# FINDING NEW CURVES USING TORSION FAMILIES AND TWISTING

BEN LEVEQUE

At the moment we have no fast, guaranteed way to find new curves from $a_p$ values or any other known data, but two methods that have proven effective to a certain extent are searching through families of curves with given torsion structures and using quadratic twists on curves already known. It is unlikely that the two methods together will find all of our missing curves, but their implementation has been both instructive and somewhat successful. At the moment, up to Galois conjugate pairs they have produced 33 of the 76 missing curves (see the last page for a list). This report will briefly describe twisting and torsion families in more detail and then give a summary of how they were used to find new curves. For proofs of the facts presented, consult Ian Connell's *Elliptic Curve Handbook*, which can be found online at http://www.ucm.es/BUCM/mat/doc8354.pdf. Connell's book, Silverman's *The Arithmetic of Elliptic Curves*, and Kubert's *Universal Bounds on the Torsion of Elliptic Curves* are the primary resources used throughout.

## 1. Quadratic Twists (and a bit of background on isomorphisms)

If $E$ is an elliptic curve defined over $K$ (in our case $\mathbb{Q}(\sqrt{5})$), then a *twist* $E'$ of $E$ is a curve isomorphic to $E$ over some extension of $K$. One way to create such isomorphisms is by defining four-parameter maps: $\tau = [r, s, t, u]$, where $r, s, t \in K$ and $u \in K^*$. These maps act on the space $\mathcal{E}$ of non-singular elliptic curves by:

$$\tau : [a_1, a_2, a_3, a_4, a_6] \mapsto [a_1', a_2', a_3', a_4', a_6'],$$

where:

$$\begin{aligned}
a_1' &= u^{-1}(a_1 + 2s), \\
a_2' &= u^{-2}(a_2 - sa_1 + 3r - s^2), \\
a_3' &= u^{-3}(a_3 + ra_1 + 2t), \\
a_4 &= u^{-4}(a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st), \\
a_6' &= u^{-6}(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1)
\end{aligned}$$

The set of these maps $\tau$ form a group ($G$) under composition, and all isomorphisms between curves over $K$ may be given by elements in $G$. Therefore, two elliptic curves are isomorphic iff they are in the same $G$-orbit of $\mathcal{E}$. Conventionally, a $G$-orbit of $\mathcal{E}$ is called an *abstract elliptic curve*, while a specific curve within an orbit is referred to as a *model*. It is worth noting that there is an explicit formula for the image of a given point $(c, d) \in E$ under the action of the map $\tau \in G$:

$$\tau : (c, d) \mapsto (u^{-2}(c - r), u^{-3}(d - sc + sr - t))$$

For example, the map $[-1]$, which sends every point on $E$ to its negative, is given by the map $\sigma$: $[0, -a_1, -a_3, -1]$ (quick sanity check: we see that if our curve is in short Weierstrass form (in particular $a_1 = a_3 = 0$), $\sigma$ indeed maps a point $(c, d)$ to its negative $(c, -d)$). We also note that the *degree* of an isomorphism of curves $\tau = [r, s, t, u]$ is equal to $[K(r, s, t, u) : K]$. A *quadratic twist* of a curve $E$ is therefore a curve $E'$ isomorphic to $E$ by a map of degree 1 or 2. If we consider $E$ in the form

$$E : y^2 = x^3 + ax^2 + bx + c,$$

then the quadratic twist of E *by* $d$, for any element $d \in K^*$, is given by the equation

$$E^d : dy^2 = x^3 + ax^2 + bx + c. \tag{1}$$

We can easily transform (1) to Weierstrass form by multiplying through by $d^3$ and making the substitutions $y' = d^2y$ and $x' = dx$. Finally, if $E : [a_1, a_2, a_3, a_4, a_6]$ is our curve, we can give the isomorphism from $E$ to $E^d$ by the map $\tau_d = [0, a_1(\frac{r-1}{2}), a_3(\frac{r^3-1}{2}), r]$, where r is a root of $r^2 = \frac{1}{d}$. In fact the map from $K^*$ to $G$ given by $d \mapsto \tau_d$ is a homomorphism.

## 2. Torsion Families

We know that for any elliptic curve $E/K$,

$$E(K) \cong \mathbb{Z}^r \times E(K)_{tors},$$

and the structure of the torsion subgroup $E(K)_{tors}$ is an important characteristic of $E$. Sheldon Kamienny and Filip Najman have shown that over $K = \mathbb{Q}(\sqrt{5})$, the torsion subgroup will be isomorphic to one of the 16 groups below, with the last case appearing only once:

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z}, & 1 \leq m \leq 10, \quad m = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, & 1 \leq m \leq 4, \\ \mathbb{Z}/15\mathbb{Z}. & \end{array}$$

Over $\mathbb{Q}$, these families have explicit parametrizations (given on page 217 of Daniel Kubert's *Universal Bounds on the Torsion of Elliptic Curves*). Over $\mathbb{Q}(\sqrt{5})$, these parametrizations are not guaranteed to produce all curves with a given torsion structure, but they are a good place to start when searching for such curves.

## 3. Finding New Curves

Our implementation of twisting to find new elliptic curves is fairly straightforward: loop through values of $i$ and $j$ up to a certain bound and twist the inputted curve $E$ by $ia + j$. The advantage of this system is that the result of a quadratic twist by $ia+j$ can have vastly different coefficients than the original curve, including *much* larger values that likely would not be recovered by a search similar to the one that found our first list of matched curves (http://wstein.org/Tables/hmf/sqrt5/finding_weierstrass_equations/matched.txt). One disadvantage is that we are still looping through values, which is very slow, especially since we must check each potential new curve against the table to see if it is isomorphic or isogenous to any known curve of the same norm conductor. However, there is an intuitive bound on how high the norm of $d$ should be (if we are twisting by $d$): the norm conductor of $E_d$ (denote as $|cond(E_d)|$) seems to be divisible by $|d \cdot cond(E)|$, so we need not consider twists by elements of norm too large for our table of curves with $N \leq 1000$.

Our implementation of the torsion family method began by looking at the parametrizations of curves that have 2-, 3-, and 7-torsion points. Our approach has included using the $a_p$ values for our unknown curves in conjunction with our isogeny code to identify unknown curves $E_{un}$ with given $p$-isogenies. These curves can be likely candidates for curves with $p$-torsion points (in the case $p = 2$, these *are* the curves with $p$-torsion points), so we can use the parametrizations to find curves that share norm conductor with $E_{un}$ in hopes of recovering the Weierstrass equation for $E_{un}$. Also helpful was Jon Bober's list of curves including predicted torsion points, as it allowed us to find such curves as:

$$E : y^2 + xy = x^3 + (121a - 211)x + 619a - 1006$$

which has a 6-torsion point. The search was fairly successful for the 2-, 3-, 5-, and 7-torsion families, and was extended to accommodate the rest of the possible torsion structures listed in §2. As was the case in our search using twists, this search was quite slow, but it was similarly effective in that it produced curves with large and diverse $a$-invariants.

## 4. Curves Found*

```
1 --- (0, -1, a, -108*a - 67, 684*a + 423)
2 --- (0, 0, 1, 1652*a - 2673, -38652*a + 62540)
3 --- (0, 0, 0, -17*a - 12, -43*a - 26)
4 --- (0, -a - 1, 0, 8*a - 12, 11*a - 18)
5 --- (0, a + 1, 0, -6*a - 5, -18*a - 12)
6 --- (0, 0, 0, -16*a - 16, 44*a + 33)
7 --- (1, 0, 0, 121*a - 211, 619*a - 1006)
8 --- (a + 1, -a, 0, 7*a - 23, -24*a + 20)
9 --- (a, 0, 0, -7*a - 16, 24*a - 4)
10 -- (1, -1, a, -44*a - 27, -215*a - 133)
11 -- (a, -a - 1, 0, 0, -40*a - 25)
12 -- (0, -1, a + 1, 108*a - 175, -685*a + 1107)
13 -- (a, -a + 1, 0, 202*a - 329, -1553*a + 2514)
14 -- (a + 1, 0, 1, -1103*a - 682, 20454*a + 12641)
15 -- (1, 0, 1, 21*a - 40, -66*a + 101)
16 -- (0, a + 1, a + 1, -226*a - 140, 1772*a + 1095)
17 -- (a, 0, a + 1, -3*a - 5, 5*a - 3)
18 -- (18*a - 28, -105*a + 170, -105*a + 170, 0, 0)
19 -- (24*a - 38, -165*a + 267, -165*a + 267, 0, 0)
20 -- (a + 1, -1, a, -54*a - 33, -63*a - 39)
21 -- (a + 1, a - 1, a, 7*a - 12, -a + 2)
22 -- (0, -a, 0, -53*a - 33, -126*a - 78)
23 -- (a + 1, 1, a + 1, 27*a + 17, 27*a + 17)
24 -- (1, -1, 1, 1, 43*a + 26)
25 -- (a + 1, -a + 1, 0, 308*a - 498, -2948*a + 4770)
26 -- (a, a - 1, a + 1, 9*a + 3, -17*a - 6)
27 -- (1, -1, 1, a, -20*a - 12)
28 -- (a + 1, a, a + 1, -10*a + 13, 19*a - 32)
29 -- (a + 1, -a, a, a - 7, -6*a + 3)
30 -- (0, 1, a, 32*a - 54, -100*a + 159)
31 -- (1, a + 1, 0, -13*a - 13, 216*a + 128)
32 -- (1, -a, 1, -734*a - 454, -11114*a - 6869)
33 -- (0, a, a + 1, -223*a - 138, -2071*a - 1280)
34 -- (0, a, a, -43*a - 28, -203*a - 126)
35 -- (0, -a, a, -133*a - 83, -820*a - 507)
36 -- (0, -a, a + 1, -133*a - 83, 242*a + 149)
37 -- (0, -a, 1, -42*a - 53, -192*a - 140)
38 -- (0, a - 1, 1, 42*a - 95, 192*a - 332)
39 -- (0, 0, a, 112510*a - 182045, 21727126*a - 35155229)
```

*Note: This list currently contains six Galois-conjugate pairs