Non-monogenic Division Fields of Elliptic Curves

HANSON SMITH

ABSTRACT. For various positive integers n, we show the existence of infinite families of elliptic curves over $\mathbb{Q}$ with n-division fields, $\mathbb{Q}(E[n])$, that are **not** monogenic, i.e., the ring of integers does not admit a power integral basis. We parametrize some of these families explicitly. Moreover, we show that every $E/\mathbb{Q}$ without CM has infinitely many non-monogenic division fields. Our main technique combines a global description of the Frobenius obtained by Duke and Tóth with a simple algorithm based on ideas of Dedekind.

1. INTRODUCTION

Denote a primitive n^{th} root of unity by ζ_n and take the cyclotomic field $\mathbb{Q}(\zeta_n)$. The arithmetic of these fields has been the inspiration for over a century of algebraic number theory. For example, Kummer first developed the notion of 'ideal numbers' in cyclotomic fields; see [21] and [22, pages 1-47]. Implicit in these investigations is the fact that the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$. To put it another way, the $\mathbb{G}_m$ division fields are monogenic. For a nice survey of the literature related to the above discussion see [24, Chapter 4.4].

Naturally, we want to know about the arithmetic of division fields of other algebraic groups. In this paper we will study the monogeneity of division fields[1] of elliptic curves. In [16], Lozano-Robledo and González-Jiménez classify the possible abelian division fields. In the process, they show that for $n = 1, 2, 3, 4$, and 5 one can have $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$. Hence, in these cases, $\mathbb{Q}(E[n])$ is monogenic. The monogeneity of a family of partial 3-torsion fields is studied in [14]. Adelmann [1] has an in-depth investigation of the splitting of primes in torsion fields. Cassou-Noguès and Taylor have studied the monogeneity of torsion fields of CM elliptic curves extensively; see [2], [3], and [4].

The outline of the paper is as follows. In Section 2, we establish which imaginary quadratic orders we need to consider, and we state a theorem of Duke and Tóth [12] that describes the action of any lift of the Frobenius at p on prime-to-p-torsion points of an elliptic curve. This theorem will be essential for our current work; however, in a forthcoming investigation into similar questions regarding abelian varieties of dimension greater than one, we will generalize Centeleghe's description of the Frobenius in [5]. In Section 3.1, we review Dedekind's criterion for non-monogeneity. With Section 4, we establish criteria for certain torsion fields of elliptic curves to be non-monogenic and remark that a positive proportion of elliptic curves fall into these families. We then use these ideas to show that every elliptic curve $E/\mathbb{Q}$ without CM has infinitely many torsion fields that are not monogenic. Section 5 establishes explicit families in terms of either one or two parameters. Lastly, Section 7 includes tables for Theorem 4.4 for $p = 3, 5, 7$, and 11; the table for $p = 2$ is included in Section 4.

[1]We will use 'division field' and 'torsion field' interchangeably to indicate an extension of the form $\mathbb{Q}(E[n])$.

2. Describing Endomorphism Rings and the Frobenius

Let p be a rational prime, E an elliptic curve over $\mathbb{F}_p$, and a_p the trace of Frobenius of E. From Hasse we have the bound $|a_p| \leq 2\sqrt{p}$. Denote the Frobenius endomorphism of E by π. Recall, π satisfies $f_\pi = x^2 - a_p x + p$. The discriminant of the Weil polynomial f_π is $\Delta_\pi := a_p^2 - 4p$, so we obtain $4p = a_p^2 - \Delta_\pi$.

We would like to know the possibilities for the endomorphism ring of E over $\mathbb{F}_p$, which we denote $\mathrm{End}_{\mathbb{F}_p}(E)$. If E is ordinary, i.e., $a_p \not\equiv 0 \bmod p$, then [28, Theorem 4.2] shows $\mathrm{End}_{\mathbb{F}_p}(E)$ can be any order in the imaginary quadratic field $\mathbb{Q}(\pi)$ containing $\mathbb{Z}[\pi]$.

If E is supersingular, $\mathrm{End}_{\overline{\mathbb{F}_p}}(E)$ is an order in a quaternion algebra. However, over $\mathbb{F}_p$, we have $\mathrm{End}_{\mathbb{F}_p}(E) \otimes \mathbb{Q} \cong \mathbb{Q}(\pi)$; see [29, Theorem 8]. Theorem 4.2 of [28] combined with some computation shows that all possible endomorphism rings occur. Specifically, if $p = 2$, then $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\sqrt{-2}\right]$ when $a_2 = 0$ and $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\sqrt{-1}\right]$ when $a_2 = \pm 2$. If $p = 3$, we have $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\sqrt{-3}\right]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ for all supersingular a_3, i.e., $0, \pm 3$. Otherwise, $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\sqrt{-p}\right]$ if $p \equiv 1 \bmod 4$ and $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\sqrt{-p}\right]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ if $p \equiv 3 \bmod 4$.

We will also make use of an explicit description of the Frobenius from Duke and Tóth [12]. For our purposes, we restrict their theorem to the case where the finite field is $\mathbb{F}_p$. Henceforth, $\mathrm{End}(E) := \mathrm{End}_{\mathbb{F}_p}(E)$ and Δ_{End} will denote the discriminant of $\mathrm{End}(E)$. Define b_p to be the unique positive integer such that $4p = a_p^2 - \Delta_{\mathrm{End}}b_p^2$. In other words, b_p is the index of the order generated by the Frobenius in $\mathrm{End}(E)$, so $\Delta_\pi = b_p^2 \Delta_{\mathrm{End}}$. Consider now the matrix

$$\sigma_p = \begin{bmatrix} \dfrac{a_p + b_p \delta_{\mathrm{End}}}{2} & b_p \\ \dfrac{b_p(\Delta_{\mathrm{End}} - \delta_{\mathrm{End}})}{4} & \dfrac{a_p - b_p \delta_{\mathrm{End}}}{2} \end{bmatrix}, \tag{1}$$

where $\delta_{\mathrm{End}} = 0, 1$ according to whether $\Delta_{\mathrm{End}} \equiv 0, 1$ modulo 4.

Theorem 2.1. *[12, Theorem 2.1] Let $\hat{E}/\mathbb{Q}$ be an elliptic curve whose reduction at p is E. For n prime to p, write $\mathbb{Q}\left(\hat{E}[n]\right)$ for the nth torsion field. Then p is unramified in $\mathbb{Q}\left(\hat{E}[n]\right)$ and the integral matrix σ_p, when reduced modulo n, represents the class of the Frobenius at p in $\mathrm{Gal}\left(\mathbb{Q}\left(\hat{E}[n]\right)/\mathbb{Q}\right)$.*

In other words, σ_p yields the action of the Frobenius on the l-adic Tate module $T_l\left(\hat{E}\right)$ for any l that is prime to p. We note that the above theorem holds with the appropriate modifications for elliptic curves over arbitrary number fields; however, we restrict to $\mathbb{Q}$ since it simplifies the exposition and suffices for our investigation.

3. Dedekind's Criterion for Non-monogeneity

We start with Dedekind's criterion, first appearing in [10], for the splitting of primes in number fields:

Theorem 3.1. *Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible with α a root. Write $K := \mathbb{Q}(\alpha)$ with $\mathcal{O}_K$ denoting the ring of integers. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, then the factorization of p in $\mathcal{O}_K$ coincides with the factorization of $f(x)$ modulo p. That is, if*

$$f(x) \equiv \phi_1(x)^{e_1} \cdots \phi_k(x)^{e_k} \bmod p$$

is a factorization of $f(x)$ into irreducibles in $\mathbb{Z}/p\mathbb{Z}[x]$, then p factors into primes in $\mathcal{O}_K$ as

$$p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}.$$

Further, the residue degree of $\mathfrak{p}_i$ is equal to the degree of ϕ_i.

Many texts on algebraic number theory contain a proof; e.g., [24, Theorem 4.33]. For a nice expository proof see Keith Conrad's note [8].

Using this criterion, Dedekind was the first to demonstrate a number field that was not monogenic. Dedekind considered the cubic field generated by a root of $x^3 - x^2 - 2x - 8$. He showed that the prime 2 split completely. If there was a possible power integral basis, then one would have to find a cubic polynomial generating the same number field that splits completely into distinct linear factors modulo 2. Since there are only two distinct linear polynomials in $\mathbb{F}_2[x]$, this is impossible. Hence the number field cannot be monogenic. We will use the same strategy as Dedekind to construct non-monogenic torsion fields.

In fact, Dedekind showed something stronger than non-monogeneity. The methods outlined above show that 2 will divide the index of any monogenic order in the maximal order. Such a prime is called an *essential discriminant divisor*.[2] Hensel [18] showed that the essential discriminant divisors are exactly the primes whose splitting is too much for the number of irreducible factors of the correct degree to accommodate.

4. Non-monogenic torsion fields

Our goal is to find torsion fields where a prime p splits into a large number of primes, but there are fewer irreducible polynomials of the correct degree in $\mathbb{F}_p[x]$. In other words, we would like to find when the prime p is an obstruction to monogeneity. As a biproduct of our methods, we will obtain an algorithm for computing the unramified essential discriminant divisors of $\mathbb{Q}(E[n])$ and a proof that an elliptic curve over $\mathbb{Q}$ without CM has infinitely many non-monogenic division fields.

It will be convenient to denote the order of the matrix σ_p modulo n, i.e., in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, by $\mathrm{ord}(\sigma_p, n)$. We are going to compute $\mathrm{ord}(\sigma_p, n)$ for a number of n that are relatively prime to p and then compare this to $[\mathbb{Q}(E[n]) : \mathbb{Q}]$. Finding $[\mathbb{Q}(E[n]) : \mathbb{Q}]$ is a difficult problem in general, so here we will focus on what we expect to be the generic case:

$$[\mathbb{Q}(E[n]) : \mathbb{Q}] = |\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})|.$$

The following corollary of Han will be useful for computing $|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})|$:

Lemma 4.1 (Corollary 2.8, [17])**.** *Let $n > 1$ be an integer and $n = p_1^{e_1} \cdots p_k^{e_k}$ its prime factorization. Then,*

$$|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})| = \prod_{i=1}^{k} |\mathrm{GL}_2\left(\mathbb{Z}/p_i^{e_i}\mathbb{Z}\right)| = \prod_{i=1}^{k} p_i^{4(e_i-1)} \left(p_i^2 - 1\right) \left(p_i^2 - p_i\right).$$

We will also need to know the number of irreducible polynomials in $\mathbb{F}_p[x]$ of degree equal to $\mathrm{ord}(\sigma_p, n)$. The goal is to demonstrate that there are not enough irreducible polynomials of the proper degree, so Dedekind's criterion cannot hold. For this we will need the following result of Gauss [15].

Lemma 4.2. *Let μ be the Möbius function. The number of irreducible polynomials of degree m in $\mathbb{F}_p[x]$ is given by*

$$\mathrm{irred}(m, p) := \frac{1}{m} \sum_{d \mid m} p^d \mu\left(\frac{m}{d}\right).$$

One can see [6] for a modern proof.

Using SageMath [11], we can compute $\mathrm{ord}(\sigma_p, n)$, $\mathrm{irred}(\mathrm{ord}(\sigma_p, n), p)$, and $\frac{|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\mathrm{ord}(\sigma_p, n)}$ for n less than 1000. Here $\frac{|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\mathrm{ord}(\sigma_p, n)}$ is the number of primes p splits into in $\mathbb{Q}(E[n])$. If

$$\mathrm{irred}(\mathrm{ord}(\sigma_p, n), p) < \frac{|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\mathrm{ord}(\sigma_p, n)},$$

---

[2]The terms *common index divisor* and, confusingly, *inessential discriminant divisor* also appear in the literature.

then p must divide the index of any monogenic order in $\mathcal{O}_{\mathbb{Q}(E[n])}$.

Example 4.3. Take $p = 2$. Over $\mathbb{F}_2$ the possible ordinary traces of Frobenius are ± 1. Hence the discriminant of the characteristic polynomial of Frobenius is

$$\Delta_\pi = 1 - 8 = -7.$$

Since -7 is square-free, we see $b_2 = 1$. For example, when $a_2 = 1$, the matrix representing the class of Frobenius is

$$\sigma_2 = \begin{bmatrix} 8/2 & (-7 \cdot 8)/4 \\ 1 & -6/2 \end{bmatrix} = \begin{bmatrix} 4 & -14 \\ 1 & -3 \end{bmatrix}.$$

We find that σ_2 has order 10 modulo 11. Assuming $[\mathbb{Q}(E[11]) : \mathbb{Q}] = |\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z})|$, we compute that 2 splits into 1320 primes in $\mathbb{Q}(E[11])$. However, there are only 99 irreducible polynomials of degree 10 in $\mathbb{F}_2[x]$. Hence, if E is an elliptic curve over $\mathbb{Q}$ such that the mod 11 Galois representation is surjective and with $a_2 = 1$, then $\mathbb{Q}(E[11])$ is not monogenic. In particular, 2 will be an essential discriminant divisor for $\mathbb{Q}(E[11])/\mathbb{Q}$.

Theorem 4.4. *Let p, a_p, b_p, and n be as in Table 1, 2, 3, 4, or 5. If E is an elliptic curve over $\mathbb{Q}$ whose reduction at p has trace of Frobenius a_p, index b_p, and such that the Galois representation*

$$\rho_{E,n} : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

*is surjective, then, for the listed n, the torsion field $\mathbb{Q}(E[n])$ is **not** monogenic. Moreover, p is an essential discriminant divisor.*

If, instead of asking $\rho_{E,n}$ to be surjective, we require that E is a Serre curve, then $\rho_{E,n}$ may have index 2 in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. For the red n, when $[\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \rho_{E,n}(\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}))] = 2$, the prime p is no longer an essential discriminant divisor.

Note that employing the process outlined above for all primes up to $[\mathbb{Q}(E[n]) : \mathbb{Q}]$, will identify all essential discriminant divisors. Thus if a positive integer n less than 1000 is not listed in one of the tables below, then the primes 2, 3, 5, 7, and 11 are not essential discriminant divisors of $\mathbb{Q}(E[n])/\mathbb{Q}$; however, even if there are no essential discriminant divisors it may still be the case that $\mathbb{Q}(E[n])$ is not monogenic over $\mathbb{Q}$.

a_2	σ_2	non-monogenic n
0	$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$	3, 5, 9, 11, 15, 17, 21, 27, 33, 43, 51, 57, 63, 85, 91, 93, 105, 117, 129, 171, 195, 255, 257, 273, 315, 331, 341, 381, 455, 513, 585, 657, 683, 771, 819, 993
1	$\begin{bmatrix} 1 & 1 \\ -2 & 0 \end{bmatrix}$	11
-1	$\begin{bmatrix} 0 & 1 \\ -2 & -1 \end{bmatrix}$	11, 23
2	$\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$	5, 13, 15, 17, 41, 51, 65, 85, 91, 105, 117, 145, 195, 205, 255, 257, 273, 315, 455, 565, 585, 771, 819
-2	$\begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}$	5, 13, 15, 17, 41, 51, 65, 85, 91, 105, 117, 145, 195, 205, 255, 257, 273, 315, 455, 565, 585, 771, 819

TABLE 1. Using the splitting of 2 in $\mathbb{Q}(E[n])$ to show non-monogeneity for $n < 1000$.

Remark 4.5. One can generalize the above algorithm to allow for elliptic curves over arbitrary number fields. If K is a number field in which there is a prime above p with residue class degree 1 and

$$[K(E[n]) : K] = |\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|,$$

then our tables still identify non-monogenic torsion fields. For the relevant generalization of Dedekind's criterion see [19, Chapter 1, Theorem 7.4].

When the residue class degree is not 1 or the degree of the n-torsion field is smaller, the mechanics of our algorithm still work. However, there will be fewer obstruction to monogeneity. Increasing the residue class degree yields more irreducible polynomials of the correct degree, and a smaller n-torsion field will lead to less splitting.

Each of the n that are not red in the tables corresponds to infinitely many elliptic curves, in fact a positive proportion of elliptic curves. To see this, we summarize a theorem of Jones:

Theorem 4.6. *[20, Theorem 4] Almost all elliptic curves are Serre curves.*

Jones counts elliptic curves by naïve height, which works amicably with our methods for for $p \geq 5$. For $p = 2$ or 3, we note that a given trace of Frobenius corresponds to a positive density of elliptic curves. Hence almost all elliptic curves with that trace of Frobenius are Serre curves. Thus every n in Tables 1, 2, 3, 4, and 5 that is not red corresponds to infinitely many elliptic curves. The interested reader should note that Radhakrishnan [25] computed an asymptotic formula for the number of non-Serre curves in his thesis.

Glancing over our tables, it appears that supersingular primes are often obstructions to monogeneity. We can make this precise in a certain case:

Theorem 4.7. *Let $p > 3$ be a prime for which E has good supersingular reduction and suppose $[\mathbb{Q}(E[p+1]) : \mathbb{Q}] > p^2 - p$, then $\mathbb{Q}(E[p+1])$ is not monogenic over $\mathbb{Q}$. Specifically, p is an essential discriminant divisor of $\mathbb{Q}(E[p+1])$ over $\mathbb{Q}$.*

Proof. Since E is supersingular at $p > 3$, we know $a_p = 0$. Thus the matrix representing the class of Frobenius is either

$$\begin{bmatrix} 0 & 1 \\ -p & 0 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 1 & 2 \\ \frac{-p-1}{2} & -1 \end{bmatrix},$$

depending on whether $b_p = 1$ or 2. We compute that both these matrices have order 2 modulo $p+1$. Thus there are more than $\frac{p^2-p}{2}$ primes above p in $\mathbb{Q}(E[p+1])$ and all of these primes above p have residue degree 2. Using Lemma 4.2, there are exactly $\frac{p^2-p}{2}$ irreducible polynomials of degree 2 in $\mathbb{F}_p[x]$. Thus the splitting of p cannot be accommodated by irreducible polynomials of degree 2 in $\mathbb{F}_p[x]$ and our result follows. $\square$

Using the estimate

$$|\operatorname{GL}_2(\mathbb{Z}/(p+1)\mathbb{Z})| \geq (p+1)^4 - \frac{1}{2}(p+1)^4 - \frac{1}{4}(p+1)^4 + \frac{1}{8}(p+1)^4 = \frac{3}{8}(p+1)^4,$$

we expect $[\mathbb{Q}(E[p+1]) : \mathbb{Q}]$ to often be much larger than $p^2 - p$. In particular, Theorem 4.7 holds for Serre curves.

Combining the ideas above we see a given elliptic curve over $\mathbb{Q}$ without CM has infinitely many non-monogenic division fields.

Corollary 4.8. *Let $E/\mathbb{Q}$ be an elliptic curve without CM, then for infinitely many $n > 1$ the division field $\mathbb{Q}(E[n])$ is not monogenic.*

Proof. Serre's open image theorem [26] shows that the image of

$$\rho_E : \operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \operatorname{Aut}\left(E_{\text{tors}}\right) \cong \operatorname{GL}_2\left(\hat{\mathbb{Z}}\right)$$

is open and hence has finite index. Write $I := \left[\mathrm{GL}_2 \left(\hat{\mathbb{Z}} \right) : \rho_E \left(\mathrm{Gal} \left(\overline{\mathbb{Q}}/\mathbb{Q} \right) \right) \right]$.

Note that all sufficiently large primes p satisfy

$$\frac{3}{16I}(p+1)^4 > p^2 - p. \tag{2}$$

Elkies [13] has shown that E has infinitely many supersingular primes. Hence there are infinitely many supersingular primes satisfying (2). For these primes, the splitting of p in $\mathbb{Q}(E[p+1])$ cannot be mirrored by the factorization of a polynomial in $\mathbb{F}_p[x]$. Thus, the division field $\mathbb{Q}(E[p+1])$ is not monogenic over $\mathbb{Q}$. $\qquad\qquad\square$

5. EXPLICIT FAMILIES

We would like to construct explicit families of elliptic curves with non-monogenic torsion fields. Daniels [9] has shown the family

$$E_t : \quad y^2 + xy = x^3 + t, \tag{3}$$

with $t \in \mathbb{Q}$, consists of Serre curves with at most 12 exceptions. Using the methods outlined about, we can quickly compute that if t is odd, then the trace of Frobenius at $p = 2$ is -1. Hence $\mathbb{Q}(E_t[11])$ and $\mathbb{Q}(E_t[23])$ are not monogenic with the exception of at most 12 values of t. Note that if t is even, then E_t is singular at 2. There is nothing particularly special about 2 here and we can do the same thing for other small primes. For example, if $t \equiv 2 \bmod 7$, then E_t is supersingular at 7 and for n equal to 4, 8, 16, 24, 43, 48, 75, 80, 86, 96, 100, 120, 150, 160, 172, 191, 200, 240, 300, 344, 382, 400, 480, 600, 684, 688, 764, 774, 800, 817, or 912, the division field $\mathbb{Q}(E[n])$ is not monogenic over $\mathbb{Q}$, again with the exception of at most 12 values of t.

For another family, we require a result of Mazur.

Theorem 5.1 (Theorem 4 of [23]). *Let $E/\mathbb{Q}$ be a semistable elliptic curve. For every prime $p \geq 11$, the Galois representation*

$$\rho_{E,p} : E[p] \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

is surjective.

Recall that for an elliptic curve E, if the standard coefficient of the short Weierstrass form c_4 and the discriminant Δ are relatively prime, then E is semistable. See [27, VII.5]. We consider an elliptic curve over $\mathbb{F}_p$ with a given trace of Frobenius. For example, the elliptic curve $y^2 + y = x^3 + x^2 + 1$ over $\mathbb{F}_2$ has trace of Frobenius $a_2 = 2$. Note that c_4 is 16 and does not depend on the coefficient a_6. Hence, the family of rational elliptic curves

$$E_s : \quad y^2 + y = x^3 + x^2 + s$$

also has $c_4 = 16$. One computes the discriminant is $\Delta_s = -432s^2 - 280s - 43$. Since Δ_s is always odd, $\gcd(\Delta_s, c_4) = 1$. Therefore, E_s is a family of semistable elliptic curves. Using Theorem 5.1 in conjunction with our methods outlined above, we find that every curve in the family E_s has non-monogenic 13 and 41 division fields.

Similarly to the above,

$$E_{u,v} : y^2 + uy = x^3 + vx^2$$

has discriminant $u^2 \left(16v^3 + 27u^2 \right)$ and the coefficient c_4 is equal to $16v^2$. If we require that u is odd, v is even, and $\gcd(3u, v) = 1$, then $E_{u,v}$ is a family of semistable elliptic curves that has trace of Frobenius $a_2 = 0$. Hence the 11, 43, 331, and 683 division fields are not monogenic over $\mathbb{Q}$.

If one is interested in a given one-parameter family, work of Cojocaru, Grant, and Jones [7], shows that in any one-parameter family with no obstructions almost all elliptic curves are Serre curves.

6. Further Questions

Two natural questions that arise after seeing that there are indeed many division fields that are not monogenic over $\mathbb{Q}$ are:

Question 6.1. Precisely when is a given torsion field $\mathbb{Q}(E[n])$ monogenic over $\mathbb{Q}$?

Question 6.2. Given an elliptic curve E/K and a torsion field $K(E[n])$, are there subfields $L \subsetneq K(E[n])$ over which $K(E[n])$ is monogenic?

Both Questions 6.1 and 6.2 are excellent motivation, but complete answers are likely somewhat far away.

Because of the Weil pairing, a natural L to consider for Question 6.2 is $K(\zeta_n)$. Looking at $\mathbb{Q}(E[2])$ over $\mathbb{Q}$ should be a nice place to test this hypothesis. Computationally, $\mathbb{Q}(E[2])$ is not often monogenic over $\mathbb{Q}$. However, there seem to be special families with monogenic 2-torsion fields. For example, Legendre form, $E_\lambda : y^2 = x(x-1)(x-\lambda)$, requires solving

$$g_\lambda : \ \lambda^6 - 3\lambda^5 + \left(6 - \frac{j}{256}\right)\lambda^4 + \left(\frac{j}{128} - 7\right)\lambda^3 + \left(6 - \frac{j}{256}\right)\lambda^2 - 3\lambda + 1,$$

where j is the j-invariant of E_λ. When $j \in \mathbb{Z}$ is divisible by 256 and $\frac{j}{64} - 27$ is square-free, then λ seems to yield a monogenic generator of $\mathbb{Q}(E_\lambda[2])$ over $\mathbb{Q}$.

7. Tables for $p = 3, 5, 7,$ and 11

For $p \geq 3$, we have possibilities for b_p other than $b_p = 1$. This means that, over $\mathbb{F}_p$ with $p \geq 3$, we have elliptic curves with endomorphism rings that are not generated by the Frobenius endomorphism.

a_3	b_3	σ_3	non-monogenic n
0	1	$\begin{bmatrix} 0 & 1 \\ -3 & 0 \end{bmatrix}$	4, 7, 8, 14, 16, 20, 28, 40, 52, 56, 61, 80, 91, 104, 122, 160, 164, 182, 205, 244, 259, 266, 328, 364, 410, 484, 488, 518, 532, 547, 656, 661, 671, 703, 728, 820, 949, 968
0	2	$\begin{bmatrix} 1 & 2 \\ -2 & -1 \end{bmatrix}$	2, 4, 7, 8, 14, 16, 20, 28, 40, 52, 56, 61, 80, 91, 104, 122, 160, 164, 182, 205, 244, 259, 266, 328, 364, 410, 484, 488, 518, 532, 547, 656, 661, 671, 703, 728, 820, 949, 968
1	1	$\begin{bmatrix} 1 & 1 \\ -3 & 0 \end{bmatrix}$	5, 40
-1	1	$\begin{bmatrix} 0 & 1 \\ -3 & -1 \end{bmatrix}$	5, 23, 40
2	1	$\begin{bmatrix} 1 & 1 \\ -2 & 1 \end{bmatrix}$	4, 11, 22, 136, 272
-2	1	$\begin{bmatrix} -1 & 1 \\ -2 & -1 \end{bmatrix}$	4, 22, 136, 272
3	1	$\begin{bmatrix} 2 & 1 \\ -1 & 1 \end{bmatrix}$	7, 14, 28, 52, 56, 91, 104, 182, 259, 266, 364, 518, 532, 703, 728, 949
-3	1	$\begin{bmatrix} -1 & 1 \\ -1 & -2 \end{bmatrix}$	7, 14, 28, 52, 56, 91, 104, 182, 259, 266, 364, 518, 532, 703, 728, 949

Table 2. Using the splitting of 3 in $\mathbb{Q}(E[n])$ to show non-monogeneity for $n < 1000$.

a_5	b_5	σ_5	non-monogenic n
0	1	$\begin{bmatrix} 0 & 1 \\ -5 & 0 \end{bmatrix}$	3, 6, 8, 12, 18, 21, 24, 39, 42, 48, 52, 63, 78, 104, 126, 156, 186, 208, 217, 248, 252, 279, 312, 372, 434, 449, 504, 521, 558, 624, 651, 744, 868, 898, 939
1	1	$\begin{bmatrix} 1 & 1 \\ -5 & 0 \end{bmatrix}$	11, 28, 56
-1	1	$\begin{bmatrix} 0 & 1 \\ -5 & -1 \end{bmatrix}$	28, 56
2	1	$\begin{bmatrix} 1 & 1 \\ -4 & 1 \end{bmatrix}$	
-2	1	$\begin{bmatrix} -1 & 1 \\ -4 & -1 \end{bmatrix}$	
2	2	$\begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}$	2, 4, 8, 48
-2	2	$\begin{bmatrix} -1 & 2 \\ -2 & -1 \end{bmatrix}$	2, 4, 8, 48
3	1	$\begin{bmatrix} 2 & 1 \\ -3 & 1 \end{bmatrix}$	3, 18, 24, 36, 72
-3	1	$\begin{bmatrix} -1 & 1 \\ -3 & -2 \end{bmatrix}$	3, 18, 24, 36, 72
4	1	$\begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix}$	8, 48
-4	1	$\begin{bmatrix} -2 & 1 \\ -1 & -2 \end{bmatrix}$	8, 48

TABLE 3. Using the splitting of 5 in $\mathbb{Q}(E[n])$ to show non-monogeneity for $n < 1000$.

a_7	b_7	σ_7	non-monogenic n
0	1	$\begin{bmatrix} 0 & 1 \\ -7 & 0 \end{bmatrix}$	4, 8, 12, 16, 24, 43, 48, 75, 80, 86, 96, 100, 120, 150, 160, 172, 191, 200, 240, 300, 344, 382, 400, 480, 516, 600, 684, 688, 764, 774, 800, 817, 911, 912
0	2	$\begin{bmatrix} 1 & 2 \\ -4 & -1 \end{bmatrix}$	4, 8, 12, 16, 24, 43, 48, 75, 80, 86, 96, 100, 120, 150, 160, 172, 191, 200, 240, 300, 344, 382, 400, 480, 516, 600, 684, 688, 764, 774, 800, 817, 911, 912
1	1	$\begin{bmatrix} 1 & 1 \\ -7 & 0 \end{bmatrix}$	
-1	1	$\begin{bmatrix} 0 & 1 \\ -7 & -1 \end{bmatrix}$	
1	3	$\begin{bmatrix} 2 & 3 \\ -3 & -1 \end{bmatrix}$	3, 36, 936
-1	3	$\begin{bmatrix} 1 & 3 \\ -3 & -2 \end{bmatrix}$	3, 9, 18, 36, 936
2	1	$\begin{bmatrix} 1 & 1 \\ -6 & 1 \end{bmatrix}$	10, 20
-2	1	$\begin{bmatrix} -1 & 1 \\ -6 & -1 \end{bmatrix}$	10, 20
3	1	$\begin{bmatrix} 2 & 1 \\ -5 & 1 \end{bmatrix}$	15
-3	1	$\begin{bmatrix} -1 & 1 \\ -5 & -2 \end{bmatrix}$	15
4	1	$\begin{bmatrix} 2 & 1 \\ -3 & 2 \end{bmatrix}$	4, 36, 936
-4	1	$\begin{bmatrix} -2 & 1 \\ -3 & -2 \end{bmatrix}$	4, 9, 36, 936
4	2	$\begin{bmatrix} 3 & 2 \\ -2 & 1 \end{bmatrix}$	4, 36, 936
-4	2	$\begin{bmatrix} -1 & 2 \\ -2 & -3 \end{bmatrix}$	4, 9, 18, 36, 936
5	1	$\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix}$	9, 18, 36, 936
-5	1	$\begin{bmatrix} -2 & 1 \\ -1 & -3 \end{bmatrix}$	36, 936

TABLE 4. Using the splitting of 7 in $\mathbb{Q}(E[n])$ to show non-monogeneity for $n < 1000$

a_{11}	b_{11}	σ_{11}	non-monogenic n
0	1	$\begin{bmatrix} 0 & 1 \\ -11 & 0 \end{bmatrix}$	6, 12, 15, 20, 24, 30, 37, 40, 60, 74, 111, 120, 148, 183, 222, 240, 244, 305, 333, 366, 444, 488, 610, 666, 732, 915, 976
0	2	$\begin{bmatrix} 1 & 2 \\ -6 & -1 \end{bmatrix}$	6, 12, 15, 20, 24, 30, 37, 40, 60, 74, 111, 120, 148, 183, 222, 240, 244, 305, 333, 366, 444, 488, 610, 666, 732, 915, 976
1	1	$\begin{bmatrix} 1 & 1 \\ -11 & 0 \end{bmatrix}$	
−1	1	$\begin{bmatrix} 0 & 1 \\ -11 & -1 \end{bmatrix}$	10
2	1	$\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$	
−2	1	$\begin{bmatrix} -1 & 1 \\ -10 & -1 \end{bmatrix}$	7
3	1	$\begin{bmatrix} 2 & 1 \\ -9 & 1 \end{bmatrix}$	
−3	1	$\begin{bmatrix} -1 & 1 \\ -9 & -2 \end{bmatrix}$	
4	1	$\begin{bmatrix} 2 & 1 \\ -7 & 2 \end{bmatrix}$	
−4	1	$\begin{bmatrix} -2 & 1 \\ -7 & -2 \end{bmatrix}$	
4	2	$\begin{bmatrix} 3 & 2 \\ -4 & 1 \end{bmatrix}$	8, 10, 16
−4	2	$\begin{bmatrix} -1 & 2 \\ -4 & -3 \end{bmatrix}$	8, 16, 86
5	1	$\begin{bmatrix} 3 & 1 \\ -5 & 2 \end{bmatrix}$	7, 14
−5	1	$\begin{bmatrix} -2 & 1 \\ -5 & -3 \end{bmatrix}$	
6	1	$\begin{bmatrix} 3 & 1 \\ -2 & 3 \end{bmatrix}$	6, 45, 90
−6	1	$\begin{bmatrix} -3 & 1 \\ -2 & -3 \end{bmatrix}$	6, 45, 90

TABLE 5. Using the splitting of 11 in $\mathbb{Q}(E[n])$ to show non-monogeneity for $n < 1000$.

References

[1] C. Adelmann. *The decomposition of primes in torsion point fields*, volume 1761 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2001. ISBN 3-540-42035-5. URL https://doi.org/10.1007/b80624.

[2] P. Cassou-Noguès and M. J. Taylor. *Elliptic functions and rings of integers*, volume 66 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1987. ISBN 0-8176-3350-2.

[3] P. Cassou-Noguès and M. J. Taylor. Unités modulaires et monogénéité d'anneaux d'entiers. In *Séminaire de Théorie des Nombres, Paris 1986–87*, volume 75 of *Progr. Math.*, pages 35–64. Birkhäuser Boston, Boston, MA, 1988.

[4] P. Cassou-Noguès and M. J. Taylor. A note on elliptic curves and the monogeneity of rings of integers. *J. London Math. Soc. (2)*, 37(1):63–72, 1988. ISSN 0024-6107. doi: 10.1112/jlms/s2-37.121.63. URL https://doi.org/10.1112/jlms/s2-37.121.63.

[5] T. G. Centeleghe. Integral Tate modules and splitting of primes in torsion fields of elliptic curves. *Int. J. Number Theory*, 12(1):237–248, 2016. ISSN 1793-0421. doi: 10.1142/S1793042116500147. URL https://doi.org/10.1142/S1793042116500147.

[6] S. K. Chebolu and J. Mináč. Counting irreducible polynomials over finite fields using the inclusion-exclusion principle. *Mathematics Magazine*, 84(5):369–371, 2011.

[7] A.-C. Cojocaru, D. Grant, and N. Jones. One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations. *Proc. Lond. Math. Soc. (3)*, 103(4):654–675, 2011. ISSN 0024-6115. doi: 10.1112/plms/pdr001. URL https://doi.org/10.1112/plms/pdr001.

[8] K. Conrad. Factoring after Dedekind. URL https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf.

[9] H. B. Daniels. An infinite family of Serre curves. *J. Number Theory*, 155:226–247, 2015. ISSN 0022-314X. doi: 10.1016/j.jnt.2015.03.016. URL https://doi.org/10.1016/j.jnt.2015.03.016.

[10] R. Dedekind. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. *Gött. Abhandlungen*, pages 1–23, 1878.

[11] T. S. Developers. *SageMath, the Sage Mathematics Software System (Version 7.3)*, 2016. http://www.sagemath.org.

[12] W. Duke and A. Tóth. The splitting of primes in division fields of elliptic curves. *Experiment. Math.*, 11(4):555–565 (2003), 2002. ISSN 1058-6458. URL http://projecteuclid.org/euclid.em/1057864664.

[13] N. D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over **Q**. *Invent. Math.*, 89(3):561–567, 1987. ISSN 0020-9910. doi: 10.1007/BF01388985. URL https://doi.org/10.1007/BF01388985.

[14] T. A. Gassert, H. Smith, and K. E. Stange. A family of monogenic S_4 quartic fields arising from elliptic curves. *J. Number Theory*, 197:361–382, 2019. ISSN 0022-314X. doi: 10.1016/j.jnt.2018.09.026. URL https://doi.org/10.1016/j.jnt.2018.09.026.

[15] C. F. Gauss. *Untersuchungen über höhere Arithmetik*. Deutsch herausgegeben von H. Maser. Chelsea Publishing Co., New York, 1965.

[16] E. González-Jiménez and Á. Lozano-Robledo. Elliptic curves with abelian division fields. *Math. Z.*, 283(3-4):835–859, 2016. ISSN 0025-5874. URL https://doi.org/10.1007/s00209-016-1623-z.

[17] J. Han. The general linear group over a ring. *Bull. Korean Math. Soc.*, 43(3):619–626, 2006. ISSN 1015-8634. doi: 10.4134/BKMS.2006.43.3.619. URL https://doi.org/10.4134/BKMS.2006.43.3.619.

[18] K. Hensel. Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung. *J. Reine Angew. Math.*, 113:128–160, 1894. ISSN 0075-4102. doi: 10.1515/crll.1894.113.128. URL https://doi.org/10.1515/crll.1894.113.128.

[19] G. J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996. ISBN 0-8218-0429-4.

[20] N. Jones. Almost all elliptic curves are Serre curves. *Trans. Amer. Math. Soc.*, 362(3):1547–1570, 2010. ISSN 0002-9947. doi: 10.1090/S0002-9947-09-04804-1. URL https://doi.org/10.1090/S0002-9947-09-04804-1.

[21] E. E. Kummer. Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren. *J. Reine Angew. Math.*, 35:327–367, 1847. ISSN 0075-4102. doi: 10.1515/crll.1847.35.327. URL https://doi.org/10.1515/crll.1847.35.327.

[22] E. E. Kummer. *Collected papers.* Springer-Verlag, Berlin-New York, 1975. Volume I: Contributions to number theory, Edited and with an introduction by André Weil.

[23] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978. ISSN 0020-9910. doi: 10.1007/BF01390348. URL https://doi.org/10.1007/BF01390348.

[24] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004. ISBN 3-540-21902-1. doi: 10.1007/978-3-662-07001-7. URL http://dx.doi.org/10.1007/978-3-662-07001-7.

[25] V. Radhakrishnan. *An asymptotic formula for the number of non-Serre curves in a two-parameter family of elliptic curves.* PhD thesis, 2008. URL https://colorado.idm.oclc.org/login?url=https://search-proquest-com.colorado.idm.oclc.org/docview/304629348?accountid=14503. Copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2019-10-17.

[26] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972. ISSN 0020-9910. doi: 10.1007/BF01405086. URL https://doi.org/10.1007/BF01405086.

[27] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. ISBN 978-0-387-09493-9. doi: 10.1007/978-0-387-09494-6. URL https://doi.org/10.1007/978-0-387-09494-6.

[28] W. C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2: 521–560, 1969. ISSN 0012-9593. URL http://www.numdam.org/item?id=ASENS_1969_4_2_4_521_0.

[29] W. C. Waterhouse and J. S. Milne. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 53–64, 1971.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CONNECTICUT, 341 MANSFIELD ROAD U1009 STORRS, CT 06269-1009 USA

Email address: hanson.smith@uconn.edu or hansonsmith101@gmail.com