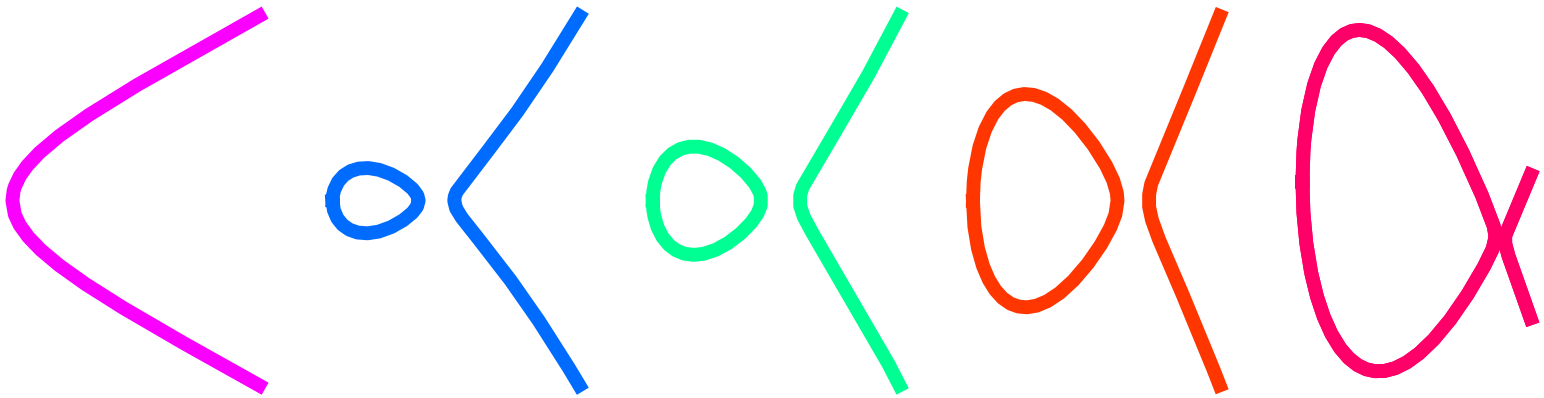
Elliptic Curves in Sage

William Stein

October 19 at ECC 2010

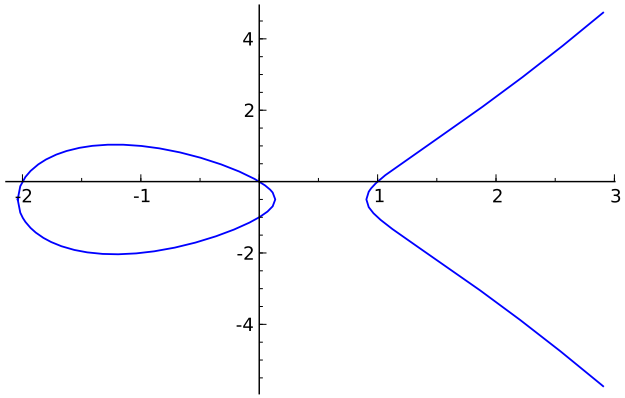


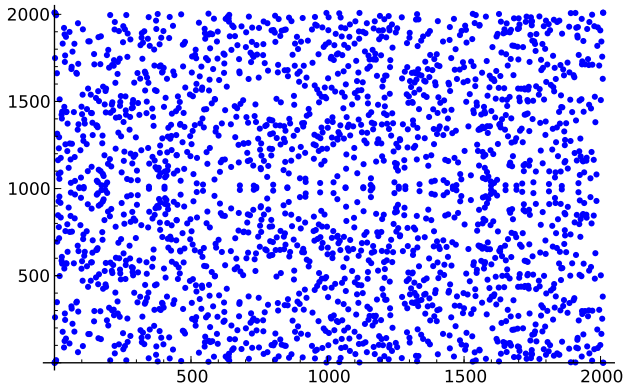
Lowest (known) conductor elliptic curves of ranks 0,1,2,3,4

Abstract

Abstract

I will describe Sage, discuss features for elliptic curves, then demonstrate some of them.





What is Sage?

Sage

- Project I started in early 2005
- Free open source software for *all* mathematics: number theory, graph theory, combinatorics, algebra, cryptography, applied math, statistics, symbolic calculus, ...
- Web site: http://sagemath.org/
- Hundreds of contributors
- Thousands of users
- Graphical user interface (web-browser based)
- Peer reviewed code
- Main user language: Python

Who Funds Sage?

The Sage project has received strong encouragement through funding, which has made it possible to support many people and run nearly *30 Sage Days workshops*.

Funding

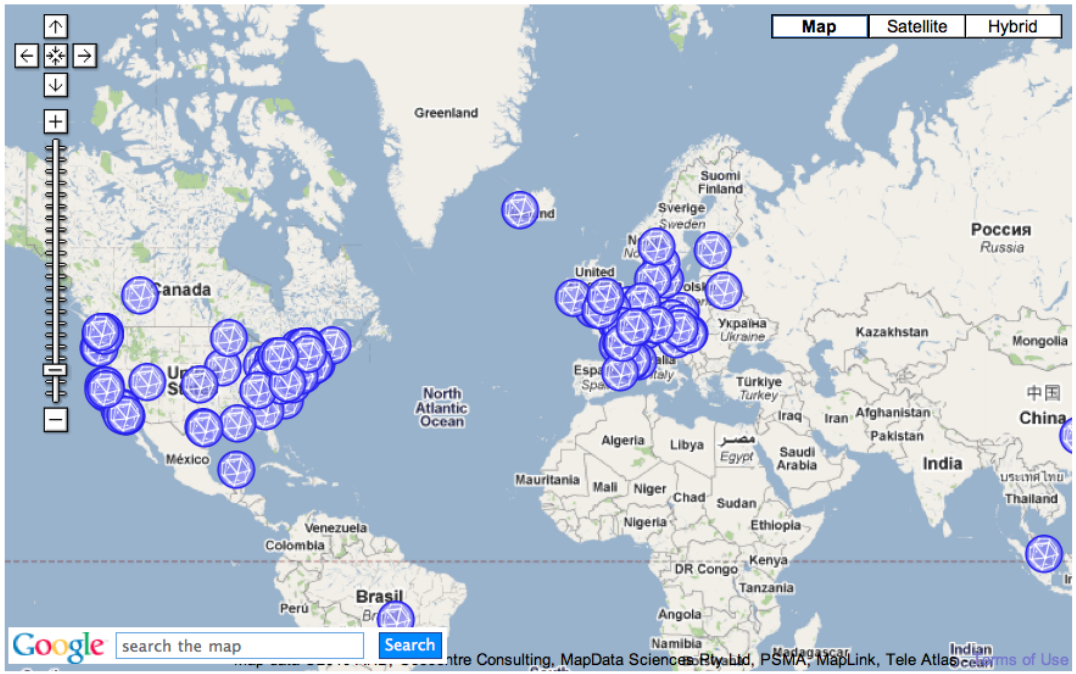
- **Companies:** Microsoft Research, Google, etc.
- **Government:** DOD, NSF – three new DOD/NSF grants in place for next few years
- **Institutes:** MSRI, CMI, IPAM, IMA, AIM, etc. Europe...
- **People:** Justin Walker, and many, many others

Example: Justin Walker and Microsoft Research are jointly funding "Sage Days 26: Women in Sage" this December.

Who Contributes Code to Sage?

Rotating release managers, etc. Sage is structured a bit like a research journal, *but is totally free to everybody* unlike vast majority of journals.

Contributors to Sage



, William Stein, Tim Abbott, Michael Abshoff, Antti Ajanki, Martin Albrecht, Nick Alexander, Bill Allombert, Ivan Andrus, Benjamin Antieau, Maite Aranes, Oscar Gerardo Lazo Arjona, Jennifer Balakrishnan, Jason Bandlow, Gregory Bard, Sébastien Barthélemy, Rob Beezer, Karim Belabas, Arnaud Bergeron, Luis Berlioz, Francois Bissey, Jonathan Bober, Tom Boothby, Nicolas Borie, Robert Bradshaw, Michael Brickenstein, Nils Bruin, Stanislav Bulygin, Dan Bump, Iftikhar Burhanuddin, Paul Butler, Ondrej Certik, Wilson Cheung, Dan Christensen, Craig Citro, Anders Claesson, Francis Clarke, Timothy Clemans, Alex Clemesha, Nathann Cohen, Jenny Cooley, John Cremona, Karl-Dieter Crisman, Fidel Barrera Cruz, Doug Cutrell, Alyson Deines, Vincent Delecroix, Jeroen Demeyer, Tom Denton, Didier Deshommes, Ryan Dingman, Dan Drake, Tom Draper, Alexander Dreyer, Tim Dumol, Nathan Dunfield, Gabriel Ebner, Burcin Erocal, Ron Evans, Richard J. Fateman, Lars Fischer, Evan Fosmark, Gary Furnish, Alex Ghitza, Andrzej Giniewicz, Amy Glen, Daniel Gordon, Chris Gorecki, Jan Groenewald, Rob Gross, Jason Grout, Carlo Hamalainen, Marshall Hampton, Jon Hanke, David Møllerller Hansen, Mike Hansen, Bill Hart, David Harvey, Leif Hille, Florent Hivert, Ryan Hinton, Neal Holtz, Golam Mortuza Hossain, Sean Howe, Alexander Hupfer, Wilfried Huss, Hamish Ivey-Law, Naqi Jaffery, Peter Jeremy, Peter Jipsen, Fredrik Johansson, David Joyner, Michael Kallweit, Josh Kantor, Kiran Kedlaya, Lloyd Kilford, Simon King, David Kirkby, Emily Kirkman, David Kohel, Ted Kosan, Ross Kyprianou, Sébastien Labbé, Yann Laigle-Chapuy, Kwankyu Lee, David Loeffler, Michael Mardaus, Robert Maŕik, Jason Martin, Alexandre Blondin Massé, Peter McNamara, Jason Merrill, Matthias Meulien, Robert Miller, Kate Minola, Joel Mohler, Peter Mora, Bobby Moretti, Rich Morin, Guillaume Moroz, Gregg Musiker, Tobias Nagel, Brett Nakashima, Pablo De Nápoli, Minh Van Nguyen, Andrey Novoseltsev, Bill Page, Ronan Paixão, Willem Jan Palenstijn, John Palmieri, Dmitrii Pasechnik, Javier López Peña, David Perkinson, Clement Pernet, John Perry, Pearu Peterson, Bill Purvis, Yi Qiang, Jordi Quer, Jens Rasch, Martin Raum, Dorian Raymer, R. Rishikesh, David Roe, Bjarke Hammersholt Roune, Gordon Royle, Serge A. Salamanka, Franco Saliola, Kyle Schalm, Anne Schilling, Harald Schilly, Jack Schmidt, Dag Sverre Seljebotn, Dan Shumow, Denis Simone, Steven Sivek, Nils-Peter Skoruppa, Jaap Spies, Kevin Stueve, Blair Sutton, Chris Swierczewski, Glenn Tarbox, Philippe Theveny, Nicolas Thiery, Griffen Thoma, Igor Tolkov, Gonzalo Tornaria, Charlie Turner, Michel Vandenbergh, Soledad Villar, John Voight, Steve Vonn, Justin Walker, Mark Watkins, Georg S. Weber, Ralf-Philipp Weinmann, Joe Wetherell, Carl Witty, Cristian Wuthrich, Soroosh Yazdani, Dal S. Yu, Gary Zablackis, Mike Zabrocki, Bin Zhang, Paul Zimmermann, Mao Ziyang

Standard Elliptic Curves Capabilities of Sage

What Does it mean to say "Sage Can Do X"?

- I am only discussing *standard functionality*, that is, functionality included in every copy of Sage.
- There are additional things Sage can do when coupled with all code out there that isn't yet included standard in Sage. (The referee and inclusion process can take a while.) Example: http://trac.sagemath.org/sage_trac/ticket/10026
- Elliptic curves reference manual: http://sagemath.org/doc/reference/plane_curves.html

The Birch and Swinnerton-Dyer Conjecture

Much work on elliptic curves in Sage motivated by research into BSD by Robert Miller, Robert Bradshaw, Chris Wuthrich, John Cremona, and me.

Conjecture (Birch and Swinnerton-Dyer)

Let E be an elliptic curve over $\mathbf{Q}$. Then

$$\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}(E(\mathbf{Q})) = r$$

and

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\prod c_p \cdot \Omega_E \cdot \mathrm{Reg}_E}{\#E(\mathbf{Q})^2_{\mathrm{tor}}} \cdot \#Ш(E).$$

(Similar formula over number fields.)

Applications (Robert Miller, Stein, Wuthrich, et al.): Verification of the full conjecture in many specific cases of curves of conductor up to 5000. (See the brand new paper by Robert Miller.)

Sage: Elliptic Curves over $\mathbf{Q}$

1. **Invariants:** conductor, Tamagawa numbers, etc.
2. **Mordell-Weil groups:** and point search (via Cremona's MWRANK, Simon's 2-descent), regulator.
3. ***S*-integral points:** new code in Sage (Cremona, Nagel, Mardaus)
4. **Complex *L*-series:** evaluation of any derivative anywhere, large-scale computation of zeros (Dokchitser, Rubinstein, Bradshaw)
5. ***p*-adic *L*-functions and *p*-adic heights**: new code (Harvey, Stein, Wuthrich)
6. **Shafarevich-Tate groups:** conjectural order, actual order in many cases (Stein, Miller, Wuthrich)
7. **Heegner points**: new algorithms and code (Stein, Bradshaw, Miller, Cremona); Kolyvagin's Euler system (Stein, Weinstein, Balakrishnan)
8. **All curves of given conductor:** Cremona's programs that he used to make his tables are in Sage, though not "exposed"
9. **Isogeny class:** of curve (Cremona)
10. **Division polynomials:** many variants (Stein, Cremona, Harvey)
11. **Image of Galois:** partial information (Stein, Wuthrich, Sutherland)
12. **Isogenies and isomorphisms:** (Shumow, Bradshaw, Cremona)
13. **Curves with same mod-5 representation:** (Rubin, Silverberg)
14. **Plotting**

Sage: Elliptic Curves over Finite Fields

1. **Point counting:** and group structure using baby-step giant-step (Cremona)
2. **Fast point counting:** for $p < 10^7$ (via PARI)
3. **SEA algorithm:** Fast pointing counting for larger p (via PARI)
4. **Weil pairing**
5. **Isogenies and isomorphisms:** (Shumow, Bradshaw, Cremona)
6. **Mestre's method of graphs:** Supersingular j-invariants; the p-isogeny graph for small p. (Stein, Burhanuddin)
7. **Eichler orders:** Fast enumeration of isogeny graphs with level N structure using rational quaternion algebras. (Stein, Bober)
8. **ECM:** Elliptic Curve Factorization (Zimmermann et al.)
9. **Plotting**

Sage: Elliptic Curves over Number Fields

Functionality

1. **Tate's algorithm:** conductor, Tamagawa numbers, etc. (Roe, Cremona)
2. **Heights** of points (Bradshaw)
3. **Mordell-Weil group** via algebraic descent (Denis Simon)
4. **Periods and elliptic logs** for both real and complex embeddings (Cremona)

A Demo

Follow Along

http://demo.sagenb.org/home/pub/42/

Improving Sage's Elliptic Curves Functionality: Some Future Plans

What is *or should be* in the pipeline

1. Finding elliptic curves over **totally real fields** via:
   - **Hilbert modular forms:** new implementations of the algorithms implemented by Dembele, Voight, and Donnelly in some expensive proprietary system.
   - **Searching:** for curves with small discriminant (current work of Elkies)
2. **3-Descent and 4-Descent:** over $\mathbf{Q}$
3. **Integral and S-integral points:** over number fields
4. **L-function:** over number fields; evaluation, zeros
5. **L-function:** over function fields (see recent work of Sal Baig and Chris Hall).
6. **2-Descent:** over function fields
7. **Image of Galois:** for curves over $\mathbf{Q}$ (code of Drew Sutherland on trac now).
8. **Massive tables:** e.g., `db.modform.org`, which is query-able over the Internet from Sage (by me).
9. **Pairings over finite fields:** seems only Weil pairing included now.
10. **Generic points:** points defined over the function field of the curve.
11. **Models:** transforming between presentations for elliptic curves (Tanja Lange's student)

Questions?

Questions?

Purple Sage: A New Project I Recently Started

About PSAGE

- http://purple.sagemath.org/
- Free open source software for *arithmetic geometry*.
- Based on a more manageable subset of Sage; only support 64-bit Linux and OS X
- **NO** 100% doctest policy; No API stability requirements; No Fortran or Lisp code (only C, C++, Python, Cython).
- A quick place to get research oriented code out there so it can be used to inspire conjectures in arithmetic geometry.
- An outlet for researchers, so that Sage itself can be a stable core without this causing too much frustration.