Finding all Elliptic Curves over $\mathbb{Q}(\sqrt{5})$ of Given Conductor

William Stein*

October 28, 2011

Abstract

Contents

*The work was supported by NSF grants...

1 Introduction

1.1 Elliptic Curves over $\mathbb{Q}$

Tables of elliptic curves over $\mathbb{Q}$ have been of great value in mathematical research. The first systematic published tables were in Antwerp IV [BK75], which included all elliptic curves over $\mathbb{Q}$ of conductor up to 200, and also a table of all elliptic curves with bad reduction only at $2, 3$.

Cremona then wrote a book [Cre97] that gave a careful and detailed description of algorithms that together would output a list of all elliptic curves over $\mathbb{Q}$ of any specific given conductor, along with extensive data about each curve. The proof that his algorithm output all curves of given conductor had to wait for [BCDT01]. Cremona has subsequently computed tables [Cre] of all elliptic curves over $\mathbb{Q}$ of conductor up to $200, 000$ with Mordell-Weil groups and other data about each, and his main current target is reaching $234, 446$, which is the smallest known conductor of a rank 4 curve.

In a different direction, Stein-Watkins (see [SW02, BMSW07]) created a huge table of 136,832,795 elliptic curves over $\mathbb{Q}$ of conductor $\leq 10^8$, and another table of 11,378,911 elliptic curves over $\mathbb{Q}$ of prime conductor $\leq 10^{10}$. For each curve, these tables contain the analytic rank numerically computed to some precision, and some other data, though the actual ranks of all of these curves has not been determined. There are also many curves of large discriminant missing from the Stein-Watkins tables, since these tables are made by enumerating curves with relatively small defining equations, and discarding those of large conductor, rather than systematically finding all curves of given conductor no matter how large the defining equation.

1.2 Why $\mathbb{Q}(\sqrt{5})$?

Like $\mathbb{Q}$, the field $F = \mathbb{Q}(\sqrt{5})$ is a totally real field, and many of the techniques that we have for studying elliptic curves over $\mathbb{Q}$ generalize, or are conjectured to generalize, to totally real fields. As is the case over $\mathbb{Q}$, there is a notion of modularity coming from Shimura curve parametrizations and Hilbert modular forms, which is now backed up by extensive theoretical [] and some computational [] evidence. Moreover, extensive work [] of Zhang has extended many results of Gross-Zagier [] and Kolyvagin [] to the context of elliptic curves over totally real fields.

If we order fields by absolute discriminant, then $F = \mathbb{Q}(\sqrt{5})$ is the next field after $\mathbb{Q}$. That 5 divides $\mathrm{disc}(F) = 5$ obstructs attempts to generalize the Taylor-Wiles method to elliptic curves over F, which makes this case even more interesting. The field F also has xx CM j-invariants, which is far more than any other field of degree ≤ 2 [[??]] (see Section 7.2). Let $\varphi = \frac{1+\sqrt{5}}{2}$. The unit group $\{\pm 1\} \times \langle \varphi \rangle$ of the ring $R = \mathcal{O}_F = \mathbb{Z}[\varphi]$ of integers of F is infinite, which leads to additional complications. Finally, the totally real field F has even degree 2, which makes computation of Hilbert modular forms and corresponding elliptic curves more difficult, since the techniques of [] are not available. In particular, some curves (e.g., with square level) can have no Shimura curve parameterization.

1.3 Modularity conjecture

The following conjecture is not yet known in general.

Conjecture 1.1 (Modularity)**.** *The set of L-functions of elliptic curves over F equals the set of L-functions associated to cuspidal Hilbert modular newforms over F of parallel* *weight* 2 *with rational Hecke eigenvalues.*

Given the huge amount of recent progress on modularity theorems, we are optimistic that Conjecture 1.1 will be proved in the near future. We officially *assume* it for the rest of this paper.

2 Computing Hilbert modular forms over F

3 Strategies for finding an elliptic curve attached to a Hilbert modular form

Let $f \in S_{(2,2)}(\mathfrak{n})$ be a rational Hilbert newforms as in Section 2. According to Conjecture 1.1, there is some elliptic curve E_f over f such that $L(f,s) = L(E_f,s)$. Note that E_f is only well defined up to isogeny. Unlike the case for elliptic curves over $\mathbb{Q}$ (see [Cre97]), there appears to be no fast direct algorithm to find E_f. Nonetheless, there are numerous approaches.

In all the sections below, we assume that Conjecture 1.1 is true and that we have computed (as in Section 2) a complete list of Hecke eigenvalues $a_\mathfrak{p}$ of all rational Hilbert newforms of some level $\mathfrak{n}$, to at least enough precision B to determine one from another.

3.1 Naive enumeration

The most naive strategy is to systematically enumerate pairs $a, b \in R$, hence elliptic curves $E : y^2 = x^3 + ax + b$ over F, and for each curve compute some L-series coefficients $a_\mathfrak{p}(E)$ at primes that do not divide the discriminant of the cubic by counting points modulo primes. If all $a_\mathfrak{p}(E)$ match with those of the input newform f, up to the bound B, we then compute the conductor $\mathcal{N}_E$, and if it equals $\mathfrak{n}$, we conclude that $L(E_f,s) = L(f,s)$.

Under our hypotheses, naive enumeration is an algorithm to solve our problem: it will terminate, and when it terminates it outputs a correct curve E_f. Unfortunately, it can be very slow because even if $\mathfrak{n}$ is small, the simplest curve in the isogeny class of E_f may have very large coefficients, for example, if each is of the form $x + \varphi y$ with x and y having coefficients around 10^5, then we would have to consider 10^{20} before finding E_f, which is not feasible.

3.2 Torsion families

We can tell whether or not $\ell \mid \#E(F)_{\mathrm{tor}}$ for some E in the isogeny class of E_f using the following proposition.

Proposition 3.1. *TODO: Explain how to tell if* $\ell \mid \#E(F)_{\mathrm{tor}}$.

Proof. Use Galois representations, and also Katz's theorem. □

Instead of searching through all curves as in Section 3.1, ...

3.3 Twisting

3.4 Curves with specified $a_{\mathfrak{p}}$

3.5 Curves with good reduction outside S

3.6 Special values of twisted L-series

3.7 Congruence families

4 Enumerating the curves in an isogeny class

5 Norm conductor 31

6 Related future projects

7 Tables

7.1 Up to norm conductor 199

[[TODO: This will be a short-as-reasonable table of curves of norm conductor ≤ 199, hence including the first curve of rank 1. It will probably be about 6 pages long.]]

7.2 CM elliptic curves over F

[[TODO: A table like in the back of [Sil94], but over $\mathbb{Q}(\sqrt{5})$. We haven't made this yet. I'm not sure how hard this is; should be fun.]]

7.3 Extended version only: up to norm conductor 1831

[[This will contain a longer version, which includes both curves and their conjugates, etc., and has all data up to 1831, and will be over 100 pages long. This will be a special version only available on our websites; we won't submit this to a journal.]]

References

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic), `http://math.stanford.edu/~conrad/papers/tswfinal.pdf`. MR 2002d:11058

[BK75] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Springer-Verlag, Berlin, 1975, Lecture Notes in Mathematics, Vol. 476.

[BMSW07] Baur Bektemirov, Barry Mazur, William Stein, and Mark Watkins, *Average ranks of elliptic curves: tension between data and conjecture*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), no. 2, 233–254 (electronic). MR 2291676

[Cre] J.E. Cremona, *Elliptic Curves Data*, `http://www.warwick.ac.uk/~masgaj/ftp/data/`.

[Cre97] ———, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997, `http://www.warwick.ac.uk/~masgaj/book/fulltext/`.

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

[SW02] William Stein and Mark Watkins, *A database of elliptic curves—first report*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, `http://wstein.org/ecdb`, pp. 267–275. MR 2041090 (2005h:11113)