Searching for [equations of] elliptic curves over $F = Q(\sqrt{5})$

Jonathan Bober
University of Washington

April 29, 2012

Problem of interest…

TURN THIS INPUT:

$(5\varphi - 2)$	$-3, -2, 2, -4, 4, 4, -4, -2, -2, 8, ?, -6, -6, 2, -4, 12, -2, 6,$
$(5\varphi - 3)$	$-3, -2, 2, 4, -4, -4, 4, -2, -2, ?, 8, -6, -6, 2, 12, -4, 6, -2,$
(6)	$?, -4, ?, 2, 2, 0, 0, 0, 0, -8, -8, 2, 2, 10, -10, -10, 2, 2, 12, 12$
$(\varphi + 6)$	$-2, -1, -4, 5, -2, 6, -1, 2, 9, 4, -10, 0, ?, -6, 4, -3, -8, 6, -$
$(\varphi - 7)$	$-2, -1, -4, -2, 5, -1, 6, 9, 2, -10, 4, ?, 0, -6, -3, 4, 6, -8, 9,$
$(6\varphi - 3)$	$-3, ?, ?, -4, -4, 4, 4, -2, -2, 0, 0, 10, 10, -14, -4, -4, -2,$
(7)	$0, -4, 5, -3, -3, 0, 0, 5, 5, 2, 2, 2, 2, ?, -10, -10, -8, -8, -8,$
$(\varphi - 8)$	$-1, ?, -2, 0, ?, -4, 8, 6, -6, 8, -4, 6, -6, 14, -12, 0, -10, 2, 0,$
$(\varphi + 7)$	$-1, ?, -2, ?, 0, 8, -4, -6, 6, -4, 8, -6, 6, 14, 0, -12, 2, -10, 0,$
(8)	$0, -2, 2, -4, -4, 4, 4, -2, -2, 0, 0, 2, 2, 10, 12, 12, -10, -10,$
$(\varphi + 8)$	$-1, 0, -2, 0, 0, 2, -4, 6, -6, 8, 2, 6, 12, -4, 6, -12, -10, -4, 6,$
$(\varphi - 9)$	$-1, 0, -2, 0, 0, -4, 2, -6, 6, 2, 8, 12, 6, -4, -12, 6, -4, -10, ?,$
$(8\varphi - 2)$	$?, -3, 1, 3, -6, ?, -7, -6, 3, 5, 5, 6, 6, -4, -12, 6, 8, 8, -9, 0$
$(8\varphi - 2)$	$?, 1, -5, -3, 2, ?, 5, -10, 5, 7, -3, 2, 2, 0, 0, 10, -8, 12, 7, -8$
$(8\varphi - 6)$	$?, -3, 1, -6, 3, -7, ?, 3, -6, 5, 5, 6, 6, -4, 6, -12, 8, 8, 0, -9$

INTO THIS OUTPUT:

$$
\begin{array}{lrcl}
(5\varphi-2) & y^2+xy+\varphi y & = & x^3+(\varphi+1)x^2+\varphi x \\
(5\varphi-3) & y^2+xy+\varphi y & = & x^3+(-\varphi-1)x^2 \\
(6) & y^2+(\varphi+1)xy+\varphi y & = & x^3+\varphi x^2 \\
(\varphi+6) & y^2+\varphi y & = & x^3+(-\varphi)x^2 \\
(\varphi-7) & y^2+(\varphi+1)y & = & x^3+(\varphi-1)x^2+(-\varphi) \\
(6\varphi-3) & y^2+xy+y & = & x^3+x^2+(-80)x+242 \\
(7) & y^2+y & = & x^3+(-\varphi+1)x^2+x \\
(\varphi-8) & y^2+xy+y & = & x^3+\varphi x^2+(\varphi-1)x \\
(\varphi+7) & y^2+xy+y & = & x^3+(-\varphi+1)x^2+(-\varphi)x \\
(8) & y^2 & = & x^3+(\varphi-1)x^2+(-\varphi)x \\
(\varphi+8) & y^2+\varphi xy+\varphi y & = & x^3+(\varphi+1)x^2+\varphi x \\
(\varphi-9) & y^2+(\varphi+1)xy+y & = & x^3+(\varphi-1)x^2 \\
(8\varphi-2) & y^2+\varphi xy+y & = & x^3+(-\varphi+1)x^2+(-1)x \\
(8\varphi-2) & y^2+xy+(\varphi+1)y & = & x^3+(-2\varphi-1)x \\
(8\varphi-6) & y^2+(\varphi+1)xy+y & = & x^3+(-\varphi-1)x
\end{array}
$$

Goal

INPUT: (L-functions of) Hilbert modular newforms over F of weight $(2, 2)$ with rational Hecke eigenvalues.

OUTPUT: (Isogeny classes of) Elliptic curves over F.

(**Implicit conjecture:** These sets are the "same thing".)

(**Weaker implicit conjecture:** INPUT $\longrightarrow$ OUTPUT.)

Short background over $\mathbb{Q}$

Over the rational numbers the equivalent problem is easy[1].

Algorithm

To obtain a list of all [isogeny/isomorphism classes of] elliptic curves over the rational numbers with conductor $< N$:

1. *Has John Cremona done it yet? If so, goto step 3; If not, continue to step 2.*
2. *Wait a little while, then go back to step* 1.
3. *Download John Cremona's tables.*

This is an effective version of the Eichler-Shimura construction.

[1] This means that someone else has already done all of the hard work.

INPUT AGAIN:

$(5\varphi-2)$	$-3, -2, 2, -4, 4, 4, -4, -2, -2, 8, ?, -6, -6, 2, -4, 12, -2, 6, -8$
$(5\varphi-3)$	$-3, -2, 2, 4, -4, -4, 4, -2, -2, ?, 8, -6, -6, 2, 12, -4, 6, -2, 0, -$
(6)	$?, -4, ?, 2, 2, 0, 0, 0, 0, -8, -8, 2, 2, 10, -10, -10, 2, 2, 12, 12$
$(\varphi+6)$	$-2, -1, -4, 5, -2, 6, -1, 2, 9, 4, -10, 0, ?, -6, 4, -3, -8, 6, -12,$
$(\varphi-7)$	$-2, -1, -4, -2, 5, -1, 6, 9, 2, -10, 4, ?, 0, -6, -3, 4, 6, -8, 9, -1$
$(6\varphi-3)$	$-3, ?, ?, -4, -4, 4, 4, -2, -2, 0, 0, 10, 10, -14, -4, -4, -2, -2, -$
(7)	$0, -4, 5, -3, -3, 0, 0, 5, 5, 2, 2, 2, 2, ?, -10, -10, -8, -8, -8, -8$
$(\varphi-8)$	$-1, ?, -2, 0, ?, -4, 8, 6, -6, 8, -4, 6, -6, 14, -12, 0, -10, 2, 0, 0$
$(\varphi+7)$	$-1, ?, -2, ?, 0, 8, -4, -6, 6, -4, 8, -6, 6, 14, 0, -12, 2, -10, 0, 0$
(8)	$0, -2, 2, -4, -4, 4, 4, -2, -2, 0, 0, 2, 2, 10, 12, 12, -10, -10, 8, 8$
$(\varphi+8)$	$-1, 0, -2, 0, 0, 2, -4, 6, -6, 8, 2, 6, 12, -4, 6, -12, -10, -4, 6, ?$
$(\varphi-9)$	$-1, 0, -2, 0, 0, -4, 2, -6, 6, 2, 8, 12, 6, -4, -12, 6, -4, -10, ?, 6$
$(8\varphi-2)$	$?, -3, 1, 3, -6, ?, -7, -6, 3, 5, 5, 6, 6, -4, -12, 6, 8, 8, -9, 0$
$(8\varphi-2)$	$?, 1, -5, -3, 2, ?, 5, -10, 5, 7, -3, 2, 2, 0, 0, 10, -8, 12, 7, -8$
$(8\varphi-6)$	$?, -3, 1, -6, 3, -7, ?, 3, -6, 5, 5, 6, 6, -4, 6, -12, 8, 8, 0, -9$

FIRST OBSERVATIONS:

$(5\varphi-2)$	$-3,-2,2,-4,4,4,-4,-2,-2,8,?,-6,-6,2,-4,12,-2,6,-8$
$(5\varphi-3)$	$-3,-2,2,4,-4,-4,4,-2,-2,?,8,-6,-6,2,12,-4,6,-2,0,-$
(6)	$?,-4,?,2,2,0,0,0,0,-8,-8,2,2,10,-10,-10,2,2,12,12$
$(\varphi+6)$	$-2,-1,-4,5,-2,6,-1,2,9,4,-10,0,?,-6,4,-3,-8,6,-12,$
$(\varphi-7)$	$-2,-1,-4,-2,5,-1,6,9,2,-10,4,?,0,-6,-3,4,6,-8,9,-1$
$(6\varphi-3)$	$-3,?,?,-4,-4,4,4,-2,-2,0,0,10,10,-14,-4,-4,-2,-2,-$
(7)	$0,-4,5,-3,-3,0,0,5,5,2,2,2,2,?,-10,-10,-8,-8,-8,-8$
$(\varphi-8)$	$-1,?,-2,0,?,-4,8,6,-6,8,-4,6,-6,14,-12,0,-10,2,0,0$
$(\varphi+7)$	$-1,?,-2,?,0,8,-4,-6,6,-4,8,-6,6,14,0,-12,2,-10,0,0$
(8)	$0,-2,2,-4,-4,4,4,-2,-2,0,0,2,2,10,12,12,-10,-10,8,8$
$(\varphi+8)$	$-1,0,-2,0,0,2,-4,6,-6,8,2,6,12,-4,6,-12,-10,-4,6,?$
$(\varphi-9)$	$-1,0,-2,0,0,-4,2,-6,6,2,8,12,6,-4,-12,6,-4,-10,?,6$
$(8\varphi-2)$	$?,-3,1,3,-6,?,-7,-6,3,5,5,6,6,-4,-12,6,8,8,-9,0$
$(8\varphi-2)$	$?,1,-5,-3,2,?,5,-10,5,7,-3,2,2,0,0,10,-8,12,7,-8$
$(8\varphi-6)$	$?,-3,1,-6,3,-7,?,3,-6,5,5,6,6,-4,6,-12,8,8,0,-9$

FIRST OBSERVATIONS:

$(5\varphi-2)$	$-3, -2, 2, -4, 4, 4, -4, -2, -2, 8, ?, -6, -6, 2, -4, 12, -2, 6, -8$
$(5\varphi-3)$	$-3, -2, 2, 4, -4, -4, 4, -2, -2, ?, 8, -6, -6, 2, 12, -4, 6, -2, 0, -$
(6)	$?, -4, ?, 2, 2, 0, 0, 0, 0, -8, -8, 2, 2, 10, -10, -10, 2, 2, 12, 12$
$(\varphi+6)$	$-2, -1, -4, 5, -2, 6, -1, 2, 9, 4, -10, 0, ?, -6, 4, -3, -8, 6, -12,$
$(\varphi-7)$	$-2, -1, -4, -2, 5, -1, 6, 9, 2, -10, 4, ?, 0, -6, -3, 4, 6, -8, 9, -1$
$(6\varphi-3)$	$-3, ?, ?, -4, -4, 4, 4, -2, -2, 0, 0, 10, 10, -14, -4, -4, -2, -2, -$
(7)	$0, -4, 5, -3, -3, 0, 0, 5, 5, 2, 2, 2, 2, ?, -10, -10, -8, -8, -8, -8$
$(\varphi-8)$	$-1, ?, -2, 0, ?, -4, 8, 6, -6, 8, -4, 6, -6, 14, -12, 0, -10, 2, 0, 0$
$(\varphi+7)$	$-1, ?, -2, ?, 0, 8, -4, -6, 6, -4, 8, -6, 6, 14, 0, -12, 2, -10, 0, 0$
(8)	$0, -2, 2, -4, -4, 4, 4, -2, -2, 0, 0, 2, 2, 10, 12, 12, -10, -10, 8, 8$
$(\varphi+8)$	$-1, 0, -2, 0, 0, 2, -4, 6, -6, 8, 2, 6, 12, -4, 6, -12, -10, -4, 6, ?$
$(\varphi-9)$	$-1, 0, -2, 0, 0, -4, 2, -6, 6, 2, 8, 12, 6, -4, -12, 6, -4, -10, ?, 6$
$(8\varphi-2)$	$?, -3, 1, 3, -6, ?, -7, -6, 3, 5, 5, 6, 6, -4, -12, 6, 8, 8, -9, 0$
$(8\varphi-2)$	$?, 1, -5, -3, 2, ?, 5, -10, 5, 7, -3, 2, 2, 0, 0, 10, -8, 12, 7, -8$
$(8\varphi-6)$	$?, -3, 1, -6, 3, -7, ?, 3, -6, 5, 5, 6, 6, -4, 6, -12, 8, 8, 0, -9$

FIRST OBSERVATIONS:

$(5\varphi - 2)$	$-3, -2, 2, -4, 4, 4, -4, -2, -2, 8, ?, -6, -6, 2, -4, 12, -2, 6, -8$
$(5\varphi - 3)$	$-3, -2, 2, 4, -4, -4, 4, -2, -2, ?, 8, -6, -6, 2, 12, -4, 6, -2, 0, -$
(6)	$?, -4, ?, 2, 2, 0, 0, 0, 0, -8, -8, 2, 2, 10, -10, -10, 2, 2, 12, 12$
$(\varphi + 6)$	$-2, -1, -4, 5, -2, 6, -1, 2, 9, 4, -10, 0, ?, -6, 4, -3, -8, 6, -12,$
$(\varphi - 7)$	$-2, -1, -4, -2, 5, -1, 6, 9, 2, -10, 4, ?, 0, -6, -3, 4, 6, -8, 9, -1$
$(6\varphi - 3)$	$-3, ?, ?, -4, -4, 4, 4, -2, -2, 0, 0, 10, 10, -14, -4, -4, -2, -2, -$
(7)	$0, -4, 5, -3, -3, 0, 0, 5, 5, 2, 2, 2, 2, ?, -10, -10, -8, -8, -8, -8$
$(\varphi - 8)$	$-1, ?, -2, 0, ?, -4, 8, 6, -6, 8, -4, 6, -6, 14, -12, 0, -10, 2, 0, 0$
$(\varphi + 7)$	$-1, ?, -2, ?, 0, 8, -4, -6, 6, -4, 8, -6, 6, 14, 0, -12, 2, -10, 0, 0$
(8)	$0, -2, 2, -4, -4, 4, 4, -2, -2, 0, 0, 2, 2, 10, 12, 12, -10, -10, 8, 8$
$(\varphi + 8)$	$-1, 0, -2, 0, 0, 2, -4, 6, -6, 8, 2, 6, 12, -4, 6, -12, -10, -4, 6, ?$
$(\varphi - 9)$	$-1, 0, -2, 0, 0, -4, 2, -6, 6, 2, 8, 12, 6, -4, -12, 6, -4, -10, ?, 6$
$(8\varphi - 2)$	$?, -3, 1, 3, -6, ?, -7, -6, 3, 5, 5, 6, 6, -4, -12, 6, 8, 8, -9, 0$
$(8\varphi - 2)$	$?, 1, -5, -3, 2, ?, 5, -10, 5, 7, -3, 2, 2, 0, 0, 10, -8, 12, 7, -8$
$(8\varphi - 6)$	$?, -3, 1, -6, 3, -7, ?, 3, -6, 5, 5, 6, 6, -4, 6, -12, 8, 8, 0, -9$

So curves (usually) occur in conjugate pairs.

(Some will be self-conjugate.)

This at least makes our job 50% easier.

First attempts…

Naive enumeration

The first thing one might try, to find the curves that we are looking for, is to just start writing down curves.

Procedure

To find all elliptic curves with norm-conductor $< N$, make a table of all Hilbert modular forms with norm-conductor $< N$, then list all curves

$$y^2 = x^3 + ax + b$$

with $a, b < B$, compute the conductors of these curves. Whenever the conductor has norm $< N$, compute the L-series and see if it is in the table. Increase B until finished.

This procedure is guaranteed to finish eventually, but if N is moderately large, **will it finish before the Earth is swallowed into the Sun?**

Example limits of naive enumeration

- Stein and Watkins found 136,832,795 curves with $|\Delta| < 10^{12}$ and $N < 10^8$ through a somewhat less naive search procedure.
- This dataset contains 661855 isogeny classes with conductor < 200000, while in fact there are 876914 isogeny classes in this range.
- So this misses 215059 isogeny classes with conductor < 200000, or around 24.5%.

Example limits of naive enumeration

- Some of the missing conductors are quite small! First missing curve (174a1) is

$$y^2 + xy + y = x^3 - 7705x + 1226492,$$

which has conductor 174.

- The list of conductors for which there are missing isogeny classes is 174, 222, 273, 291, 330, 354, 357, 390, 420, 442, 462, 493, 522, 546, 570, 574, 606, 616, 645, 658, 666, 690, 714, 740, 741, 742, 762, 777, 780, 786, 805, 806, 819, 830, 834, 858, 861, 873, 874, 886, 897, 901, 902, 906, 910, 924, 930, 940, 942, 966, 970, 978, 986, 987, 988, 990, 1001, 1012, 1015, 1020, 1034, 1062, 1070, 1071, 1085, 1090, 1092, 1102, 1110, 1120, 1122, 1128, 1155, 1158, 1170, 1173, 1178, 1185, 1194, 1218, 1230, 1232, 1242, 1245, 1246, 1254, 1260, 1281, 1288, 1290, 1295, 1302, 1326, 1330, 1334, 1340, 1349, 1356, 1378, 1380, 1386, 1392, 1394, 1406, 1407, 1410, 1428, 1430, 1462, 1479, 1482, 1490, 1495, 1498, 1506, 1512, 1518, 1524, 1526, 1530, 1558, 1560, 1586, 1590, 1596, 1610, 1612, 1634, 1638, 1640, 1641,

A less naive search…

Sieving

For a given prime $\mathfrak{p}$, there are only finitely many elliptic curves over $\mathcal{O}_F/\mathfrak{p}$. If we are looking for a curve with given $a_\mathfrak{p}$, we can write down all of these curves over $\mathcal{O}_F/\mathfrak{p}$, and keep just the ones with the $a_\mathfrak{p}$ that we are looking for.

Lifting these curves to F now gives a much more efficient search procedure than the process of searching through every single curve.

We can also improve this method by specifying multiple $a_\mathfrak{p}$ at a time and using the Chinese Remainder Theorem to work over $\mathcal{O}_F/\prod \mathfrak{p}$.

- This process seems to work surprisingly well in practice.
- 7/21/2011, 12:17 p.m. email from William Stein: “I don’t think this works at all in practice, since most (=1-eps) of the lifts will have enormous conductor.”
- 7/21/2011, 4:38 p.m. email from Andrew Ohana: “We found the curve of norm conductor 179!!!: [a+1,1,a,-15*a-11,-50*a-33]”

Some important points to make this method fast.

- To keep coefficients relatively small, don't search for curves in short Weierstrass form, but instead search for a minimal model directly.
- We know the conductor of the curve that we are looking for, so for a candidate curve first compute the discriminant and check if the conductor could be the one that we want.
- (Computing the conductor is really slow, but checking if the conductor is a certain value can be pretty fast.)

At this point, if we have done things properly, we have found a pretty good percentage of the curves that we are looking for. (50 to 90%?) (We haven't pushed this sieving as far as it can go, or used it really systematically, so I don't know just how effective it is.)

To move forward, we will have to turn to other methods which are either more specialized or more difficult.

But first, we can use the curves that we already know about to find a few more.

Twisting

We can get a few new curves from the curves that we already have by twisting.

Proposition

If E, with conductor $\mathfrak{n}$, is given by the equation $y^2 = x^3 + ax + b$ and $d \in F^*$ is relatively prime to $\mathfrak{n}$, then the curve

$$dy^2 = x^3 + ax + b$$

has conductor divisible by $d\mathfrak{n}$.

This means that if we are looking for all curves with norm conductor $\leq B$, and we know a curve E with norm conductor C, we should twist E by all d with $\mathrm{Norm}(d) \leq \sqrt{B/C}$.
The set of new curves that we get this way is somewhat small, as the conductors grow rather quickly, but we can get these curves with (almost) no additional work.

As discussed a bit yesterday, we can sometimes get complete lists of curves using only information about the discriminant.

Good reduction outside a finite set

Given a finite set of primes S, there are only finitely many elliptic curves with good redution outside S, and there is an algorithm of Cremona and Lingham that should, in principle, determine this set of curves.

In particular, this would give a way to list all curves of a given conductor.

However, the algorithm involves requires finding all S-integral points on some elliptic curves $y^2 = x^3 + k$, which currently limits its effectivity.

Look at input again:

$(5\varphi-2)$	$-3, -2, 2, -4, 4, 4, -4, -2, -2, 8, ?, -6, -6, 2, -4, 12, -2, 6, -8$
$(5\varphi-3)$	$-3, -2, 2, 4, -4, -4, 4, -2, -2, ?, 8, -6, -6, 2, 12, -4, 6, -2, 0, -$
(6)	$?, -4, ?, 2, 2, 0, 0, 0, 0, -8, -8, 2, 2, 10, -10, -10, 2, 2, 12, 12$
$(\varphi+6)$	$-2, -1, -4, 5, -2, 6, -1, 2, 9, 4, -10, 0, ?, -6, 4, -3, -8, 6, -12,$
$(\varphi-7)$	$-2, -1, -4, -2, 5, -1, 6, 9, 2, -10, 4, ?, 0, -6, -3, 4, 6, -8, 9, -1$
$(6\varphi-3)$	$-3, ?, ?, -4, -4, 4, 4, -2, -2, 0, 0, 10, 10, -14, -4, -4, -2, -2, -$
(7)	$0, -4, 5, -3, -3, 0, 0, 5, 5, 2, 2, 2, 2, ?, -10, -10, -8, -8, -8, -8$
$(\varphi-8)$	$-1, ?, -2, 0, ?, -4, 8, 6, -6, 8, -4, 6, -6, 14, -12, 0, -10, 2, 0, 0$
$(\varphi+7)$	$-1, ?, -2, ?, 0, 8, -4, -6, 6, -4, 8, -6, 6, 14, 0, -12, 2, -10, 0, 0$
(8)	$0, -2, 2, -4, -4, 4, 4, -2, -2, 0, 0, 2, 2, 10, 12, 12, -10, -10, 8, 8$
$(\varphi+8)$	$-1, 0, -2, 0, 0, 2, -4, 6, -6, 8, 2, 6, 12, -4, 6, -12, -10, -4, 6, ?$
$(\varphi-9)$	$-1, 0, -2, 0, 0, -4, 2, -6, 6, 2, 8, 12, 6, -4, -12, 6, -4, -10, ?, 6$
$(8\varphi-2)$	$?, -3, 1, 3, -6, ?, -7, -6, 3, 5, 5, 6, 6, -4, -12, 6, 8, 8, -9, 0$
$(8\varphi-2)$	$?, 1, -5, -3, 2, ?, 5, -10, 5, 7, -3, 2, 2, 0, 0, 10, -8, 12, 7, -8$
$(8\varphi-6)$	$?, -3, 1, -6, 3, -7, ?, 3, -6, 5, 5, 6, 6, -4, 6, -12, 8, 8, 0, -9$

ANOTHER OBSERVATION:

$(5\varphi - 2)$ $-3, -2, 2, -4, 4, 4, -4, -2, -2, 8, ?, -6, -6, 2, -4, 12, -2, 6, -8$

$(5\varphi - 3)$ $-3, -2, 2, 4, -4, -4, 4, -2, -2, ?, 8, -6, -6, 2, 12, -4, 6, -2, 0, -$

(6) $?, -4, ?, 2, 2, 0, 0, 0, 0, -8, -8, 2, 2, 10, -10, -10, 2, 2, 12, 12$

$(\varphi + 6)$ $-2, -1, -4, 5, -2, 6, -1, 2, 9, 4, -10, 0, ?, -6, 4, -3, -8, 6, -12,$

$(\varphi - 7)$ $-2, -1, -4, -2, 5, -1, 6, 9, 2, -10, 4, ?, 0, -6, -3, 4, 6, -8, 9, -1$

$(6\varphi - 3)$ $-3, ?, ?, -4, -4, 4, 4, -2, -2, 0, 0, 10, 10, -14, -4, -4, -2, -2, -$

(7) $0, -4, 5, -3, -3, 0, 0, 5, 5, 2, 2, 2, 2, ?, -10, -10, -8, -8, -8, -8$

$(\varphi - 8)$ $-1, ?, -2, 0, ?, -4, 8, 6, -6, 8, -4, 6, -6, 14, -12, 0, -10, 2, 0, 0$

$(\varphi + 7)$ $-1, ?, -2, ?, 0, 8, -4, -6, 6, -4, 8, -6, 6, 14, 0, -12, 2, -10, 0, 0$

(8) $0, -2, 2, -4, -4, 4, 4, -2, -2, 0, 0, 2, 2, 10, 12, 12, -10, -10, 8, 8$

$(\varphi + 8)$ $-1, 0, -2, 0, 0, 2, -4, 6, -6, 8, 2, 6, 12, -4, 6, -12, -10, -4, 6, ?$

$(\varphi - 9)$ $-1, 0, -2, 0, 0, -4, 2, -6, 6, 2, 8, 12, 6, -4, -12, 6, -4, -10, ?, 6$

$(8\varphi - 2)$ $?, -3, 1, 3, -6, ?, -7, -6, 3, 5, 5, 6, 6, -4, -12, 6, 8, 8, -9, 0$

$(8\varphi - 2)$ $?, 1, -5, -3, 2, ?, 5, -10, 5, 7, -3, 2, 2, 0, 0, 10, -8, 12, 7, -8$

$(8\varphi - 6)$ $?, -3, 1, -6, 3, -7, ?, 3, -6, 5, 5, 6, 6, -4, 6, -12, 8, 8, 0, -9$

Something special is clearly happening with all of these even numbers.

Torsion

To see what is going on, we can use $a_{\mathfrak{p}}$ to calculate the number of points on E mod $\mathfrak{p}$ for curve that we are looking for.

$$a_{\mathfrak{p}} = \mathrm{Norm}(\mathfrak{p}) - \#(E \bmod \mathfrak{p}) + 1$$

so

$$\#(E \bmod \mathfrak{p}) = \mathrm{Norm}(\mathfrak{p}) - a_{\mathfrak{p}} - 1.$$

point counts from earlier table

$(5\varphi-2)$	8, 8, 8, 16, 8, 16, 24, 32, 32, 24, ?, 48, 48, 48, 64, 48, 64, 56, 80, 72
$(5\varphi-3)$	8, 8, 8, 8, 16, 24, 16, 32, 32, ?, 24, 48, 48, 48, 48, 64, 56, 64, 72, 80
(6)	?, 10, ?, 10, 10, 20, 20, 30, 30, 40, 40, 40, 40, 40, 70, 70, 60, 60, 60
$(\varphi+6)$	7, 7, 14, 7, 14, 14, 21, 28, 21, 28, 42, 42, ?, 56, 56, 63, 70, 56, 84, 6
$(\varphi-7)$	7, 7, 14, 14, 7, 21, 14, 21, 28, 42, 28, ?, 42, 56, 63, 56, 56, 70, 63, 8
$(-6\varphi+3)$	8, ?, ?, 16, 16, 16, 16, 32, 32, 32, 32, 32, 32, 64, 64, 64, 64, 64, 80,
(7)	5, 10, 5, 15, 15, 20, 20, 25, 25, 30, 30, 40, 40, ?, 70, 70, 70, 70, 80,
$(-\varphi+8)$	6, ?, 12, 12, ?, 24, 12, 24, 36, 24, 36, 36, 48, 36, 72, 60, 72, 60, 72,
$(\varphi+7)$	6, ?, 12, ?, 12, 12, 24, 36, 24, 36, 24, 48, 36, 36, 60, 72, 60, 72, 72,
(8)	5, 8, 8, 16, 16, 16, 16, 32, 32, 32, 32, 40, 40, 40, 48, 48, 72, 72, 64,
$(\varphi+8)$	6, 6, 12, 12, 12, 18, 24, 24, 36, 24, 30, 36, 30, 54, 54, 72, 72, 66, 66
$(\varphi-9)$	6, 6, 12, 12, 12, 24, 18, 36, 24, 30, 24, 30, 36, 54, 72, 54, 66, 72, ?,
$(-8\varphi+2)$	?, 9, 9, 9, 18, ?, 27, 36, 27, 27, 27, 36, 36, 54, 72, 54, 54, 54, 81, 72
$(-8\varphi+2)$	?, 5, 15, 15, 10, ?, 15, 40, 25, 25, 35, 40, 40, 50, 60, 50, 70, 50, 65,
$(-8\varphi+6)$	?, 9, 9, 18, 9, 27, ?, 27, 36, 27, 27, 36, 36, 54, 54, 72, 54, 54, 72, 81
$(-8\varphi+6)$	?, 5, 15, 10, 15, 15, ?, 25, 40, 35, 25, 40, 40, 50, 50, 60, 50, 70, 80,

So lots of the curves that we are looking for look like they have nontrivial torsion.

Theorem (Katz, 1981)

If a curve "looks" like it has (an isogenous curve with) nontrivial torsion, then it does have (an isogenous curve with) nontrivial torsion.

More precisely, Let ℓ be a prime and E a curve over F. Then $\ell \mid \#E'(F)_{\text{tor}}$ for some curve E' in the isogeny class of E if and only if $\ell \mid \text{Norm}(\mathfrak{p}) + 1 - a_{\mathfrak{p}}$ for all odd primes $\mathfrak{p}$ at which E has good reduction.

This is nice because curves with torsion form a rather thin subset of all elliptic curves, so if we know that some curves we are looking for have torsion, we know where to focus a search.

From: Kubert, Universal bounds on the torsion of elliptic curves, PLMS 1976

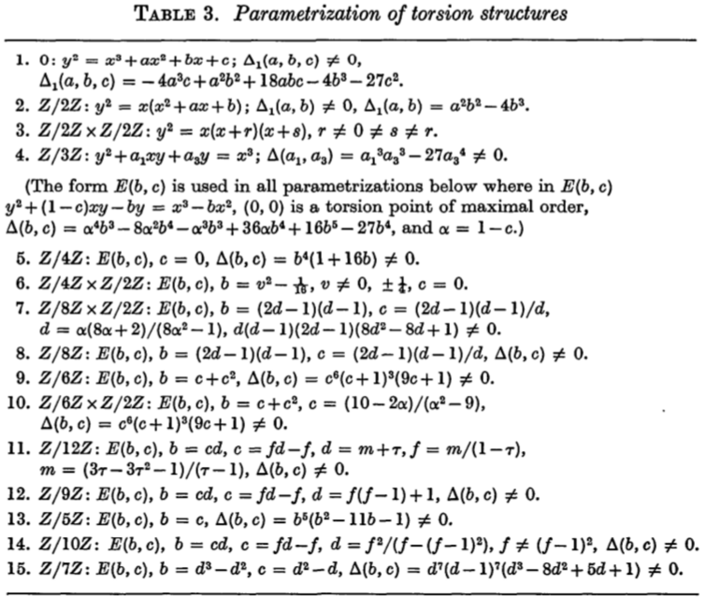

TABLE 3. *Parametrization of torsion structures*

1. $0: y^2 = x^3+ax^2+bx+c$; $\Delta_1(a, b, c) \neq 0$,
$\Delta_1(a, b, c) = -4a^3c+a^2b^2+18abc-4b^3-27c^2$.
2. $Z/2Z: y^2 = x(x^2+ax+b)$; $\Delta_1(a, b) \neq 0$, $\Delta_1(a, b) = a^2b^2-4b^3$.
3. $Z/2Z \times Z/2Z: y^2 = x(x+r)(x+s)$, $r \neq 0 \neq s \neq r$.
4. $Z/3Z: y^2+a_1xy+a_3y = x^3$; $\Delta(a_1, a_3) = a_1{}^3a_3{}^3-27a_3{}^4 \neq 0$.

(The form $E(b, c)$ is used in all parametrizations below where in $E(b, c)$ $y^2+(1-c)xy-by = x^3-bx^2$, $(0, 0)$ is a torsion point of maximal order, $\Delta(b, c) = \alpha^4b^3-8\alpha^2b^4-\alpha^3b^3+36\alpha b^4+16b^5-27b^4$, and $\alpha = 1-c$.)

5. $Z/4Z$: $E(b, c)$, $c = 0$, $\Delta(b, c) = b^4(1+16b) \neq 0$.
6. $Z/4Z \times Z/2Z$: $E(b, c)$, $b = v^2-\frac{1}{16}$, $v \neq 0, \pm\frac{1}{4}$, $c = 0$.
7. $Z/8Z \times Z/2Z$: $E(b, c)$, $b = (2d-1)(d-1)$, $c = (2d-1)(d-1)/d$,
$d = \alpha(8\alpha+2)/(8\alpha^2-1)$, $d(d-1)(2d-1)(8d^2-8d+1) \neq 0$.
8. $Z/8Z$: $E(b, c)$, $b = (2d-1)(d-1)$, $c = (2d-1)(d-1)/d$, $\Delta(b, c) \neq 0$.
9. $Z/6Z$: $E(b, c)$, $b = c+c^2$, $\Delta(b, c) = c^6(c+1)^3(9c+1) \neq 0$.
10. $Z/6Z \times Z/2Z$: $E(b, c)$, $b = c+c^2$, $c = (10-2\alpha)/(\alpha^2-9)$,
$\Delta(b, c) = c^6(c+1)^3(9c+1) \neq 0$.
11. $Z/12Z$: $E(b, c)$, $b = cd$, $c = fd-f$, $d = m+\tau$, $f = m/(1-\tau)$,
$m = (3\tau-3\tau^2-1)/(\tau-1)$, $\Delta(b, c) \neq 0$.
12. $Z/9Z$: $E(b, c)$, $b = cd$, $c = fd-f$, $d = f(f-1)+1$, $\Delta(b, c) \neq 0$.
13. $Z/5Z$: $E(b, c)$, $b = c$, $\Delta(b, c) = b^5(b^2-11b-1) \neq 0$.
14. $Z/10Z$: $E(b, c)$, $b = cd$, $c = fd-f$, $d = f^2/(f-(f-1)^2)$, $f \neq (f-1)^2$, $\Delta(b, c) \neq 0$.
15. $Z/7Z$: $E(b, c)$, $b = d^3-d^2$, $c = d^2-d$, $\Delta(b, c) = d^7(d-1)^7(d^3-8d^2+5d+1) \neq 0$.

For example, we first found the curve E given by

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

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

As this point, we are only missing a handful of curves with norm conductor < 2000.

Using special values of L-functions

There is a general method of Lassina Dembele for finding a curve from a newform f by computing the central value of $L(f, s)$ and twists of f.

We will use these central values to compute (or at least guess) periods of the curve E that we are looking for, and use these periods to find the curve.

Periods

A curve E over F has two period lattices corresponding to the two embeddings of F into $\mathbb{R}$ We'll write Ω_E^+ and Ω_E^- for the least real and imaginary periods for one embedding and $\Omega_{\overline{E}}^+$ and $\Omega_{\overline{E}}^-$ for the other embedding.
These periods naturally come mixed together, so we write

$$\begin{aligned} \Omega_E^{++} &= \Omega_E^+ \Omega_{\overline{E}}^+ & \Omega_E^{+-} &= \Omega_E^+ \Omega_{\overline{E}}^- \\ \Omega_E^{-+} &= \Omega_E^- \Omega_{\overline{E}}^+ & \Omega_E^{--} &= \Omega_E^- \Omega_{\overline{E}}^-. \end{aligned}$$

If we know all of these values, then we can more or less recover the curve that we are looking for.

We still do not know the discriminant of the curve that we are looking for, so we don't know the lattice types, but we can compute possible embeddings of $j(E)$. The first embedding will be either $j(\tau_1(E))$ or $j(\tau_2(E))$ and the second embedding will be either $j(\tau_1(\overline{E}))$ or $j(\tau_2(\overline{E}))$, where

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

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

and $j(\tau)$ is the familiar

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

(The choices of τ depens of the signs of the embeddings of the discriminant. We don't know these, but there are only 4 combinations to try.)

- If we know $j(E)$ to enough precision, we can recognize it as an algebraic number, write down a curve with this j-invariant, and then find a minimal twist.
- In practice, it seems that it is better to use (a guess for) $j(E)$ and (a guess for) the discriminant to compute (a guess for) c_4, then compute c_6, then use these to write down E.
- This might sound like a lot of guesswork, but if we have the periods to enough precision it is only the discriminant that we need to guess, and we at least know factors of the discriminant.

Finding the mixed periods

To compute the mixed periods, Dembele using the following conjecture, distilled from a conjecture of Oda.

Conjecture

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

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

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

Finding the mixed periods

This only gives us multiples of the mixed periods. To try to figure out which multiples, we can compute a few of them and try to recognize ratios of them as rational numbers.

At this point, we still only have guesses for the mixed periods, so we just introduce some more guesswork into the procedure.

This method seems to work very well, but it is currently limited by the complexity of computing enough Fourier coefficients to compute the L-function. For some examples we have needed all $a_{\mathfrak{p}}$ with $\mathrm{Norm}(\mathfrak{p}) < 20000$ (or maybe larger). Computation of all $a_{\mathfrak{p}}$ with $\mathrm{Norm}(\mathfrak{p}) < 50000$ currently takes about 10 hours and uses a large precomputation.

If we had done everything correctly, the methods described so far should have been enough to find all elliptic curves over F with norm conductor less than 2000. In fact, there were some mistakes made along the way.

There was one curve with conductor < 1831 that we were unable to find for some time, and one more curve with conductor < 2000.

Another application of point counting

From

$$y^2 + (\varphi + 1)y = x^3 + (\varphi - 1)x^2 - 2\varphi x$$

we get the sequence of a_p

$-2, -3, -1, 0, -5, 3, -8, -1, -2, 6, 6, 1, -6, -10, 7, -8, 8, 6, -9, -6, 1, -1$

Meanwhile, there is a curve that we are looking for which has the list

$1, 4, -1, 0, 2, -4, 6, -8, -2, -8, -8, 1, -6, -10, -14, 6, 8, -8, 12, 8, 8, 16, 6$

Another application of point counting

From

$$y^2 + (\varphi + 1)y = x^3 + (\varphi - 1)x^2 - 2\varphi x$$

we get the sequence of point counts

$7, 9, 11, 12, 17, 17, 28, 31, 32, 26, 26, 41, 48, 60, 53, 68, 54, 56, 81, 78, 79, 92,$

Meanwhile, there is a curve that we are looking for which has the list

$4, 2, 11, 12, 10, 24, 14, 38, 32, 40, 40, 41, 48, 60, 74, 54, 54, 70, 60, 64, 72, 64,$

This strongly suggests that $E[7] \cong E'[7]$.

Another application of point counting

Since $\ell = 7$ is in the set $\{7, 11\}$, Tom Fisher has Magma code which will list all curves $E'[\ell]$ with $E'[\ell] \cong E[\ell]$.

This involves finding rational points on a quartic surface, so it might be difficult sometimes, but we were lucky here, and this found the curve

$$\begin{aligned} y^2 + \varphi xy = x^3 + (\varphi - 1)x^2 + \\ (-257364\varphi - 159063)x + (-75257037\varphi - 46511406) \end{aligned}$$

As of yesterday, we were still missing exactly one curve with norm conductor < 2000. At 4 a.m. this morning, Lassina sent me

$$[0, \varphi + 1, 0, -6\varphi + 7, -7\varphi + 3],$$

which he found using “a search routine that has been implemented in Magma by Steve Donnelly based on an idea of Elkies.” I believe this will complete the list up to 2000.

We should have found this curve using the sieving procedure described earlier, but for some reason we didn’t.

TODO: Systematize these methods and make bigger tables!