The elliptic curve database to 120000

John Cremona
University of Nottingham, UK

SECANTS 27: Oxford, 22 October 2005

Plan of the talk

- Background and history
- Remarks on the method
- Remarks on the program
- Summary of data and highlights of results

Background and history

"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.ucsd.edu/scans/antwerp/`.

Contains various tables, including "all" elliptic curves of conductor $N \leq 200$, together with ranks and generators (in most cases), arranged in isogeny classes.

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

- Swinnerton-Dyer searched for curves with small coefficients and kept those with conductor $N \leq 200$; added curves obtained vie a succession of 2- and 3-isogenies.

- Higher degree isogenies were checked using Vélu's method, and 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 were computed by James Davenport, using BSD's method (2-descent).
- List known to be complete for certain N, such as $N = 2^a 3^b$.
- Tingley's thesis (1975) contains further curves with $200 < N \leq 320$ found via modular symbols, newforms and periods.

No more systematic enumeration occurred between 1972 and the mid 1980s.

My tables before 1992

In 1988 I submitted a paper to Mathematics of Computation containing a list of elliptic curves of conductor up to 600. No isogenies, ranks, generators.

The paper was rejected in 1989, but I was invited to submit a revised form with no implementation details and fuller tables, including isogenies and ranks and generators.

In 1990 I submitted again to Mathematics of Computation with longer tables to conductor 1000 and ranks and generators. While they were considering this I was approached by several publishers interested in publishing this as a book, and eventually withdrew it from Math Comp (who wanted to publish it with the tables on microfiche, which was rather old-fashioned even in 1990.)

Cambridge University Press won, and the book "Algorithms for Modular Elliptic Curves" with tables for curves to conductor 1000 was published on 8 October 1992, priced $£35$ for 5089 curves (those for $N = 702$ were missing), or $0.687p$ per curve.

Remarks on the method

Finding the curves

The method is similar to that used by Tingley, though with certain improvements. For each N one computes the space of $\Gamma_0(N)$-modular symbols, and the action of the Hecke algebra on the space, to find one-dimensional eigenspaces with rational (integer) eigenvalues. Each corresponds to a rational newform f and hence to an elliptic curve of conductor N and L-series $L(E,s) = L(f,s)$. To find E we compute the period lattice of f, and hence find the periods of E, from which the invariants c_4, c_6 may be deetermined approximately; but they are known to be integers.

For details see Chapter 2 of the book, which is available online at `http://www.maths.nott.ac.uk/personal/jec/book/fulltext/`.

Information about the curves

We compute the analytic ranks from the newform, and when >1 we check that it equals the Mordell-Weil rank using 2-descent.

Generators are found using (1) search; (2) 2-descent; (3) Heegner points (using MAGMA); plus saturation methods.

We also compute isogenies, and all data on the isogenous curves.

Remarks on the program

In essence, the program has not changed since the original `Algol68` version in the 1980s, though now in `C++`. But there are a large number of efficiency improvements, without which it would have been impossible to have progressed so far.

Some of these have been developed in collaboration with William Stein, who has written more general programs for computing with higher weights and characters: implemented originally in `C++`, then in MAGMA, and most recently in his package `SAGE` (see `http://modular.ucsd.edu/sage/`).

Probably the most important single programming improvement is the use of sparse matrices throughout. Even so, some levels around 120000 require more than 2GB or RAM in which to run.

Machines

The other factor which has had an enormous impact since spring 2005 is the availability in Nottingham of a 1024-processor cluster, on which I may use between 100 and 250 processors simultaneously, thus handling a hundred levels at a time. The processors are arranged in 512 nodes, with each node (a "V20z dual opteron") having its own 2GB of RAM.

Some "hard" levels are run separately on a machine with 8GB of RAM.

Milestones

Date	Conductor reached
Sep 2001	10000
Oct 2002	15000
Apr 2003	20000
Jun 2004	25000
Feb 2005	30000
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
? Oct 2005	130000

A typical log file (node 26)

```
running nfhpcurve on level 120026 at Fri Sep 23 18:26:48 BST 2005
running nfhpcurve on level 120197 at Fri Sep 23 20:12:31 BST 2005
running nfhpcurve on level 120224 at Fri Sep 23 20:58:18 BST 2005
running nfhpcurve on level 120312 at Fri Sep 23 23:35:19 BST 2005
running nfhpcurve on level 120431 at Sat Sep 24 04:19:54 BST 2005
running nfhpcurve on level 120568 at Sat Sep 24 10:42:18 BST 2005
running nfhpcurve on level 120631 at Sat Sep 24 13:56:49 BST 2005
running nfhpcurve on level 120646 at Sat Sep 24 14:48:21 BST 2005
running nfhpcurve on level 120679 at Sat Sep 24 15:59:54 BST 2005
running nfhpcurve on level 120717 at Sat Sep 24 18:11:20 BST 2005
running nfhpcurve on level 120738 at Sat Sep 24 19:13:11 BST 2005
running nfhpcurve on level 120875 at Sun Sep 25 02:20:27 BST 2005
running nfhpcurve on level 120876 at Sun Sep 25 02:20:28 BST 2005
running nfhpcurve on level 120918 at Sun Sep 25 04:58:32 BST 2005
running nfhpcurve on level 120978 at Sun Sep 25 08:08:00 BST 2005
```

Summary of data and highlights of results

Full data is available from `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`. The data is mostly in plain ascii files for ease of use by other programs, rather than in typeset tables as in the book.

Other ways of accessing the data:

- William Stein keeps a mirror at `http://modular.ucsd.edu/cremona/`;
- he also has a Modular Forms Database at `http://modular.ucsd.edu/Tables/` with links to many other tables
- There's a nice interface by Gonzalo Tornaria at `http://www.math.utexas.edu/users/tornaria/cnt/cremona.html`, but only for $N < 20000$.

- pari/gp now has the full elliptic curve database in it. For example

```
(11:58) gp > ellinit("5077a1")
%9 = [0, 0, 1, -7, 6, 0, -14, 25, -49, 336, -5400, 5077, 37933056/5077,
(11:58) gp > ellidentify(ellinit([1,2,3,4,5]))
%10 = [["10351a1", [1, -1, 0, 4, 3], [[2, 3]]], [1, -1, 0, -1]]
```

- SAGE also has all the data available and many ways of working with it.

Number of isogeny classes of curves of conductor $N < 120000$

range of N	#	$r = 0$	$r = 1$	$r = 2$	$r = 3$
0-9999	38042	16450	19622	1969	1
10000-19999	43175	17101	22576	3490	8
20000-29999	44141	17329	22601	4183	28
30000-39999	44324	16980	22789	4517	38
40000-49999	44519	16912	22826	4727	54
50000-59999	44301	16728	22400	5126	47
60000-69999	44361	16568	22558	5147	88
70000-79999	44449	16717	22247	5400	85
80000-89999	44861	17052	22341	5369	99
90000-99999	43651	16370	21756	5442	83
100000-109999	44274	16599	22165	5369	141
110000-119999	44071	16307	22173	5453	138
0-119999	524169	201113	266054	56192	810

Total number of curves of conductor $N < 120000$

range of N	# isogeny classes	# isomorphism classes
0-9999	38042	64687
10000-19999	43175	67848
20000-29999	44141	66995
30000-39999	44324	66561
40000-49999	44519	66275
50000-59999	44301	65393
60000-69999	44361	65209
70000-79999	44449	64687
80000-89999	44861	64864
90000-99999	43651	63287
100000-109999	44274	63410
110000-119999	44071	63277
0-119999	524169	782493

Largest and smallest generators

Curve 108174c2: $[1, 1, 0, -330505909530535, -2312687660697986706251]$ has a generator of canonical height 1193.35: $(a/c^2, b/c^3)$ where

$a = -13632833703140681033503023679128670529558218420063432397971439281876168936925608099278686103768271165751$

$437633556213041024136275990157472508801182302454436678900455860307034813576105868447511602833327656978462$

$242557413116494486538310447476190358439933060717111176029723557330999410077664104893597013481236052075987$

$42554713521099294186837422237009896297109549762937178684101535289410605736729335307780613198224770325365111$

$296070756137349249522158278253743039282375024853516001988744749085116423499171358836518920399114139315005$

$c = 113966855669333292896328833690552943933212422262287285858336471843279644076647486592460242089049033370292$

$4852507561210566800730781138060496574877596413908434778098874122035844096418444116068236428572188929747$

$7694986150009319617653662693006650248126059704441347$

Curve 61050cs1: $[1, 0, 0, -23611588, 39078347792]$ has a generator of canonical height 0.0148: $(-3718, 276584)$.

Torsion orders

Order	# curves	percentage
1	397707	50.83
2	319717	40.86
3	17310	2.21
4	43082	5.51
5	664	0.08486
6	3003	0.38380
7	49	0.00626
8	851	0.10880
9	13	0.001661
10	26	0.003323
12	67	0.008562
16	4	0.000511

Degree of modular parametrization

The largest is for 96054k1: $\deg(\varphi) = 32035843840 = 2^8 \cdot 5 \cdot 7 \cdot 11^2 \cdot 13 \cdot 2273.$

Size of isogeny classes

Size	$\#$ classes	percentage
1	341329	65.12
2	147205	28.08
3	2706	0.52
4	29998	5.72
6	2402	0.46
8	529	0.10

Average size $= 1.493$.

(Analytic) orders of Ш

$\sqrt{\lvert Ш \rvert}$	#
2	33920
3	10510
4	3663
5	1801
6	376
7	424
8	223
9	78
10	48
11	66
12	15
13	15
14	8

$\sqrt{\lvert Ш \rvert}$	#
15	1
16	5
17	4
18	0
19	2
20	3
21	2
22	0
23	4
24	0
25	0
26	1
total	51169