SAGE: Software for Algebra and Geometry Experimentation

William Stein

April 29, 2006: SFSU AMS Meeting

What is SAGE?

I started SAGE last year, and it has since mushroomed. There are now dozens of contributors all over the world and an extremely active mailing list.

1. **Completely free and open source.**

2. **A new computer algebra system:** Uses a *mainstream* language (unlike Magma, Gap, Mathematica, Maple, etc.)

3. **A new way to use your software:** use *all* your favorite (**commercial** or free) mathematics software *together*.

Does Open Source Matter for Math Research?

"You can read Sylow's Theorem and its proof in Huppert's book in the library [...] then you can use Sylow's Theorem for the rest of your life free of charge, but for many computer algebra systems license fees have to be paid regularly [...]. You press buttons and you get answers in the same way as you get the bright pictures from your television set but you cannot control how they were made in either case.

With this situation **two of the most basic rules of conduct in mathematics are violated**: In mathematics **information is passed on free of charge** and **everything is laid open for checking**. Not applying these rules to computer algebra systems that are made for mathematical research [...] means **moving in a most undesirable direction**. Most important: Can we expect somebody to believe a result of a program that he is not allowed to see? "

– J. Neubüser in **1993** (he started GAP in 1986).

SAGE: A New Computer Algebra System

```
algebras     edu          interfaces  modular   schemes
categories   ext          lfunctions  modules   sets
coding       functions    libs        monoids   structure
crypto       geometry     matrix      plot      tests
databases    groups       misc        rings
```

```
$ cat */*.py */*/*.py */*/*/*.py */*.pyx */*/*.pyx |sort|un
58858
```

```
$ cat */*.py */*/*.py */*.pyx */*/*.pyx |sort|uniq|grep "sa
6845          <-------- EXAMPLE INPUT LINES!
```

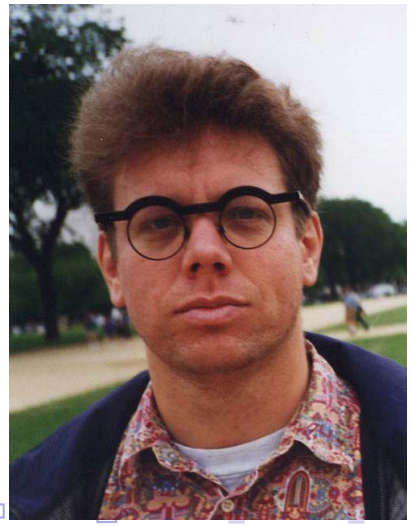
Cooperation: "Everything Under One Roof"

SAGE has many interfaces (**bold included** with SAGE):

- **GAP** (started 1986)– groups, discrete math
- **Singular** (started 1987) – polynomial computation
- **PARI/GP** (started 1987) – number theory
- **Maxima** (started 1967) – symbolic manipulation
- **mwrank, ec, simon, sea** – elliptic curves
- Macaulay2 (started 1993) – (soon to be included)
- KANT/KASH – sophisticated algebraic number theory
- Magma (started 1973) – high-quality research math environment
- Maple – symbolic, educational
- Mathematica – symbolic, numerical, educational
- Octave (started 1992) – numerical analysis
- Specialized: mwrank, gfan, sympow, ntl, genus2reduction, polymake, lcalc (Rubinstein), dokchitser; more to come...!

Python: A Mainstream Programming Language

- Guido van Rossum released first Python in 1991.
- A **"gluing language"**, i.e., design to be easier to use libraries and other programs.
- **VAST range of libraries**: graphics, 3d simulation, web programming, numerical analysis, etc.
- **Easy to read** code
- `function?` gives documentation about function and `function??` gives the **source code**.
- **IPython:** Awesome!



Pyrex: Compiled Python-like language

1. Written by **Greg Ewing** of New Zealand.
2. Code converted to C code that is **compiled by a C compiler**.
3. Easy to use C/C++ code and libraries from Pyrex.
4. **Time-critical** SAGE code gets implemented in Pyrex, which is (as fast as) C code, but easier to read (e.g., since all variables and scopes are explicit).

Examples! Examples! Examples!

```
sage: E = EllipticCurve('681b'); E
Elliptic Curve defined by
     y^2 + x*y  = x^3 + x^2 - 1154*x - 15345  ...
sage: E.analytic_rank()
0
sage: E.sha_an()
9
sage: E.non_surjective()
[(2, '2-torsion')]
sage: E.heegner_discriminants_list(10)
[-8, -20, -35, -56, -68, -83, -95, -107, -119, -143]
sage: n = E.heegner_index(-20); n
[8.99999215656, 9.00000831615]
sage: parent(n)
Float interval arithmetic pseudoring.
sage: n^2 + 10
[90.9998588182, 91.0001496907]
```

L-functions

```
sage: E = EllipticCurve('681b')
sage: L = E.Lseries_dokchitser()  # T. Dokchitser
sage: L(1)
1.844815206126820 8
sage: L(2)
1.176002881044164 3
sage: L(1+I)
0.2876958106057646 0 - 0.5978138350069388 5*I
sage: E.Lseries_zeros(5)          # M. Rubinstein
[1.1931974371, 2.9775032355, 4.1340673324, 5.1249133553, 5.
sage: E.Lseries_sympow(2,16)      # M. Watkins
'1.010475324678458E+00'
```

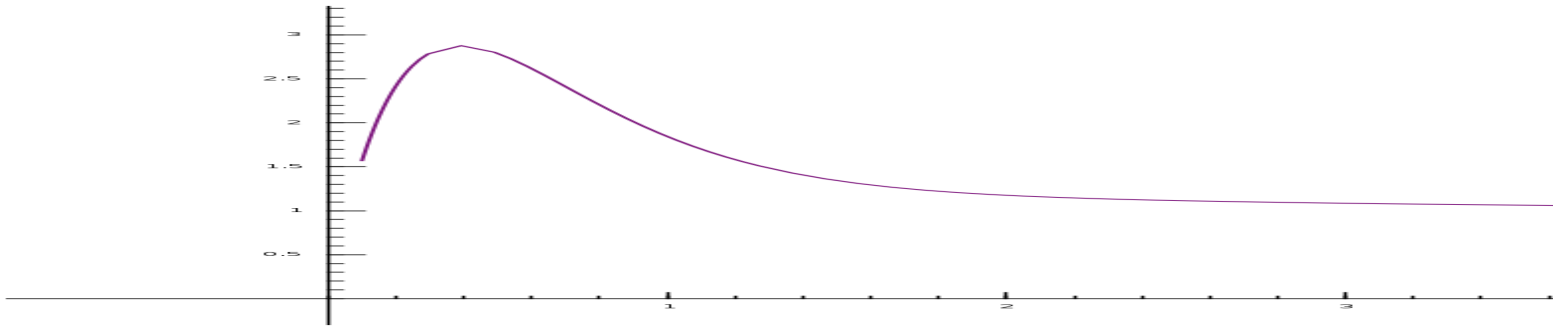
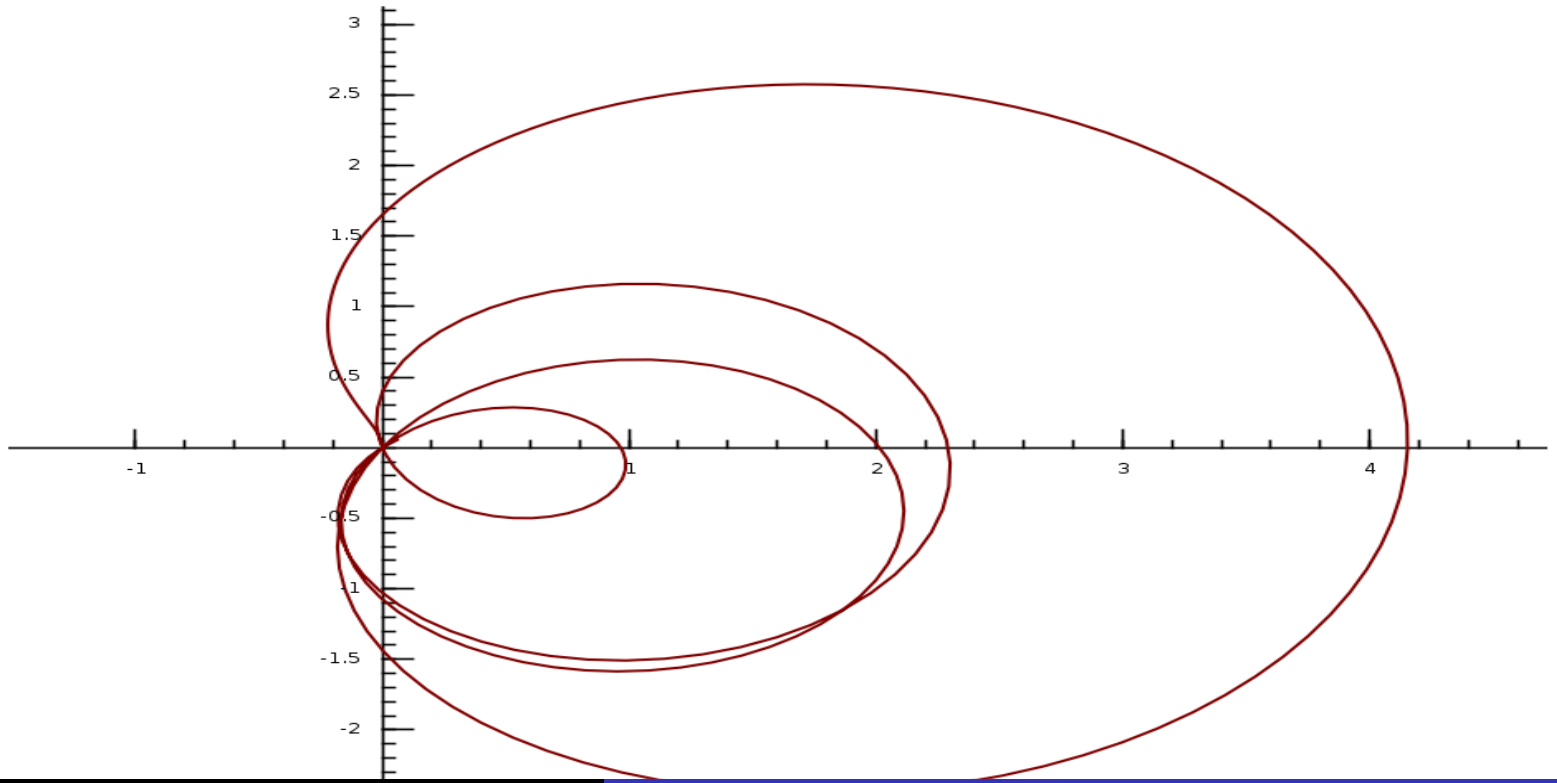


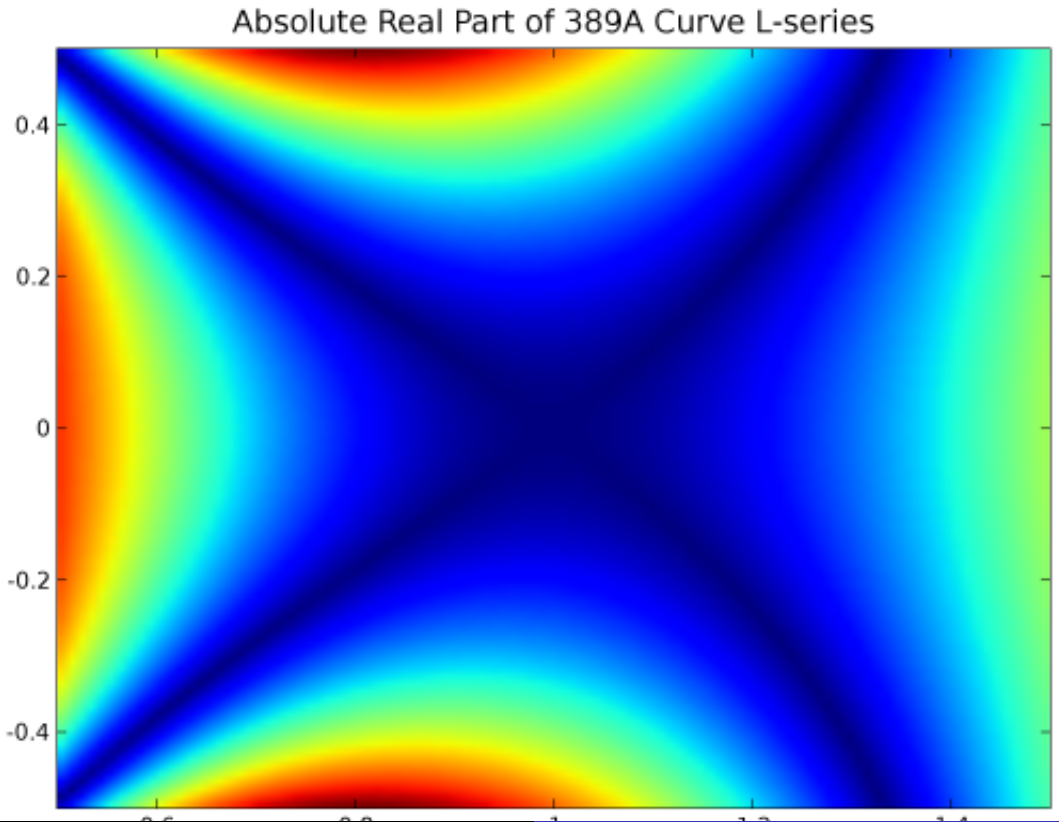
Image of a line segment under $L(E, s)$

```
sage: E = EllipticCurve('37a')
sage: v = E.Lseries_values_along_line(1, 1+10*I, 300)
sage: w = [(z[1].real(), z[1].imag()) for z in v]
sage: L = line(w, rgbcolor=(0.5,0,0))
sage: L.save('line.png')
```



Graphing a Complex L-series

```
sage: E = EllipticCurve('389a')
sage: L = E.Lseries_dokchitser()
sage: L(1+I)
-0.63840993858803874 + 0.71549523920466740*I
sage: L(1+0.2*I,  50)
-0.030658879217008016 + 0.0035873942766903410*I
```



Arithmetic of our favorite rank 1 curve

```
sage: E = EllipticCurve('37a')
sage: E.sha_an()                --> 1
sage: E.non_surjective()        --> []
sage: E.sha_an()                --> 1
sage: E.regulator()             --> 0.051111408239999996
sage: E.gens()                  --> [(0 : 0 : 1)]
sage: E.heegner_discriminants(50)  --> [-3, -4, -7, -11, -4
sage: E.heegner_index(-7)  # Kolyvagin ==> Sha trivial
[0.999990645298, 1.00000935475]
sage: E.q_expansion(5)
            --> q - 2*q^2 - 3*q^3 + 2*q^4 + O(q^5)
sage: E.simon_two_descent ()
(1, 1, [(0 : 108 : 1)])
sage: E.sea(next_prime(10^50))
100000000000000000000001917684156174529696959920
```

Saving and Loading Objects

Most objects in SAGE can easily be loaded and saved in a compressed format. (This is a standard feature of Python!)

```
sage: M = ModularSymbols(Gamma1(13),2); M
Full Modular Symbols space for Gamma_1(13) ...dimension 15
sage: D = M.decomposition(3)
sage: [A.dimension() for A in D]
[1, 1, 1, 2, 2, 2, 2, 4]
sage: save(M, 'modsym13')
... <quit and restart > ...
sage: M = load('modsym13')
sage: D = M.decomposition(3)    # instant!
sage: D[-1].hecke_operator(2).charpoly().factor()
(x^2 + 3*x + 3)^2
```

SAGE is not only for number theory!

```
sage: P.<x,y,z,w> = ProjectiveSpace(3,QQ)
sage: C = P.subscheme([y^2-x*z, z^2-y*w, x*w-y*z])
sage: len(C.irreducible_components())   # twisted cubic
1
sage: J = C.defining_ideal()
sage: G = J.groebner_fan()
sage: len(G.reduced_groebner_bases())
8
sage: G.fvector()
(1, 8, 8)
sage: f = prod(J.gens())     # \/-- newton polytope
sage: NP = polymake.convex_hull(f.exponents())
sage: NP.facets()
[(3/2, 5/2, -1, 0), (3, 1, -1, 0), (1, 0, 0, 0),
 (-3/2, 2, 1, 0), (3, -1, 4, 0), (-3, 1, 5, 0)]
```

(And Stein is not only a number theorist anymore...)

SAGE: A Future?

- August 2006: **MSRI grad student Workshop** on Computing with Modular Forms (with SAGE).
- October 2006: **SAGE Days 2** in Seattle.
- UW *startup money*: Very generous financial support for SAGE development (hiring a team of students, mainly undergrads).
- **Most** SAGE users are coauthors/developers of SAGE.