WORKING WITH LIFTS AND $a_{\mathfrak{p}}$-VALUES TO FIND CURVES

BEN LEVEQUE

In our attempt to find new elliptic curves over $K = \mathbb{Q}(\sqrt{5})$, we have turned to $a_{\mathfrak{p}}$-values as a major source of information. The $a_{\mathfrak{p}}$-value of a curve E at a prime $\mathfrak{p} \in K$ can be explicitly given by: $a_{\mathfrak{p}} = N(\mathfrak{p}) - \#E(\mathbb{F}_p) + 1$, so it is fairly easy to compute using Sage's built-in point counting methods. It is also referred to as the trace of Frobenius, for in the endomorphism ring $End(E/\mathbb{F}_p)$,

$$Frob_p^2 + a_{\mathfrak{p}} Frob_p + N(\mathfrak{p}) = 0,$$

where $Frob_p$ is the Frobenius map sending $(x, y) \mapsto (x^p, y^p) \in E/\mathbb{F}_p$.

Our method for finding an unknown curve E_{un} involves finding all curves in $\mathcal{O}_K/(p)$ which have the correct $a_{\mathfrak{p}_1}$ and $a_{\mathfrak{p}_2}$ values (for p a split prime with factorization $p = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ in K). This provides congruence conditions on the space of possible candidates for E_{un} and dramatically reduces the number of curves we must search through after lifting each of these candidates to $\mathcal{O}_K$.

1. Method

1.1. Curves in $\mathcal{O}_K/\mathfrak{p}$.

Let $\mathfrak{p}$ be a prime above the split prime p. We know that in characteristic not 2 or 3, we can reduce any elliptic curve to short Weierstrass form (SWF), and since we are only considering primes $\mathfrak{p}$ above split primes, we will never run into issues. The first step in our method is to create a dictionary of all nonsingular SWF curves in $\mathcal{O}_K/\mathfrak{p}$, where the keys are $a_{\mathfrak{p}}$-values and the entries are the curves which have that $a_{\mathfrak{p}}$-value. Since $\mathfrak{p}$ is a maximal ideal in $\mathcal{O}_K$, $\mathcal{O}_K/\mathfrak{p}$ is a field of size p, so this amounts to finding all SWF curves E with coefficients in $\mathbb{Z}/p\mathbb{Z}$:

$$E: \quad y^2 = x^3 + Ax + B, \qquad\qquad A, B \in \mathbb{Z}/p\mathbb{Z}$$

Using Sage's point-counting functionality, we can easily find the $a_{\mathfrak{p}}$ value for each of these curves and thus construct our dictionary.

1.2. Curves in $\mathcal{O}_K/(p)$.

Let $p = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ in K, and let $\mathfrak{p}_1$ be the prime at which the dictionary method described in 1.1 found *fewer* possible curves. In order to find curves in $\mathcal{O}_K/(p)$ that have correct values at both $\mathfrak{p}_1$ and $\mathfrak{p}_2$, we first lift each curve found in $\mathcal{O}_K/\mathfrak{p}_1$ to its p^2 possible images in $\mathcal{O}_K/(p)$ (p images for both $a_4 = A$ and $a_6 = B$). We can then reduce each lift modulo $\mathfrak{p}_2$ and see if the resulting curve is in the list of possible curves in $\mathcal{O}_K/\mathfrak{p}_2$. If so, we save this lift as a curve over $\mathcal{O}_K/(p)$ having the proper $a_{\mathfrak{p}_1}$- and $a_{\mathfrak{p}_2}$-values.

1.3. **Reduced Models and Lifts.**

Now that we have a list of valid SWF curves in $\mathcal{O}_K/(p)$, we may consider various reduced models of each curve in our attempt to find E_{un}. Reduced models have the form:

$$\begin{aligned}&E_{red}: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad \text{where:}\\ &a_1, a_3 \in \{0, 1, a, a+1\} \quad \text{and}\\ &a_2 \in \{0, \pm 1, \pm a, \pm a \pm 1\}\end{aligned}$$

By allowing a_1, a_2, and a_3 to be non-zero, there is perhaps a better chance for a_4 and a_6 to be smaller than they would be in a short Weierstrass model, making it more likely that we encounter a reduced model of E_{un} itself using a fairly low-bound search.

In order to find the reduced models of our curves over $\mathcal{O}_K/(p)$, we can look at isomorphisms of the form $\tau = [r, s, t, 1]$ which take each curve to one of the desired form. If $E : [a_1, a_2, a_3, a_4, a_6]$ is one of our SWF curves in $\mathcal{O}_K/(p)$, we know that $a_1 = a_2 = a_3 = 0$. Therefore, when looking at an isomorphism of the form τ from E to a curve $E' : [a'_1, a'_2, a'_3, a'_4, a'_6]$ that we wish to be in reduced form, our expressions for $a'_1 - a'_3$ simplify to:

$$\begin{array}{lcll} a'_1 & = & 2s & \Rightarrow 2s \in \{0, 1, a, a+1\} \\ a'_2 & = & 3r - s^2 & \Rightarrow 3r - s^2 \in \{0, \pm 1, \pm a, \pm a \pm 1\} \\ a'_3 & = & 2t & \Rightarrow 2t \in \{0, 1, a, a+1\} \end{array}$$

Since we are working in $\mathcal{O}_K/(p)$, we can choose s, r, and t as follows (where 3^{-1} represents the inverse of 3 mod p):

$$s \in \{0, \tfrac{p+1}{2}, \tfrac{p+1}{2}a, \tfrac{p+1}{2}(a+1)\}$$

$$r \in \{3^{-1}s^2, 3^{-1}(s^2 \pm 1), 3^{-1}(s^2 \pm a), 3^{-1}(s^2 \pm a \pm 1)\}$$

$$t \in \{0, \tfrac{p+1}{2}, \tfrac{p+1}{2}a, \tfrac{p+1}{2}(a+1)\}$$

These stipulations produce 144 different isomorphisms $\tau = [r, s, t, 1]$ from E to its reduced forms, giving us curves with a nice variety of coefficients as well. It is important to note that we are working in $\mathcal{O}_K/(p)$, so we must remember to reduce all coefficients modulo p. The exception is that we still want the components (i.e. the coefficients of the basis elements 1 and a) of a_2 to lie in the desired range, and reduction mod p might not accomplish this (if $a_2 = -1$, for example). The simple fix is that if reduction takes any component of a_2 to $p - 1$, we subtract p from this component.

We may now lift each of the 144 different curves from $\mathcal{O}_K/(p)$ to $\mathcal{O}_K$. One possible lift of a curve E is to take the natural image of E (i.e. leave each coefficient as it is, but consider them as elements of $\mathcal{O}_K$). Additionally, we can lift by adding or subtracting multiples of p from any component of any coefficient. Since we want our lift to be in reduced form, a_1, a_2, and a_3 should maintain their values under any lift, so we only alter a_4 and a_6. In order to produce a reasonably-sized yet varied collection of lifts to consider, we alter each in four ways (for $i \in \{4, 6\}$):

$$\begin{aligned} a_i &\mapsto a_i \\ a_i &\mapsto a_i - p \\ a_i &\mapsto a_i - pa \\ a_i &\mapsto a_i - p(a+1) \end{aligned}$$

We therefore get reduced models in $\mathcal{O}_K$ with $-11 \leq a_4[0], a_4[1], a_6[0], a_6[1] < 11$, where the indices indicate which component of each coefficient is being considered. This gives us a decent breadth of curves to search through, while still limiting the coefficients to a reasonable range. We note that at no point in this process do we construct the curves. All manipulations to this point are on the coefficients, so for efficiency we store the "curves" as tuples. Once we have our lifts in $\mathcal{O}_K$, we use a custom function to quickly calculate the norm of the discriminant of each and check to see if the conductor norm of E_{un} divides it. If so, we construct the curve and calculate its conductor to see if we have found E_{un}. As a final check, we quickly calculate the $a_{\mathfrak{p}}$-values of the found curve to make sure that they match at all places with the $a_{\mathfrak{p}}$-values of E_{un}.

2. Bite-Sized Algorithm to find E_{un}

1. Factor $p = \mathfrak{p}_1 \cdot \mathfrak{p}_2$
2. Find all curves in $\mathcal{O}_K/\mathfrak{p}_1$ and $\mathcal{O}_K/\mathfrak{p}_2$ that have the correct $a_{\mathfrak{p}_1}$- and $a_{\mathfrak{p}_2}$-values
3. Lift curves from $\mathcal{O}_K/\mathfrak{p}_1$ to $\mathcal{O}_K/(p)$ in various ways, reduce each to $\mathcal{O}_K/\mathfrak{p}_2$
4. If the reduction is a "valid" curve in $\mathcal{O}_K/\mathfrak{p}_2$, save it
5. Lift the reduced models of these saved curves to $\mathcal{O}_K$ in various ways
6. If any of these lifts have the same conductor as E_{un}, quickly check against all $a_{\mathfrak{p}}$-values
7. If all $a_{\mathfrak{p}}$-values match, this is E_{un}