^3$ reduced modulo $(2, 3, 2)$ and for all $(a_4, a_6) \in \mathcal{O}_K^2$ with coefficients lying in a box (with respect to a fixed integral basis for $\mathcal{O}_K$), write down every equation!

Enumeration methods

This is the simplest approach:

- For each triple $(a_1, a_2, a_3) \in \mathcal{O}_K^3$ reduced modulo $(2, 3, 2)$ and for all $(a_4, a_6) \in \mathcal{O}_K^2$ with coefficients lying in a box (with respect to a fixed integral basis for $\mathcal{O}_K$), write down every equation!
- Throw away those not wanted (e.g. conductor norm too large) and keep the rest.

Enumeration methods

This is the simplest approach:

- For each triple $(a_1, a_2, a_3) \in \mathcal{O}_K^3$ reduced modulo $(2, 3, 2)$ and for all $(a_4, a_6) \in \mathcal{O}_K^2$ with coefficients lying in a box (with respect to a fixed integral basis for $\mathcal{O}_K$), write down every equation!
- Throw away those not wanted (e.g. conductor norm too large) and keep the rest.
- Sort by conductor, isogeny class and isomorphism class.

Enumeration methods

This is the simplest approach:

- For each triple $(a_1, a_2, a_3) \in \mathcal{O}_K^3$ reduced modulo $(2, 3, 2)$ and for all $(a_4, a_6) \in \mathcal{O}_K^2$ with coefficients lying in a box (with respect to a fixed integral basis for $\mathcal{O}_K$), write down every equation!
- Throw away those not wanted (e.g. conductor norm too large) and keep the rest.
- Sort by conductor, isogeny class and isomorphism class.
- Compute curves isogenous to each found and kept.

Enumeration methods

This is the simplest approach:

- For each triple $(a_1, a_2, a_3) \in \mathcal{O}_K^3$ reduced modulo $(2, 3, 2)$ and for all $(a_4, a_6) \in \mathcal{O}_K^2$ with coefficients lying in a box (with respect to a fixed integral basis for $\mathcal{O}_K$), write down every equation!
- Throw away those not wanted (e.g. conductor norm too large) and keep the rest.
- Sort by conductor, isogeny class and isomorphism class.
- Compute curves isogenous to each found and kept.

This is slow! It is basically what I did in 1981 (with a small box!).

Enumeration methods

This is the simplest approach:

- For each triple $(a_1, a_2, a_3) \in \mathcal{O}_K^3$ reduced modulo $(2, 3, 2)$ and for all $(a_4, a_6) \in \mathcal{O}_K^2$ with coefficients lying in a box (with respect to a fixed integral basis for $\mathcal{O}_K$), write down every equation!
- Throw away those not wanted (e.g. conductor norm too large) and keep the rest.
- Sort by conductor, isogeny class and isomorphism class.
- Compute curves isogenous to each found and kept.

This is slow! It is basically what I did in 1981 (with a small box!). Over $\mathbb{Q}$ an efficient version of this was used to create the Stein-Watkins database.

Sieved enumeration

A refinement of the enumeration method is to use sieving. This only makes sense if we know in advance something about the curves we expect to find (their conductors and L-functions).

Sieved enumeration

A refinement of the enumeration method is to use sieving. This only makes sense if we know in advance something about the curves we expect to find (their conductors and L-functions).

Where could such knowledge come from?

Sieved enumeration

A refinement of the enumeration method is to use sieving. This only makes sense if we know in advance something about the curves we expect to find (their conductors and L-functions).

Where could such knowledge come from?

$\boxed{\text{Modularity!}}$

Sieved enumeration

A refinement of the enumeration method is to use sieving. This only makes sense if we know in advance something about the curves we expect to find (their conductors and L-functions).

Where could such knowledge come from?

$\boxed{\text{Modularity!}}$

So we will come back to this after talking about modularity.

Modularity I: over $\mathbb{Q}$

Over $\mathbb{Q}$, while the first tables of elliptic curves were obtained by plain enumeration as described above, this was soon augmented by Birch's student Tingley. In his 1975 thesis, Tingley used modular symbols to find elliptic curves of conductors up to about 300.

Modularity I: over $\mathbb{Q}$

Over $\mathbb{Q}$, while the first tables of elliptic curves were obtained by plain enumeration as described above, this was soon augmented by Birch's student Tingley. In his 1975 thesis, Tingley used modular symbols to find elliptic curves of conductors up to about 300.

This relied on the **Eichler-Shimura construction**: to every rational newform $f \in S_2(\Gamma_0(N))$ is attached an elliptic curve E_f defined over $\mathbb{Q}$ and of conductor N [Carayol *et al*].

Modularity I: over $\mathbb{Q}$

Over $\mathbb{Q}$, while the first tables of elliptic curves were obtained by plain enumeration as described above, this was soon augmented by Birch's student Tingley. In his 1975 thesis, Tingley used modular symbols to find elliptic curves of conductors up to about 300.

This relied on the **Eichler-Shimura construction**: to every rational newform $f \in S_2(\Gamma_0(N))$ is attached an elliptic curve E_f defined over $\mathbb{Q}$ and of conductor N [Carayol *et al*].
The construction can be made very explicit, using the periods of $2\pi i f(z) dz$ to compute the period lattice of E_f, and hence its coefficients, numerically.

Modularity I: over $\mathbb{Q}$

Over $\mathbb{Q}$, while the first tables of elliptic curves were obtained by plain enumeration as described above, this was soon augmented by Birch's student Tingley. In his 1975 thesis, Tingley used modular symbols to find elliptic curves of conductors up to about 300.

This relied on the **Eichler-Shimura construction**: to every rational newform $f \in S_2(\Gamma_0(N))$ is attached an elliptic curve E_f defined over $\mathbb{Q}$ and of conductor N [Carayol *et al*].
The construction can be made very explicit, using the periods of $2\pi i f(z)dz$ to compute the period lattice of E_f, and hence its coefficients, numerically. I will not talk about this today!

Modularity I: over $\mathbb{Q}$

Over $\mathbb{Q}$, while the first tables of elliptic curves were obtained by plain enumeration as described above, this was soon augmented by Birch's student Tingley. In his 1975 thesis, Tingley used modular symbols to find elliptic curves of conductors up to about 300.

This relied on the **Eichler-Shimura construction**: to every rational newform $f \in S_2(\Gamma_0(N))$ is attached an elliptic curve E_f defined over $\mathbb{Q}$ and of conductor N [Carayol *et al*].
The construction can be made very explicit, using the periods of $2\pi i f(z) dz$ to compute the period lattice of E_f, and hence its coefficients, numerically. I will not talk about this today!
Except to stress that there is no such construction for any number field other than $\mathbb{Q}$.

Modularity over $\mathbb{Q}$ (continued)

Moreover: every elliptic curve over $\mathbb{Q}$ is modular [Wiles *et al*], i.e. is isogenous to one of the E_f.

Modularity over $\mathbb{Q}$ (continued)

Moreover: every elliptic curve over $\mathbb{Q}$ is modular [Wiles *et al*], i.e. is isogenous to one of the E_f.

So if we use modularity to compute elliptic curves over $\mathbb{Q}$, we will obtain **complete** tables for each conductor N.

Modularity over $\mathbb{Q}$ (continued)

Moreover: every elliptic curve over $\mathbb{Q}$ is modular [Wiles *et al*], i.e. is isogenous to one of the E_f.

So if we use modularity to compute elliptic curves over $\mathbb{Q}$, we will obtain **complete** tables for each conductor N.

This was not known when the tables were first published (Antwerp IV 1976 or AMEC 1st edn. 1992), but that did not stop the tables being welcomed, and useful.

Modularity over quadratic fields

As we will see in Samir's talk, all elliptic curves over **real** quadratic fields are modular [Siksek *et al*], so over such fields we have a hope of computing tables which are known to be complete.

Modularity over quadratic fields

As we will see in Samir's talk, all elliptic curves over **real** quadratic fields are modular [Siksek *et al*], so over such fields we have a hope of computing tables which are known to be complete. See Alyson's talk!

Modularity over quadratic fields

As we will see in Samir's talk, all elliptic curves over **real** quadratic fields are modular [Siksek *et al*], so over such fields we have a hope of computing tables which are known to be complete. See Alyson's talk!
Computing the curves is still not as "easy" as over $\mathbb{Q}$...

Modularity over quadratic fields

As we will see in Samir's talk, all elliptic curves over **real** quadratic fields are modular [Siksek *et al*], so over such fields we have a hope of computing tables which are known to be complete. See Alyson's talk!
Computing the curves is still not as "easy" as over $\mathbb{Q}$…

This brings us back to **imaginary** quadratic fields.

Modularity over quadratic fields

As we will see in Samir's talk, all elliptic curves over **real** quadratic fields are modular [Siksek *et al*], so over such fields we have a hope of computing tables which are known to be complete. See Alyson's talk!
Computing the curves is still not as "easy" as over $\mathbb{Q}$...

This brings us back to **imaginary** quadratic fields.

Here, a lot less is known; and also, less is true!

Modularity over imaginary quadratic fields

Let K be imaginary quadratic. For each "level" $\mathfrak{n} \lhd \mathcal{O}_K$ we define the congruence subgroup $\Gamma_0(\mathfrak{n})$ of the Bianchi groups $\mathrm{GL}_2(\mathcal{O}_K)$ in the normal way.

Modularity over imaginary quadratic fields

Let K be imaginary quadratic. For each "level" $\mathfrak{n} \lhd \mathcal{O}_K$ we define the congruence subgroup $\Gamma_0(\mathfrak{n})$ of the Bianchi groups $\mathrm{GL}_2(\mathcal{O}_K)$ in the normal way.

There is a finite-dimensional complex vector space $S_2(\mathfrak{n})$ of "cusp forms of weight 2 for $\Gamma_0(\mathfrak{n})$". These are functions on hyperbolic 3-space $\mathcal{H}_3$ with values in $\mathbb{C}^3$, associated to harmonic differentials on the compact orbifold $\Gamma_0(\mathfrak{n})\backslash\mathcal{H}_3^*$, with Hecke action,...

Modularity over imaginary quadratic fields

Let K be imaginary quadratic. For each "level" $\mathfrak{n} \lhd \mathcal{O}_K$ we define the congruence subgroup $\Gamma_0(\mathfrak{n})$ of the Bianchi groups $\mathrm{GL}_2(\mathcal{O}_K)$ in the normal way.

There is a finite-dimensional complex vector space $S_2(\mathfrak{n})$ of "cusp forms of weight 2 for $\Gamma_0(\mathfrak{n})$". These are functions on hyperbolic 3-space $\mathcal{H}_3$ with values in $\mathbb{C}^3$, associated to harmonic differentials on the compact orbifold $\Gamma_0(\mathfrak{n})\backslash\mathcal{H}_3^*$, with Hecke action,. . . . . . but can be explicitly computed using a generalization of modular symbols!

Modularity over imaginary quadratic fields

Let K be imaginary quadratic. For each "level" $\mathfrak{n} \lhd \mathcal{O}_K$ we define the congruence subgroup $\Gamma_0(\mathfrak{n})$ of the Bianchi groups $\mathrm{GL}_2(\mathcal{O}_K)$ in the normal way.

There is a finite-dimensional complex vector space $S_2(\mathfrak{n})$ of "cusp forms of weight 2 for $\Gamma_0(\mathfrak{n})$". These are functions on hyperbolic 3-space $\mathcal{H}_3$ with values in $\mathbb{C}^3$, associated to harmonic differentials on the compact orbifold $\Gamma_0(\mathfrak{n})\backslash\mathcal{H}_3^*$, with Hecke action,......but can be explicitly computed using a generalization of modular symbols!

I will omit all details of this today.

Modularity over imaginary quadratic fields

Let K be imaginary quadratic. For each "level" $\mathfrak{n} \lhd \mathcal{O}_K$ we define the congruence subgroup $\Gamma_0(\mathfrak{n})$ of the Bianchi groups $\mathrm{GL}_2(\mathcal{O}_K)$ in the normal way.

There is a finite-dimensional complex vector space $S_2(\mathfrak{n})$ of "cusp forms of weight 2 for $\Gamma_0(\mathfrak{n})$". These are functions on hyperbolic 3-space $\mathcal{H}_3$ with values in $\mathbb{C}^3$, associated to harmonic differentials on the compact orbifold $\Gamma_0(\mathfrak{n})\backslash\mathcal{H}_3^*$, with Hecke action,. . . . . . but can be explicitly computed using a generalization of modular symbols!
I will omit all details of this today.

This has been implemented for a variety of imaginary quadratic fields by me and my students, and there is a version (based on some different ideas) by Dan Yasaki in Magma.

Modularity over imaginary quadratic fields

Let K be imaginary quadratic. For each "level" $\mathfrak{n} \lhd \mathcal{O}_K$ we define the congruence subgroup $\Gamma_0(\mathfrak{n})$ of the Bianchi groups $\mathrm{GL}_2(\mathcal{O}_K)$ in the normal way.

There is a finite-dimensional complex vector space $S_2(\mathfrak{n})$ of "cusp forms of weight 2 for $\Gamma_0(\mathfrak{n})$". These are functions on hyperbolic 3-space $\mathcal{H}_3$ with values in $\mathbb{C}^3$, associated to harmonic differentials on the compact orbifold $\Gamma_0(\mathfrak{n})\backslash\mathcal{H}_3^*$, with Hecke action,……but can be explicitly computed using a generalization of modular symbols!
I will omit all details of this today.

This has been implemented for a variety of imaginary quadratic fields by me and my students, and there is a version (based on some different ideas) by Dan Yasaki in Magma. Today I will give you data for the first five fields only, for which I have most well-developed and efficient code (at `https://github.com/JohnCremona/bianchi-progs`).

Imaginary quadratic newforms

In 2013 I extended my old (1981) tables of rational newforms over the first five imaginary quadratic fields to cover all levels of norm $\leq 10^4$ (and going further would not be hard):

Field	norm $\leq$	#rational cuspidal newforms
$\mathbb{Q}(\sqrt{-1})$	10000	3157
$\mathbb{Q}(\sqrt{-2})$	10000	6236
$\mathbb{Q}(\sqrt{-3})$	10000	2210
$\mathbb{Q}(\sqrt{-7})$	10000	5923
$\mathbb{Q}(\sqrt{-11})$	10000	5203

Imaginary quadratic newforms

In 2013 I extended my old (1981) tables of rational newforms over the first five imaginary quadratic fields to cover all levels of norm $\leq 10^4$ (and going further would not be hard):

Field	norm $\leq$	#rational cuspidal newforms
$\mathbb{Q}(\sqrt{-1})$	10000	3157
$\mathbb{Q}(\sqrt{-2})$	10000	6236
$\mathbb{Q}(\sqrt{-3})$	10000	2210
$\mathbb{Q}(\sqrt{-7})$	10000	5923
$\mathbb{Q}(\sqrt{-11})$	10000	5203

I also recruited a final year undergraduate, Warren Moore, who is doing his Masters dissertation on finding elliptic curves to match all these, or as many as he can, using whatever methods we can think of.

Imaginary quadratic newforms

In 2013 I extended my old (1981) tables of rational newforms over the first five imaginary quadratic fields to cover all levels of norm $\leq 10^4$ (and going further would not be hard):

Field	norm $\leq$	#rational cuspidal newforms
$\mathbb{Q}(\sqrt{-1})$	10000	3157
$\mathbb{Q}(\sqrt{-2})$	10000	6236
$\mathbb{Q}(\sqrt{-3})$	10000	2210
$\mathbb{Q}(\sqrt{-7})$	10000	5923
$\mathbb{Q}(\sqrt{-11})$	10000	5203

I also recruited a final year undergraduate, Warren Moore, who is doing his Masters dissertation on finding elliptic curves to match all these, or as many as he can, using whatever methods we can think of.

Here is how far he has got to (as of a few days ago):

Imaginary quadratic progress

Field	norm $\leq$	#newforms	#classes	#curves	#missing
$\mathbb{Q}(\sqrt{-1})$	10000	3157	2993	11254	164
$\mathbb{Q}(\sqrt{-2})$	10000	6236	5382	11755	854
$\mathbb{Q}(\sqrt{-3})$	10000	2210	2020	5452	188!
$\mathbb{Q}(\sqrt{-7})$	10000	5923	5259	12267	664
$\mathbb{Q}(\sqrt{-11})$	10000	5203	4139	8444	1064

Imaginary quadratic progress

Field	norm $\leq$	#newforms	#classes	#curves	#missing
$\mathbb{Q}(\sqrt{-1})$	10000	3157	2993	11254	164
$\mathbb{Q}(\sqrt{-2})$	10000	6236	5382	11755	854
$\mathbb{Q}(\sqrt{-3})$	10000	2210	2020	5452	188!
$\mathbb{Q}(\sqrt{-7})$	10000	5923	5259	12267	664
$\mathbb{Q}(\sqrt{-11})$	10000	5203	4139	8444	1064

- Over $K = \mathbb{Q}(\sqrt{-3})$ there are 2210 rational newforms but two of these, of levels (75) and (81), are base changes of modular abelian surfaces over $\mathbb{Q}$ of levels 225 and 243, which do **not** split over K.

Imaginary quadratic progress

Field	norm $\leq$	#newforms	#classes	#curves	#missing
$\mathbb{Q}(\sqrt{-1})$	10000	3157	2993	11254	164
$\mathbb{Q}(\sqrt{-2})$	10000	6236	5382	11755	854
$\mathbb{Q}(\sqrt{-3})$	10000	2210	2020	5452	188!
$\mathbb{Q}(\sqrt{-7})$	10000	5923	5259	12267	664
$\mathbb{Q}(\sqrt{-11})$	10000	5203	4139	8444	1064

- Over $K = \mathbb{Q}(\sqrt{-3})$ there are 2210 rational newforms but two of these, of levels (75) and (81), are base changes of modular abelian surfaces over $\mathbb{Q}$ of levels 225 and 243, which do **not** split over K.
- These numbers do not include curves with CM by an order in K.

Sieved enumeration using newform data

Each newform F at level $\mathfrak{n}$ has an L-function $L(F,s)$ which "looks like" the (degree 4) L-function of an elliptic curve over K, with Euler product, analytic continuation to $\mathbb{C}$, functional equation. This is completely determined by knowing (1) the conductor $\mathfrak{n}$ and (2) the Hecke eigenvalues $a_{\mathfrak{p}}$ at primes $\mathfrak{p}$.

Sieved enumeration using newform data

Each newform F at level $\mathfrak{n}$ has an L-function $L(F,s)$ which "looks like" the (degree 4) L-function of an elliptic curve over K, with Euler product, analytic continuation to $\mathbb{C}$, functional equation. This is completely determined by knowing (1) the conductor $\mathfrak{n}$ and (2) the Hecke eigenvalues $a_{\mathfrak{p}}$ at primes $\mathfrak{p}$.

So in looking for the curves we can use a sieve as follows: take a small number r of primes $\mathfrak{p}_i$ of degree 1, and do pre-computations so that it is very quick to compute the map

$$[a_1,a_2,a_3,a_4,a_6] \in \mathcal{O}_K^5 \mapsto \prod_i \mathbb{F}_{p_i}^5 \mapsto (a_{\mathfrak{p}_1},\dots,a_{\mathfrak{p}_r}) \in \mathbb{Z}^r$$

giving the traces of Frobenius of the elliptic curve $[a_1,a_2,a_3,a_4,a_6]$ at each $\mathfrak{p}_i$.

Sieved enumeration using newform data

Each newform F at level $\mathfrak{n}$ has an L-function $L(F,s)$ which "looks like" the (degree 4) L-function of an elliptic curve over K, with Euler product, analytic continuation to $\mathbb{C}$, functional equation. This is completely determined by knowing (1) the conductor $\mathfrak{n}$ and (2) the Hecke eigenvalues $a_{\mathfrak{p}}$ at primes $\mathfrak{p}$.

So in looking for the curves we can use a sieve as follows: take a small number r of primes $\mathfrak{p}_i$ of degree 1, and do pre-computations so that it is very quick to compute the map

$$[a_1, a_2, a_3, a_4, a_6] \in \mathcal{O}_K^5 \mapsto \prod_i \mathbb{F}_{p_i}^5 \mapsto (a_{\mathfrak{p}_1}, \ldots, a_{\mathfrak{p}_r}) \in \mathbb{Z}^r$$

giving the traces of Frobenius of the elliptic curve $[a_1, a_2, a_3, a_4, a_6]$ at each $\mathfrak{p}_i$. Also, read in the lists of $(a_{\mathfrak{p}_i})$ which we expect to find. Now when we loop over equations in a box we can very quickly check whether it is likely to be one which we are looking for.

Other tricks

- apply quadratic twists to existing curves
- work with $|a_{\mathfrak{p}_i}|$ to find twists with the sieve
- recognise base-change forms and use curves $/\mathbb{Q}$
- use Chinese remaindering to target hard-to-find curves in a larger box

Exceptions I

Over imaginary quadratic fields K, we do **not** expect an exact bijection between (a) rational cuspidal newforms of weight 2 for $\Gamma_0(\mathfrak{n})$ over K and (b) isogeny classes of elliptic curves E of conductor $\mathfrak{n}$ defined over K! There are exceptions on both sides:

Exceptions I

Over imaginary quadratic fields K, we do **not** expect an exact bijection between (a) rational cuspidal newforms of weight 2 for $\Gamma_0(\mathfrak{n})$ over K and (b) isogeny classes of elliptic curves E of conductor $\mathfrak{n}$ defined over K! There are exceptions on both sides:

- If E has CM by an order in K then E is a twist of a curve defined over $\mathbb{Q}$ which is of course modular; but the base-change from $\mathbb{Q}$ to K of the cusp form over $\mathbb{Q}$ is not cuspidal!

Exceptions I

Over imaginary quadratic fields K, we do **not** expect an exact bijection between (a) rational cuspidal newforms of weight 2 for $\Gamma_0(\mathfrak{n})$ over K and (b) isogeny classes of elliptic curves E of conductor $\mathfrak{n}$ defined over K! There are exceptions on both sides:

- If E has CM by an order in K then E is a twist of a curve defined over $\mathbb{Q}$ which is of course modular; but the base-change from $\mathbb{Q}$ to K of the cusp form over $\mathbb{Q}$ is not cuspidal!

This can only happen when $h_K = 1$.

Exceptions I

Over imaginary quadratic fields K, we do **not** expect an exact bijection between (a) rational cuspidal newforms of weight 2 for $\Gamma_0(\mathfrak{n})$ over K and (b) isogeny classes of elliptic curves E of conductor $\mathfrak{n}$ defined over K! There are exceptions on both sides:

- If E has CM by an order in K then E is a twist of a curve defined over $\mathbb{Q}$ which is of course modular; but the base-change from $\mathbb{Q}$ to K of the cusp form over $\mathbb{Q}$ is not cuspidal!

This can only happen when $h_K = 1$.

For example the elliptic curve $Y^2 = X^3 - X$ (32a1) has $j = 1728$ and conductor $\mathfrak{n} = (64)$ over $\mathbb{Q}(\sqrt{-1})$, but $S_2(\mathfrak{n})$ is trivial.

Exceptions II

- If $f \in S_2(N)$ over $\mathbb{Q}$ is quadratic and with "extra twist" by $K = \mathbb{Q}(\sqrt{-d})$: this means that the coefficients of f lie in a (necessarily real) quadratic field $K_f = \mathbb{Q}(\sqrt{e})$ and

$$f \otimes \chi = f^\sigma$$

where χ is the quadratic character associated to $K/\mathbb{Q}$ and σ generates $\mathrm{Gal}(K_f/\mathbb{Q})$. Attached to f is an abelian surface A_f such that

$$\mathrm{End}(A_f) \otimes \mathbb{Q} \cong \left(\frac{-d, e}{\mathbb{Q}}\right)$$

which may or may not split. If it does not then A_f is absolutely simple. But the base-change of f from $\mathbb{Q}$ to K is a cusp form F with **rational** coefficients, and this F will then not have an associated elliptic curve.

Exceptions II example

In $S_2(3^5)$ (over $\mathbb{Q}$) there is a newform f with

$$a_2 = \sqrt{6}, \quad a_5 = -\sqrt{6}, \quad a_7 = 2, \quad a_{11} = \sqrt{6};$$

in general, $a_p \in \mathbb{Z}$ for $p \equiv 1$ and $a_p/\sqrt{6} \in \mathbb{Z}$ for $p \equiv 2 \pmod 3$.

Exceptions II example

In $S_2(3^5)$ (over $\mathbb{Q}$) there is a newform f with

$$a_2 = \sqrt{6}, \quad a_5 = -\sqrt{6}, \quad a_7 = 2, \quad a_{11} = \sqrt{6};$$

in general, $a_p \in \mathbb{Z}$ for $p \equiv 1$ and $a_p/\sqrt{6} \in \mathbb{Z}$ for $p \equiv 2 \pmod 3$.

The base change F of f to $\mathbb{Q}(\sqrt{-3})$ has level (81) and rational $a_\mathfrak{p}$: if $p \equiv 1 \pmod 3$ then $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ and $a_\mathfrak{p} = a_{\overline{\mathfrak{p}}} = a_p \in \mathbb{Z}$, while if $p \equiv 2 \pmod 3$ then $(p) = \mathfrak{p}$ and $a_\mathfrak{p} = a_p^2 - 2p \in \mathbb{Z}$.

Exceptions II example

In $S_2(3^5)$ (over $\mathbb{Q}$) there is a newform f with

$$a_2 = \sqrt{6}, \quad a_5 = -\sqrt{6}, \quad a_7 = 2, \quad a_{11} = \sqrt{6};$$

in general, $a_p \in \mathbb{Z}$ for $p \equiv 1$ and $a_p/\sqrt{6} \in \mathbb{Z}$ for $p \equiv 2 \pmod 3$.

The base change F of f to $\mathbb{Q}(\sqrt{-3})$ has level (81) and rational $a_{\mathfrak{p}}$: if $p \equiv 1 \pmod 3$ then $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ and $a_{\mathfrak{p}} = a_{\bar{\mathfrak{p}}} = a_p \in \mathbb{Z}$, while if $p \equiv 2 \pmod 3$ then $(p) = \mathfrak{p}$ and $a_{\mathfrak{p}} = a_p^2 - 2p \in \mathbb{Z}$.

But the quaternion algebra $\left(\frac{-3,6}{\mathbb{Q}}\right)$ is not split so A_f is simple (over $\mathbb{Q}(\sqrt{-3})$ and absolutely): there is **no** elliptic curve E over $\mathbb{Q}(\sqrt{-3})$ with conductor (81) such that $L(E,s) = L(F,s)$.

Exceptions II example

In $S_2(3^5)$ (over $\mathbb{Q}$) there is a newform f with

$$a_2 = \sqrt{6}, \quad a_5 = -\sqrt{6}, \quad a_7 = 2, \quad a_{11} = \sqrt{6};$$

in general, $a_p \in \mathbb{Z}$ for $p \equiv 1$ and $a_p/\sqrt{6} \in \mathbb{Z}$ for $p \equiv 2 \pmod 3$.

The base change F of f to $\mathbb{Q}(\sqrt{-3})$ has level (81) and rational $a_{\mathfrak{p}}$: if $p \equiv 1 \pmod 3$ then $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ and $a_{\mathfrak{p}} = a_{\overline{\mathfrak{p}}} = a_p \in \mathbb{Z}$, while if $p \equiv 2 \pmod 3$ then $(p) = \mathfrak{p}$ and $a_{\mathfrak{p}} = a_p^2 - 2p \in \mathbb{Z}$.

But the quaternion algebra $\left(\frac{-3,6}{\mathbb{Q}}\right)$ is not split so A_f is simple (over $\mathbb{Q}(\sqrt{-3})$ and absolutely): there is **no** elliptic curve E over $\mathbb{Q}(\sqrt{-3})$ with conductor (81) such that $L(E,s) = L(F,s)$.

This phenomenon cannot happen for **real** quadratic fields!

Filling the gaps

We do not find all elliptic curves to match newforms using sieved enumeration, since some have coefficients too large (“outside the box”!), even after twisting and other tricks have been tried.

Filling the gaps

We do not find all elliptic curves to match newforms using sieved enumeration, since some have coefficients too large ("outside the box"!), even after twisting and other tricks have been tried.

Can we construct the sought elliptic curves using the periods of the newform F?

Filling the gaps

We do not find all elliptic curves to match newforms using sieved enumeration, since some have coefficients too large ("outside the box"!), even after twisting and other tricks have been tried.

Can we construct the sought elliptic curves using the periods of the newform F? Over imaginary quadratic fields: **NO!**

Filling the gaps

We do not find all elliptic curves to match newforms using sieved enumeration, since some have coefficients too large ("outside the box"!), even after twisting and other tricks have been tried.

Can we construct the sought elliptic curves using the periods of the newform F? Over imaginary quadratic fields: **NO!**

Another method is often useful: to make explicit Shafarevich's theorem that the number of elliptic curves of any given conductor is finite, or more generally, the number of elliptic curves defined over a fixed number field K with good reduction outside a given finite set $\mathcal{S}$ of primes of K.

Filling the gaps

We do not find all elliptic curves to match newforms using sieved enumeration, since some have coefficients too large ("outside the box"!), even after twisting and other tricks have been tried.

Can we construct the sought elliptic curves using the periods of the newform F? Over imaginary quadratic fields: **NO!**

Another method is often useful: to make explicit Shafarevich's theorem that the number of elliptic curves of any given conductor is finite, or more generally, the number of elliptic curves defined over a fixed number field K with good reduction outside a given finite set $\mathcal{S}$ of primes of K.

This is the last method I will discuss today.

Curves with fixed conductor (or set of primes of bad reduction)

If $\mathcal{S}$ is a finite set of primes of the number field K there are only finitely many (isomorphism classes of elliptic curves defined over K with good reduction outside $\mathcal{S}$.

Taking $\mathcal{S} = \{\mathfrak{p} : \mathfrak{p} \mid \mathfrak{n}\}$ we can restrict to curves of conductor exactly $\mathfrak{n}$.

Curves with fixed conductor (or set of primes of bad reduction)

If $\mathcal{S}$ is a finite set of primes of the number field K there are only finitely many (isomorphism classes of elliptic curves defined over K with good reduction outside $\mathcal{S}$.
Taking $\mathcal{S} = \{\mathfrak{p} : \mathfrak{p} \mid \mathfrak{n}\}$ we can restrict to curves of conductor exactly $\mathfrak{n}$.

This can be made explicit. There are two steps:

1. find all possible j-invariants;
2. find all E with each j.

Curves with fixed conductor (or set of primes of bad reduction)

If $\mathcal{S}$ is a finite set of primes of the number field K there are only finitely many (isomorphism classes of elliptic curves defined over K with good reduction outside $\mathcal{S}$.
Taking $\mathcal{S} = \{\mathfrak{p} : \mathfrak{p} \mid \mathfrak{n}\}$ we can restrict to curves of conductor exactly $\mathfrak{n}$.

This can be made explicit. There are two steps:

1. find all possible j-invariants;
2. find all E with each j.

The second step is quite straightforward: assuming that $j \neq 0, 1728$ and that $\mathcal{S}$ contains all primes dividing 6, the curves form a complete set of quadratic twists by elements of $K(\mathcal{S}, 2)$.
For details see Cremona-Lingham 2007.

Finding the j-invariants for given $\mathcal{S}$: I

[Continue to assume that $\mathfrak{p} \mid 6 \implies \mathfrak{p} \in \mathcal{S}$ and $j \neq 0, 1728$.]

The j-invariants which occur are those such that

$$j^2(j - 1728)^3 \in K(\mathcal{S}, 6)_{12}.$$

Finding the j-invariants for given $\mathcal{S}$: I

[Continue to assume that $\mathfrak{p} \mid 6 \implies \mathfrak{p} \in \mathcal{S}$ and $j \neq 0, 1728$.]
The j-invariants which occur are those such that

$$j^2(j - 1728)^3 \in K(\mathcal{S}, 6)_{12}.$$

Here,

$$K(\mathcal{S}, m) = \{x \mid \mathrm{ord}_{\mathfrak{p}}(x) \equiv 0 \pmod{m} \forall \mathfrak{p} \notin \mathcal{S}\}/K^{*m} \leqslant K^*/K^{*m}$$

and

$$K(\mathcal{S}, m)_{mn} = \mathrm{im}(K(\mathcal{S}, mn) \to K(\mathcal{S}, m)).$$

Finding the j-invariants for given $\mathcal{S}$: I

[Continue to assume that $\mathfrak{p} \mid 6 \implies \mathfrak{p} \in \mathcal{S}$ and $j \neq 0, 1728$.]
The j-invariants which occur are those such that

$$j^2(j-1728)^3 \in K(\mathcal{S},6)_{12}.$$

Here,

$$K(\mathcal{S},m) = \{x \mid \mathrm{ord}_{\mathfrak{p}}(x) \equiv 0 \pmod{m} \forall \mathfrak{p} \notin \mathcal{S}\}/K^{*m} \leqslant K^*/K^{*m}$$

and

$$K(\mathcal{S},m)_{mn} = \mathrm{im}(K(\mathcal{S},mn) \to K(\mathcal{S},m)).$$

If $w = j^2(j-1728)^3 \in K(\mathcal{S},6)_{12}$, take $u \in K^*$ such that $(3u)^6 w \in K(\mathcal{S},12)$; then

$$Y^2 = X^3 - 3u^2 j(j-1728)X - 2u^3 j(j-1728)^2$$

has good reduction outside $\mathcal{S}$, and all such curves are twists of this by elements of $K(\mathcal{S},2)$.

Finding the j-invariants for given $\mathcal{S}$: II

In Cremona-Lingham, one method for finding such j is described: $j = x^3/w$ where (x, y) is an $\mathcal{S}$-integral point on $Y^2 = X^3 - 1728w$ with $w \in K(\mathcal{S}, 6)_{12}$.

Finding the j-invariants for given $\mathcal{S}$: II

In Cremona-Lingham, one method for finding such j is described: $j = x^3/w$ where (x, y) is an $\mathcal{S}$-integral point on $Y^2 = X^3 - 1728w$ with $w \in K(\mathcal{S}, 6)_{12}$.

I implemented this in Magma (and in Sage over $\mathbb{Q}$), but:

Finding the j-invariants for given $\mathcal{S}$: II

In Cremona-Lingham, one method for finding such j is described: $j = x^3/w$ where (x, y) is an $\mathcal{S}$-integral point on $Y^2 = X^3 - 1728w$ with $w \in K(\mathcal{S}, 6)_{12}$.

I implemented this in Magma (and in Sage over $\mathbb{Q}$), but:

– the problem in practice is that finding all $\mathcal{S}$-integral points on elliptic curves is not easy (and not implemented in general); my Magma code just searches for $\mathcal{S}$-integral points.

Finding the j-invariants for given $\mathcal{S}$: II

In Cremona-Lingham, one method for finding such j is described: $j = x^3/w$ where (x, y) is an $\mathcal{S}$-integral point on $Y^2 = X^3 - 1728w$ with $w \in K(\mathcal{S}, 6)_{12}$.

I implemented this in Magma (and in Sage over $\mathbb{Q}$), but:

$-$ the problem in practice is that finding all $\mathcal{S}$-integral points on elliptic curves is not easy (and not implemented in general); my Magma code just searches for $\mathcal{S}$-integral points.

$+$ The code has been used to find some of the "missing curves", over both real and imaginary quadratic fields (and has also been used for some higher degree fields).

Finding the j-invariants for given $\mathcal{S}$: II

In Cremona-Lingham, one method for finding such j is described: $j = x^3/w$ where (x, y) is an $\mathcal{S}$-integral point on $Y^2 = X^3 - 1728w$ with $w \in K(\mathcal{S}, 6)_{12}$.

I implemented this in Magma (and in Sage over $\mathbb{Q}$), but:

$-$ the problem in practice is that finding all $\mathcal{S}$-integral points on elliptic curves is not easy (and not implemented in general); my Magma code just searches for $\mathcal{S}$-integral points.

$+$ The code has been used to find some of the "missing curves", over both real and imaginary quadratic fields (and has also been used for some higher degree fields).

$++$ A new idea is now under development...

Finding the j-invariants for given $\mathcal{S}$: III

After I gave a talk about this at MSRI in 2010, Elkies had an idea: instead of finding the j-invariants directly, find the λ-invariants. This is now joint work with Angelos Koutsianas.

Finding the j-invariants for given $\mathcal{S}$: III

After I gave a talk about this at MSRI in 2010, Elkies had an idea: instead of finding the j-invariants directly, find the λ-invariants. This is now joint work with Angelos Koutsianas.

Recall that $j = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$. This is the covering map from $X(2)$ to $X(1)$, both curves over $\mathbb{Q}$ of genus 0.

Finding the j-invariants for given $\mathcal{S}$: III

After I gave a talk about this at MSRI in 2010, Elkies had an idea: instead of finding the j-invariants directly, find the λ-invariants. This is now joint work with Angelos Koutsianas.

Recall that $j = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$. This is the covering map from $X(2)$ to $X(1)$, both curves over $\mathbb{Q}$ of genus 0.

If j is an $\mathcal{S}$-integer then λ is an $\mathcal{S}$-unit. And since $j(\lambda) = j(1-\lambda)$ we also have that $1-\lambda$ is an $\mathcal{S}$-unit. So we can find λ, and hence j, by solving the $\mathcal{S}$-unit equation $\lambda + \mu = 1$.

Finding the j-invariants for given $\mathcal{S}$: III

After I gave a talk about this at MSRI in 2010, Elkies had an idea: instead of finding the j-invariants directly, find the λ-invariants. This is now joint work with Angelos Koutsianas.

Recall that $j = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$. This is the covering map from $X(2)$ to $X(1)$, both curves over $\mathbb{Q}$ of genus 0.

If j is an $\mathcal{S}$-integer then λ is an $\mathcal{S}$-unit. And since $j(\lambda) = j(1-\lambda)$ we also have that $1-\lambda$ is an $\mathcal{S}$-unit. So we can find λ, and hence j, by solving the $\mathcal{S}$-unit equation $\lambda + \mu = 1$.

There are now two sub-problems:

1. find all possible 2-division fields $L = K(\lambda)$;
2. solve the $\mathcal{S}$-unit equation in each L.

Finding the λ-invariants for given $\mathcal{S}$

The first problem has been solved, and implemented; we use Kummer Theory to find all extensions L/K which are Galois, with group either C_1, C_2, C_3 or S_3.

Finding the λ-invariants for given $\mathcal{S}$

The first problem has been solved, and implemented; we use Kummer Theory to find all extensions L/K which are Galois, with group either C_1, C_2, C_3 or S_3.

The second problem (solving $\mathcal{S}$-unit equations over number fields) has been worked on by many people for years, but there are **no** existing implementations. Angelos has working code for this, but we are trying to make it faster, since it can be slow when the number of primes (of L dividing the primes of K in $\mathcal{S}$) is large. We hope to make use of the fact that our $\mathcal{S}$-unit equations are not random but are associated with the elliptic curve problem to make this more efficient.

Finding the λ-invariants for given $\mathcal{S}$

The first problem has been solved, and implemented; we use Kummer Theory to find all extensions L/K which are Galois, with group either C_1, C_2, C_3 or S_3.

The second problem (solving $\mathcal{S}$-unit equations over number fields) has been worked on by many people for years, but there are **no** existing implementations. Angelos has working code for this, but we are trying to make it faster, since it can be slow when the number of primes (of L dividing the primes of K in $\mathcal{S}$) is large. We hope to make use of the fact that our $\mathcal{S}$-unit equations are not random but are associated with the elliptic curve problem to make this more efficient.

Work in progress!