ENUMERATING ISOGENY CLASSES USING BILLEREY'S ALGORITHM

ARIAH KLAGES-MUNDT

1. Enumerating the curves in an isogeny class

Given an elliptic curve E/F, we would like to identify all isomorphism classes of elliptic curves E'/F that are isogenous to E via an isogeny defined over F. Recall that two elliptic curves in an isogeny class are linked by a chain of prime degree isogenies — in particular, to enumerate an isogeny class we need to find all isogenies of prime degree, of which there are finitely many for curves that do not admit CM over the given number field. Over $\mathbb{Q}$, there is an algorithmic solution to this problem described in [5] that is based on the following:

(1) Mazur's theorem that states that if $\psi : E \to E'$ is a $\mathbb{Q}$-rational isogeny of prime degree, then $deg\ \psi \leq 163$.
(2) Vélu's formulas, which provide an explicit way to enumerate all prime degree isogenies with a given domain E (see [14] III Prop. 4.12 for an important result and [5] III Section 3.8 for a discussion of these formulas).

Vélu's formulas are valid for any number field (in fact, they are valid for a field of any characteristic) and are implemented in Sage, but there is currently no generalization of Mazur's theorem that gives us an explicit bound on the possible prime degree isogenies defined over a general number field.

Since we are interested in specific isogeny classes, we solve this problem by taking a less general perspective: we determine which prime degree isogenies are possible for a specific isogeny class using the following well-known result.

Theorem 1.0.1. *Let E be an elliptic curve over a number field K. For each prime number $\ell \in \mathbb{Z}$, let*

$$\rho_{E,\ell} : Gal(\overline{\mathbb{Q}}/K) \to GL(E[\ell]) \cong GL_2(\mathbb{Z}/\ell\mathbb{Z})$$

be the associated Galois representation on ℓ-torsion points, where $E[\ell]$ is the set (actually group) of ℓ-torsion points in $E(\overline{K})$. There exists an isogeny $E \to E'$ defined over K of prime degree ℓ if and only if $\rho_{E,\ell}$ is reducible over $\mathbb{F}_\ell$. In particular, if $\rho_{E,\ell}$ is irreducible (over the algebraic closure of $\mathbb{F}_\ell$), then there can be no isogenies $E \to E'$ of prime degree ℓ.

In this section, we describe our implementation of an algorithm described in [1] that outputs a provably finite list of primes p such that a given elliptic curve E over a number field K might have a p-isogeny. For simplicity, we will work solely with the case that $[K : \mathbb{Q}]$ is odd, although there is a similar algorithm that can deal with the even case. We first develop the necessary machinery in 1.1 and then describe the implementation of algorithm in 1.2.

1.1. **Definitions and machinery.** Proofs of all statements in this section can be found in [1].

Definition. Let A be an integral domain with field of fractions L and $\overline{L}$ an algebraic closure of L. We define M_A to be the subset of $A[X]$ of all monic polynomials that do not vanish at 0.

For an integral domain A, we wish to define a commutative monoid operation $*$ on a subset of $A[X]$.

Lemma 1.1.1. *The operation $M_A \times M_A \to A[X]$ given by*

$$(P, Q) \mapsto (P * Q)(X) = Res_Z(P(Z), Q(X/Z)Z^{degQ}),$$

where Res_Z is the resultant with respect to Z, has an image contained in M_A. It defines an act of a commutative monoid on M_A with neutral element $\psi_A(X) = X - 1$. Moreover, if $P, Q \in M_A$ are written

$$P(X) = \prod_{i=1}^{n}(X - \alpha_i) \text{ and } Q(X) = \prod_{j=1}^{m}(X - \beta_j)$$

then in $\overline{L}[X]$ we have

$$(P * Q)(X) = \prod_{1\leq i\leq n,\ 1\leq j\leq m}(X - \alpha_i\beta_j).$$

In particular,

$$(P * Q)(0) = (-1)^{degP\cdot degQ}P(0)^{degQ}Q(0)^{degP}.$$

Lemma 1.1.2. *Let $r \geq 1$ and $P \in M_A$. Then there exists a unique polynomial $P^{(r)} \in M_A$ such that $P^{(r)}(X^r) = (P*\Psi_r)(X)$ where $\Psi_r(X) = X^r - 1$. The mapping $P \mapsto P^{(r)}$ is a monoid morphism for the operation $*$. Moreover, if $P \in M_A$ factors on $\overline{L}$ to the form*

$$P(X) = \prod_{i=q}^{n}(X - \alpha_i), \text{ then } P^{(r)}(X) = \prod_{i=1}^{n}(X - \alpha_i^r).$$

Let K be a number field and fix an elliptic curve E/K that does not admit CM over K. Let ℓ be a prime number such that E has good reduction at every prime ideal of $\mathcal{O}_K$ dividing

$$\ell\mathcal{O}_K = \prod_{\mathfrak{q}_i|\ell}\mathfrak{q}_i^{v_{\mathfrak{q}_i}(\ell)},$$

where the right-hand side is the decomposition product of prime ideals of $\mathcal{O}_K$ — in particular, $v_{\mathfrak{q}_i}(\ell)$ is the ramification index of prime $\mathfrak{q}_i$ in $\ell\mathcal{O}_K$. By abuse of language, we say that E has good reduction at ℓ. In this case, we associate with ℓ the polynomial P_ℓ^* with integer coefficients

$$P_\ell^* = P_{\mathfrak{q}_1}^{(12v_{\mathfrak{q}_1}(\ell))} * \ldots * P_{\mathfrak{q}_s}^{(12v_{\mathfrak{q}_s}(\ell))} \in \mathbb{Z}[X]$$

for $\mathfrak{q}_i$ such that $\mathfrak{q}_i|\ell$, and $P_\mathfrak{q}$ is defined in the following way:

Suppose E has good reduction at $\mathfrak{q}$. Then we define

$$P_\mathfrak{q}(X) = X^2 - a_\mathfrak{q}X + N(\mathfrak{q}) \in \mathbb{Z}[X]$$

where $N(\mathfrak{q}) = \#\mathcal{O}_K/\mathfrak{q}$ and $a_\mathfrak{q} = N(\mathfrak{q}) + 1 - \#E(\mathcal{O}_K/\mathfrak{q})$.

We then define the integer B_ℓ as follows:

$$B_\ell = \prod_{k=0}^{[\frac{d}{2}]} P_\ell^*(\ell^{12k})$$

where d is the degree of $K/\mathbb{Q}$, $[\frac{d}{2}]$ denotes the integer part of $\frac{d}{2}$, and P_ℓ^* is evaluated at ℓ^{12k}.

With this machinery, we have the following theorem:

Theorem 1.1.3. *Let p be a reducible prime for E/K — i.e., a prime such that E admits a p-isogeny defined over K. Then one of the following is true:*
(1) *p divides $6\Delta_K N_{K/\mathbb{Q}}(\Delta_E)$*
(2) *For all primes ℓ, the number B_ℓ is divisible by p (if $K = \mathbb{Q}$, consider only $\ell \neq p$).*

Remark 1.1.4. The above criterion is effectively useful only if not all of the B_ℓ's are zero. Corollary 0.2 in [1] shows that this is the case when the degree d of the extension of $K/\mathbb{Q}$ is odd since then all roots of P_ℓ^* have absolute value ℓ^{6d} and $12k \neq 6d$.

1.2. **The algorithm.** Let K be a number field of odd degree and E/K an elliptic curve without complex multiplication over K given by a Weierstrass equation with coefficients in $\mathcal{O}_K$ — these are the inputs to the algorithm. The following algorithm then outputs a provably finite set of primes containing $Red(E/K)$, the set of primes p such that E has a p-isogeny (i.e., such that the Galois representation is reducible — see Theorem 1.0.1).

(1) Compute the set S_1 of prime divisors of $6\Delta_K N_{K/\mathbb{Q}}(\Delta_E)$.
(2) Let ℓ_0 be the smallest prime number not in S_1. The curve E has good reduction at ℓ_0. If $B_{\ell_0} \neq 0$, proceed to the next step. Otherwise, reiterate this step with the smallest prime number ℓ_1 not in S_1 and such that $\ell_1 > \ell_0$ etc. until we have some $B_\ell \neq 0$.
(3) We now have a non-zero integer B_ℓ. For greater efficiency, we can reiterate step 2 to obtain more such $B_\ell \neq 0$. We then define S_2 to be the set of prime factors of the greatest common divisor of the B_ℓ's we have obtained and define $S = S_1 \cup S_2$.
(4) The set S then contains $Red(E/K)$, although it may contain other primes. We can eliminate some of these primes by calculating polynomials $P_\mathfrak{q}$ for some prime ideals $\mathfrak{q}$ of good reduction — in particular, if $P_\mathfrak{q}$ is irreducible modulo p (with $\mathfrak{q}$ not dividing p), then $p \notin Red(E/K)$. The subset S' of S of prime numbers remaining is then usually small.

Let K be a cubic number field. Note that CM isogenies are defined over imaginary quadratic fields. Since, by the Tower Theorem, K contains no such subfield, there are no CM isogenies defined over K. Therefore, by using this algorithm in combination with Vélu's formulas, we are able to enumerate any isogeny class of elliptic curves over one of our number fields given that we have already found a representative of the said isogeny class using methods from Section **??**.

References

[1] Nicolas Billerey, *Critères d'irréductibilité pour les représentations des courbes elliptiques*, Int. J. Number Theory **7** (2011), no. 4, 1001-1032, `http://arxiv.org/abs/0908.1084`.

[2] Jon Bober, Alyson Deines, Ariah Klages-Mundt, Benjamin LeVeque, R. Andrew Ohana, Ashwath Rabindranath, Paul Sharaba, and William Stein, *A database of elliptic curves over* $\mathbb{Q}(\sqrt{5})$ *— first report*, to appear in Proceedings of Algorithmic Number Theory Symposium X (2012), http://arxiv.org/abs/1202.6612.

[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235-265, Computational algebra and number theory (London, 1993).

[4] C. Breuil, B. Condrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843-939, http://math.stanford.edu/~conrad/papers/tswfinal.pdf.

[5] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1997, Second Edition, http://www.warwick.ac.uk/~masgaj/book/fulltext/.

[6] 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, http://projecteuclid.org/euclid.em/1204928531.

[7] Paul E. Gunnells, Farshid Hajir, and Dan Yasaki, *Modular forms and elliptic curves over the field of fifth roots of unity*, to appear in Experiment. Math. (2012), http://arxiv.org/abs/1005.2752.

[8] Paul E. Gunnells and Dan Yasaki, *Modular forms and elliptic curves over the cubic field of discriminant* -23, submitted 2012, http://arxiv.org/abs/1201.4132v1.

[9] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481-502, http://www.springerlink.com/content/k625300v27x258g8/.

[10] Ariah Klages-Mundt, *A Database of Elliptic Curves over Complex Cubic Fields*, 2012 https://www.amherst.edu/users/K/aklagesmundt12.

[11] Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proceedings of the London Mathematical Society **s3-33** (1976), no. 2, 193-237, http://plms.oxfordjournals.org/content/s3-33/2/193.full.pdf.

[12] Filip Najman, *Torsion of elliptic curves over cubic fields*, J. Number Theory **132** (2012), 26-36, http://arxiv.org/abs/1108.3709.

[13] R. Andrew Ohana, "Canonical Models", E-mails to Ariah Klages-Mundt, March 12 - March 30 2012.

[14] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, Corrected reprint of the 1986 original, 1992 http://www.springer.com/mathematics/algebra/book/978-0-387-09493-9.

[15] William Stein et al., *Sage Mathematics Software (Version 4.8)*, The Sage Development Team, 2012, http://www.sagemath.org.

Department of Mathematics, Amherst College, Amherst, MA 01002
E-mail address: aklagesmundt12@alumni.amherst.edu