Tables of elliptic curves

John Cremona

University of Warwick

22 June 2010

Overview of the lectures

1. Introduction; the elliptic curve database
2. Optimality and the Manin conjecture
3. Computing isogenies
4. Finding elliptic curves with good reduction outside a given set of primes

Introduction: Why make tables of elliptic curves?

Introduction: 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.

Introduction: 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.

Introduction: 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. Now life is much easier!

Packages such as SAGE, MAGMA and PARI/GP contain the elliptic curve databases (sometimes as optional add-ons as they are large) and of course the internet makes accessing even "printed" tables much easier.

What is a table?

We will be exclusively concerned with elliptic curves defined over number fields, with a special emphasis on curves defined over $\mathbb{Q}$. We are not interested (at least, not right now) on curves defined over finite fields, or over function fields.

What is a table?

We will be exclusively concerned with elliptic curves defined over number fields, with a special emphasis on curves defined over $\mathbb{Q}$. We are not interested (at least, not right now) on curves defined over finite fields, or over function fields.

How do we order elliptic curves?

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

There are several possibilities:

What is a table?

We will be exclusively concerned with elliptic curves defined over number fields, with a special emphasis on curves defined over $\mathbb{Q}$. We are not interested (at least, not right now) on curves defined over finite fields, or over function fields.

How do we order elliptic curves?

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

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 (better) $\max\{|c_4|^{1/3}, |c_6|^{1/2}\}$
- By discriminant Δ
- By conductor N

Databases past, present . . . and future

- Brumer and McGuinness (1980s): prime $|\Delta| < 10^8$, 310711 curves. Produced surprising rank distributions.

Databases past, present ... and future

- Brumer and McGuinness (1980s): prime $|\Delta| < 10^8$, 310711 curves. Produced surprising rank distributions.
- Stein and Watkins (see ANTS-V 2002): $N \leq 10^{10}$ and Δ prime, or $N \leq 10^8$ and $|\Delta| \leq 10^{12}$ (approximately): 44 million curves.

Databases past, present . . . and future

- Brumer and McGuinness (1980s): prime $|\Delta| < 10^8$, 310711 curves. Produced surprising rank distributions.
- Stein and Watkins (see ANTS-V 2002): $N \leq 10^{10}$ and Δ prime, or $N \leq 10^8$ and $|\Delta| \leq 10^{12}$ (approximately): 44 million curves.

These tables contain huge numbers of curves. Though they are not complete (for example, Stein-Watkins does not contain 174a=[1,0,1,-7705,1226492]) they provide lots of useful data.

Databases past, present . . . and future

- Brumer and McGuinness (1980s): prime $|\Delta| < 10^8$, 310711 curves. Produced surprising rank distributions.
- Stein and Watkins (see ANTS-V 2002): $N \leq 10^{10}$ and Δ prime, or $N \leq 10^8$ and $|\Delta| \leq 10^{12}$ (approximately): 44 million curves.

These tables contain huge numbers of curves. Though they are not complete (for example, Stein-Watkins does not contain 174a=[1,0,1,-7705,1226492]) they provide lots of useful data. See William A. Stein and Mark Watkins, ”A database of elliptic curves – first report”, ANTS V Proceedings (Sydney 2002) Springer LNCS 2369 (Fieker and Kohel, eds.), pages 267 - 275.

The Antwerp tables

"Antwerp IV" := *Modular function of One Variable IV*, edited by Birch and Kuyk, Proceedings of an International Summer School in Antwerp, July 17 - August 3, 1972. See `http://modular.math.washington.edu/scans/antwerp/`.

The tables in Antwerp IV

1. "All" elliptic curves of conductor $N \leq 200$, together with most ranks, arranged in isogeny classes.
2. Generators for the (rank 1) curves in Table 1. [Stephens, Davenport]
3. Hecke eigenvalues for $p < 100$ for the associated newforms. [Vélu, Stephens, Tingley]
4. All elliptic curves of conductor $N = 2^a 3^b$. [Coghlan]
5. Dimensions of spaces of newforms for $\Gamma_0(N)$ for $N \leq 300$. [Atkin, Tingley]
6. Factorized supersingular j-polynomials for $p \leq 307$. [Atkin]

Antwerp IV Table 1

"The origins of Table 1 are ... complicated".

Antwerp IV Table 1

"The origins of Table 1 are ... complicated".

- Swinnerton-Dyer searched for curves with small coefficients, kept those with conductor $N \leq 200$, added curves obtained via a succession of 2- and 3-isogenies.
- Higher degree isogenies checked using Vélu's method; some curves added.
- Tingley computed newforms for $N \leq 300$, revealing 30 gaps, which were then filled, in some cases by computing the period lattice of the newform. For example

$$78A: \qquad Y^2 + XY = X^3 + X^2 - 19X + 685.$$

- Ranks computed by James Davenport using 2-descent.
- List complete for certain N, such as $N = 2^a 3^b$.
- Tingley's thesis (1975) contains curves with $200 < N \leq 320$ found via modular symbols, newforms and periods.

1972–1982–1992–2002

- No more systematic enumeration by conductor occurred between 1972 and the mid 1980s.
- 1985–1988: Implementation of modular symbols for $\Gamma_0(N)$ and $\Gamma_1(N)$ in `Algol68`
- 1988–1992: Preparation of tables for $N \leq 1000$ (with ranks, generators, isogenies), published in 1992.
- 1992–1997: Revisions, corrections, additional data (modular parmetrization degrees), range extended to 5077 for online tables.
- 1997–2002: slow growth of conductor range. Online publication: `http://www.warwick.ac.uk/staff/J.E.Cremona/book/fulltext/`.

Algorithms and Implementation

- Use modular symbols modulo N
  - Compute space of $\Gamma_0(N)$-modular symbols [fast]

Algorithms and Implementation

- Use modular symbols modulo N
  - Compute space of $\Gamma_0(N)$-modular symbols [fast]
- Find newforms for $\Gamma_0(N)$ with Hecke eigenvalues
  - Compute action of the Hecke algebra [quite fast]
  - Find one-dimensional rational eigenspaces: each corresponds to a rational newform f [slow for large levels: requires much RAM and is currently the main obstruction to extending the tables.]

Algorithms and Implementation

- Use modular symbols modulo N
  - Compute space of $\Gamma_0(N)$-modular symbols [fast]
- Find newforms for $\Gamma_0(N)$ with Hecke eigenvalues
  - Compute action of the Hecke algebra [quite fast]
  - Find one-dimensional rational eigenspaces: each corresponds to a rational newform f [slow for large levels: requires much RAM and is currently the main obstruction to extending the tables.]
- For each f, compute its periods and hence the associated elliptic curve E_f [quite fast]

Algorithms and Implementation

- Use modular symbols modulo N
  - Compute space of $\Gamma_0(N)$-modular symbols [fast]
- Find newforms for $\Gamma_0(N)$ with Hecke eigenvalues
  - Compute action of the Hecke algebra [quite fast]
  - Find one-dimensional rational eigenspaces: each corresponds to a rational newform f [slow for large levels: requires much RAM and is currently the main obstruction to extending the tables.]
- For each f, compute its periods and hence the associated elliptic curve E_f [quite fast]
- Use any available method to find Mordell-Weil groups, isogenous curves, etc. [usually fast]

2001-2005

Date	Conductor reached
Mar 2001	10000
Oct 2002	15000
Apr 2003	20000
Jun 2004	25000
Feb 2005	30000

2001-2005

Date	Conductor reached
Mar 2001	10000
Oct 2002	15000
Apr 2003	20000
Jun 2004	25000
Feb 2005	30000

Then the new computer was delivered. . .

2001-2005

Date	Conductor reached
Mar 2001	10000
Oct 2002	15000
Apr 2003	20000
Jun 2004	25000
Feb 2005	30000
Then the new computer was delivered. . .	
22 Apr 2005	40000
27 May 2005	50000
9 Jun 2005	60000
20 Jun 2005	70000
14 Jul 2005	80000
26 Aug 2005	90000
31 Aug 2005	100000
18 Sep 2005	120000
3 Nov 2005	130000

2006-2010

- The reason for stopping at 130000 was that the new machine had 1024 processors but each only had 2G of RAM, and more and more levels needed more than that.

2006-2010

- The reason for stopping at 130000 was that the new machine had 1024 processors but each only had 2G of RAM, and more and more levels needed more than that.
- During 2006 I rewrote the program, in particular the sparse linear algebra code, hoping for an improvement.

2006-2010

- The reason for stopping at 130000 was that the new machine had 1024 processors but each only had 2G of RAM, and more and more levels needed more than that.
- During 2006 I rewrote the program, in particular the sparse linear algebra code, hoping for an improvement.
- From 2006-07-21 to 2006-09-06, i.e. 47 days, only 43 more levels were managed, reaching 130043.

2006-2010

- The reason for stopping at 130000 was that the new machine had 1024 processors but each only had 2G of RAM, and more and more levels needed more than that.
- During 2006 I rewrote the program, in particular the sparse linear algebra code, hoping for an improvement.
- From 2006-07-21 to 2006-09-06, i.e. 47 days, only 43 more levels were managed, reaching 130043.
- Recently (on 2010-06-11) I restarted at $N = 130044$, which took 66 hours (but only 2.5G max). Currently running: $N = 130052$.

2006-2010

- The reason for stopping at 130000 was that the new machine had 1024 processors but each only had 2G of RAM, and more and more levels needed more than that.
- During 2006 I rewrote the program, in particular the sparse linear algebra code, hoping for an improvement.
- From 2006-07-21 to 2006-09-06, i.e. 47 days, only 43 more levels were managed, reaching 130043.
- Recently (on 2010-06-11) I restarted at $N = 130044$, which took 66 hours (but only 2.5G max). Currently running: $N = 130052$.
- More work is needed on the code to get substantially further.

The next goal

Of course, this could go on for ever! So what is a reasonable goal to aim for?

The next goal

Of course, this could go on for ever! So what is a reasonable goal to aim for?
All elliptic curves with $N \leq 130000$ have rank $r \leq 3$. (The number with $r = 3$ is 908.)

The next goal

Of course, this could go on for ever! So what is a reasonable goal to aim for?
All elliptic curves with $N \leq 130000$ have rank $r \leq 3$. (The number with $r = 3$ is 908.) What is the smallest conductor of a curve of rank 4?

```
sage : [(r, elliptic_curves.rank(r)[0].conductor())
for r in range(6)]
```

$$[(0, 11), (1, 37), (2, 389), (3, 5077), (4, 234446), (5, 19047851)]$$

The next goal

Of course, this could go on for ever! So what is a reasonable goal to aim for?
All elliptic curves with $N \leq 130000$ have rank $r \leq 3$. (The number with $r = 3$ is 908.) What is the smallest conductor of a curve of rank 4?

```
sage : [(r, elliptic_curves.rank(r)[0].conductor())
for r in range(6)]
```

$$[(0,11),(1,37),(2,389),(3,5077),(4,234446),(5,19047851)]$$

To prove that $N = 234446$ is the smallest rank 4 conductor would require finding all elliptic curves for $130001 \leq N \leq 234445$, which would take a few hundred processor-years with the current code.

Verifying BSD by computing ranks

In order to verify “weak BSD” for a given curve, we need to compute two numbers:

1. the analytic rank r_{an} of E
2. the algebraic rank r_E of $E(\mathbb{Q})$

and check that they are equal.

Verifying BSD by computing ranks

In order to verify "weak BSD" for a given curve, we need to compute two numbers:

1. the analytic rank r_{an} of E
2. the algebraic rank r_E of $E(\mathbb{Q})$

and check that they are equal. We know that $r_{an} \leq 1 \implies r_E = r_{an}$, but in this case we still have to prove that $r_{an} = 0$ or 1!

Verifying BSD by computing ranks

In order to verify “weak BSD” for a given curve, we need to compute two numbers:

1. the analytic rank r_{an} of E
2. the algebraic rank r_E of $E(\mathbb{Q})$

and check that they are equal. We know that $r_{an} \leq 1 \implies r_E = r_{an}$, but in this case we still have to prove that $r_{an} = 0$ or 1!
To determine r_{an}, we use the L-series $L(E, s) = L(f, s)$, where f is the associated modular form.

Verifying BSD by computing ranks

In order to verify "weak BSD" for a given curve, we need to compute two numbers:

1. the analytic rank r_{an} of E
2. the algebraic rank r_E of $E(\mathbb{Q})$

and check that they are equal. We know that $r_{an} \leq 1 \implies r_E = r_{an}$, but in this case we still have to prove that $r_{an} = 0$ or 1!

To determine r_{an}, we use the L-series $L(E,s) = L(f,s)$, where f is the associated modular form.

For r_E, we use 2-descent (for example) –unless $r_{an} \leq 1$.

Determining the analytic rank I: the good news

As before let E be an elliptic curve with associated rational newform f.

Determining the analytic rank I: the good news

As before let E be an elliptic curve with associated rational newform f.Modular symbol computations can tell us

1. The sign of the functional equation of $L(f,s)$ ($=$ minus the eigenvalus of the Fricke involution W_N on f);
2. the value of $L(f,1)/\Omega_0(f) \in \mathbb{Q}$, and in particular whether it is 0.

Determining the analytic rank I: the good news

As before let E be an elliptic curve with associated rational newform f.Modular symbol computations can tell us

1. The sign of the functional equation of $L(f,s)$ ($=$ minus the eigenvalus of the Fricke involution W_N on f);
2. the value of $L(f,1)/\Omega_0(f) \in \mathbb{Q}$, and in particular whether it is 0.

Hence we can easily decide whether $r_{an} = 0$, r_{an} is positive and odd, or r_{an} is positive and even.

Determining the analytic rank I: the good news

As before let E be an elliptic curve with associated rational newform f.Modular symbol computations can tell us

1. The sign of the functional equation of $L(f,s)$ ($=$ minus the eigenvalus of the Fricke involution W_N on f);
2. the value of $L(f,1)/\Omega_0(f) \in \mathbb{Q}$, and in particular whether it is 0.

Hence we can easily decide whether $r_{an} = 0$, r_{an} is positive and odd, or r_{an} is positive and even.

If r_{an} is positive and odd, we compute $L'(f,1)$; if that is nonzero we know that $r_{an} = 1$ (and hence $r_E = 1$).

Determining the analytic rank I: the good news

As before let E be an elliptic curve with associated rational newform f.Modular symbol computations can tell us

1. The sign of the functional equation of $L(f, s)$ ($=$ minus the eigenvalus of the Fricke involution W_N on f);
2. the value of $L(f, 1)/\Omega_0(f) \in \mathbb{Q}$, and in particular whether it is 0.

Hence we can easily decide whether $r_{an} = 0$, r_{an} is positive and odd, or r_{an} is positive and even.
If r_{an} is positive and odd, we compute $L'(f, 1)$; if that is nonzero we know that $r_{an} = 1$ (and hence $r_E = 1$).
If r_{an} is positive and even, we compute $L''(f, 1)$; if nonzero then $r_{an} = 2$. Now we also verify that $r_E = 2$ and are done.

Determining the analytic rank II: the bad news

What if r_{an} is odd and $L'(f, 1)$ appears to be 0?

Determining the analytic rank II: the bad news

What if r_{an} is odd and $L'(f, 1)$ appears to be 0? We then expect that $r_{an} = 3$. We can prove that $r_{an} \geq 3$ by checking that $r_E \geq 3$ (for example, by 2-descent). Then we may then compute $L'''(f, 1)$, expecting it to be nonzero when $r_E = 3$ so that also $r_{an} = 3$.

Determining the analytic rank II: the bad news

What if r_{an} is odd and $L'(f,1)$ appears to be 0? We then expect that $r_{an} = 3$. We can prove that $r_{an} \geq 3$ by checking that $r_E \geq 3$ (for example, by 2-descent). Then we may then compute $L'''(f,1)$, expecting it to be nonzero when $r_E = 3$ so that also $r_{an} = 3$. So far so good!

Determining the analytic rank II: the bad news

What if r_{an} is odd and $L'(f,1)$ appears to be 0? We then expect that $r_{an} = 3$. We can prove that $r_{an} \geq 3$ by checking that $r_E \geq 3$ (for example, by 2-descent). Then we may then compute $L'''(f,1)$, expecting it to be nonzero when $r_E = 3$ so that also $r_{an} = 3$. So far so good!

What if r_{an} is even and $L''(f,1)$ appears to be 0? (This happens with a newform at level 234446, for example.) Now we have **no way** to prove that $r_{an} > 2$! So we can **not** verify BSD in such a case (even though, as in this example, $r_E = 4$).

Determining the analytic rank II: the bad news

What if r_{an} is odd and $L'(f,1)$ appears to be 0? We then expect that $r_{an} = 3$. We can prove that $r_{an} \geq 3$ by checking that $r_E \geq 3$ (for example, by 2-descent). Then we may then compute $L'''(f,1)$, expecting it to be nonzero when $r_E = 3$ so that also $r_{an} = 3$. So far so good!

What if r_{an} is even and $L''(f,1)$ appears to be 0? (This happens with a newform at level 234446, for example.) Now we have **no way** to prove that $r_{an} > 2$! So we can **not** verify BSD in such a case (even though, as in this example, $r_E = 4$).

In summary: if $r_{an} \leq 3$ then we can determine its value unconditionally and hence verify (weak) BSD;

Determining the analytic rank II: the bad news

What if r_{an} is odd and $L'(f,1)$ appears to be 0? We then expect that $r_{an} = 3$. We can prove that $r_{an} \geq 3$ by checking that $r_E \geq 3$ (for example, by 2-descent). Then we may then compute $L'''(f,1)$, expecting it to be nonzero when $r_E = 3$ so that also $r_{an} = 3$. So far so good!

What if r_{an} is even and $L''(f,1)$ appears to be 0? (This happens with a newform at level 234446, for example.) Now we have **no way** to prove that $r_{an} > 2$! So we can **not** verify BSD in such a case (even though, as in this example, $r_E = 4$).

In summary: if $r_{an} \leq 3$ then we can determine its value unconditionally and hence verify (weak) BSD; while if $r_{an} \geq 4$ we have no way of determining its value exactly.