THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

A database of elliptic curves over $\mathbb{Q}(\sqrt{5})$: a first report

Jonathan Bober, Alyson Deines, Ariah Klages-Mundt, Benjamin LeVeque, R. Andrew Ohana, Ashwath Rabindranath, Paul Sharaba, and William Stein

msp

THE OPEN BOOK SERIES 1 (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.145

A database of elliptic curves over $\mathbb{Q}(\sqrt{5})$: a first report

Jonathan Bober, Alyson Deines, Ariah Klages-Mundt,
Benjamin LeVeque, R. Andrew Ohana,
Ashwath Rabindranath, Paul Sharaba, and William Stein

We describe a tabulation of (conjecturally) modular elliptic curves over the field $\mathbb{Q}(\sqrt{5})$ up to the first elliptic curve of rank 2. Using an efficient implementation of an algorithm of Lassina Dembélé, we computed tables of Hilbert modular forms of weight $(2, 2)$ over $\mathbb{Q}(\sqrt{5})$, and via a variety of methods we constructed corresponding elliptic curves, including (again, conjecturally) all elliptic curves over $\mathbb{Q}(\sqrt{5})$ that have conductor with norm less than or equal to 1831.

1. Introduction

1A. ***Elliptic curves over*** $\mathbb{Q}$**.** Tables of elliptic curves over $\mathbb{Q}$ have been of great value in mathematical research. Some of the first such tables were those in Antwerp IV [4], 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 and 3.

Cremona's book [10] gives a detailed description of algorithms that together output a list of all elliptic curves over $\mathbb{Q}$ of any given conductor, along with extensive data about each curve. The proof that his algorithm outputs *all* curves of given conductor had to wait for the proof of the full modularity theorem in [8]. Cremona has subsequently computed tables [12] of all elliptic curves over $\mathbb{Q}$ of conductor up to 300,000, including Mordell-Weil groups and other extensive data about each curve.

In another direction, Stein and Watkins (see [33; 1]) created a table of 136,832,795 elliptic curves over $\mathbb{Q}$ of conductor $\leq 10^8$, and a table of 11,378,911 elliptic curves over $\mathbb{Q}$ of prime conductor $\leq 10^{10}$. There are many curves of large discriminant

MSC2010: primary 11-04; secondary 11G05.
Keywords: elliptic curves, totally real number fields, Hilbert modular forms, tables, sage.

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.

1B. ***Why*** $\mathbb{Q}(\sqrt{5})$***?*** Like $\mathbb{Q}$, the field $F = \mathbb{Q}(\sqrt{5})$ is a totally real field, and many of the theorems and ideas about elliptic curves over $\mathbb{Q}$ have been generalized to totally real fields. As is the case over $\mathbb{Q}$, there is a notion of modularity of elliptic curves over F, and work of Zhang [36] has extended many results of Gross and Zagier [20] and Kolyvagin [24] to the context of elliptic curves over totally real fields.

If we order totally real number fields K by the absolute value of their discriminant, then $F = \mathbb{Q}(\sqrt{5})$ comes next after $\mathbb{Q}$ (the Minkowski bound implies that $|D_K| \geq (n^n/n!)^2$, where $n = [K : \mathbb{Q}]$, so if $n \geq 3$ then $|D_K| > 20$). That 5 divides $\mathrm{disc}(F) = 5$ thwarts attempts to easily generalize the method of Taylor and Wiles to elliptic curves over F, which makes $\mathbb{Q}(\sqrt{5})$ even more interesting. Furthermore F is a PID and elliptic curves over F admit global minimal models and have well-defined notions of minimal discriminants. The field F also has 31 CM j-invariants, which is far more than any other quadratic field (see Section 5). Letting $\varphi = \frac{1+\sqrt{5}}{2}$, we have that the group of units $\{\pm 1\} \times \langle \varphi \rangle$ of the ring $R = \mathcal{O}_F = \mathbb{Z}[\varphi]$ of integers of F is infinite, leading to additional complications. Finally, F has even degree, which makes certain computations more difficult, as the cohomological techniques of [19] are not available.

1C. ***Modularity conjecture.*** The following conjecture is open:

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 weight $(2, 2)$ with rational Hecke eigenvalues.*

Given the progress on modularity theorems initiated by [35], we are optimistic that Conjecture 1.1 will be proved. *We assume Conjecture 1.1 for the rest of this paper.*

In Section 2 we sketch how to compute Hilbert modular forms using arithmetic in quaternion algebras. Section 3 gives numerous methods for finding an elliptic curve corresponding to a Hilbert modular form. It should be noted that these are the methods *originally* used to make the tables – in hindsight, it was discovered that some of the elliptic curves found using the more specific techniques could be found using a better implementation of the sieved enumeration of Section 3B. Section 4 addresses how to find all curves that are isogenous to a given curve. In Section 5 we enumerate the CM j-invariants in F. We discuss some projects for future work in Section 6. Finally, Section 7 contains tables that summarize various information about our dataset [5].

2. Computing Hilbert modular forms over F

In Section 2A we sketch Dembélé's approach to computing Hilbert modular forms over F, then in Section 2B we make some remarks about our fast implementation.

2A. ***Hilbert modular forms and quaternion algebras.*** Dembélé [14] introduced an algebraic approach via the Jacquet-Langlands correspondence to computing Hilbert modular forms of weight $(2,2)$ over F. The Hamiltonian quaternion algebra $F[i,j,k]$ over F is ramified exactly at the two infinite places, and contains the maximal order

$$S = R\big[\tfrac{1}{2}(1-\bar{\varphi}i+\varphi j),\ \tfrac{1}{2}(-\bar{\varphi}i+j+\varphi k),\ \tfrac{1}{2}(\varphi i-\bar{\varphi}j+k),\ \tfrac{1}{2}(i+\varphi j-\bar{\varphi}k)\big].$$

For any nonzero ideal $\mathfrak{n}$ in $R=\mathcal{O}_F$, let $\mathbb{P}^1(R/\mathfrak{n})$ be the set of equivalence classes of column vectors with two coprime entries $a,b\in R/\mathfrak{n}$ modulo the action of $(R/\mathfrak{n})^*$. We use the notation $[a:b]$ to denote the equivalence class of $\left(\begin{smallmatrix}a\\b\end{smallmatrix}\right)$. For each prime $\mathfrak{p}\mid\mathfrak{n}$, we fix a choice of isomorphism $F[i,j,k]\otimes F_\mathfrak{p}\approx M_2(F_\mathfrak{p})$, which induces a left action of S^* on $\mathbb{P}^1(R/\mathfrak{n})$. The action of $T_\mathfrak{p}$, for $p\nmid\mathfrak{n}$, is $T_\mathfrak{p}([x])=\sum[\alpha x]$, where the sum is over the classes $[\alpha]\in S/S^*$ with $N_{\mathrm{red}}(\alpha)=\pi_\mathfrak{p}$ (reduced quaternion norm), where $\pi_\mathfrak{p}$ is a fixed choice of totally positive generator of $\mathfrak{p}$. The Jacquet-Langlands correspondence implies that the space of Hilbert modular forms of level $\mathfrak{n}$ and weight $(2,2)$ is noncanonically isomorphic as a module over the Hecke algebra

$$\mathbb{T}=\mathbb{Z}[\,T_\mathfrak{p}:\mathfrak{p}\text{ nonzero prime ideal of }R\,]$$

to the finite dimensional complex vector space $V=\mathbb{C}[S^*\backslash\mathbb{P}^1(R/\mathfrak{n})]$.

2B. ***Remarks on computing with*** $\mathbb{P}^1(R/\mathfrak{n})$**.** In order to implement the algorithm sketched in Section 2A, it is critical that we can compute with $\mathbb{P}^1(R/\mathfrak{n})$ very, very quickly. For example, to apply the method of Section 3G below, in some cases we have to compute tens of thousands of Hecke operators. Thus in this section we make some additional remarks about this fast implementation.

When $\mathfrak{n}=\mathfrak{p}^e$ is a prime power, it is straightforward to efficiently enumerate representative elements of $\mathbb{P}^1(R/\mathfrak{p}^e)$, since each element $[x:y]$ of $\mathbb{P}^1(R/\mathfrak{p}^e)$ has a unique representative of the form $[1:b]$ or $[a:1]$ with a divisible by $\mathfrak{p}$, and these are all distinct. It is easy to put any $[x:y]$ in this canonical form and enumerate the elements of $\mathbb{P}^1(R/\mathfrak{p}^e)$, after choosing a way to enumerate the elements of $R/\mathfrak{p}^e$. An enumeration of $R/\mathfrak{p}^e$ is easy to give once we decide on how to represent $R/\mathfrak{p}^e$.

In general, consider the factorization $\mathfrak{n}=\prod_{i=1}^m\mathfrak{p}_i^{e_i}$. We have a bijection between $\mathbb{P}^1(R/\mathfrak{n})$ and $\prod_{i=1}^m\mathbb{P}^1(R/\mathfrak{p}_i^{e_i})$, which allows us to reduce to the prime power case, at the expense of having to compute the bijection $R/\mathfrak{n}\cong\prod R/\mathfrak{p}_i^{e_i}$. To this end, we *represent elements* of $R/\mathfrak{n}$ as m-tuples in $\prod R/\mathfrak{p}_i^{e_i}$, thus making computation of the bijection trivial.

To minimize dynamic memory allocation, thus speeding up the code by an order of magnitude, in the implementation we make some arbitrary bounds; this is not a serious constraint, since the linear algebra needed to isolate eigenforms for levels beyond this bound is prohibitive. We assume $m \leq 16$ and each individual $p_i^{e_i} \leq 2^{31}$, where p_i is the residue characteristic of $\mathfrak{p}_i$. In all cases, we represent an element of $R/\mathfrak{p}_i^{e_i}$ as a pair of 64-bit integers, and represent an element of $R/\mathfrak{n}$ as an array of 16 pairs of 64-bit integers. We use this representation in all cases, even if $\mathfrak{n}$ is divisible by less than 16 primes; the gain in speed coming from avoiding dynamic memory allocation more than compensates for the wasted memory.

Let $\mathfrak{p}^e$ be one of the prime power factors of $\mathfrak{n}$, and let p be the residue characteristic of $\mathfrak{p}$. We have one of the following cases:

- $\mathfrak{p}$ splits in R; then $R/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$ and we represent elements of $R/\mathfrak{p}^e$ as pairs $(a, 0) \bmod p^e$ with the usual addition and multiplication in the first factor.
- $\mathfrak{p}$ is inert in R; then $R/\mathfrak{p}^e \cong (\mathbb{Z}/p^e\mathbb{Z})[x]/(x^2 - x - 1)$, and we represent elements by pairs $(a, b) \in \mathbb{Z}/p^e\mathbb{Z}$ with multiplication

$$(a, b)(c, d) = (ac + bd, ad + bd + bc) \mod p^e.$$

- $\mathfrak{p}$ is ramified and $e = 2f$ is even; this is exactly the same as the case when $\mathfrak{p}$ is inert but with e replaced by f, since $R/\mathfrak{p}^e R \cong (\mathbb{Z}/p^f\mathbb{Z})[x]/(x^2 - x - 1)$.
- $\mathfrak{p}$ is ramified (so $p = 5$) and $e = 2f - 1$ is odd; the ring $A = R/\mathfrak{p}^e$ is trickier than the rest, because it is *not* of the form $\mathbb{Z}[x]/(m, g)$ where $m \in \mathbb{Z}$ and $g \in \mathbb{Z}[x]$. We have $A \approx (\mathbb{Z}/5^f\mathbb{Z})[x]/(x^2 - 5, 5^{f-1}x)$, and represent elements of A as pairs $(a, b) \in (\mathbb{Z}/5^f) \times (\mathbb{Z}/5^{f-1}\mathbb{Z})$, with arithmetic given by

$$(a, b) + (c, d) = (a + c \mod 5^f,\ b + d \mod 5^{f-1})$$
$$(a, b) \cdot (c, d) = (ac + 5bd \mod 5^f,\ ad + bc \mod 5^{f-1}).$$

  We find that $\varphi \in R \mapsto (1/2, 1/2)$.

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

In this section we describe various strategies to find an elliptic curve associated to each of the Hilbert modular forms computed in Section 2. Let f be a rational cuspidal Hilbert newform of weight $(2, 2)$ 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 [10]), there seems to be no known *efficient* direct algorithm to find E_f. Nonetheless, there are several approaches coming from various directions, which are each efficient in some cases.

Everywhere below, we continue to assume that Conjecture 1.1 is true and assume that we have computed (as in Section 2) the Hecke eigenvalues $a_{\mathfrak{p}} \in \mathbb{Z}$ of all rational Hilbert newforms of some level $\mathfrak{n}$, for $\mathrm{Norm}(\mathfrak{p}) \le B$ a good prime, where B is large enough to distinguish newforms. In some cases we will need far more $a_{\mathfrak{p}}$ in order to compute with the L-function attached to a newform. We will also need the $a_{\mathfrak{p}}$ for bad $\mathfrak{p}$ in a few cases, which we obtain using the functional equation for the L-function (as an application of Dokchitser's algorithm [16]).

We define the *norm conductor* of an elliptic curve over F to be the absolute norm of the conductor ideal of the curve.

In Section 3A we give a very simple enumeration method for finding curves, then in Section 3B we refine it by taking into account point counts modulo primes; together, these two methods found a substantial fraction of our curves. Sections 3C and 3D describe methods for searching in certain families of curves, for example, curves with a torsion point of given order or curves with a given irreducible mod ℓ Galois representation. Section 3E is about how to find all twists of a curve with bounded norm conductor. In Section 3F we mention the Cremona-Lingham algorithm, which relies on computing all S-integral points on many auxiliary curves. Finally, Section 3G explains in detail an algorithm of Dembélé that uses explicit computations with special values of L-functions to find curves.

3A. ***Extremely naïve enumeration.*** The most naïve strategy is to systematically enumerate elliptic curves $E\colon y^2 = x^3 + ax + b$, with $a, b \in R$, and for each E, to compute $a_{\mathfrak{p}}(E)$ for $\mathfrak{p}$ not dividing $\mathrm{Disc}(E)$ by counting points on E reduced modulo $\mathfrak{p}$. If all the $a_{\mathfrak{p}}(E)$ match with those of the input newform f up to the bound B, we then compute the conductor $\mathfrak{n}_E$, and if it equals $\mathfrak{n}$, we conclude from the sufficient largeness of B that E is in the isogeny class of E_f.

Under our hypotheses, this approach provides a deterministic and terminating algorithm to find all E_f. However, it can be extremely slow when $\mathfrak{n}$ is small but the simplest curve in the isogeny class of E_f has large coefficients. For example, using this search method it would be infeasible to find the curve (1) computed by Fisher using the visibility of Ш[7].

3B. ***Sieved enumeration.*** A refinement to the approach discussed above uses the $a_{\mathfrak{p}}$ values to impose congruence conditions modulo $\mathfrak{p}$ on E. If f is a newform with Hecke eigenvalues $a_{\mathfrak{p}}$, then $\#\tilde{E}_f(R/\mathfrak{p}) = \boldsymbol{N}(\mathfrak{p}) + 1 - a_{\mathfrak{p}}$. Given $\mathfrak{p}$ not dividing the level $\mathfrak{n}$, we can find all elliptic curves modulo $\mathfrak{p}$ with the specified number of points, especially when $\boldsymbol{N}(\mathfrak{p}) + 1 - a_{\mathfrak{p}}$ has few prime factors. We impose these congruence conditions at multiple primes $\mathfrak{p}_i$, use the Chinese remainder theorem, and lift the resulting elliptic curves modulo $R/\prod \mathfrak{p}_i$ to nonsingular elliptic curves over R.

While this method, like the previous one, will eventually terminate, it too is very ineffective if every E in the class of isogenous elliptic curves corresponding to f has large coefficients. However in practice, by optimally choosing the number of primes $\mathfrak{p}_i$, a reasonably efficient implementation of this method can be obtained.

3C. ***Torsion families.*** We find elliptic curves of small conductor by specializing explicit parametrizations of families of elliptic curves over F having specified torsion subgroups. We use the parametrizations of [25].

Theorem 3.1 (Kamienny and Najman, [22]). *The following is a complete list of torsion structures for elliptic curves over F:*

$$\begin{aligned} &\mathbb{Z}/m\mathbb{Z}, && 1 \le m \le 10,\ m = 12,\\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, && 1 \le m \le 4,\\ &\mathbb{Z}/15\mathbb{Z}. \end{aligned}$$

Moreover, there is a unique elliptic curve over F with 15-torsion.

We use the following proposition to determine in which family to search.

Proposition 3.2. *Let ℓ be a prime and let E be an elliptic curve over F. Then $\ell \mid \#E'(F)_{\mathrm{tor}}$ for some elliptic curve E' in the isogeny class of E if and only if $\ell \mid \boldsymbol{N}(\mathfrak{p}) + 1 - a_{\mathfrak{p}}$ for all odd primes $\mathfrak{p}$ at which E has good reduction.*

Proof. If $\ell \mid \#E'(F)_{\mathrm{tor}}$, from the injectivity of the reduction map at good primes [23, Appendix], we have that $\ell \mid \#\tilde{E}'(\mathbb{F}_{\mathfrak{p}}) = \boldsymbol{N}(\mathfrak{p}) + 1 - a_{\mathfrak{p}}$. The converse statement is one of the main results of [23]. □

By applying Proposition 3.2 for all $a_{\mathfrak{p}}$ with $\mathfrak{p}$ up to some bound, we can decide whether or not it is *likely* that some elliptic curve in the isogeny class of E contains an F-rational ℓ-torsion point. If this is the case, then we search over those families of elliptic curves with rational ℓ-torsion. With a relatively small search space, we thus find many elliptic curves with large coefficients more quickly than with the algorithm of Section 3A. For example, we first found the elliptic curve E given by

$$y^2 + \varphi y = x^3 + (27\varphi - 43)\, x + (-80\varphi + 128)$$

with norm conductor 145 by searching for elliptic curves with torsion subgroup $\mathbb{Z}/7\mathbb{Z}$.

3D. ***Congruence families.*** Suppose that we are searching for an elliptic curve E and we already know another elliptic curve E' with $E[\ell] \approx E'[\ell]$, where ℓ is some prime and $E[\ell]$ is irreducible. Twists of the modular curve $X(\ell)$ parametrize pairs of elliptic curves with isomorphic ℓ-torsion subgroups, so finding rational points on the correct twist allows us to find curves with the same mod ℓ Galois representation

as E'. Using this idea, we found the curve E given by

$$y^2 + \varphi xy = x^3 + (\varphi - 1)\,x^2 + (-257364\varphi - 159063)\,x + (-75257037\varphi - 46511406) \quad (1)$$

with conductor $-6\varphi + 42$, which has norm 1476. Just given the $a_{\mathfrak{p}}$, we noticed that $E[7] \approx E'[7]$, where E' has norm conductor 369. The curve E' had already been found via naïve search, since it is given by the equation $y^2 + (\varphi + 1)\,y = x^3 + (\varphi - 1)\,x^2 + (-2\varphi)\,x$. For any elliptic curve, the equation for the correct twist of $X(7)$ was found both by Halberstadt and Kraus [21] and by Fisher [18], whose methods also yield formulas for the appropriate twists of $X(9)$ and $X(11)$.

Fisher had already implemented Magma [6] routines to find ℓ-congruent elliptic curves over $\mathbb{Q}$ using these equations and was able to modify his work for $\mathbb{Q}(\sqrt{5})$. Fortunately, our curve E was then easily found.

3E. ***Twisting.*** Let E be an elliptic curve over F. A *twist* E' of E is an elliptic curve over F that is isomorphic to E over some extension of F. A *quadratic twist* is a twist in which the extension has degree 2. We can use twisting to find elliptic curves that may otherwise be difficult to find as follows: Starting with a known elliptic curve E of some (small) conductor, we compute its twists of conductor up to some bound, and add them to our table.

More explicitly, if E is given by $y^2 = x^3 + ax + b$ and $d \in F^*$, then the twist E^d of E by d is given by $dy^2 = x^3 + ax + b$; in particular, we may assume that d is squarefree. The following is well known:

Proposition 3.3. *If* $\mathfrak{n}$ *is the conductor of* E *and* $d \in \mathcal{O}_F$ *is nonzero, squarefree and coprime to* $\mathfrak{n}$, *then the conductor of* E^d *is divisible by* $d^2\mathfrak{n}$.

Proof. There are choices of Weierstrass equations such that $\Delta(E^d) = 2^{12}d^6\Delta(E)$, where Δ is the discriminant. Thus the elliptic curve E^d has bad reduction at each prime that divides d, because twisting introduces a 6th power of the squarefree d into the discriminant, and d is coprime to $\Delta(E)$, so no change of Weierstrass equation can remove this 6th power. Moreover, E^d is isomorphic to E over an extension of the base field, so E^d has potentially good reduction at each prime dividing d. Thus the reduction at each prime dividing d is additive. The conductor is unchanged at the primes dividing $\mathfrak{n}$ because of the formula relating the conductor, discriminant and reduction type (see [31, App. C,§15]), that formation of Néron models commutes with unramified base change, and the fact that at the primes that divide $\mathfrak{n}$ the minimal discriminant of E^d is the same as that of E. □

To find all twists E^d with norm conductor at most B, we twist E by all d of the form $\pm\varphi^\delta d_0 d_1$, where $\delta \in \{0, 1\}$, d_0 is a product of a fixed choice of generators for the prime divisors of $\mathfrak{n}$, d_1 is a squarefree product of a fixed choice of generators of

primes not dividing $\mathfrak{n}$, and $|N(d_1)| \leq \sqrt{B/C}$, where C is the norm of the product of the primes that exactly divide $\mathfrak{n}$. We know from 3.3 that this search is exhaustive.

For example, let E be given by $y^2 + xy + \varphi y = x^3 + (-\varphi - 1)\,x^2$ of conductor $5\varphi - 3$ having norm 31. Following the above strategy to find twists of norm conductor $\leq B := 1831$, we have $C = 31$ and squarefree d_1 such that $|N(d_1)| \leq \sqrt{B/C} \approx 7.6\ldots$. Thus $d_1 \in \{1, 2, \varphi, 2\varphi\}$ and checking all possibilities for $\varphi^\delta d_0 d_1$, we find the elliptic curve $E^{-\varphi-2}$ having norm conductor 775 and the elliptic curve $E^{5\varphi-3}$ having norm conductor 961. Other twists have larger norm conductors; for example, E^2 has norm conductor $126976 = 2^{12} \cdot 31$.

3F. ***Elliptic Curves with good reduction outside S.*** We use the algorithm of Cremona and Lingham from [11] to find all elliptic curves E having good reduction at primes outside of a finite set $\mathcal{S}$ of primes in F. This algorithm has limitations over a general number field K due to the difficulty of finding a generating set for $E(K)$ and points on E defined over $\mathcal{O}_K$. Using Cremona's Magma implementation of the algorithm, we found several elliptic curves not found by other methods, for example, $y^2 + (\varphi + 1)\,xy + y = x^3 - x^2 + (-19\varphi - 39)\,x + (-143\varphi - 4)$, which has norm conductor 1331.

3G. ***Special values of twisted L-series.*** In [15], Lassina Dembélé outlines some methods for finding modular elliptic curves from Hilbert modular forms over real quadratic fields. Formally, these methods are not proven to be any better than a direct search procedure, as they involve making a large number of guesses, and a priori we do not know just how many guesses we will need to make. And unlike other methods described in this paper, this method requires many Hecke eigenvalues, and computing these takes a lot of time. However, this method certainly works extremely well in many cases, and after tuning it by using large tables of elliptic curves that we had already computed, we are able to use it to find more elliptic curves that we would have had no hope of finding otherwise; we will give an example of one of these elliptic curves later.

When the level $\mathfrak{n}$ is not square, Dembélé's method relies on computing or guessing periods of the elliptic curve by using special values of L-functions of twists of the elliptic curve. In particular, the only inputs required are the level of the Hilbert modular form and its L-series. So we suppose that we know the level $\mathfrak{n} = (N)$ of the form, where N is totally positive, and that we have sufficiently many coefficients of its L-series $a_{\mathfrak{p}_1}, a_{\mathfrak{p}_2}, a_{\mathfrak{p}_3}, \ldots$.

Let σ_1 and σ_2 denote the embeddings of F into the real numbers, with $\sigma_1(\varphi) \approx 1.61803\ldots$. For an elliptic curve E over F we get two associated embeddings into the complex numbers, and hence a pair of period lattices. Let Ω_E^+ denote the smallest positive real period corresponding to the embedding σ_1, and similarly define Ω_E^- to be the smallest period which lies on the positive imaginary axis. We

will refer to these as the periods of E, and as the period lattices are interchanged when E is replaced with its conjugate elliptic curve, we let $\Omega_{\overline{E}}^{+}$ and $\Omega_{\overline{E}}^{-}$ denote the least real and imaginary periods of the lattice under the embedding σ_2.

For ease, we write

$$\Omega_E^{++} = \Omega_E^{+}\Omega_{\overline{E}}^{+} \qquad \Omega_E^{+-} = \Omega_E^{+}\Omega_{\overline{E}}^{-}$$
$$\Omega_E^{-+} = \Omega_E^{-}\Omega_{\overline{E}}^{+} \qquad \Omega_E^{--} = \Omega_E^{-}\Omega_{\overline{E}}^{-}.$$

We refer to these numbers as the *mixed periods* of E.

3G.1. *Recovering the elliptic curve from its mixed periods.* If we know these mixed periods to sufficient precision, it is not hard to recover the elliptic curve E. Without the knowledge of the discriminant of the elliptic curve, we do not know the lattice type of the elliptic curve and its conjugate, but there are only a few possibilities for what they might be. This gives us a few possibilities for the j-invariant of E. Observe that $\sigma_1(j(E))$ is either $j(\tau_1(E))$ or $j(\tau_2(E))$ and $\sigma_2(j(E))$ is either $j(\tau_1(\overline{E}))$ or $j(\tau_2(\overline{E}))$, where

$$\tau_1(E) = \frac{\Omega_E^{-+}}{\Omega_E^{++}} = \frac{\Omega_E^{-}}{\Omega_E^{+}} \qquad \tau_2(E) = \frac{1}{2}\left(1 + \frac{\Omega_E^{-+}}{\Omega_E^{++}}\right) = \frac{1}{2}\left(1 + \frac{\Omega_E^{-}}{\Omega_E^{+}}\right)$$
$$\tau_1(\overline{E}) = \frac{\Omega_E^{+-}}{\Omega_E^{++}} = \frac{\Omega_E^{-}}{\Omega_E^{+}} \qquad \tau_2(\overline{E}) = \frac{1}{2}\left(1 + \frac{\Omega_E^{+-}}{\Omega_E^{++}}\right) = \frac{1}{2}\left(1 + \frac{\Omega_{\overline{E}}^{-}}{\Omega_{\overline{E}}^{+}}\right)$$

and $j(\tau)$ is the familiar

$$j(\tau) = e^{-2\pi i\tau} + 744 + 196884e^{2\pi i\tau} + 21493760e^{4\pi i\tau} + \cdots.$$

We try each pair of possible embeddings for $j(E)$ in turn, and recognize possibilities for $j(E)$ as an algebraic number. We then construct elliptic curves E' corresponding to each possibility for $j(E)$. By computing a few $a_{\mathfrak{p}}(E)$, we should be able to determine whether we have chosen the correct j-invariant, in which case E' will be a twist of E. We can then recognize which twist it is in order to recover E.

In practice, of course, as we have limited precision, and as $j(E)$ will not be an algebraic integer, it may not be feasible to directly determine its exact value, especially if its denominator is large.

To get around the problem of limited precision, we suppose that we have some extra information; namely, the discriminant Δ_E of the elliptic curve we are looking for. With Δ_E in hand we can directly determine which τ to choose: If $\sigma_1(\Delta_E) > 0$ then $\sigma_1(j(E)) = j(\tau_1(E))$, and if $\sigma_1(\Delta_E) < 0$ then $\sigma_1(j(E)) = j(\tau_2(E))$, and similarly for σ_2. We then compute $\sigma_1(c_4(E)) = (j(\tau)\sigma_1(\Delta_E))^{1/3}$ and $\sigma_2(c_4(E)) = (j(\tau')\sigma_2(\Delta_E))^{1/3}$.

Using the approximations of the two embeddings of c_4, we can recognize c_4 approximately as an algebraic integer. Specifically, we compute

$$\alpha = \frac{\sigma_1(c_4) + \sigma_2(c_4)}{2} \quad \text{and} \quad \beta = \frac{\sigma_1(c_4) - \sigma_2(c_4)}{2\sqrt{5}}.$$

Then $c_4 = \alpha + \beta\sqrt{5}$, and we can find c_6.

In practice, there are two important difficulties we must overcome: We do not know Δ_E and it may be quite difficult to get high precision approximations to the mixed periods, and thus we may not be able to easily compute c_4. Thus, we actually proceed by choosing a Δ_{guess} from which we compute half-integers α and β and an integer $a + b\varphi \approx \alpha + \beta\sqrt{5}$, arbitrarily rounding either a or b if necessary. We then make some choice of search range M, and for each pair of integers m and n, bounded in absolute value by M, we try each $c_{4,\text{guess}} = (a+m) + (b+n)\varphi$.

Given $c_{4,\text{guess}}$, we attempt to solve

$$c_{6,\text{guess}} = \pm\sqrt{c_{4,\text{guess}}^3 - 1728\Delta_{\text{guess}}},$$

and, if we can, we use these to construct a elliptic curve E_{guess}. If E_{guess} has the correct conductor and the correct Hecke eigenvalues, we declare that we have found the correct elliptic curve; otherwise, we proceed to the next guess.

For a choice of Δ_{guess}, we will generally start with the conductor N_E, and then continue by trying unit multiples and by adding in powers of factors of N_E.

3G.2. *Guessing the mixed periods.* We have thus far ignored the issue of actually finding the mixed periods of the elliptic curve that we are looking for. Finding them presents an extra difficulty as our procedure involves even more guesswork. Dembélé's idea is to use special values of twists of the L-function $L(f,s)$. Specifically, we twist by primitive quadratic Dirichlet characters over $\mathcal{O}_F$, which are homomorphisms $\chi\colon (\mathcal{O}_F/\mathfrak{c})^* \to \pm 1$, pulled back to $\mathcal{O}_F$.

In the case of odd prime conductor, which we will stick to here, there is just a single primitive quadratic character, which is the quadratic residue symbol. A simple way to compute it is by making a table of squares, or by choosing a primitive root of $g \in (\mathcal{O}_F/\mathfrak{c})^*$, assigning $\chi(g) = -1$, and again making a table by extending multiplicatively. Alternatively, one could use a reciprocity formula as described in [7]. For general conductor, one can compute with products of characters having prime conductor.

For a given f and a primitive χ, we can construct the twisted L-function

$$L(f,\chi,s) = \sum_{\mathfrak{m}\subseteq\mathcal{O}_F} \frac{\chi(m)a_{\mathfrak{m}}}{N(\mathfrak{m})^s},$$

where m is a totally positive generator of $\mathfrak{m}$. (Note that χ is not well defined

on ideals, but *is* well defined on totally positive generators of ideals.) $L(f, \chi, s)$ will satisfy a functional equation similar to that of $L(f, s)$, but the conductor is multiplied by $\mathrm{Norm}(\mathfrak{c})^2$ and the sign is multiplied by $\chi(-N)$.

Oda [28] conjectured relations between the periods of f and the associated elliptic curve E and gave some relations between the periods of f and central values of $L(s, \chi, 1)$. Stronger versions of these relations are conjectured, and they are what Dembélé uses to obtain information about the mixed periods of E. Specifically, Dembélé distills the following conjecture from [2], which we further simplify to state specifically for $\mathbb{Q}(\sqrt{5})$.

Conjecture 3.4. *If χ is a primitive quadratic character with conductor $\mathfrak{c}$ relatively prime to the conductor of E, with $\chi(\varphi) = s'$ and $\chi(1-\varphi) = s$, (where $s, s' \in \{+, -\} = \{\pm 1\}$), then*

$$\Omega_E^{s,s'} = c_\chi \tau(\overline{\chi}) L(E, \chi, 1)\sqrt{5},$$

for some integer c_χ, where $\tau(\chi)$ is the Gauss sum

$$\tau(\chi) = \sum_{\alpha \bmod \mathfrak{c}} \chi(\alpha) \exp\left(2\pi i \,\mathrm{Tr}\left(\alpha/m\sqrt{5}\right)\right),$$

with m a totally positive generator of $\mathfrak{c}$.

Remark. The Gauss sum is more innocuous than it seems. For odd conductor $\mathfrak{c}$ it is of size $\sqrt{\mathrm{Norm}(\mathfrak{c})}$, while for an even conductor it is of size $\sqrt{2\,\mathrm{Norm}(\mathfrak{c})}$. Its sign is a 4-th root of unity, and whether it is real or imaginary can be deduced directly from the conjecture, as it matches with the sign of $\Omega_E^{s,s'}$. In particular, $\tau(\chi)$ is real when $\chi(-1) = 1$ and imaginary when $\chi(-1) = -1$, which is a condition on $\mathrm{Norm}(\mathfrak{c}) \bmod 4$, as $\chi(-1) \equiv \mathrm{Norm}(\mathfrak{c}) \pmod 4$. This can all be deduced, for example, from [7].

Also, note that Dembélé writes this conjecture with an additional factor of $4\pi^2$; this factor does not occur with the definition of $L(f, s)$ that we have given.

Remark. Contained in this conjecture is the obstruction to carrying out the method described here when $\mathfrak{n}$ is a square. If the sign of the functional equation of $L(f, s)$ is ϵ_f, then the sign of $L(f, \chi, s)$ will be $\chi(-N)\epsilon_f$. When $\mathfrak{n}$ is a perfect square, this is completely determined by whether or not $\chi(\varphi) = \chi(1-\varphi)$, so we can only obtain information about either Ω^{--} and Ω^{++} or Ω^{-+} and Ω^{+-}, and we need three of these values to find E.

With this conjecture in place, we can describe a method for guessing the mixed periods of E. Now, to proceed, we construct four lists of characters up to some conductor bound M (we are restricting to odd prime modulus here for simplicity,

as primitivity is ensured, but this is not necessary):

$$S^{s,s'} = \{\chi \bmod \mathfrak{p} : \chi(\varphi) = s',\ \chi(1-\varphi) = s,\ (\mathfrak{p}, \mathfrak{n}) = 1, \mathrm{Norm}(\mathfrak{p}) < M,\ \chi(-N) = \epsilon_f\}.$$

Here $s, s' \in \{+,-\} = \{\pm 1\}$ again, and we restrict our choice of characters to force the functional equation of $L(s, \chi, f)$ to have positive sign so that there is a good chance that it does not vanish as the central point. We will consider these lists to be ordered by the norms of the conductors of the characters in increasing order, and index their elements as $\chi_0^{s,s'}, \chi_1^{s,s'}, \chi_2^{s,s'}, \ldots$. For each character we compute the central value of the twisted L-function to get four new lists

$$\mathcal{L}^{s,s'} = \{i^{ss'}\sqrt{5\,\mathrm{Norm}(\mathfrak{p})}L(E, \chi, 1), \chi \in S^{s,s'}\} = \{\mathcal{L}_0^{s,s'}, \mathcal{L}_1^{s,s'}, \ldots\}.$$

These numbers should now all be integer multiples of the mixed periods, so to get an idea of which integer multiples they might be, we compute each of the ratios

$$\frac{\mathcal{L}_0^{s,s'}}{\mathcal{L}_k^{s,s'}} = \frac{c_{\chi_0^{s,s'}}}{c_{\chi_k^{s,s'}}} \in \mathbb{Q}, \quad k = 1, 2, \ldots,$$

attempt to recognize these as rational numbers, and choose as an initial guess

$$\Omega_{E,\mathrm{guess}}^{ss'} = \mathcal{L}_0^{s,s'}\left(\ \mathrm{lcm}\left\{\ \mathrm{numerator}\left(\frac{\mathcal{L}_0^{s,s'}}{\mathcal{L}_k^{s,s'}}\right)\ :\ k = 1, 2, \ldots\right\}\right)^{-1}.$$

3G.3. *An example.* We give an example of an elliptic curve that we were only able to find by using this method. At level $\mathfrak{n} = (-38\varphi + 26)$ we found a newform f, computed

$$\begin{aligned} a_{(2)}(f) &= -1, \qquad a_{(-2\varphi+1)}(f) = 1, \\ a_{(3)}(f) &= -1, \qquad a_{(-3\varphi+1)}(f) = -1, \quad a_{(-3\varphi+2)}(f) = -6, \\ &\ldots, \\ a_{(200\varphi-101)}(f) &= 168, \end{aligned}$$

and determined, by examining the L-function, that the sign of the functional equation should be -1. (In fact, we do not really need to know the sign of the functional equation, as we would quickly determine that $+1$ is wrong when attempting to find the mixed periods.) Computing the sets of characters described above, and choosing the first 3 of each, we have

$$\begin{aligned} S^{--} &= \{\chi_{(\varphi+6)}, \chi_{(7)}, \chi_{(7\varphi-4)}\}, & S^{-+} &= \{\chi_{(-3\varphi+1)}, \chi_{(5\varphi-2)}, \chi_{(\varphi-9)}\} \\ S^{+-} &= \{\chi_{(-4\varphi+3)}, \chi_{(5\varphi-3)}, \chi_{(-2\varphi+13)}\} & S^{++} &= \{\chi_{(\varphi+9)}, \chi_{(9\varphi-5)}, \chi_{(\varphi+13)}\}. \end{aligned}$$

By using the 5133 eigenvalues above as input to Rubinstein's `lcalc` [29], we compute the lists of approximate values

$$\begin{aligned}
\mathcal{L}^{--} &= \{-33.5784397862407,\ -3.73093775400387,\ -18.6546887691646\ \},\\
\mathcal{L}^{-+} &= \{\ 18.2648617736017i,\ 32.8767511924831i,\ 3.65297235421633i\},\\
\mathcal{L}^{+-} &= \{\ 41.4805656925342i,\ 8.29611313850694i,\ 41.4805677827298i\ \},\\
\mathcal{L}^{++} &= \{\ 32.4909970742969,\ 162.454985515474,\ 162.454973589303\ \}.
\end{aligned}$$

Note that `lcalc` will warn us that we do not have enough coefficients to obtain good accuracy, and we make no claim as far as the accuracy of these values is concerned. Hoping that the ends will justify the means, we proceed forward.

Dividing each list by the first entry, and recognizing the quotients as rational numbers, we get the lists

$$\begin{aligned}
&\{1.000,\ 9.00000000005519,\ \ 1.80000000009351\ \} \approx \{1, 9, 9/5\},\\
&\{1.000,\ 0.555555555555555,\ 5.00000000068986\ \} \approx \{1, 5/9, 5\},\\
&\{1.000,\ 4.99999999999994,\ \ 0.999999949610245\} \approx \{1, 5, 1\},\\
&\{1.000,\ 0.199999999822733,\ 0.200000014505165\} \approx \{1, 1/5, 1/5\},
\end{aligned}$$

which may give an indication of the accuracy of our values. We now proceed with the guesses

$$\begin{aligned}
\Omega^{--}_{E,\mathrm{guess}} &\approx -33.5784397862407/9 \approx -3.73093775402141,\\
\Omega^{-+}_{E,\mathrm{guess}} &\approx\ \ 18.2648617736017i/5 \approx\ \ 3.65297235472034i,\\
\Omega^{+-}_{E,\mathrm{guess}} &\approx\ \ 41.4805656925342i/5 \approx\ \ 8.29611313850683i,\\
\Omega^{++}_{E,\mathrm{guess}} &\approx\ \ 32.4909970742969\ \ \ \ = 32.4909970742969.
\end{aligned}$$

These cannot possibly be all correct, as $\Omega_E^{--}\Omega_E^{++} = \Omega_E^{-+}\Omega_E^{+-}$. Still, we can choose any three and get a reasonable guess, and in fact we may choose all possible triples, dividing some of the guesses by small rational numbers, and choosing the fourth guess to be consistent with the first three; we build a list of possible embeddings of $j(E)$, which will contain the possibility $\sigma_1(j(E)) \approx 1.365554233954 \times 10^{12}$, $\sigma_2(j(E)) \approx 221270.95861123$, which is a possibility if

$$\Omega_E^{-+} = \Omega^{-+}_{E,\mathrm{guess}},\quad \Omega_E^{+-} = \Omega^{+-}_{E,\mathrm{guess}},\quad \Omega_E^{-+} = \frac{\Omega^{-+}_{E,\mathrm{guess}}}{2},\quad \Omega_E^{++} = \frac{\Omega^{++}_{E,\mathrm{guess}}}{8}.$$

Cycling through many discriminants, we eventually try

$$\Delta_{\mathrm{guess}} = \varphi \cdot 2^5 \cdot (19\varphi - 13),$$

which leads us to the guess

$$\sigma_1(c_{4,\text{guess}}) = (\sigma_1(j(E))\sigma_1(\Delta_{\text{guess}}))^{1/3} \approx 107850.372979378,$$
$$\sigma_2(c_{4,\text{guess}}) = (\sigma_2(j(E))\sigma_2(\Delta_{\text{guess}}))^{1/3} \approx 476.625892034286.$$

We have enough precision to easily recognize this as

$$c_{4,\text{guess}} = \frac{108327 + 48019\sqrt{5}}{2} = 48019\varphi + 30154,$$

and

$$\sqrt{c_{4,\text{guess}}^3 - 1728\Delta_{\text{guess}}}$$

does in fact have two square roots: $\pm(15835084\varphi + 9796985)$. We try both of them, and the choice with the minus sign gives the elliptic curve

$$y^2 + \varphi xy + \varphi y = x^3 + (\varphi - 1)\,x^2 + (-1001\varphi - 628)\,x + (17899\varphi + 11079)\,,$$

which has the correct conductor. We compute a few values of $a_{\mathfrak{p}}$ for this elliptic curve, and it turns out to be the one that we are looking for.

4. Enumerating the elliptic curves in an isogeny class

Given an elliptic curve E/F, we wish to find representatives up to isomorphism for all elliptic curves E'/F that are isogenous to E via an isogeny defined over F. The analogue of this problem over $\mathbb{Q}$ has an algorithmic solution as explained in [10, §3.8]; it relies on:

(1) Mazur's theorem [27] that if $\psi\colon E \to E'$ is a $\mathbb{Q}$-rational isogeny of prime degree, then $\deg(\psi) \leq 163$.

(2) Formulas of Vélu [34] that provide a way to explicitly enumerate all p-isogenies (if any) with domain E. Vélu's formulas are valid for any number field, but so far there has not been an explicit generalization of Mazur's theorem for any number field other than $\mathbb{Q}$.

Remark. Assume the generalized Riemann hypothesis. Then work of Larson and Vaintrob from [26] implies that there is an effectively computable constant C_F such that if $\varphi\colon E \to E'$ is a prime-degree isogeny defined over F and E' and E are not isomorphic over F, then φ has degree at most C_F.

Since we are interested in specific isogeny classes, we can use the algorithm described in [3] that takes as input a specific non-CM elliptic curve E over a number field K, and outputs a provably finite list of primes p such that E might have a p-isogeny. The algorithm is particularly easy to implement in the case when K is a quadratic field, as explained in [3, §2.3.4]. Using this algorithm combined with

Vélu's formulas, we were able to enumerate *all* isomorphism classes of elliptic curves isogenous to the elliptic curves we found via the methods of Section 3, and thus divide our isogeny classes into isomorphism classes.

5. CM elliptic curves over F

In this section we make some general remarks about CM elliptic curves over F. The main surprise is that there are 31 distinct $\overline{\mathbb{Q}}$-isomorphism classes of CM elliptic curves defined over F, more than for any other quadratic field.

Proposition 5.1. *The field F has more isomorphism classes of CM elliptic curves than any other quadratic field.*

Proof. Let K be a quadratic extension of $\mathbb{Q}$. Let H_D denote the Hilbert class polynomial of the CM order $\mathcal{O}_D$ of discriminant D, so $H_D \in \mathbb{Q}[X]$ is the minimal polynomial of the j-invariant j_D of any elliptic curve $E = E_D$ with CM by $\mathcal{O}_D$. Since K is Galois, we have $j_D \in K$ if and only if H_D is either linear or quadratic with both roots in K. The D for which H_D is linear are the thirteen values $-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$. According to [9], the D for which H_D is quadratic are the following 29 discriminants:

$$-15, -20, -24, -32, -35, -36, -40, -48, -51, -52, -60,$$
$$-64, -72, -75, -88, -91, -99, -100, -112, -115, -123,$$
$$-147, -148, -187, -232, -235, -267, -403, -427.$$

By computing discriminants of these Hilbert class polynomials, we obtain Table 1. The claim follows because the $\mathbb{Q}(\sqrt{5})$ row is largest, containing 9 entries. There are thus $31 = 2 \cdot 9 + 13$ distinct CM j-invariants in $\mathbb{Q}(\sqrt{5})$. □

6. Related future projects

It would be natural to extend the tables to the first known elliptic curve of rank 3 over F, which may be the elliptic curve $y^2 + y = x^3 - 2x + 1$ of norm conductor $163^2 = 26569$. It would also be interesting to make a table in the style of [33], and compute analytic ranks of the large number of elliptic curves that we would find; this would benefit from Sutherland's `smalljac` program, which has very fast code for computing L-series coefficients. Some aspects of the tables could also be generalized to modular abelian varieties A_f attached to Hilbert modular newforms with not necessarily rational Hecke eigenvalues; in particular, we could enumerate the A_f up to some norm conductor, and numerically compute their analytic ranks.

K	D
$\mathbb{Q}(\sqrt{2})$	$-24, -32, -64, -88$
$\mathbb{Q}(\sqrt{3})$	$-36, -48$
$\mathbb{Q}(\sqrt{5})$	$-15, -20, -35, -40, -60, -75, -100, -115, -235$
$\mathbb{Q}(\sqrt{6})$	-72
$\mathbb{Q}(\sqrt{7})$	-112
$\mathbb{Q}(\sqrt{13})$	$-52, -91, -403$
$\mathbb{Q}(\sqrt{17})$	$-51, -187$
$\mathbb{Q}(\sqrt{21})$	-147
$\mathbb{Q}(\sqrt{29})$	-232
$\mathbb{Q}(\sqrt{33})$	-99
$\mathbb{Q}(\sqrt{37})$	-148
$\mathbb{Q}(\sqrt{41})$	-123
$\mathbb{Q}(\sqrt{61})$	-427
$\mathbb{Q}(\sqrt{89})$	-267

Table 1. Quadratic fields K and the values of D for which H_D has roots in K but not in $\mathbb{Q}$.

7. Tables

As explained in Sections 3 and 4, assuming Conjecture 1.1, we found the complete list of elliptic curves with norm conductor up to 1831, which is the first norm conductor of a rank 2 elliptic curve over F. The complete dataset can be downloaded from [5].

In each of the following tables #isom refers to the number of isomorphism classes of elliptic curves, #isog refers to the number of isogeny classes of elliptic curves, $\mathfrak{n}$ refers to the conductor of the given elliptic curve, $\boldsymbol{N}(\mathfrak{n})$ is the norm of the conductor, and Weierstrass equations are given in the form $[\![a_1, a_2, a_3, a_4, a_6]\!]$.

Table 2 gives the number of elliptic curves and isogeny classes we found. Note that in these counts we do not exclude conjugate elliptic curves, that is, if σ denotes

Rank	#Isog	#Isom	Smallest $\boldsymbol{N}(\mathfrak{n})$
0	745	2174	31
1	667	1192	199
2	2	2	1831
Total	1414	3368	—

Table 2. Number of isogeny classes and number of isomorphism classes of elliptic curves over F of norm conductor at most 1831.

	Size of isogeny class							
Bound on $N(\mathfrak{n})$	1	2	3	4	6	8	10	Total
199	2	21	3	20	8	9	1	64
1831	498	530	36	243	66	38	3	1414

Table 3. Number of isogeny classes of a given size for elliptic curves over F with norm conductors no larger than a given bound.

the nontrivial element of $\mathrm{Gal}(F/\mathbb{Q})$, then we count E and E^σ separately if they are not isomorphic.

Table 3 gives counts of the number of isogeny classes of elliptic curves in our data of each size; note that we find some isogeny classes of cardinality 10, which is bigger than what one observes with elliptic curves over $\mathbb{Q}$.

Table 4 gives the number of elliptic curves and isogeny classes up to a given norm conductor bound. Note that the first elliptic curve of rank 1 has norm conductor 199, and there are no elliptic curves of norm conductor 200.

	#Isogeny classes				#Isomorphism classes			
	Rank				Rank			
Bound on $N(\mathfrak{n})$	0	1	2	Total	0	1	2	Total
200	62	2	0	64	257	6	0	263
400	151	32	0	183	580	59	0	639
600	246	94	0	340	827	155	0	982
800	334	172	0	506	1085	285	0	1370
1000	395	237	0	632	1247	399	0	1646
1200	492	321	0	813	1484	551	0	2035
1400	574	411	0	985	1731	723	0	2454
1600	669	531	0	1200	1970	972	0	2942
1800	729	655	0	1384	2128	1178	0	3306
1831	745	667	2	1414	2174	1192	2	3368

Table 4. Number of isogeny classes and number of isomorphism classes of elliptic curves over F with specified rank and with norm conductors no larger than a given bound.

Table 5 gives the number of elliptic curves and isogeny classes with isogenies of each degree; note that we do not see all possible isogeny degrees. For example, the elliptic curve $X_0(19)$ has rank 1 over F, so there are infinitely many elliptic curves over F with degree 19 isogenies (unlike over $\mathbb{Q}$ where $X_0(19)$ has rank 0). We

Type	#Isog	#Isom	Example curve	$N(\mathfrak{n})$
none	498	498	$[\![\varphi+1, 1, 1, 0, 0]\!]$	991
deg 2	652	2298	$[\![\varphi, -\varphi+1, 0, -4, 3\varphi-5]\!]$	99
deg 3	289	950	$[\![\varphi, -\varphi, \varphi, -2\varphi-2, 2\varphi+1]\!]$	1004
deg 5	65	158	$[\![1, 0, 0, -28, 272]\!]$	900
deg 7	19	38	$[\![0, \varphi+1, \varphi+1, \varphi-1, -3\varphi-3]\!]$	1025

Table 5. Number of isogeny classes and number of isomorphism classes of elliptic curves over F of norm conductor at most 1831 having isogenies of a given type. "None" indicates curves having no cyclic isogenies.

also give an example of an elliptic curve (that need not have minimal conductor) with an isogeny of the given degree.

Table 6 gives the number of elliptic curves with each torsion structure, along with an example of an elliptic curve (again, not necessarily with minimal conductor) with that torsion structure.

Group structure	#Isom	Example curve	$N(\mathfrak{n})$
0	796	$[\![0, -1, 1, -8, -7]\!]$	225
$\mathbb{Z}/2\mathbb{Z}$	1453	$[\![\varphi, -1, 0, -\varphi-1, \varphi-3]\!]$	164
$\mathbb{Z}/3\mathbb{Z}$	202	$[\![1, 0, 1, -1, -2]\!]$	100
$\mathbb{Z}/4\mathbb{Z}$	243	$[\![\varphi+1, \varphi-1, \varphi, 0, 0]\!]$	79
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	312	$[\![0, \varphi+1, 0, \varphi, 0]\!]$	256
$\mathbb{Z}/5\mathbb{Z}$	56	$[\![1, 1, 1, 22, -9]\!]$	100
$\mathbb{Z}/6\mathbb{Z}$	183	$[\![1, \varphi, 1, \varphi-1, 0]\!]$	55
$\mathbb{Z}/7\mathbb{Z}$	13	$[\![0, \varphi-1, \varphi+1, 0, -\varphi]\!]$	41
$\mathbb{Z}/8\mathbb{Z}$	21	$[\![1, \varphi+1, \varphi, \varphi, 0]\!]$	31
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	51	$[\![\varphi+1, 0, 0, -4, -3\varphi-2]\!]$	99
$\mathbb{Z}/9\mathbb{Z}$	6	$[\![\varphi, -\varphi+1, 1, -1, 0]\!]$	76
$\mathbb{Z}/10\mathbb{Z}$	12	$[\![\varphi+1, \varphi, \varphi, 0, 0]\!]$	36
$\mathbb{Z}/12\mathbb{Z}$	6	$[\![\varphi, \varphi+1, 0, 2\varphi-3, -\varphi+2]\!]$	220
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	11	$[\![0, 1, 0, -1, 0]\!]$	80
$\mathbb{Z}/15\mathbb{Z}$	1	$[\![1, 1, 1, -3, 1]\!]$	100
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	2	$[\![1, 1, 1, -5, 2]\!]$	45

Table 6. Number of isomorphism classes of elliptic curves over F of norm conductor at most 1831 having given torsion subgroups.

We computed the invariants in the Birch and Swinnerton-Dyer conjecture for our elliptic curves, and solved for the conjectural order of Ш; Table 7 gives the number of elliptic curves in our data having each order of Ш, and Table 8 lists elliptic curves of minimal conductor exhibiting each of these orders.

#Ш	1	4	9	16	25	36
#Isom	3191	84	43	16	2	2

Table 7. Number of isomorphism classes of elliptic curves over F of norm conductor at most 1831 having given order of Ш.

#Ш	First elliptic curve over F having Ш of this order	$N(\mathfrak{n})$
1	$[\![1, \varphi+1, \varphi, \varphi, 0]\!]$	31
4	$[\![1, 1, 1, -110, -880]\!]$	45
9	$[\![\varphi+1, -\varphi, 1, -54686\varphi-35336, -7490886\varphi-4653177]\!]$	76
16	$[\![1, \varphi, \varphi+1, -4976733\varphi-3075797, -6393196918\varphi-3951212998]\!]$	45
25	$[\![0, -1, 1, -7820, -263580]\!]$	121
36	$[\![1, -\varphi+1, \varphi, 1326667\varphi-2146665, 880354255\varphi-1424443332]\!]$	1580

Table 8. Elliptic curves over F of smallest norm conductor having Ш of a given order.

Acknowledgments

We would like to thank John Cremona, Noam Elkies, Tom Fisher, Richard Taylor, John Voight, and the anonymous referee for helpful conversations. We would especially like to thank Joanna Gaski for providing (via the method of Section 3A) the explicit table of elliptic curves that kickstarted this project. We used Sage [32] extensively throughout this project. This work was supported by NSF grant DMS-0757627, administered by the American Institute of Mathematics

References

[1] 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. MR 2009e:11107

[2] Massimo Bertolini, Henri Darmon, and Peter Green, *Periods and points attached to quadratic algebras*, in Darmon and Zhang [13], 2004, pp. 323–367. MR 2005e:11062

[3] Nicolas Billerey, *Critères d'irréductibilité pour les représentations des courbes elliptiques*, Int. J. Number Theory **7** (2011), no. 4, 1001–1032. MR 2012f:11109

[4] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable, IV: Proceedings of the International Summer School on Modular Functions of One Variable and Arithmetical Applications, RUCA, University of Antwerp, July 17–August 3, 1972*, Lecture Notes in Mathematics, no. 476, Springer, Berlin, 1975. MR 51 #12708

[5] Jon Bober, Alyson Deines, Ariah Klages-Mundt, Ben LeVeque, R. Andrew Ohana, Ashwath Rabindranath, Paul Sharaba, and William Stein, *A Database of Elliptic Curves over* $\mathbf{Q}(\sqrt{5})$, 2012. http://wstein.org/papers/sqrt5

[6] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR 1484478

[7] Hatice Boylan and Nils-Peter Skoruppa, *Explicit formulas for Hecke Gauss sums in quadratic number fields*, Abh. Math. Semin. Univ. Hambg. **80** (2010), no. 2, 213–226. MR 2012c:11163

[8] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: Wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939. MR 2002d:11058

[9] J. E. Cremona, *Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields*, J. London Math. Soc. (2) **45** (1992), no. 3, 404–416. MR 93h:11056

[10] ———, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, 1997. MR 99e:11068

[11] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. **16** (2007), no. 3, 303–312. MR 2008k:11057

[12] John Cremona, *Elliptic curve data*, 2012. http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html

[13] Henri Darmon and Shou-Wu Zhang (eds.), *Heegner points and Rankin L-series: Papers from the Workshop on Special Values of Rankin L-Series held in Berkeley, CA, December 2001*, Mathematical Sciences Research Institute Publications, no. 49, Cambridge University Press, Cambridge, 2004. MR 2005b:11002

[14] Lassina Dembélé, *Explicit computations of Hilbert modular forms on* $\mathbf{Q}(\sqrt{5})$, Experiment. Math. **14** (2005), no. 4, 457–466. MR 2006h:11050

[15] ———, *An algorithm for modular elliptic curves over real quadratic fields*, Experiment. Math. **17** (2008), no. 4, 427–438. MR 2010a:11119

[16] Tim Dokchitser, *Computing special values of motivic L-functions*, Experiment. Math. **13** (2004), no. 2, 137–149. MR 2005f:11128

[17] Claus Fieker and David R. Kohel (eds.), *Algorithmic number theory: Proceedings of the 5th International Symposium (ANTS-V) held at the University of Sydney, July 7–12, 2002*, Lecture Notes in Computer Science, no. 2369, Berlin, Springer, 2002. MR 2004j:11002

[18] T. A. Fisher, *On families of n-congruent elliptic curves*, 2011. https://www.dpmms.cam.ac.uk/~taf1000/papers/highercongr.html

[19] Matthew Greenberg and John Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms*, Math. Comp. **80** (2011), no. 274, 1071–1092. MR 2012c:11103

[20] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. http://resolver.sub.uni-goettingen.de/purl?GDZPPN002102773 MR 87j:11057

[21] Emmanuel Halberstadt and Alain Kraus, *Sur la courbe modulaire* $X_E(7)$, Experiment. Math. **12** (2003), no. 1, 27–40. MR 2004m:11090

[22] Sheldon Kamienny and Filip Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta Arith. **152** (2012), no. 3, 291–305. MR 2885789

[23] Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502. MR 82d:14025

[24] Victor Alecsandrovich Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, in Satake [30], 1991, pp. 429–436. http://www.mathunion.org/ICM/ICM1990.1/Main/icm1990.1.0429.0436.ocr.pdf MR 93c:11046

[25] Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237. MR 55 #7910

[26] Eric Larson and Dmitry Vaintrob, *Determinants of Subquotients of Galois Representations Associated to Abelian Varieties*, 2011. arXiv 1110.0255 [math.NT]

[27] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR 80h:14022

[28] Takayuki Oda, *Periods of Hilbert modular surfaces*, Progress in Mathematics, no. 19, Birkhäuser, Boston, 1982. MR 83k:10057

[29] Michael O. Rubinstein, `lcalc`, 2012. http://code.google.com/p/l-calc/

[30] Ichirō Satake (ed.), *Proceedings of the International Congress of Mathematicians* (*Kyoto*, 1990), vol. 1, Tokyo, Mathematical Society of Japan, 1991. MR 92m:00054

[31] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, no. 106, Springer, Dordrecht, 2009. MR 2010i:11005

[32] W. A. Stein et al., *Sage Mathematics Software (version 4.8)*, The Sage Development Team, 2012. http://www.sagemath.org

[33] William A. Stein and Mark Watkins, *A database of elliptic curves—first report*, in Fieker and Kohel [17], 2002, pp. 267–275. MR 2005h:11113

[34] Jacques Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241. http://gallica.bnf.fr/ark:/12148/bpt6k56191248/f52.image MR 45 #3414

[35] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR 96d:11071

[36] Shouwu Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147. MR 2002g:11081

JONATHAN BOBER: `jwbober@math.washington.edu`
Department of Mathematics, University of Washington, Seattle, WA 98195-4350, United States
Current address: *Howard House, University of Bristol, Queens Avenue, Bristol, BS8 1SN, United Kingdom*
http://sage.math.washington.edu/home/bober/www/

ALYSON DEINES: `adeines@math.washington.edu`
Department of Mathematics, University of Washington, Amherst, MA 01002, United States
http://www.math.washington.edu/~adeines/Alyson_Deines/Welcome.html

ARIAH KLAGES-MUNDT: `aklagesmundt12@amherst.edu`
Department of Mathematics, Amherst College, 1555 Keefe Campus Center, Amherst, MA 01002, United States
https://www.amherst.edu/users/K/aklagesmundt12

BENJAMIN LEVEQUE: `ben.leveque@gmail.com`
Mathematics Department, Brown University, Providence, RI 02906, United States

R. ANDREW OHANA: `ohanar@math.washington.edu`
Department of Mathematics, University of Washington, Seattle, WA 98195, United States

ASHWATH RABINDRANATH: `ashwathr@umich.edu`
Department of Mathematics, University of Michigan, 2074 East Hall, 530 Church Street, Ann Arbor, MI 48109-1043, United States

PAUL SHARABA: `paul.sharaba@gmail.com`
Department of Mathematics, Cleveland State University, Cleveland, OH 44115, United States

WILLIAM STEIN: `wstein@uw.edu`

Department of Mathematics, University of Washington, 423 Padelford Hall, Seattle, WA 98195-4361, United States
http://www.williamstein.org

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS