Finding all elliptic curves with good reduction outside a given set of primes

John Cremona
University of Nottingham, UK

6 September, 2005

Plan of the talk

- Background and statement of the problem
- Some history and previous results
- Algebraic preliminaries
- The method
  - ⋆ finding all possible j-invariants
  - ⋆ finding curves with given j-invariant
- Some results
  - ⋆ Over $\mathbb{Q}$
  - ⋆ Over number fields

Plan of the talk

- Background and statement of the problem
- Some history and previous results
- Algebraic preliminaries
- The method
  - ⋆ finding all possible j-invariants
  - ⋆ finding curves with given j-invariant
- Some results
  - ⋆ Over $\mathbb{Q}$
  - ⋆ Over number fields

Plan of the talk

- Background and statement of the problem
- Some history and previous results
- Algebraic preliminaries
- The method
  - ⋆ finding all possible j-invariants
  - ⋆ finding curves with given j-invariant
- Some results
  - ⋆ Over $\mathbb{Q}$
  - ⋆ Over number fields

Plan of the talk

- Background and statement of the problem
- Some history and previous results
- Algebraic preliminaries
- The method
  - ⋆ finding all possible j-invariants
  - ⋆ finding curves with given j-invariant
- Some results
  - ⋆ Over $\mathbb{Q}$
  - ⋆ Over number fields

Plan of the talk

- Background and statement of the problem
- Some history and previous results
- Algebraic preliminaries
- The method
  - ⋆ finding all possible j-invariants
  - ⋆ finding curves with given j-invariant
- Some results
  - ⋆ Over $\mathbb{Q}$
  - ⋆ Over number fields

Background to the problem

Theorem. [Shafarevich] *Let K be an algebraic number field and $\mathcal{S}$ a finite set of primes of K. Then the set*

$$\mathcal{E}_{K,\mathcal{S}} := \{\textit{elliptic curves } E/K \textit{ with good reduction at all primes } \mathfrak{p} \notin \mathcal{S}\} \,/\, \cong$$

is finite.

Examples:

- $\mathcal{E}_{\mathbb{Q},\emptyset} = \emptyset$ (no elliptic curve over $\mathbb{Q}$ has everywhere good reduction)
- $\#\mathcal{E}_{\mathbb{Q},\{2\}} = 24$ (Ogg) [$<$ 5s]
- $\#\mathcal{E}_{\mathbb{Q},\{2,3\}} = 752$ (Coghlan, 1966) [$\approx$1m]

Background to the problem

Theorem. [Shafarevich] *Let K be an algebraic number field and $\mathcal{S}$ a finite set of primes of K. Then the set*

$$\mathcal{E}_{K,\mathcal{S}} := \{\text{elliptic curves } E/K \text{ with good reduction at all primes } \mathfrak{p} \notin \mathcal{S}\} \,/\, \cong$$

is finite.

Examples:

- $\mathcal{E}_{\mathbb{Q},\emptyset} = \emptyset$ (no elliptic curve over $\mathbb{Q}$ has everywhere good reduction)
- $\#\mathcal{E}_{\mathbb{Q},\{2\}} = 24$ (Ogg) [$<$ 5s]
- $\#\mathcal{E}_{\mathbb{Q},\{2,3\}} = 752$ (Coghlan, 1966) [$\approx$1m]

- $\mathcal{E}_{\mathbb{Q}(\sqrt{-23}),\emptyset} = \emptyset$

The last example arose during work of Mark Lingham (Nottingham) who used modular symbols to show that there are no cusp forms of weight 2 and level 1 for $K = \mathbb{Q}(\sqrt{-23})$, so we expected that there should be no elliptic curves with everywhere good reduction over K. But this case had not previously been treated....

Statement of the problem

Given K and $\mathcal{S}$, find $\mathcal{E}_{K,\mathcal{S}}$ explicitly!

Some history I: over $\mathbb{Q}$

1. Ogg (1966) found all elliptic curves with conductor $N = 2^e$, then Coghlan did the same for $N = 2^{e_2}3^{e_3}$ (see Antwerp IV tables). Our MAGMA program verifies Coghlan's table in about one minute.

2. Certain sets $\mathcal{S} = \{2, p\}$ arise in solving Fermat-type equations (c.f. work of M. Bennett). Conductor N up to 2^8p^2, so for $p > 20$ these are hard to find using modular symbol methods.

   [Remark: $N = \mathrm{cond}_E = \prod p^{e_p}$ with $e_2 \leq 8$, $e_3 \leq 5$, $e_p \leq 2$ for $p \geq 5$.]

3. $\mathcal{S} = \{2, 3, 5, 7\}$ and $\mathcal{S} = \{2, 3, 11\}$: joint work with de Weger (1993) produced tables but BdW never claimed his data was complete.

Some history I: over $\mathbb{Q}$

1. Ogg (1966) found all elliptic curves with conductor $N = 2^e$, then Coghlan did the same for $N = 2^{e_2}3^{e_3}$ (see Antwerp IV tables). Our MAGMA program verifies Coghlan's table in about one minute.

2. Certain sets $\mathcal{S} = \{2, p\}$ arise in solving Fermat-type equations (c.f. work of M. Bennett). Conductor N up to 2^8p^2, so for $p > 20$ these are hard to find using modular symbol methods.

   [Remark: $N = \mathrm{cond}_E = \prod p^{e_p}$ with $e_2 \leq 8$, $e_3 \leq 5$, $e_p \leq 2$ for $p \geq 5$.]

3. $\mathcal{S} = \{2, 3, 5, 7\}$ and $\mathcal{S} = \{2, 3, 11\}$: joint work with de Weger (1993) produced tables but BdW never claimed his data was complete.

Some history I: over $\mathbb{Q}$

1. Ogg (1966) found all elliptic curves with conductor $N = 2^e$, then Coghlan did the same for $N = 2^{e_2}3^{e_3}$ (see Antwerp IV tables). Our MAGMA program verifies Coghlan's table in about one minute.

2. Certain sets $\mathcal{S} = \{2, p\}$ arise in solving Fermat-type equations (c.f. work of M. Bennett). Conductor N up to 2^8p^2, so for $p > 20$ these are hard to find using modular symbol methods.

   [Remark: $N = \mathrm{cond}_E = \prod p^{e_p}$ with $e_2 \leq 8$, $e_3 \leq 5$, $e_p \leq 2$ for $p \geq 5$.]

3. $\mathcal{S} = \{2, 3, 5, 7\}$ and $\mathcal{S} = \{2, 3, 11\}$: joint work with de Weger (1993) produced tables but BdW never claimed his data was complete.

Some history I: over $\mathbb{Q}$

1. Ogg (1966) found all elliptic curves with conductor $N = 2^e$, then Coghlan did the same for $N = 2^{e_2}3^{e_3}$ (see Antwerp IV tables). Our MAGMA program verifies Coghlan's table in about one minute.

2. Certain sets $\mathcal{S} = \{2, p\}$ arise in solving Fermat-type equations (c.f. work of M. Bennett). Conductor N up to 2^8p^2, so for $p > 20$ these are hard to find using modular symbol methods.

   [Remark: $N = \mathrm{cond}_E = \prod p^{e_p}$ with $e_2 \leq 8$, $e_3 \leq 5$, $e_p \leq 2$ for $p \geq 5$.]

3. $\mathcal{S} = \{2, 3, 5, 7\}$ and $\mathcal{S} = \{2, 3, 11\}$: joint work with de Weger (1993) produced tables but BdW never claimed his data was complete.

Some history II: over number fields

1. It is an open problem to determine those fields K for which $\mathcal{E}_{K,\emptyset}$ is not empty, i.e., for which fields there exist elliptic curves with everywhere good reduction.

2. Much work has been done for the case of quadratic fields:

   - R. J. Stroeker (1970s): $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.
   - R. G. E. Pinch (1980s):
     - ⋆ $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.
     - ⋆ $K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{S} = \{\mathfrak{p} \mid 3\}$.
     - ⋆ $K = \mathbb{Q}(\sqrt{5})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.

     Method:

     (a) show $E(K)[2]$ is nontrivial, using tables of cubic fields;
     (b) then solve several Diophantine equations;
     (c) not possible to generalize!

Some history II: over number fields

1. It is an open problem to determine those fields K for which $\mathcal{E}_{K,\emptyset}$ is not empty, i.e., for which fields there exist elliptic curves with everywhere good reduction.

2. Much work has been done for the case of quadratic fields:

   - R. J. Stroeker (1970s): $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.
   - R. G. E. Pinch (1980s):
     - ⋆ $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.
     - ⋆ $K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{S} = \{\mathfrak{p} \mid 3\}$.
     - ⋆ $K = \mathbb{Q}(\sqrt{5})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.

     Method:

   (a) show $E(K)[2]$ is nontrivial, using tables of cubic fields;

   (b) then solve several Diophantine equations;

   (c) not possible to generalize!

Some history II: over number fields

1. It is an open problem to determine those fields K for which $\mathcal{E}_{K,\emptyset}$ is not empty, i.e., for which fields there exist elliptic curves with everywhere good reduction.

2. Much work has been done for the case of quadratic fields:

   - R. J. Stroeker (1970s): $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.
   - R. G. E. Pinch (1980s):
     - ⋆ $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.
     - ⋆ $K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{S} = \{\mathfrak{p} \mid 3\}$.
     - ⋆ $K = \mathbb{Q}(\sqrt{5})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.

     Method:

     (a) show $E(K)[2]$ is nontrivial, using tables of cubic fields;

     (b) then solve several Diophantine equations;

     (c) not possible to generalize!

Some history II: over number fields

1. It is an open problem to determine those fields K for which $\mathcal{E}_{K,\emptyset}$ is not empty, i.e., for which fields there exist elliptic curves with everywhere good reduction.

2. Much work has been done for the case of quadratic fields:

   - R. J. Stroeker (1970s): $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.
   - R. G. E. Pinch (1980s):
     - ⋆ $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.
     - ⋆ $K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{S} = \{\mathfrak{p} \mid 3\}$.
     - ⋆ $K = \mathbb{Q}(\sqrt{5})$ and $\mathcal{S} = \{\mathfrak{p} \mid 2\}$.

     Method:

   (a) show $E(K)[2]$ is nontrivial, using tables of cubic fields;
   (b) then solve several Diophantine equations;
   (c) not possible to generalize!

- Kida and Kagawa (following Comalada, Ishii, Pinch) have determined $\mathcal{E}_{K,\emptyset}$ for $K = \mathbb{Q}(\sqrt{d})$ for many d with $-100 < d < 100$, but several were missing (including $d = -23$);
- Setzer (1978) gave necessary and sufficient conditions for the existence of $E \in \mathcal{E}_{K,\emptyset}$ with $E(K)[2] \neq 0$, K imaginary quadratic: for example, $\mathcal{E}_{\mathbb{Q}(\sqrt{-65}),\emptyset} \neq \emptyset$.
- Stroeker proved: if $[K:\mathbb{Q}] = 2$ and $\gcd(h_K, 6) = 1$ then $\mathcal{E}_{K,\emptyset} = \emptyset$.

- Kida and Kagawa (following Comalada, Ishii, Pinch) have determined $\mathcal{E}_{K,\emptyset}$ for $K = \mathbb{Q}(\sqrt{d})$ for many d with $-100 < d < 100$, but several were missing (including $d = -23$);
- Setzer (1978) gave necessary and sufficient conditions for the existence of $E \in \mathcal{E}_{K,\emptyset}$ with $E(K)[2] \neq 0$, K imaginary quadratic: for example, $\mathcal{E}_{\mathbb{Q}(\sqrt{-65}),\emptyset} \neq \emptyset$.
- Stroeker proved: if $[K : \mathbb{Q}] = 2$ and $\gcd(h_K, 6) = 1$ then $\mathcal{E}_{K,\emptyset} = \emptyset$.

- Kida and Kagawa (following Comalada, Ishii, Pinch) have determined $\mathcal{E}_{K,\emptyset}$ for $K = \mathbb{Q}(\sqrt{d})$ for many d with $-100 < d < 100$, but several were missing (including $d = -23$);
- Setzer (1978) gave necessary and sufficient conditions for the existence of $E \in \mathcal{E}_{K,\emptyset}$ with $E(K)[2] \neq 0$, K imaginary quadratic: for example, $\mathcal{E}_{\mathbb{Q}(\sqrt{-65}),\emptyset} \neq \emptyset$.
- Stroeker proved: if $[K:\mathbb{Q}] = 2$ and $\gcd(h_K, 6) = 1$ then $\mathcal{E}_{K,\emptyset} = \emptyset$.

Algebraic preliminaries: m-Selmer groups

In our method an important role is played by the so-called "m-Selmer groups" for the number field K. These are subgroups of K^*/K^{*m}:

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

So (the class of) $x \in K^*$ lies in $K(\mathcal{S}, m)$ if the $\mathcal{O}_{K,\mathcal{S}}$-ideal it generates is an m'th power, and we have the exact sequence:

$$1 \to \mathcal{O}_{K,\mathcal{S}}^*/\mathcal{O}_{K,\mathcal{S}}^{*m} \to K(\mathcal{S}, m) \xrightarrow{\alpha_m} \mathcal{C}_{K,\mathcal{S}}[m] \to 1$$

This is analogous to the Kummer sequence for elliptic curves:

$$0 \to E(K)/mE(K) \to \mathrm{Sel}^{(m)}(K, E) \to Ш[m] \to 0.$$

Algebraic preliminaries: m-Selmer groups

In our method an important role is played by the so-called "m-Selmer groups" for the number field K. These are subgroups of K^*/K^{*m}:

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

So (the class of) $x \in K^*$ lies in $K(\mathcal{S}, m)$ if the $\mathcal{O}_{K,\mathcal{S}}$-ideal it generates is an m'th power, and we have the exact sequence:

$$1 \to \mathcal{O}_{K,\mathcal{S}}^*/\mathcal{O}_{K,\mathcal{S}}^{*m} \to K(\mathcal{S}, m) \xrightarrow{\alpha_m} \mathcal{C}_{K,\mathcal{S}}[m] \to 1$$

This is analogous to the Kummer sequence for elliptic curves:

$$0 \to E(K)/mE(K) \to \mathrm{Sel}^{(m)}(K, E) \to \text{Ш}[m] \to 0.$$

Algebraic preliminaries: m-Selmer groups

In our method an important role is played by the so-called "m-Selmer groups" for the number field K. These are subgroups of K^*/K^{*m}:

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

So (the class of) $x \in K^*$ lies in $K(\mathcal{S}, m)$ if the $\mathcal{O}_{K,\mathcal{S}}$-ideal it generates is an m'th power, and we have the exact sequence:

$$1 \to \mathcal{O}^*_{K,\mathcal{S}}/\mathcal{O}^{*m}_{K,\mathcal{S}} \to K(\mathcal{S}, m) \xrightarrow{\alpha_m} \mathcal{C}_{K,\mathcal{S}}[m] \to 1$$

This is analogous to the Kummer sequence for elliptic curves:

$$0 \to E(K)/mE(K) \to \mathrm{Sel}^{(m)}(K, E) \to Ш[m] \to 0.$$

Computing m-Selmer groups of K

- We will need to use these m-Selmer groups for $m = 2$ primarily, but also for $m \in \{3, 4, 6, 12\}$.

- When m is prime, the computation of $K(\mathcal{S}, m)$ is a standard task of computational algebraic number theory, and is provided (for example) in MAGMA with the command `pSelmerGroup`.

- When $\gcd(m, n) = 1$ then $K(\mathcal{S}, mn) \cong K(\mathcal{S}, m) \times K(\mathcal{S}, n)$.

- in general...

Computing m-Selmer groups of K

- We will need to use these m-Selmer groups for $m = 2$ primarily, but also for $m \in \{3, 4, 6, 12\}$.

- When m is prime, the computation of $K(\mathcal{S}, m)$ is a standard task of computational algebraic number theory, and is provided (for example) in MAGMA with the command `pSelmerGroup`.

- When $\gcd(m, n) = 1$ then $K(\mathcal{S}, mn) \cong K(\mathcal{S}, m) \times K(\mathcal{S}, n)$.

- in general...

Computing m-Selmer groups of K

- We will need to use these m-Selmer groups for $m = 2$ primarily, but also for $m \in \{3, 4, 6, 12\}$.

- When m is prime, the computation of $K(\mathcal{S}, m)$ is a standard task of computational algebraic number theory, and is provided (for example) in MAGMA with the command `pSelmerGroup`.

- When $\gcd(m, n) = 1$ then $K(\mathcal{S}, mn) \cong K(\mathcal{S}, m) \times K(\mathcal{S}, n)$.

- in general...

Computing m-Selmer groups of K

- We will need to use these m-Selmer groups for $m = 2$ primarily, but also for $m \in \{3, 4, 6, 12\}$.

- When m is prime, the computation of $K(\mathcal{S}, m)$ is a standard task of computational algebraic number theory, and is provided (for example) in Magma with the command `pSelmerGroup`.

- When $\gcd(m, n) = 1$ then $K(\mathcal{S}, mn) \cong K(\mathcal{S}, m) \times K(\mathcal{S}, n)$.

- in general...

Computing m-Selmer groups of K

$$
\begin{array}{ccccccccccccc}
 & & 1 & & 1 & & 1 & & 1 & & & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & \mu_{m,n} & \longrightarrow & \mathcal{O}_{K,\mathcal{S}}^{*}/\mathcal{O}_{K,\mathcal{S}}^{*n} & \xrightarrow{m} & \mathcal{O}_{K,\mathcal{S}}^{*}/\mathcal{O}_{K,\mathcal{S}}^{*mn} & \longrightarrow & \mathcal{O}_{K,\mathcal{S}}^{*}/\mathcal{O}_{K,\mathcal{S}}^{*m} & \longrightarrow & 1 & & \\
 & & \| & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_{m,n} & \longrightarrow & K(\mathcal{S},n) & \xrightarrow{m} & K(\mathcal{S},mn) & \longrightarrow & K(\mathcal{S},m) & \xrightarrow{\alpha_{m,n}} & \dfrac{\mathcal{C}_{K,\mathcal{S}}[m]}{n\mathcal{C}_{K,\mathcal{S}}[mn]} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \| & & \\
 & & 1 & \longrightarrow & \mathcal{C}_{K,\mathcal{S}}[n] & \longrightarrow & \mathcal{C}_{K,\mathcal{S}}[mn] & \xrightarrow{n} & \mathcal{C}_{K,\mathcal{S}}[m] & \longrightarrow & \dfrac{\mathcal{C}_{K,\mathcal{S}}[m]}{n\mathcal{C}_{K,\mathcal{S}}[mn]} & \longrightarrow & 1 \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & & 1 & & 1 & &
\end{array}
$$

where

$$\mu_{m,n} = \mu_m(K)/(\mu_{mn}(K))^n.$$

An analogous diagram

$$
\begin{array}{ccccccccccccc}
 & & 0 & & 0 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \text{Ker} & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \xrightarrow{m} & E(\mathbb{Q})/mnE(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q})/mE(\mathbb{Q}) & \longrightarrow & 0 & & \\
 & & \| & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \text{Ker} & \longrightarrow & S^{(n)}(E/\mathbb{Q}) & \longrightarrow & S^{(mn)}(E/\mathbb{Q}) & \longrightarrow & S^{(m)}(E/\mathbb{Q}) & \longrightarrow & \text{Coker} & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & \longrightarrow & Ш(E/\mathbb{Q})[n] & \longrightarrow & Ш(E/\mathbb{Q})[mn] & \xrightarrow{n} & Ш(E/\mathbb{Q})[m] & \longrightarrow & \text{Coker} & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & & 0 & & 0 & &
\end{array}
$$

where

$$\text{Ker} = E(\mathbb{Q})[m]/nE(\mathbb{Q})[mn], \qquad \text{Coker} = Ш(E/\mathbb{Q})[m]/nШ(E/\mathbb{Q})[mn].$$

Computing m-Selmer groups of K

For example, to compute $K(\mathcal{S},4)$ we first compute $K(\mathcal{S},2)$ and then "lift" to $K(\mathcal{S},4)$: the obstruction to this lift is measured by a quotient of the 2-torsion in the $\mathcal{S}$-class group of K.

If we denote the image of $K(\mathcal{S},mn)$ in $K(\mathcal{S},m)$ by $K(\mathcal{S},m)_{mn}$, then the (finite abelian) group $K(\mathcal{S},mn)$ is an extension of $K(\mathcal{S},n)$ by $K(\mathcal{S},m)_{mn}$.

Application: We will use these Selmer groups in two related ways: most obviously, to parametrize elliptic curves with given j-invariant (using $m=2$ unless $j=0,1728$); and also in obtaining restrictions of the possible j-invariants which need to be considered.

For simplicity, in this talk we will

- **omit** the cases $j=0$ and $j=1728$;
- **assume** that $\mathcal{S}$ contains all primes $\mathfrak{p}$ dividing 2 or 3.

Computing m-Selmer groups of K

For example, to compute $K(\mathcal{S},4)$ we first compute $K(\mathcal{S},2)$ and then "lift" to $K(\mathcal{S},4)$: the obstruction to this lift is measured by a quotient of the 2-torsion in the $\mathcal{S}$-class group of K.

If we denote the image of $K(\mathcal{S},mn)$ in $K(\mathcal{S},m)$ by $K(\mathcal{S},m)_{mn}$, then the (finite abelian) group $K(\mathcal{S},mn)$ is an extension of $K(\mathcal{S},n)$ by $K(\mathcal{S},m)_{mn}$.

Application: We will use these Selmer groups in two related ways: most obviously, to parametrize elliptic curves with given j-invariant (using $m=2$ unless $j=0,1728$); and also in obtaining restrictions of the possible j-invariants which need to be considered.

For simplicity, in this talk we will

- **omit** the cases $j=0$ and $j=1728$;
- **assume** that $\mathcal{S}$ contains all primes $\mathfrak{p}$ dividing 2 or 3.

Our method: overview

There are two main steps in our method; the first step for the case $\mathcal{S} = \emptyset$ is similar to Kida's method. Given K and $\mathcal{S}$,

- Step A: Find a finite set of possible j-invariants
- Step B: Find all possible curves for each j-invariant

Step B is quite straightforward (details below) while Step A leads us to the complete solution of several Diophantine Equations (over K): specifically, we need to find the complete (finite) set of all $\mathcal{S}$-integral points on many elliptic curves of the form $Y^2 = X^3 - w$ (with $w \in K$). We use all currently available tools for this! In fact our method is not very original (though it has some original features), but it aims to be an (almost) automatic combination of the (almost) standard tools which are now available and becoming more sophisticated and powerful. Our implementation is in MAGMA.

Our method: overview

There are two main steps in our method; the first step for the case $\mathcal{S} = \emptyset$ is similar to Kida's method. Given K and $\mathcal{S}$,

- Step A: Find a finite set of possible j-invariants
- Step B: Find all possible curves for each j-invariant

Step B is quite straightforward (details below) while Step A leads us to the complete solution of several Diophantine Equations (over K): specifically, we need to find the complete (finite) set of all $\mathcal{S}$-integral points on many elliptic curves of the form $Y^2 = X^3 - w$ (with $w \in K$). We use all currently available tools for this! In fact our method is not very original (though it has some original features), but it aims to be an (almost) automatic combination of the (almost) standard tools which are now available and becoming more sophisticated and powerful. Our implementation is in MAGMA.

Our method: overview

There are two main steps in our method; the first step for the case $\mathcal{S} = \emptyset$ is similar to Kida's method. Given K and $\mathcal{S}$,

- Step A: Find a finite set of possible j-invariants
- Step B: Find all possible curves for each j-invariant

Step B is quite straightforward (details below) while Step A leads us to the complete solution of several Diophantine Equations (over K): specifically, we need to find the complete (finite) set of all $\mathcal{S}$-integral points on many elliptic curves of the form $Y^2 = X^3 - w$ (with $w \in K$). We use all currently available tools for this! In fact our method is not very original (though it has some original features), but it aims to be an (almost) automatic combination of the (almost) standard tools which are now available and becoming more sophisticated and powerful. Our implementation is in MAGMA.

Our method: overview

There are two main steps in our method; the first step for the case $\mathcal{S} = \emptyset$ is similar to Kida's method. Given K and $\mathcal{S}$,

- Step A: Find a finite set of possible j-invariants
- Step B: Find all possible curves for each j-invariant

Step B is quite straightforward (details below) while Step A leads us to the complete solution of several Diophantine Equations (over K): specifically, we need to find the complete (finite) set of all $\mathcal{S}$-integral points on many elliptic curves of the form $Y^2 = X^3 - w$ (with $w \in K$). We use all currently available tools for this! In fact our method is not very original (though it has some original features), but it aims to be an (almost) automatic combination of the (almost) standard tools which are now available and becoming more sophisticated and powerful. Our implementation is in MAGMA.

The condition on j

The following result characterizes the j-invariants we seek:

Proposition. *Let E be an elliptic curve defined over K with good reduction at all primes $\mathfrak{p} \notin \mathcal{S}$. Set $w = j^2(j-1728)^3$. Then*

$$\Delta \in K(\mathcal{S}, 12); \qquad j \in \mathcal{O}_{K,\mathcal{S}}; \qquad w \in K(\mathcal{S}, 6)_{12}.$$

Conversely, if $j \in \mathcal{O}_{K,\mathcal{S}}$ with $j^2(j-1728)^3 \in K(\mathcal{S}, 6)_{12}$ then there exist elliptic curves E with $j(E) = j$ and good reduction outside $\mathcal{S}$.

To apply this, we first determine the group $K(\mathcal{S}, 6)_{12}$ to find the set of possible w. Then for each w we determine whether the class of w contains a representative w' such that $w' = j^2(j-1728)^3$ with $j \in \mathcal{O}_{K,\mathcal{S}}$.

The condition on j

The following result characterizes the j-invariants we seek:

Proposition. *Let E be an elliptic curve defined over K with good reduction at all primes $\mathfrak{p} \notin \mathcal{S}$. Set $w = j^2(j-1728)^3$. Then*

$$\Delta \in K(\mathcal{S}, 12); \qquad j \in \mathcal{O}_{K,\mathcal{S}}; \qquad w \in K(\mathcal{S}, 6)_{12}.$$

Conversely, if $j \in \mathcal{O}_{K,\mathcal{S}}$ with $j^2(j-1728)^3 \in K(\mathcal{S}, 6)_{12}$ then there exist elliptic curves E with $j(E) = j$ and good reduction outside $\mathcal{S}$.

To apply this, we first determine the group $K(\mathcal{S}, 6)_{12}$ to find the set of possible w. Then for each w we determine whether the class of w contains a representative w' such that $w' = j^2(j-1728)^3$ with $j \in \mathcal{O}_{K,\mathcal{S}}$.

The auxiliary curves

Proposition. *Let* $w \in K(\mathcal{S}, 6)$*. Then each* $j \in \mathcal{O}_{K,\mathcal{S}}$ *(*$j \neq 0, 1728$*) with* $j^2(j-1728)^3 \equiv w \pmod{(K^*)^6}$ *has the form* $j = x^3/w = 1728 + y^2/w$*, where* $P = (x, y)$ *is an* $\mathcal{S}$*-integral point on the elliptic curve*

$$E_w : \qquad Y^2 = X^3 - 1728w$$

with $xy \neq 0$*.*

Moreover, suppose that we also have $w \in K(\mathcal{S}, 6)_{12}$*. Choose* $u_0 \in K^*$ *such that* $(3u_0)^6 w \in K(\mathcal{S}, 12)$*; then the elliptic curve*

$$E : \qquad Y^2 = X^3 - 3xu_0^2 X - 2yu_0^3$$

has j*-invariant* j *and good reduction outside* $\mathcal{S}$*. Moreover, the complete set of curves with good reduction outside* $\mathcal{S}$ *having* j*-invariant* j *is the set of quadratic twists* $E^{(u)}$ *for* $u \in K(\mathcal{S}, 2)$*.*

The auxiliary curves

Proposition. *Let* $w \in K(\mathcal{S},6)$*. Then each* $j \in \mathcal{O}_{K,\mathcal{S}}$ *(*$j \neq 0, 1728$*) with* $j^2(j-1728)^3 \equiv w \pmod{(K^*)^6}$ *has the form* $j = x^3/w = 1728 + y^2/w$*, where* $P = (x,y)$ *is an* $\mathcal{S}$*-integral point on the elliptic curve*

$$E_w : \qquad Y^2 = X^3 - 1728w$$

with $xy \neq 0$*.*

Moreover, suppose that we also have $w \in K(\mathcal{S},6)_{12}$*. Choose* $u_0 \in K^*$ *such that* $(3u_0)^6 w \in K(\mathcal{S},12)$*; then the elliptic curve*

$$E : \qquad Y^2 = X^3 - 3xu_0^2X - 2yu_0^3$$

has j*-invariant* j *and good reduction outside* $\mathcal{S}$*. Moreover, the complete set of curves with good reduction outside* $\mathcal{S}$ *having* j*-invariant* j *is the set of quadratic twists* $E^{(u)}$ *for* $u \in K(\mathcal{S},2)$*.*

Summary: Step A

Step A of our algorithm is thus:

1. list all $w \in K(\mathcal{S}, 6)_{12}$ (taking $\mathcal{S}$-integral representatives); for each:
2. construct the curve $E_w: \quad Y^2 = X^3 - 1728w$;
3. find $E_w(K)$ (an explicit $\mathbb{Z}$-basis);
4. find $E_w(\mathcal{O}_{K,\mathcal{S}})$ (all $\mathcal{S}$-integral points).

With $K = \mathbb{Q}$ the number of w to consider is $2 \cdot 6^{\#\mathcal{S}}$; for general K we get extra contributions from units and the 2- and 3-parts of the class group $\mathcal{C}\ell_K$.

After finishing Step A we will have all possible values of j, namely $j = x^3/w$ where $(x, y) \in E_w(K)$ is an $\mathcal{S}$-integral point.

Summary: Step A

Step A of our algorithm is thus:

1. list all $w \in K(\mathcal{S}, 6)_{12}$ (taking $\mathcal{S}$-integral representatives); for each:

2. construct the curve $E_w: \quad Y^2 = X^3 - 1728w$;

3. find $E_w(K)$ (an explicit $\mathbb{Z}$-basis);

4. find $E_w(\mathcal{O}_{K,\mathcal{S}})$ (all $\mathcal{S}$-integral points).

With $K = \mathbb{Q}$ the number of w to consider is $2 \cdot 6^{\#\mathcal{S}}$; for general K we get extra contributions from units and the 2- and 3-parts of the class group $\mathcal{C}\ell_K$.

After finishing Step A we will have all possible values of j, namely $j = x^3/w$ where $(x, y) \in E_w(K)$ is an $\mathcal{S}$-integral point.

Summary: Step A

Step A of our algorithm is thus:

1. list all $w \in K(\mathcal{S},6)_{12}$ (taking $\mathcal{S}$-integral representatives); for each:

2. construct the curve $E_w : \quad Y^2 = X^3 - 1728w$;

3. find $E_w(K)$ (an explicit $\mathbb{Z}$-basis);

4. find $E_w(\mathcal{O}_{K,\mathcal{S}})$ (all $\mathcal{S}$-integral points).

With $K = \mathbb{Q}$ the number of w to consider is $2 \cdot 6^{\#\mathcal{S}}$; for general K we get extra contributions from units and the 2- and 3-parts of the class group $\mathcal{C}\ell_K$.

After finishing Step A we will have all possible values of j, namely $j = x^3/w$ where $(x, y) \in E_w(K)$ is an $\mathcal{S}$-integral point.

Summary: Step A

Step A of our algorithm is thus:

1. list all $w \in K(\mathcal{S},6)_{12}$ (taking $\mathcal{S}$-integral representatives); for each:
2. construct the curve $E_w : \quad Y^2 = X^3 - 1728w$;
3. find $E_w(K)$ (an explicit $\mathbb{Z}$-basis);
4. find $E_w(\mathcal{O}_{K,\mathcal{S}})$ (all $\mathcal{S}$-integral points).

With $K = \mathbb{Q}$ the number of w to consider is $2 \cdot 6^{\#\mathcal{S}}$; for general K we get extra contributions from units and the 2- and 3-parts of the class group $\mathcal{C}\ell_K$.

After finishing Step A we will have all possible values of j, namely $j = x^3/w$ where $(x, y) \in E_w(K)$ is an $\mathcal{S}$-integral point.

Summary: Step A

Step A of our algorithm is thus:

1. list all $w \in K(\mathcal{S},6)_{12}$ (taking $\mathcal{S}$-integral representatives); for each:
2. construct the curve $E_w: \quad Y^2 = X^3 - 1728w$;
3. find $E_w(K)$ (an explicit $\mathbb{Z}$-basis);
4. find $E_w(\mathcal{O}_{K,\mathcal{S}})$ (all $\mathcal{S}$-integral points).

With $K = \mathbb{Q}$ the number of w to consider is $2 \cdot 6^{\#\mathcal{S}}$; for general K we get extra contributions from units and the 2- and 3-parts of the class group $\mathcal{C}\ell_K$.
After finishing Step A we will have all possible values of j, namely $j = x^3/w$ where $(x,y) \in E_w(K)$ is an $\mathcal{S}$-integral point.

Step B: finding the curves from their j-invariants

As is well-known, the j-invariant determines the isomorphism class of the elliptic curve up to **quadratic twist** (since we have excluded the cases $j = 0$ and $j = 1728$).

The last part of the previous Proposition lists precisely which quadratic twists actually do have good reduction outside $\mathcal{S}$: we find a first such twist from the information that $w \in K(\mathcal{S}, 6)_{12}$ (and not just $\in K(\mathcal{S}, 6)$); then the other valid twists are the twists of this base curve parametrized by $K(\mathcal{S}, 2)$.

Remarks:

1. If $\mathcal{S}$ does not contain all primes dividing 6, some of the curves will need to be discarded as they may not have good reduction at such primes;

2. For $j = 0, 1728$ we must consider sextic and quartic twists respectively. The exact set of twists to be considered is left as an exercise!

Step B: finding the curves from their j-invariants

As is well-known, the j-invariant determines the isomorphism class of the elliptic curve up to **quadratic twist** (since we have excluded the cases $j = 0$ and $j = 1728$).

The last part of the previous Proposition lists precisely which quadratic twists actually do have good reduction outside $\mathcal{S}$: we find a first such twist from the information that $w \in K(\mathcal{S}, 6)_{12}$ (and not just $\in K(\mathcal{S}, 6)$); then the other valid twists are the twists of this base curve parametrized by $K(\mathcal{S}, 2)$.

Remarks:

1. If $\mathcal{S}$ does not contain all primes dividing 6, some of the curves will need to be discarded as they may not have good reduction at such primes;

2. For $j = 0, 1728$ we must consider sextic and quartic twists respectively. The exact set of twists to be considered is left as an exercise!

Step B: finding the curves from their j-invariants

As is well-known, the j-invariant determines the isomorphism class of the elliptic curve up to **quadratic twist** (since we have excluded the cases $j = 0$ and $j = 1728$).

The last part of the previous Proposition lists precisely which quadratic twists actually do have good reduction outside $\mathcal{S}$: we find a first such twist from the information that $w \in K(\mathcal{S}, 6)_{12}$ (and not just $\in K(\mathcal{S}, 6)$); then the other valid twists are the twists of this base curve parametrized by $K(\mathcal{S}, 2)$.

Remarks:

1. If $\mathcal{S}$ does not contain all primes dividing 6, some of the curves will need to be discarded as they may not have good reduction at such primes;

2. For $j = 0, 1728$ we must consider sextic and quartic twists respectively. The exact set of twists to be considered is left as an exercise!

Problems

- There are many curves E_w to consider in Step A
- To find all $\mathcal{S}$-integral points on each we must first find the full Mordell-Weil group $E_w(K)$; then use the method of elliptic logarithms, LLL, ...
- Over $\mathbb{Q}$, MAGMA now has good tools for finding $E_w(\mathbb{Q})$ (including descent methods and Heegner points), and a function (due to Herrmann) for finding $\mathcal{S}$-integral points automatically. But there are still curves for which MAGMA cannot find $E_w(\mathbb{Q})$ without some help (see examples to follow).
- Over general number fields K, everything is more difficult. in many cases MAGMA can now find the M-W group (using new 2-descent functionality provided mainly by Nils Bruin). **BUT** there is not yet an implementation of the $\mathcal{S}$-integral point function, except for Herrmann's own code (from 2003), not publicly available–yet.

Problems

- There are many curves E_w to consider in Step A
- To find all $\mathcal{S}$-integral points on each we must first find the full Mordell-Weil group $E_w(K)$; then use the method of elliptic logarithms, LLL, ...
- Over $\mathbb{Q}$, MAGMA now has good tools for finding $E_w(\mathbb{Q})$ (including descent methods and Heegner points), and a function (due to Herrmann) for finding $\mathcal{S}$-integral points automatically. But there are still curves for which MAGMA cannot find $E_w(\mathbb{Q})$ without some help (see examples to follow).
- Over general number fields K, everything is more difficult. in many cases MAGMA can now find the M-W group (using new 2-descent functionality provided mainly by Nils Bruin). **BUT** there is not yet an implementation of the $\mathcal{S}$-integral point function, except for Herrmann's own code (from 2003), not publicly available–yet.

Problems

- There are many curves E_w to consider in Step A
- To find all $\mathcal{S}$-integral points on each we must first find the full Mordell-Weil group $E_w(K)$; then use the method of elliptic logarithms, LLL, ...
- Over $\mathbb{Q}$, MAGMA now has good tools for finding $E_w(\mathbb{Q})$ (including descent methods and Heegner points), and a function (due to Herrmann) for finding $\mathcal{S}$-integral points automatically. But there are still curves for which MAGMA cannot find $E_w(\mathbb{Q})$ without some help (see examples to follow).
- Over general number fields K, everything is more difficult. in many cases MAGMA can now find the M-W group (using new 2-descent functionality provided mainly by Nils Bruin). **BUT** there is not yet an implementation of the $\mathcal{S}$-integral point function, except for Herrmann's own code (from 2003), not publicly available–yet.

Problems

- There are many curves E_w to consider in Step A
- To find all $\mathcal{S}$-integral points on each we must first find the full Mordell-Weil group $E_w(K)$; then use the method of elliptic logarithms, LLL, ...
- Over $\mathbb{Q}$, MAGMA now has good tools for finding $E_w(\mathbb{Q})$ (including descent methods and Heegner points), and a function (due to Herrmann) for finding $\mathcal{S}$-integral points automatically. But there are still curves for which MAGMA cannot find $E_w(\mathbb{Q})$ without some help (see examples to follow).
- Over general number fields K, everything is more difficult. in many cases MAGMA can now find the M-W group (using new 2-descent functionality provided mainly by Nils Bruin). **BUT** there is not yet an implementation of the $\mathcal{S}$-integral point function, except for Herrmann's own code (from 2003), not publicly available–yet.

- Apart from the one example $K = \mathbb{Q}(\sqrt{-23})$, $\mathcal{S} = \emptyset$ where Herrmann kindly verified that our sets of integral points on $Y^2 = X^3 \pm 1728$ (over K) were complete, our results over number fields are all currently *conditional* on our lists of $\mathcal{S}$-integral points being complete.

Examples/Results over $\mathbb{Q}$

- $\mathcal{S} = \emptyset \implies \mathbb{Q}(\mathcal{S}, 6) = \{\pm 1\}$ so we consider $Y^2 = X^3 \pm 1728$ which both have rank 0 and $(\mp 12, 0)$ are the only integral points, so the only candidate j is $j = 1728$, leading to no curves with conductor 1.

- $\mathcal{S} = \{2\}$ leads to 13 possible j and 24 curves with conductors $32, 64, 128, 256$.

- $\mathcal{S} = \{2, 3\}$ leads to 83 possible j and 752 curves with conductors $2^a 3^b$.

Examples/Results over $\mathbb{Q}$

- $\mathcal{S} = \emptyset \implies \mathbb{Q}(\mathcal{S}, 6) = \{\pm 1\}$ so we consider $Y^2 = X^3 \pm 1728$ which both have rank 0 and $(\mp 12, 0)$ are the only integral points, so the only candidate j is $j = 1728$, leading to no curves with conductor 1.

- $\mathcal{S} = \{2\}$ leads to 13 possible j and 24 curves with conductors $32, 64, 128, 256$.

- $\mathcal{S} = \{2, 3\}$ leads to 83 possible j and 752 curves with conductors $2^a 3^b$.

Examples/Results over $\mathbb{Q}$

- $\mathcal{S} = \emptyset \implies \mathbb{Q}(\mathcal{S}, 6) = \{\pm 1\}$ so we consider $Y^2 = X^3 \pm 1728$ which both have rank 0 and $(\mp 12, 0)$ are the only integral points, so the only candidate j is $j = 1728$, leading to no curves with conductor 1.

- $\mathcal{S} = \{2\}$ leads to 13 possible j and 24 curves with conductors $32, 64, 128, 256$.

- $\mathcal{S} = \{2, 3\}$ leads to 83 possible j and 752 curves with conductors $2^a 3^b$.

- $\mathcal{S} = \{2, 17\}$ leads to 42 possible j. During Step A:
  - ⋆ $w = -17^5$ gives a curve of rank 0 with Selmer rank 2, so we used the analytic rank;
  - ⋆ The curves for $w = 2^5 17^5, 2^2 17^4, -2^5 17^4, -2^4 17^4$ have rank 1 with large generators. For example, the generator for $w = 2^5 17^5$ has x-coordinate with denominator d^2 with

$$d = 3 \cdot 5 \cdot 64189 \cdot 259907 \cdot 20745658643 \cdot 79102726763$$

which we computed using a Heegner point. So this curve has no $\mathcal{S}$-integral points – but there should be an easier way to show that!

- Complete lists for $\mathcal{S} = \{2, 3\}$ (752 curves), $\mathcal{S} = \{2, 3, 5\}$ (7552 curves), $\mathcal{S} = \{2, 3, 7\}$ (7168 curves), $\mathcal{S} = \{2, 3, 11\}$ (6640 curves) are available at `http://www.maths.nottingham.ac.uk/personal/jec/ftp/data/extra.html`.

- $\mathcal{S} = \{2, 17\}$ leads to 42 possible j. During Step A:
  - ⋆ $w = -17^5$ gives a curve of rank 0 with Selmer rank 2, so we used the analytic rank;
  - ⋆ The curves for $w = 2^5 17^5, 2^2 17^4, -2^5 17^4, -2^4 17^4$ have rank 1 with large generators. For example, the generator for $w = 2^5 17^5$ has x-coordinate with denominator d^2 with

$$d = 3 \cdot 5 \cdot 64189 \cdot 259907 \cdot 20745658643 \cdot 79102726763$$

    which we computed using a Heegner point. So this curve has no $\mathcal{S}$-integral points – but there should be an easier way to show that!

- Complete lists for $\mathcal{S} = \{2, 3\}$ (752 curves), $\mathcal{S} = \{2, 3, 5\}$ (7552 curves), $\mathcal{S} = \{2, 3, 7\}$ (7168 curves), $\mathcal{S} = \{2, 3, 11\}$ (6640 curves) are available at `http://www.maths.nottingham.ac.uk/personal/jec/ftp/data/extra.html`.

Examples/Results over quadratic fields

- $K = \mathbb{Q}(\sqrt{-23})$, $\mathcal{S} = \emptyset$: $K(\mathcal{S}, 6) = \{\pm1, \pm(1+\omega), \pm(2-\omega)\}$ where $\omega = (1+\sqrt{-23})/2$ (class number 3, units ±1). Four $w \in K(\mathcal{S}, 6)$ gives curves with trivial Mordell-Weil group; the other two are $Y^2 = X^3 \pm 1728$ which both have rank 1 over K; we found a generator for each and (with help from Herrmann) showed that only $j = 0, \pm1728$ are candidates, but none gives a curve with everywhere good reduction over K. Hence there are no such curves.

- $K = \mathbb{Q}(\sqrt{-1})$, $\mathcal{S} = \{1+i\}$ (treated by Stroeker): we find 22 possible j and 64 curves with condutor $(1+i)^e$, in agreement with Stroeker:

e	6	8	9	10	12	13	14
#	2	2	8	12	8	16	16

Our result here is conditional on our lists of $(1+i)$-integral points being complete.

Examples/Results over quadratic fields

- $K = \mathbb{Q}(\sqrt{-23})$, $\mathcal{S} = \emptyset$: $K(\mathcal{S},6) = \{\pm1, \pm(1+\omega), \pm(2-\omega)\}$ where $\omega = (1+\sqrt{-23})/2$ (class number 3, units ±1). Four $w \in K(\mathcal{S},6)$ gives curves with trivial Mordell-Weil group; the other two are $Y^2 = X^3 \pm 1728$ which both have rank 1 over K; we found a generator for each and (with help from Herrmann) showed that only $j = 0, \pm1728$ are candidates, but none gives a curve with everywhere good reduction over K. Hence there are no such curves.

- $K = \mathbb{Q}(\sqrt{-1})$, $\mathcal{S} = \{1+i\}$ (treated by Stroeker): we find 22 possible j and 64 curves with condutor $(1+i)^e$, in agreement with Stroeker:

e	6	8	9	10	12	13	14
#	2	2	8	12	8	16	16

Our result here is conditional on our lists of $(1+i)$-integral points being complete.

- $K = \mathbb{Q}(\sqrt{-23})$, $\mathcal{S} = \{\mathfrak{p}_2\}$ where $N(\mathfrak{p}_2) = 2$ and the class of $\mathfrak{p}_2$ generates the class group. We (conditionally) find $\mathcal{E}_{K,\mathcal{S}} = \emptyset$, in agreement with the prediction from Mark Lingham's modular symbol computations.

- $K = \mathbb{Q}(\sqrt{-23})$: for certain small integral ideals $\mathfrak{n}$, Mark Lingham computed cusp forms of weight 2 and level $\mathfrak{n}$ but found no matching elliptic curves of conductor $\mathfrak{n}$. Using our program we found some of these curves. For example, the curve with coefficients $[0, 0, 0, -53160w - 43995, -5067640w + 19402006]$ and conductor $\mathfrak{n} = \mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3^2\overline{\mathfrak{p}_3}$ of norm 108 was found this way.

- $K = \mathbb{Q}(\sqrt{38})$: we found the following curve with everywhere good reduction: $Y^2 = X^3 + a_4 X + a_6$ where where $\varepsilon = 6\sqrt{38} + 37$ is a unit and

$$a_4 = -3^3 \cdot 5 \cdot \varepsilon^{-1} = 810\sqrt{38} - 4995,$$

$$a_6 = 2 \cdot 3^3 \cdot 7(\sqrt{38} - 2)\varepsilon^{-1} = 27594\sqrt{38} - 170100.$$

- $K = \mathbb{Q}(\sqrt{-23})$, $\mathcal{S} = \{\mathfrak{p}_2\}$ where $N(\mathfrak{p}_2) = 2$ and the class of $\mathfrak{p}_2$ generates the class group. We (conditionally) find $\mathcal{E}_{K,\mathcal{S}} = \emptyset$, in agreement with the prediction from Mark Lingham's modular symbol computations.

- $K = \mathbb{Q}(\sqrt{-23})$: for certain small integral ideals $\mathfrak{n}$, Mark Lingham computed cusp forms of weight 2 and level $\mathfrak{n}$ but found no matching elliptic curves of conductor $\mathfrak{n}$. Using our program we found some of these curves. For example, the curve with coefficients $[0, 0, 0, -53160w - 43995, -5067640w + 19402006]$ and conductor $\mathfrak{n} = \mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3^2\overline{\mathfrak{p}_3}$ of norm 108 was found this way.

- $K = \mathbb{Q}(\sqrt{38})$: we found the following curve with everywhere good reduction: $Y^2 = X^3 + a_4X + a_6$ where where $\varepsilon = 6\sqrt{38} + 37$ is a unit and

$$a_4 = -3^3 \cdot 5 \cdot \varepsilon^{-1} = 810\sqrt{38} - 4995,$$

$$a_6 = 2 \cdot 3^3 \cdot 7(\sqrt{38} - 2)\varepsilon^{-1} = 27594\sqrt{38} - 170100.$$

- $K = \mathbb{Q}(\sqrt{-23})$, $\mathcal{S} = \{\mathfrak{p}_2\}$ where $N(\mathfrak{p}_2) = 2$ and the class of $\mathfrak{p}_2$ generates the class group. We (conditionally) find $\mathcal{E}_{K,\mathcal{S}} = \emptyset$, in agreement with the prediction from Mark Lingham's modular symbol computations.

- $K = \mathbb{Q}(\sqrt{-23})$: for certain small integral ideals $\mathfrak{n}$, Mark Lingham computed cusp forms of weight 2 and level $\mathfrak{n}$ but found no matching elliptic curves of conductor $\mathfrak{n}$. Using our program we found some of these curves. For example, the curve with coefficients $[0, 0, 0, -53160w - 43995, -5067640w + 19402006]$ and conductor $\mathfrak{n} = \mathfrak{p}_2\overline{\mathfrak{p}_2}\mathfrak{p}_3^2\overline{\mathfrak{p}_3}$ of norm 108 was found this way.

- $K = \mathbb{Q}(\sqrt{38})$: we found the following curve with everywhere good reduction: $Y^2 = X^3 + a_4X + a_6$ where where $\varepsilon = 6\sqrt{38} + 37$ is a unit and

$$a_4 = -3^3 \cdot 5 \cdot \varepsilon^{-1} = 810\sqrt{38} - 4995,$$

$$a_6 = 2 \cdot 3^3 \cdot 7(\sqrt{38} - 2)\varepsilon^{-1} = 27594\sqrt{38} - 170100.$$