The elliptic curve database to 130000

John Cremona
University of Nottingham, UK

ANTS 7: Berlin, 26 July 2006

Plan of the talk

- Background and history
- Algorithms and Implementation
- Summary of data and highlights of results
  (including a new result concerning the Manin Constant)

Plan of the talk

- Background and history
- Algorithms and Implementation
- Summary of data and highlights of results
  (including a new result concerning the Manin Constant)

Plan of the talk

- Background and history
- Algorithms and Implementation
- Summary of data and highlights of results
(including a new result concerning the Manin Constant)

Plan of the talk

- Background and history
- Algorithms and Implementation
- Summary of data and highlights of results
  (including a new result concerning the Manin Constant)

Background and history

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 and generators, arranged in isogeny classes. [See below]

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]

The tables in Antwerp IV

1. "All" elliptic curves of conductor $N \leq 200$, together with most ranks and generators, arranged in isogeny classes. [See below]

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]

The tables in Antwerp IV

1. “All” elliptic curves of conductor $N \leq 200$, together with most ranks and generators, arranged in isogeny classes. [See below]

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]

The tables in Antwerp IV

1. "All" elliptic curves of conductor $N \leq 200$, together with most ranks and generators, arranged in isogeny classes. [See below]

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]

The tables in Antwerp IV

1. "All" elliptic curves of conductor $N \leq 200$, together with most ranks and generators, arranged in isogeny classes. [See below]

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]

The tables in Antwerp IV

1. "All" elliptic curves of conductor $N \leq 200$, together with most ranks and generators, arranged in isogeny classes. [See below]

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]

Table 1 in Antwerp IV

"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

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

Table 1 in Antwerp IV

"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

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

Table 1 in Antwerp IV

"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

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

Table 1 in Antwerp IV

"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

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

Antwerp IV Table 1 (contd.)

- 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 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.

Antwerp IV Table 1 (contd.)

- 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 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.

Antwerp IV Table 1 (contd.)

- 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 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.

Antwerp IV Table 1 (contd.)

- 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 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.

The origin of the 1992 tables

1985-1988: Implementation of modular symbols for $\Gamma_0(N)$ and $\Gamma_1(N)$ in `Algol68`

1988: Paper submitted to Mathematics of Computation including all elliptic curves of conductor $N \leq 600$. (No isogenies, ranks, generators.)

1989: Paper rejected. Resubmission invited, to include (1) no implementation details and (2) fuller tables, including isogenies and ranks and generators.

1990: Paper resubmitted to Math Comp: tables for $N \leq 1000$ with ranks, generators, isogenies. Math Comp offered to publish tables on microfiche. Paper withdrawn.

1991: Contract signed with Cambridge University Press.

8 October 1992: *Algorithms for Modular Elliptic Curves* published: full tables to conductor 1000 (except $N = 702$).

The origin of the 1992 tables

1985-1988: Implementation of modular symbols for $\Gamma_0(N)$ and $\Gamma_1(N)$ in `Algol68`

1988: Paper submitted to Mathematics of Computation including all elliptic curves of conductor $N \leq 600$. (No isogenies, ranks, generators.)

1989: Paper rejected. Resubmission invited, to include (1) no implementation details and (2) fuller tables, including isogenies and ranks and generators.

1990: Paper resubmitted to Math Comp: tables for $N \leq 1000$ with ranks, generators, isogenies. Math Comp offered to publish tables on microfiche. Paper withdrawn.

1991: Contract signed with Cambridge University Press.

8 October 1992: *Algorithms for Modular Elliptic Curves* published: full tables to conductor 1000 (except $N = 702$).

The origin of the 1992 tables

1985-1988: Implementation of modular symbols for $\Gamma_0(N)$ and $\Gamma_1(N)$ in `Algol68`

1988: Paper submitted to Mathematics of Computation including all elliptic curves of conductor $N \leq 600$. (No isogenies, ranks, generators.)

1989: Paper rejected. Resubmission invited, to include (1) no implementation details and (2) fuller tables, including isogenies and ranks and generators.

1990: Paper resubmitted to Math Comp: tables for $N \leq 1000$ with ranks, generators, isogenies. Math Comp offered to publish tables on microfiche. Paper withdrawn.

1991: Contract signed with Cambridge University Press.

8 October 1992: *Algorithms for Modular Elliptic Curves* published: full tables to conductor 1000 (except $N = 702$).

The origin of the 1992 tables

1985-1988: Implementation of modular symbols for $\Gamma_0(N)$ and $\Gamma_1(N)$ in `Algol68`

1988: Paper submitted to Mathematics of Computation including all elliptic curves of conductor $N \leq 600$. (No isogenies, ranks, generators.)

1989: Paper rejected. Resubmission invited, to include (1) no implementation details and (2) fuller tables, including isogenies and ranks and generators.

1990: Paper resubmitted to Math Comp: tables for $N \leq 1000$ with ranks, generators, isogenies. Math Comp offered to publish tables on microfiche. Paper withdrawn.

1991: Contract signed with Cambridge University Press.

8 October 1992: *Algorithms for Modular Elliptic Curves* published: full tables to conductor 1000 (except $N = 702$).

The origin of the 1992 tables

1985-1988: Implementation of modular symbols for $\Gamma_0(N)$ and $\Gamma_1(N)$ in `Algol68`

1988: Paper submitted to Mathematics of Computation including all elliptic curves of conductor $N \leq 600$. (No isogenies, ranks, generators.)

1989: Paper rejected. Resubmission invited, to include (1) no implementation details and (2) fuller tables, including isogenies and ranks and generators.

1990: Paper resubmitted to Math Comp: tables for $N \leq 1000$ with ranks, generators, isogenies. Math Comp offered to publish tables on microfiche. Paper withdrawn.

1991: Contract signed with Cambridge University Press.

8 October 1992: *Algorithms for Modular Elliptic Curves* published: full tables to conductor 1000 (except $N = 702$).

The origin of the 1992 tables

1985-1988: Implementation of modular symbols for $\Gamma_0(N)$ and $\Gamma_1(N)$ in `Algol68`

1988: Paper submitted to Mathematics of Computation including all elliptic curves of conductor $N \leq 600$. (No isogenies, ranks, generators.)

1989: Paper rejected. Resubmission invited, to include (1) no implementation details and (2) fuller tables, including isogenies and ranks and generators.

1990: Paper resubmitted to Math Comp: tables for $N \leq 1000$ with ranks, generators, isogenies. Math Comp offered to publish tables on microfiche. Paper withdrawn.

1991: Contract signed with Cambridge University Press.

8 October 1992: *Algorithms for Modular Elliptic Curves* published: full tables to conductor 1000 (except $N = 702$).

The 1997 tables

A revised edition of the 1992 book and tables appeared in 1997.

- Various corrections; "missing" curves of conductor 702 included;
- new table of degrees of modular parametrizations;
- links to online data for $N \leq 5077$.

Full text available online since around 2002 at `http://www.maths.nott.ac.uk/personal/jec/book/fulltext/`.

The 1997 tables

A revised edition of the 1992 book and tables appeared in 1997.

- Various corrections; “missing” curves of conductor 702 included;
- new table of degrees of modular parametrizations;
- links to online data for $N \leq 5077$.

Full text available online since around 2002 at
`http://www.maths.nott.ac.uk/personal/jec/book/fulltext/`.

The 1997 tables

A revised edition of the 1992 book and tables appeared in 1997.

- Various corrections; "missing" curves of conductor 702 included;
- new table of degrees of modular parametrizations;
- links to online data for $N \leq 5077$.

Full text available online since around 2002 at
`http://www.maths.nott.ac.uk/personal/jec/book/fulltext/`.

The 1997 tables

A revised edition of the 1992 book and tables appeared in 1997.

- Various corrections; “missing” curves of conductor 702 included;
- new table of degrees of modular parametrizations;
- links to online data for $N \leq 5077$.

Full text available online since around 2002 at
`http://www.maths.nott.ac.uk/personal/jec/book/fulltext/`.

Algorithms and Implementation

Overview

- Use modular symbols modulo N
- Find newforms for $\Gamma_0(N)$ with Hecke eigenvalues
- Compute their periods and hence the associated elliptic curves
- Use any available method to find Mordell-Weil groups, isogenous curves, etc.

Algorithms and Implementation

Overview

- Use modular symbols modulo N
- Find newforms for $\Gamma_0(N)$ with Hecke eigenvalues
- Compute their periods and hence the associated elliptic curves
- Use any available method to find Mordell-Weil groups, isogenous curves, etc.

Algorithms and Implementation

Overview

- Use modular symbols modulo N
- Find newforms for $\Gamma_0(N)$ with Hecke eigenvalues
- Compute their periods and hence the associated elliptic curves
- Use any available method to find Mordell-Weil groups, isogenous curves, etc.

Algorithms and Implementation

Overview

- Use modular symbols modulo N
- Find newforms for $\Gamma_0(N)$ with Hecke eigenvalues
- Compute their periods and hence the associated elliptic curves
- Use any available method to find Mordell-Weil groups, isogenous curves, etc.

Finding the newforms at level N

- Compute space of $\Gamma_0(N)$-modular symbols [fast]
- Compute action of the Hecke algebra on it [quite fast]
- Find one-dimensional rational eigenspaces: each corresponds to a rational newform f [slow for large levels]

This step requires much RAM and is currently the main obstruction to extending the tables, despite the use of sparse algorithms for linear algebra.

Finding the newforms at level N

- Compute space of $\Gamma_0(N)$-modular symbols [fast]
- Compute action of the Hecke algebra on it [quite fast]
- Find one-dimensional rational eigenspaces: each corresponds to a rational newform f [slow for large levels]

This step requires much RAM and is currently the main obstruction to extending the tables, despite the use of sparse algorithms for linear algebra.

Finding the newforms at level N

- Compute space of $\Gamma_0(N)$-modular symbols [fast]
- Compute action of the Hecke algebra on it [quite fast]
- Find one-dimensional rational eigenspaces: each corresponds to a rational newform f [slow for large levels]

This step requires much RAM and is currently the main obstruction to extending the tables, despite the use of sparse algorithms for linear algebra.

Finding the newforms at level N

- Compute space of $\Gamma_0(N)$-modular symbols [fast]
- Compute action of the Hecke algebra on it [quite fast]
- Find one-dimensional rational eigenspaces: each corresponds to a rational newform f [slow for large levels]

This step requires much RAM and is currently the main obstruction to extending the tables, despite the use of sparse algorithms for linear algebra.

Finding the curves from the newforms

- Compute many Hecke eigenvalues ($=$ Fourier coefficients of f)
- Compute homology information from modular symbols
- Integrate $2\pi i f(z)dz$ along appropriate paths in upper half-plane
- Obtain the periods of f, and hence of associated elliptic curve E of conductor N and L-series $L(E,s) = L(f,s)$; finite precision!
- Compute coefficients of E (approximately, but they are integers).

For levels around 130000 we may need up to 3500 Hecke eigenvalues.

Memory requirements and time to compute periods are negligible.

Finding the curves from the newforms

- Compute many Hecke eigenvalues ($=$ Fourier coefficients of f)
- Compute homology information from modular symbols
- Integrate $2\pi i f(z)dz$ along appropriate paths in upper half-plane
- Obtain the periods of f, and hence of associated elliptic curve E of conductor N and L-series $L(E,s) = L(f,s)$; finite precision!
- Compute coefficients of E (approximately, but they are integers).

For levels around 130000 we may need up to 3500 Hecke eigenvalues.

Memory requirements and time to compute periods are negligible.

Finding the curves from the newforms

- Compute many Hecke eigenvalues ($=$ Fourier coefficients of f)
- Compute homology information from modular symbols
- Integrate $2\pi i f(z)dz$ along appropriate paths in upper half-plane
- Obtain the periods of f, and hence of associated elliptic curve E of conductor N and L-series $L(E,s) = L(f,s)$; finite precision!
- Compute coefficients of E (approximately, but they are integers).

For levels around 130000 we may need up to 3500 Hecke eigenvalues.

Memory requirements and time to compute periods are negligible.

Finding the curves from the newforms

- Compute many Hecke eigenvalues ($=$ Fourier coefficients of f)
- Compute homology information from modular symbols
- Integrate $2\pi i f(z)dz$ along appropriate paths in upper half-plane
- Obtain the periods of f, and hence of associated elliptic curve E of conductor N and L-series $L(E,s) = L(f,s)$; finite precision!
- Compute coefficients of E (approximately, but they are integers).

For levels around 130000 we may need up to 3500 Hecke eigenvalues.

Memory requirements and time to compute periods are negligible.

Finding the curves from the newforms

- Compute many Hecke eigenvalues ($=$ Fourier coefficients of f)
- Compute homology information from modular symbols
- Integrate $2\pi i f(z)dz$ along appropriate paths in upper half-plane
- Obtain the periods of f, and hence of associated elliptic curve E of conductor N and L-series $L(E,s) = L(f,s)$; finite precision!
- Compute coefficients of E (approximately, but they are integers).

For levels around 130000 we may need up to 3500 Hecke eigenvalues.

Memory requirements and time to compute periods are negligible.

Finding the curves from the newforms

- Compute many Hecke eigenvalues ($=$ Fourier coefficients of f)
- Compute homology information from modular symbols
- Integrate $2\pi i f(z) dz$ along appropriate paths in upper half-plane
- Obtain the periods of f, and hence of associated elliptic curve E of conductor N and L-series $L(E,s) = L(f,s)$; finite precision!
- Compute coefficients of E (approximately, but they are integers).

For levels around 130000 we may need up to 3500 Hecke eigenvalues.

Memory requirements and time to compute periods are negligible.

Information about the curves

- Analytic ranks computed from newform; checked with Mordell-Weil ranks found by 2-descent.

- Generators found by search, 2- and 4-descent, Heegner points, plus saturation.

- Isogenies computed via periods and division polynomials.

- "Analytic $|\text{Ш}|$" computed using BSD formula.

All this is automated, but hard cases need human intervention!

Information about the curves

- Analytic ranks computed from newform; checked with Mordell-Weil ranks found by 2-descent.
- Generators found by search, 2- and 4-descent, Heegner points, plus saturation.
- Isogenies computed via periods and division polynomials.
- “Analytic $|\text{Ш}|$” computed using BSD formula.

All this is automated, but hard cases need human intervention!

Information about the curves

- Analytic ranks computed from newform; checked with Mordell-Weil ranks found by 2-descent.

- Generators found by search, 2- and 4-descent, Heegner points, plus saturation.

- Isogenies computed via periods and division polynomials.

- "Analytic $|Ш|$" computed using BSD formula.

All this is automated, but hard cases need human intervention!

Information about the curves

- Analytic ranks computed from newform; checked with Mordell-Weil ranks found by 2-descent.

- Generators found by search, 2- and 4-descent, Heegner points, plus saturation.

- Isogenies computed via periods and division polynomials.

- "Analytic $|\text{Ш}|$" computed using BSD formula.

All this is automated, but hard cases need human intervention!

Implementation: software

1980s: `Algol68` (includes code from Richard Pinch).

1990s++: Rewritten in `C++`, using various libraries (Shoup's `NTL`, Buchmann's `LiDIA`, `gmp`, `pari/gp`).

Many algorithmic improvements developed in collaboration with William Stein.

Most important single programming improvement: use of sparse matrices.

Example: Stein–Watkins (ANTS V, 2002) gave an example of a curve of rank 2, rational 5-torsion, conductor 13881, then "beyond the range of Cremona's tables". Computing the four curves (up to isogeny) with $N = 13881$ now takes less than 2 minutes and 60MB of RAM.

[Most of the computation time is taken up finding the eigenspaces for the first Hecke operator T_2 on the modular symbol space of dimension 1768.]

Implementation: software

1980s: `Algol68` (includes code from Richard Pinch).

1990s$++$: Rewritten in `C++`, using various libraries (Shoup's `NTL`, Buchmann's `LiDIA`, `gmp`, `pari/gp`).

Many algorithmic improvements developed in collaboration with William Stein.

Most important single programming improvement: use of sparse matrices.

Example: Stein–Watkins (ANTS V, 2002) gave an example of a curve of rank 2, rational 5-torsion, conductor 13881, then "beyond the range of Cremona's tables". Computing the four curves (up to isogeny) with $N = 13881$ now takes less than 2 minutes and 60MB of RAM.

[Most of the computation time is taken up finding the eigenspaces for the first Hecke operator T_2 on the modular symbol space of dimension 1768.]

Implementation: software

1980s: `Algol68` (includes code from Richard Pinch).

1990s++: Rewritten in `C++`, using various libraries (Shoup's `NTL`, Buchmann's `LiDIA`, `gmp`, `pari/gp`).

Many algorithmic improvements developed in collaboration with William Stein.
Most important single programming improvement: use of sparse matrices.
Example: Stein–Watkins (ANTS V, 2002) gave an example of a curve of rank 2, rational 5-torsion, conductor 13881, then "beyond the range of Cremona's tables". Computing the four curves (up to isogeny) with $N = 13881$ now takes less than 2 minutes and 60MB of RAM.

[Most of the computation time is taken up finding the eigenspaces for the first Hecke operator T_2 on the modular symbol space of dimension 1768.]

Implementation: software

1980s: `Algol68` (includes code from Richard Pinch).

1990s++: Rewritten in `C++`, using various libraries (Shoup's `NTL`, Buchmann's `LiDIA`, `gmp`, `pari/gp`).

Many algorithmic improvements developed in collaboration with William Stein.

Most important single programming improvement: use of sparse matrices.

Example: Stein–Watkins (ANTS V, 2002) gave an example of a curve of rank 2, rational 5-torsion, conductor 13881, then "beyond the range of Cremona's tables". Computing the four curves (up to isogeny) with $N = 13881$ now takes less than 2 minutes and 60MB of RAM.

[Most of the computation time is taken up finding the eigenspaces for the first Hecke operator T_2 on the modular symbol space of dimension 1768.]

Implementation: hardware

Until 2005: between 0 and 3 shared machines.

Since spring 2005: availability of a 1024-processor cluster in Nottingham!

- Up to 250 processors simultaneously, handling hundred levels or more at a time.
- Processors in 512 nodes, each a V20z dual opteron with 2GB of RAM.
- Some hard levels run separately on a machine with 8GB of RAM.
- Levels 30000–130000 in only nine months!

Implementation: hardware

Until 2005: between 0 and 3 shared machines.

Since spring 2005: availability of a 1024-processor cluster in Nottingham!

- Up to 250 processors simultaneously, handling hundred levels or more at a time.
- Processors in 512 nodes, each a V20z dual opteron with 2GB of RAM.
- Some hard levels run separately on a machine with 8GB of RAM.
- Levels 30000–130000 in only nine months!

Implementation: hardware

Until 2005: between 0 and 3 shared machines.

Since spring 2005: availability of a 1024-processor cluster in Nottingham!

- Up to 250 processors simultaneously, handling hundred levels or more at a time.
- Processors in 512 nodes, each a V20z dual opteron with 2GB of RAM.
- Some hard levels run separately on a machine with 8GB of RAM.
- Levels 30000–130000 in only nine months!

Implementation: hardware

Until 2005: between 0 and 3 shared machines.

Since spring 2005: availability of a 1024-processor cluster in Nottingham!

- Up to 250 processors simultaneously, handling hundred levels or more at a time.
- Processors in 512 nodes, each a V20z dual opteron with 2GB of RAM.
- Some hard levels run separately on a machine with 8GB of RAM.
- Levels 30000–130000 in only nine months!

Milestones: pre-2005

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

Milestones in 2005

Date	Conductor reached
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

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

Availability of the data

All the tables from the Book are available online at `http://www.maths.nott.ac.uk/personal/jec/book/fulltext/` (conductors to 1000 only).

Full raw data for conductors to 130000 is available from `http://www.maths.nott.ac.uk/personal/jec/ftp/data/` with a mirror at `http://modular.math.washington.edu/cremona/INDEX.html`.

Typeset versions (similar to the book) are in preparation.

There are now several other ways of accessing and using the data. . .

- A web-based interface by Gonzalo Tornaria is at `http://www.math.utexas.edu/users/tornaria/cnt/cremona.html`, covering $N < 100000$. This provides an attractive interactive interface to the data; as a bonus, information on quadratic twists is included.

Summary of data and highlights of results

Availability of the data

All the tables from the Book are available online at `http://www.maths.nott.ac.uk/personal/jec/book/fulltext/` (conductors to 1000 only).

Full raw data for conductors to 130000 is available from `http://www.maths.nott.ac.uk/personal/jec/ftp/data/` with a mirror at `http://modular.math.washington.edu/cremona/INDEX.html`.

Typeset versions (similar to the book) are in preparation.

There are now several other ways of accessing and using the data...

- A web-based interface by Gonzalo Tornaria is at `http://www.math.utexas.edu/users/tornaria/cnt/cremona.html`, covering $N < 100000$. This provides an attractive interactive interface to the data; as a bonus, information on quadratic twists is included.

- The free open-source number theory package `pari/gp` (see `http://pari.math.u-bordeaux.fr/`) makes the full elliptic curve database available (though not installed by default), thanks to Bill Allombert. For example:

```
(12:05) gp > ellsearch(5077)
%1 = [["5077a1", [0, 0, 1, -7, 6], [[-2, 3], [-1, 3], [0, 2]]]]
(12:05) gp > ellinit("5077a1")
%2 = [0, 0, 1, -7, 6, 0, -14, 25, -49, 336, -5400, 5077, ...
(12:05) gp > ellidentify(ellinit([1,2,3,4,5]))
%3 = [["10351a1", [1, -1, 0, 4, 3], [[2, 3]]], [1, -1, 0, -1]]
```

The output of `ellsearch` contains all matching curves with their generators, while `ellidentify` locates a curve in the database.

- The free open-source number theory package `pari/gp` (see `http://pari.math.u-bordeaux.fr/`) makes the full elliptic curve database available (though not installed by default), thanks to Bill Allombert. For example:

```
(12:05) gp > ellsearch(5077)
%1 = [["5077a1", [0, 0, 1, -7, 6], [[-2, 3], [-1, 3], [0, 2]]]]
(12:05) gp > ellinit("5077a1")
%2 = [0, 0, 1, -7, 6, 0, -14, 25, -49, 336, -5400, 5077, ...
(12:05) gp > ellidentify(ellinit([1,2,3,4,5]))
%3 = [["10351a1", [1, -1, 0, 4, 3], [[2, 3]]], [1, -1, 0, -1]]
```

  The output of `ellsearch` contains all matching curves with their generators, while `ellidentify` locates a curve in the database.

- William Stein's free open-source package `SAGE` (Software for Algebra and Geometry Experimentation, see `http://sage.scipy.org/sage`) also has all our data available and many ways of working with it, including a transparent interface to many other pieces of elliptic curve (and other) software. For example:

```
sage: E = EllipticCurve("389a"); E
Elliptic Curve defined by y^2 + y = x^3 + x^2 - 2*x  over Rational Field
sage: E.rank()
2
sage: E.gens()                                 # Cremona's mwrank
[(-1 : 1 : 1), (0 : 0 : 1)]
sage: L = E.Lseries_dokchitser(); L(1+I)    # Tim Dokchitser's program
-0.638409938588038743 + 0.715495239204667400*I
sage: E.Lseries_zeros(4)                       # Mike Rubinstein's program
[0.00000000000, 0.00000000000, 2.8760990715, 4.4168960843]
```

- William Stein's free open-source package `SAGE` (Software for Algebra and Geometry Experimentation, see `http://sage.scipy.org/sage`) also has all our data available and many ways of working with it, including a transparent interface to many other pieces of elliptic curve (and other) software. For example:

```
sage: E = EllipticCurve("389a"); E
Elliptic Curve defined by y^2 + y = x^3 + x^2 - 2*x  over Rational Field
sage: E.rank()
2
sage: E.gens()                               # Cremona's mwrank
[(-1 : 1 : 1), (0 : 0 : 1)]
sage: L = E.Lseries_dokchitser(); L(1+I)    # Tim Dokchitser's program
-0.63840993858803874 + 0.71549523920466740*I
sage: E.Lseries_zeros(4)                     # Mike Rubinstein's program
[0.00000000000, 0.00000000000, 2.8760990715, 4.4168960843]
```

- MAGMA (see `http://magma.maths.usyd.edu.au/magma/`) has the database for conductors up to 130000 (as of version 2.13-1, released 14 July 2006); and also (optionally) the Stein–Watkins database:

```
> CDB:=CremonaDatabase(); NumberOfCurves(CDB);
845960
> LargestConductor(CDB);
130000
> E:=EllipticCurve(CDB,"389a1"); Rank(E);
2
> SWDB:=SteinWatkinsDatabase(); NumberOfCurves(SWDB);
136924520
> LargestConductor(SWDB);
99999999
```

Counting curves: isogeny classes

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
120000-129999	44655	16288	22621	5648	98
0-129999	568824	217401	288675	61840	908

Counting curves: isomorphism classes

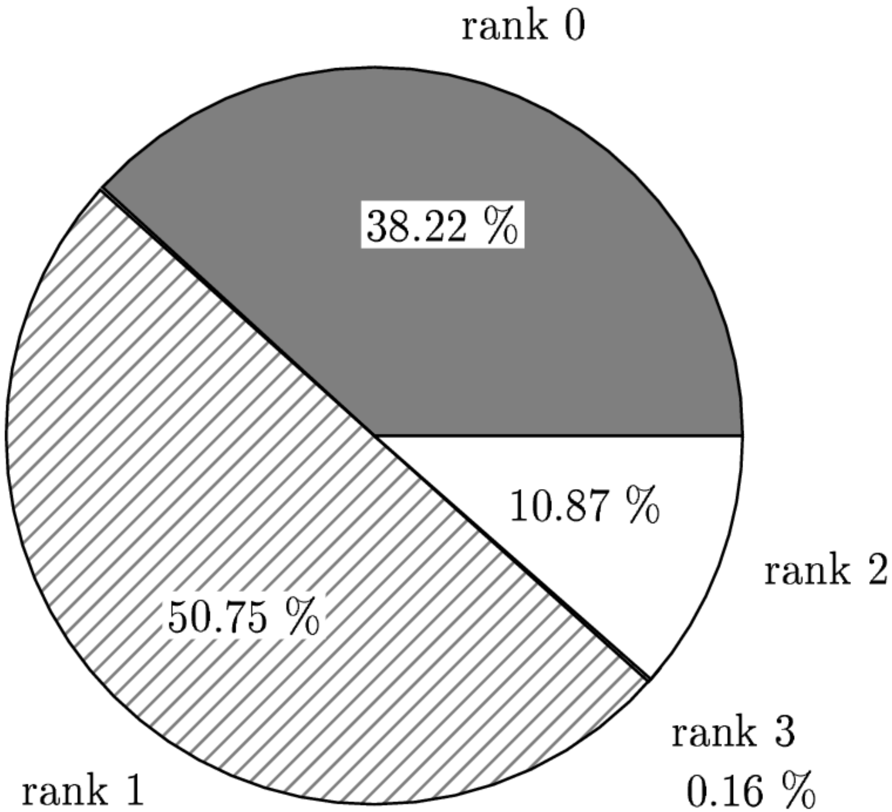
range of N	# isogeny classes	# isomorphism classes
0-9999	38042	64687
10000-19999	43175	67848
20000-29999	44141	66995
30000-39999	44324	66561
40000-49999	44519	66275
50000-59999	44301	65393
60000-69999	44361	65209
70000-79999	44449	64687
80000-89999	44861	64864
90000-99999	43651	63287
100000-109999	44274	63410
110000-119999	44071	63277
120000-129999	44655	63467
0-129999	568824	845960

Distribution of isogeny class sizes and degrees

D	Size	$\#$ classes	%
1	1	372191	65.43
2	2	123275	21.67
3	2	31372	5.52
4	4	27767	4.88
5	2	2925	0.51
6	4	3875	0.68
7	2	808	0.14
8	6	2388	0.42
9	3	2709	0.48
10	4	271	0.05
11	2	60	0.01
12	8	286	0.05
13	2	130	0.02

D	Size	$\#$ classes	%
14	4	28	< 0.01
15	4	58	0.01
16	8	270	0.05
17	2	8	< 0.01
18	6	162	0.03
19	2	12	< 0.01
21	4	30	0.01
25	3	134	0.02
27	4	33	0.01
37	2	20	< 0.01
43	2	7	< 0.01
67	2	4	< 0.01
163	2	1	< 0.01

Mordell-Weil groups I: Distribution of ranks



Mordell-Weil groups: higher ranks?

All curves with conductor < 130000 have rank ≤ 3. The smallest known conductor of a rank 4 curve is $N = 234446$.

In fact there are three curves with conductor 234446:

234446	a	1	[1,1,0,-696,6784]	3	1
234446	b	1	[1,-1,0,-79,289]	4	1
234446	c	1	[1,1,1,-949,-7845]	3	1

The other two both have rank 3! Data in the Stein–Watkins database shows that no curve with prime conductor less than 234446 has rank 4, but it is possible that a rank 4 curve with smaller composite conductor does exist. One way of answering this question would be to extend the database to fill in the range $130000 < N < 234446$.

Mordell-Weil groups: higher ranks?

All curves with conductor < 130000 have rank ≤ 3. The smallest known conductor of a rank 4 curve is $N = 234446$.

In fact there are three curves with conductor 234446:

234446	a	1	[1,1,0,-696,6784]	3	1
234446	b	1	[1,-1,0,-79,289]	4	1
234446	c	1	[1,1,1,-949,-7845]	3	1

The other two both have rank 3! Data in the Stein–Watkins database shows that no curve with prime conductor less than 234446 has rank 4, but it is possible that a rank 4 curve with smaller composite conductor does exist. One way of answering this question would be to extend the database to fill in the range $130000 < N < 234446$.

Mordell-Weil groups: higher ranks?

All curves with conductor < 130000 have rank ≤ 3. The smallest known conductor of a rank 4 curve is $N = 234446$.

In fact there are three curves with conductor 234446:

234446	a	1	[1,1,0,-696,6784]	3	1
234446	b	1	[1,-1,0,-79,289]	4	1
234446	c	1	[1,1,1,-949,-7845]	3	1

The other two both have rank 3! Data in the Stein–Watkins database shows that no curve with prime conductor less than 234446 has rank 4, but it is possible that a rank 4 curve with smaller composite conductor does exist. One way of answering this question would be to extend the database to fill in the range $130000 < N < 234446$.

Mordell-Weil groups: higher ranks?

All curves with conductor < 130000 have rank ≤ 3. The smallest known conductor of a rank 4 curve is $N = 234446$.

In fact there are three curves with conductor 234446:

234446	a	1	[1,1,0,-696,6784]	3	1
234446	b	1	[1,-1,0,-79,289]	4	1
234446	c	1	[1,1,1,-949,-7845]	3	1

The other two both have rank 3! Data in the Stein–Watkins database shows that no curve with prime conductor less than 234446 has rank 4, but it is possible that a rank 4 curve with smaller composite conductor does exist. One way of answering this question would be to extend the database to fill in the range $130000 < N < 234446$.

Mordell-Weil groups II: distribution of torsion structures

Structure	# curves	%
C_1	432622	51.14
C_2	344010	40.67
C_3	18512	2.19
C_4	12832	1.52
$C_2 \times C_2$	33070	3.91
C_5	698	0.08
C_6	3155	0.37
C_7	50	< 0.01
C_8	101	0.01
$C_2 \times C_4$	793	0.09
C_9	16	< 0.01
C_{10}	28	< 0.01
C_{12}	11	< 0.01
$C_2 \times C_6$	58	< 0.01
$C_2 \times C_8$	4	< 0.01

Order parity	# curves	%
Odd	451898	53.42
Even	394062	46.58
All	845960	100.00

Mordell-Weil groups III: largest generator

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

$$a = -1363283370314068103350302367912867052955821842006343239797143928187616893692560809927868610376827116575 1$$

$$437633556213041024136275990157472508801182302454436678900455860307034813576105868447511602833327656978462$$

$$242557413116494486538310447476190358439933060717111176029723557330999410077664104893597013481236052075987$$

$$4255471352109929418683742223700989629710954976293717868410153528941060573672933530778061319822477032536511 1$$

$$296070756137349249522158278253743039282375024853516001988744749085116423499171358836518920399114139315005$$

$$c = 113966855669333292896328833690552943933212422262287285858336471843279644076647486592460242089049033370292$$

$$485250756121056680073078113806049657487759641390843477809887412203584409641844116068236428572188929747$$

$$769498615000931961765366269300665024812605970444134 7$$

Finding large generators

How is such a large rational point found? When the rank is 1, it is as easy (and quick) as this (using MAGMA's Heegner Point package, implemented by Mark Watkins):

```
> E:=EllipticCurve([1,1,0,-330505909530535,-2312687660697986706251]);
> time HeegnerPoint(E);

true (-13632833.../12988444... : 77684538.../14802521... : 1)
Time: 26.680
```

Finding large generators

How is such a large rational point found? When the rank is 1, it is as easy (and quick) as this (using MAGMA's Heegner Point package, implemented by Mark Watkins):

```
> E:=EllipticCurve([1,1,0,-330505909530535,-2312687660697986706251]);
> time HeegnerPoint(E);

true (-13632833.../12988444... : 77684538.../14802521... : 1)
Time: 26.680
```

Nontrivial (analytic) orders of Ш

$\sqrt{\lvert Ш \rvert}$	#
2^2	37074
3^2	11512
4^2	4013
5^2	1954
6^2	426
7^2	468
8^2	250
9^2	85
10^2	52
11^2	73
12^2	20
13^2	19
14^2	9

$\sqrt{\lvert Ш \rvert}$	#
15^2	2
16^2	6
17^2	4
19^2	2
20^2	3
21^2	2
23^2	4
26^2	1
all>1	55979

The Manin Constant

The Manin constant for an elliptic curve E of conductor N is the rational number c such that

$$\varphi^*(\omega_E) = c(2\pi i f(z) dz),$$

where ω_E is a Néron differential on E, f is the normalized newform for $\Gamma_0(N)$ associated to E, and $\varphi : X_0(N) \to E$ is the modular parametrization.

A long-standing conjecture is that $c = 1$ for all elliptic curves over $\mathbb{Q}$ which are optimal $J_0(N)$-quotients ("strong Weil curves"). It is known by work of Edixhoven and others that $c \in \mathbb{Z}$, and there are many results restricting the primes which may divide c.

In a recent paper by Agashe, Ribet and Stein these conditions have been strengthened considerably. In an appendix to that paper, there is an account of numerical verifications I have carried out which establish the conjecture for **all** the curves in the tables.

The Manin Constant

The Manin constant for an elliptic curve E of conductor N is the rational number c such that

$$\varphi^*(\omega_E) = c(2\pi i f(z)dz),$$

where ω_E is a Néron differential on E, f is the normalized newform for $\Gamma_0(N)$ associated to E, and $\varphi : X_0(N) \to E$ is the modular parametrization.

A long-standing conjecture is that $c = 1$ for all elliptic curves over $\mathbb{Q}$ which are optimal $J_0(N)$-quotients ("strong Weil curves"). It is known by work of Edixhoven and others that $c \in \mathbb{Z}$, and there are many results restricting the primes which may divide c.

In a recent paper by Agashe, Ribet and Stein these conditions have been strengthened considerably. In an appendix to that paper, there is an account of numerical verifications I have carried out which establish the conjecture for **all** the curves in the tables.

The Manin Constant

The Manin constant for an elliptic curve E of conductor N is the rational number c such that

$$\varphi^*(\omega_E) = c(2\pi i f(z)dz),$$

where ω_E is a Néron differential on E, f is the normalized newform for $\Gamma_0(N)$ associated to E, and $\varphi : X_0(N) \to E$ is the modular parametrization.

A long-standing conjecture is that $c = 1$ for all elliptic curves over $\mathbb{Q}$ which are optimal $J_0(N)$-quotients ("strong Weil curves"). It is known by work of Edixhoven and others that $c \in \mathbb{Z}$, and there are many results restricting the primes which may divide c.

In a recent paper by Agashe, Ribet and Stein these conditions have been strengthened considerably. In an appendix to that paper, there is an account of numerical verifications I have carried out which establish the conjecture for **all** the curves in the tables.

The Manin Constant: a new Theorem

Theorem. *For all $N \leq 130000$, every optimal elliptic quotient of $J_0(N)$ has Manin constant equal to* 1.

Moreover, for $N < 60000$ the optimal curve in each class is the one whose identifying number in the tables is 1 *(except for class* $990h$ *where the optimal curve is* $990h3$*).*

The second part of the Theorem for all $N < 130000$ would follow from Stevens' conjecture that in each isogeny class the curve with minimal Faltings height is the optimal $\Gamma_1(N)$-quotient: this can be verified in each case using Mark Watkins's program ec.

Verifying the second part for all $N < 130000$ would require more computations with modular symbols; see

A. Agashe, K. A. Ribet and W. A. Stein, *The Manin Constant*, JPAM Coates Volume, `http://modular.math.washington.edu/papers/ars-manin/` (2006).

The Manin Constant: a new Theorem

Theorem. *For all $N \leq 130000$, every optimal elliptic quotient of $J_0(N)$ has Manin constant equal to* 1.

Moreover, for $N < 60000$ the optimal curve in each class is the one whose identifying number in the tables is 1 (except for class $990h$ where the optimal curve is $990h3$).

The second part of the Theorem for all $N < 130000$ would follow from Stevens' conjecture that in each isogeny class the curve with minimal Faltings height is the optimal $\Gamma_1(N)$-quotient: this can be verified in each case using Mark Watkins's program ec.

Verifying the second part for all $N < 130000$ would require more computations with modular symbols; see

A. Agashe, K. A. Ribet and W. A. Stein, *The Manin Constant*, JPAM Coates Volume, `http://modular.math.washington.edu/papers/ars-manin/` (2006).

The Manin Constant: a new Theorem

Theorem. *For all $N \leq 130000$, every optimal elliptic quotient of $J_0(N)$ has Manin constant equal to 1.*

Moreover, for $N < 60000$ the optimal curve in each class is the one whose identifying number in the tables is 1 (except for class $990h$ where the optimal curve is $990h3$).

The second part of the Theorem for all $N < 130000$ would follow from Stevens' conjecture that in each isogeny class the curve with minimal Faltings height is the optimal $\Gamma_1(N)$-quotient: this can be verified in each case using Mark Watkins's program ec.

Verifying the second part for all $N < 130000$ would require more computations with modular symbols; see

A. Agashe, K. A. Ribet and W. A. Stein, *The Manin Constant*, JPAM Coates Volume, `http://modular.math.washington.edu/papers/ars-manin/` (2006).

The Manin Constant: a new Theorem

Theorem. *For all $N \leq 130000$, every optimal elliptic quotient of $J_0(N)$ has Manin constant equal to 1.*

Moreover, for $N < 60000$ the optimal curve in each class is the one whose identifying number in the tables is 1 (except for class $990h$ where the optimal curve is $990h3$).

The second part of the Theorem for all $N < 130000$ would follow from Stevens' conjecture that in each isogeny class the curve with minimal Faltings height is the optimal $\Gamma_1(N)$-quotient: this can be verified in each case using Mark Watkins's program ec.

Verifying the second part for all $N < 130000$ would require more computations with modular symbols; see

A. Agashe, K. A. Ribet and W. A. Stein, *The Manin Constant*, JPAM Coates Volume, `http://modular.math.washington.edu/papers/ars-manin/` (2006).