5-2010

On the Frequency of Finitely Anomalous Elliptic Curves

Penny Catherine Ridgdill
University of Massachusetts Amherst

ON THE FREQUENCY OF FINITELY ANOMALOUS ELLIPTIC CURVES

A Dissertation Presented

by

PENNY C. RIDGDILL

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2010

Mathematics and Statistics

ON THE FREQUENCY OF FINITELY ANOMALOUS ELLIPTIC CURVES

A Dissertation Presented

by

PENNY C. RIDGDILL

Approved as to style and content by:

Tom Weston, Chair

Farshid Hajir, Member

Siman Wong, Member

Kevin Fu, Member

George Avrunin, Department Head
Mathematics and Statistics

Dedication

I would like to dedicate this to my mother, Nita (aka Mama). She instilled in me a love of learning at a very early age and consistently encouraged me to challenge myself intellectually. It was this thirst for knowledge that ultimately led me to pursue a Ph.D. in mathematics, and for that, I will always be grateful.

Thank you Mama. I love you very much.

ACKNOWLEDGMENTS

I would like to thank the following people.

Tom Weston: for being a brilliant and incredibly supportive adviser and mentor. He helped me to believe in myself academically, and supported me with patience and compassion through many personal difficulties during my studies. His knowledge and advice have been invaluable to me.

My Family and Friends: for being loving, supportive and generally amazing through this whole process. I could not have done this without them. There are far too many to name individually and I would feel terrible if I left one of them out.

Farshid Hajir, Siman Wong, and Kevin Fu: for serving on my committee and taking an interest in my work. They have all been very kind and supportive to me. Additional thanks to Siman and Farshid for the really neat math that I have learned from them in courses and seminars.

Rod Canfield: for giving me the courage to get my PhD in the first place. He was an amazing undergraduate adviser and I learned some really cool, fun, powerful, and exciting math and computer science from him.

Malcom Adams, Dan Nakano, Brian Boe, Peter Norman, Eduardo Cattani, Nelson Rushton, David Galewski (in loving memory), Franz Pedit, David Lowenthal, Bill Meeks, Nathaniel Whitaker, Andrea Nahmod, Mike Sullivan, Eileen Kramer, Helga Enko, and Eyal Markman: for be-

ing exceptional teachers, for teaching awesome classes, and for being incredibly accessible and supportive of my career.

George Avrunin: for making sure they got all of my paperwork when part of my application for grad school didn't make it, and for being a very encouraging department head.

Arline Norkin: for supporting my teaching and always giving me good teaching assignments.

Lucy Hemmendinger: for providing excellent counseling and stress management advice.

Finally, I would like to express my gratitude to the entire Mathematics Department at the University of Massachusetts and the Mathematics and Computer Science Departments at the University of Georgia. They have all been very good to me, and I feel lucky to have been a part of both places.

ABSTRACT

ON THE FREQUENCY OF FINITELY ANOMALOUS ELLIPTIC CURVES

MAY 2010

PENNY C. RIDGDILL, B.S. UNIVERSITY OF GEORGIA

M.S., UNIVERSITY OF MASSACHUSETTS AMHERST

Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Tom Weston

Given an elliptic curve E over $\mathbb{Q}$, we can then consider E over the finite field $\mathbf{F}_p$. If N_p is the number of points on the curve over $\mathbf{F}_p$, then we define $a_p(E) = p+1-N_p$. We say primes p for which $a_p(E) = 1$ are anomalous. In this paper, we search for curves E so that this happens for only a finite number of primes. We call such curves finitely anomalous. This thesis deals with the frequency of their occurrence and finds several examples.

TABLE OF CONTENTS

LIST OF TABLES

C H A P T E R 1

INTRODUCTION

1.1 Finitely Anomalous Elliptic Curves

For a fixed elliptic curve E over $\mathbb{Q}$, for any prime p we can consider E over $\mathbf{F}_p$ by reducing the coefficients of the equation of the curve modulo p. Now, there are a finite number of points, N_p, on the curve over $\mathbf{F}_p$. Standard estimates suggest that $N_p \approx p + 1$[7](§5), so we define $a_p = p + 1 - N_p$.

Given an elliptic curve E, suppose that we have $a_p(E) = 1$ for some p. Following Mazur [5], such a p is called an *anomalous prime* for the curve E. In other words, p is anomalous if the curve has p points over $\mathbf{F}_p$. The conjecture of Lang–Trotter [6], predicts that the proportion of primes $p \leq x$ with $a_p = 1$ is $C \cdot \frac{\sqrt{x}}{\log x}$, where C is some constant. However, under various local obstructions, one can have $C = 0$. We call an elliptic curve *finitely anomalous* if this is the case; that is if there are only finitely many p so that $a_p(E) = 1$. These curves are of particular interest to those studying Iwasawa theory [5](proposition 8.2), deformation theory [10](theorem 1), and elliptic curve cryptography [9].

Let $E[N]$ be the set of N-torsion points for the curve E. Then $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on these points by acting on the coordinates of the points. After choosing a basis for $E[N]$, we have that $\mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. This gives us a representation

of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$,

$$\rho_{E,N} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}),$$

which we call the (mod N) Galois representation.

We know that if we choose $Frob_p$ to be some p-power Frobenius element of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, then the trace of its image under the representation $\rho_{E,N}$ is congruent to $a_p \pmod N$ for primes p which do not divide N or the conductor of E by [7](§5). Suppose there is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ which has no elements with trace 1, and that we have a curve whose image under its (mod N) Galois representation lands inside this subgroup. Then we are able to guarantee that $a_p(E) \not\equiv 1 \pmod N$ for any p which does not divide NN_E (where N_E is the conductor of E), and thus the curve is finitely anomalous.

Given an elliptic curve $E/\mathbb{Q}$, let

$$\mathcal{O}(E) = \{N \text{ such that the image of } \rho_{E,N} \text{ is trace 1 free}\}$$

be the set of *obstructions* to anomalous primes for E. If we can show that $\mathcal{O}(E) \neq \emptyset$ then the curve will be finitely anomalous. If however the set is empty, then Lang–Trotter would predict that the curve would be infinitely anomalous. Thus, we try to find finitely anomalous curves by trying to find some member $N \in \mathcal{O}(E)$.

1.2 General Approach

A theorem of Serre [2] tells us that given a non-CM elliptic curve over $\mathbb{Q}$, the (mod ℓ) Galois representation is non-surjective only finitely often, as we vary over primes ℓ. If the representation is surjective, then $\ell \notin \mathcal{O}(E)$. Thus, we need only concern ourselves with those representations which are non-surjective. Swinnerton-

Dyer [1] tells us that the possible images of non-surjective (mod ℓ) representations are limited to certain types of subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. These are Borel subgroups, normalizers of split or non-split Cartan subgroups, or the exceptional groups A_4, S_4, A_5. We can look at these various types of subgroups individually and search for those that are trace 1 free. We also address a small number of composite values N where the (mod N) representation is contained in a Borel subgroup. Let $\mathcal{O}_B(E)$ be the set of obstructions N so that the image of $\rho_{E,N}$ is contained in a Borel subgroup. We will call these the *Borel obstructions*. Similarly, we can define $\mathcal{O}_S(E)$, $\mathcal{O}_N(E)$, and $\mathcal{O}_E(E)$ for the split Cartan, non-split Cartan, and exceptional cases respectively. Then we have

$$\mathcal{O}(E) = \mathcal{O}_B(E) \cup \mathcal{O}_S(E) \cup \mathcal{O}_N(E) \cup \mathcal{O}_E(E).$$

Now, studying the obstructions can be reduced to studying them within each type of subgroup individually. In this paper, we focus on the Borel obstructions and the split Cartan obstructions.

1.3 Results

We should remark that any elliptic curve which has 2-torsion is always finitely anomalous. This is because for $p > 2$ where p does not divide the conductor of E, $a_p(E)$ will always be even.

For the Borel case, the results can be summed up in Table 1, which contains all those curves E such that $\mathcal{O}_B(E)$ is not empty, and thus are finitely anomalous. It also contains any quadratic twists of those curves which are finitely anomalous as well.

Table 1. Finitely Anomalous Borel Curves

Conductor	Class	Curve	Finitely Anomalous (Quadratic) Twists
121	2	1	No Twists
50	1	1	All Twists
50	2	1	Twist by -3
361	1	1	Twist by -19
162	2	1	Twist by -3
162	3	1	Twisty by -3
1849	1	1	Twist by -43
4489	1	1	Twist by -67

For the split Cartan case, we conjecture that one picks up no new obstructions. For $\ell \equiv 3 (\mathrm{mod}\, 4)$ (where ℓ is some prime), we prove that $\ell \notin \mathcal{O}_S(E)$. We also prove this for $\ell \equiv 1 (\mathrm{mod}\, 8)$, and have strong indications that it will be true for $\ell \equiv 5 (\mathrm{mod}\, 8)$. In other words, our conjecture is that for any prime ℓ, $\ell \notin \mathcal{O}_S(E)$. While there could potentially be obstructions for composite N, we do not deal with that in this thesis as the theory is not currently well-developed.

CHAPTER 2

BOREL SUBGROUP

2.1 Borel Curves

First, we need to find those elliptic curves E which have the image of their (mod N) Galois representations inside of a Borel subgroup. The following result allows us to relate this to the rational isogenies of the curve.

Proposition 2.1 *An elliptic curve E has $\mathrm{im}(\rho_{E,N})$ contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ if and only if it has a cyclic, rational N-isogeny.*

Proof. Let

$$\Phi : E \longrightarrow \tilde{E}$$

be a cyclic N-isogeny which is defined over $\mathbb{Q}$. Then we have that $\ker(\Phi) \cong (\mathbb{Z}/N\mathbb{Z})$. Let P be a generator for $\ker(\Phi)$. We know that $P \in E[N]$. We can then find $Q \in E[N]$ so that (P, Q) is a basis for $E[N]$, since $E[N] \cong (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$. Let σ be some element of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then

$$\rho_{E,N}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where $\rho_{E,N}$ is with respect to basis (P, Q). Thus $\sigma(P) = aP + cQ$ and $\sigma(Q) = bP + dQ$. We need to show that $c = 0$ for any σ. Since Φ is defined over $\mathbb{Q}$, we

have that $\sigma(\Phi(P)) = \Phi(\sigma(P)$. This gives that $\sigma(P)$ is also in $\ker(\Phi)$, which shows that c must be zero. Thus, if we have such an isogeny, we know that the image of the Galois representation is contained in a Borel subgroup.

Now, suppose that we have $\mathrm{im}(\rho_{E,N})$ contained in some Borel subgroup. Let $\{P, Q\}$ be the basis for $E[N]$ giving rise to this representation. Let $G = \langle P \rangle$, a finite subgroup of $E[N]$. Our representation having image inside a Borel subgroup shows that G must be Galois stable. By Proposition 4.12 in [7] and the remarks that follow, we are able to construct the desired rational N-isogeny, $E \to E/G$. $\diamond$

Now, [4] gives us a complete classification of elliptic curves (up to twist) which have rational N-isogenies, thus giving us a list of curves (up to twist) which have images contained in a Borel subgroup. This allows us to reduce our search to a finite number of curves and their twists.

2.2 Computing $a_p(E) (\mathrm{mod}\ \ell)$

We first do the computation for $N = \ell$, prime. Suppose we have that

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

has its image inside a Borel subgroup. Then we know that after conjugation (i.e., a change of basis), it has the property

$$\rho_{E,\ell}(\mathrm{Frob}_p) = \begin{pmatrix} \chi_1(p) & * \\ 0 & \chi_2(p) \end{pmatrix},$$

where $\chi_1\chi_2 = \omega$, the ℓth cyclotomic character. Moreover, we know that $a_p(E) \equiv \mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_p))(\mathrm{mod}\ \ell)$[7](§5.2). This gives us that

$$a_p(E) \equiv \chi_1(p) + \omega\chi_1^{-1}(p) (\mathrm{mod}\ \ell)$$

We are able to compute $a_p(\mathrm{mod}\,\ell)$ by finding $\chi = \chi_1$. If E has an ℓ-isogeny, then it has ℓ-torsion defined over some abelian extension of $\mathbb{Q}$. We look at the defining polynomial for the ℓ-torsion subgroup over $\mathbb{Q}$ (which we call the *ℓ-torsion polynomial*), whose roots we know to be the x-coordinates of ℓ-torsion points. We then take the lowest degree factor and find the discriminant of its splitting field. By factoring the discriminant, we can find the smallest s so that the splitting field is contained in the cyclotomic field $\mathbb{Q}(\zeta_s)$. We know such an s exists by the Kronecker-Weber theorem (since these are abelian extensions). We then factor this lowest degree polynomial factor in the cyclotomic field. Once we have a root, we have an x-coordinate. We then put into the Weirstrass equation for the curve to find the y-coordinate to get the point P. When we take ζ_s to ζ_s^i, it takes P to mP for some $1 \leq m < \ell$ with $\gcd(\ell, m) = 1$. We then define $\chi(i) = m$. Then using that $\omega(\mathrm{Frob}_p) = p(\mathrm{mod}\,\ell)$, we are able to compute $a_p(E)(\mathrm{mod}\,\ell)$ using the formula above.

In the case that we are dealing with an N-isogeny where N is composite, the process is not very different. In the case that N is 15 or 21, we use the same process as above on the prime factors ℓ_i of N and then use the Chinese Remainder Theorem to combine the resulting χ_i's to compute χ and then a_p. In the case where N is 27, since we cannot use the Chinese Remainder Theorem, we simply find a point of order 27 and use the same process as above.

Fiinally, let

$$\mathcal{A}_N(E) = \{p(\mathrm{mod}\,\tilde{s}) \text{ such that } a_p(E) \equiv 1(\mathrm{mod}\,N)\},$$

where $\tilde{s}$ is the least common multiple of s (as above) and N. If $\mathcal{A}_N(E) = \emptyset$, then $N \in \mathcal{O}_B(E)$, and we have found a finitely anomalous elliptic curve. Otherwise, $N \notin \mathcal{O}_B(E)$.

Proposition 2.2 *Let E be an elliptic curve over $\mathbb{Q}$. Then $\mathcal{O}_B(E) \neq \emptyset \iff$ there exists some N such that:*

1. *E has a cyclic rational N-isogeny.*

2. *$\mathcal{A}_N(E) = \emptyset$.*

Proof. We know that in order to have a Borel obstruction, the curve must have a Borel representation. These must have rational cyclic N-isogenies by the first proposition. It is clear that if $\mathcal{A}_N(E)$ is empty, then we have $N \in \mathcal{O}_B(E)$. Since these are the only possible Borel obstructions, if $\mathcal{A}_N(E)$ is non-empty, we have that the set of obstructions would be empty. $\diamond$

This gives us a way to find Borel curves which are finitely anomalous. These are given in Table 1 in the first chapter. We illustrate this process via example in the next section.

2.3 Example

We illustrate this process by an example. We use the Cremona tables to find a curve of lowest conductor with an 11-isogeny. This is the curve of conductor 121 with Weirstrass equation $y^2 + xy = x^3 + x^2 - x - 7$. The 11-torsion polynomial factors in $\mathbb{Q}(\zeta_{11})$ and the resulting torsion point P is

$$(-2\zeta_{11}^8 + 2\zeta_{11}^7 - \zeta_{11}^6 - \zeta_{11}^5 + 2\zeta_{11}^4 - 2\zeta_{11}^3 - 3 :$$
$$12\zeta_{11}^9 + 3\zeta_{11}^8 + 2\zeta_{11}^7 + 10\zeta_{11}^6 + 5\zeta_{11}^4 + 8\zeta_{11}^3 - 3\zeta_{11}^2 + 9\zeta_{11} + 6 : 1).$$

If we define $\sigma_i(\zeta_{11}) = \zeta_{11}^i$,then we get the values for $\chi(i)$ found in the following table.

Table 2. Action of Sigma on the Torsion Point P

σ_i	P	mP	$\chi(i)$
σ_1	P	P	1
σ_2	P	$7P$	7
σ_3	P	$9P$	9
σ_4	P	$5P$	5
σ_5	P	$3P$	3
σ_6	P	$8P$	8
σ_7	P	$7P$	6
σ_8	P	$2P$	2
σ_9	P	$4P$	4
σ_{10}	P	$10P$	10

We then compute the values for $a_p (\text{mod } 11)$ using the formula, and we get the following table.

Table 3. a_p Table for Example

$i \equiv p (\text{mod } 11)$	$a_p (\text{mod } 11)$
1	2
2	1
3	2
4	8
5	1
6	6
7	9
8	6
9	9
10	0

In this example, $\mathcal{A}_{11}(E) = \{2, 5\}$. Therefore, $11 \notin \mathcal{O}_B(E)$, and this curve has no other rational isogenies, thus we have $\mathcal{O}_B(E) = \emptyset$ by the proposition.

2.4 Twisting

Now, once we have found the a_p tables for each of the curves (see appendix A) and thus found $\mathcal{O}_B(E)$ for each one, we must also deal with the twists of these curves.

In this paper we deal only with the case of quadratic twists, as most of the curves of this type only admit quadratic twists (see appendix A). For curves with other types of twists, one can find formulas for computing a_p in [8].

Let D be a square-free integer and let E_D be the quadratic twist of a curve E by a quadratic character $\chi_D = \left(\frac{D}{\cdot}\right)$. Then [7] gives us that

$$a_p(E_D) = \left(\frac{D}{\cdot}\right) a_p(E).$$

This gives that twisting an elliptic curve will only change a_p by a factor of ± 1. Thus, if the a_p table has no values which are either 1 or -1, we are guaranteed that this will remain true for any twist of the curve. Thus, if a curve has an a_p table with no 1 or -1, it and all of its twists are finitely anomalous.

To deal with the curves which do have values of ± 1 in their a_p tables, we must consider twists which would flip the sign of those values, thus changing the curve from finitely anomalous to potentially infinitely anomalous, or vice versa. The following lemma shows that there are only finitely many such twists to check.

Lemma 2.3 *Let $\chi : (\mathbb{Z}/s\mathbb{Z})^* \longrightarrow (\mathbb{Z}/N\mathbb{Z})^*$ be a Dirichlet character. Suppose there exists $b \in (\mathbb{Z}/s\mathbb{Z})^*$ and $t|s$ so that*

$$\chi(b) \equiv \chi(a) (\text{mod } N) \quad \text{for all } a \equiv b (\text{mod } t)$$

Then, the conductor of χ divides t.

Proof. Proof 1: If $\chi(b) \equiv \chi(a) (\text{mod } N)$ for all $a \equiv b (\text{mod } t)$, then

$$1 \equiv \chi(b)\chi^{-1}(a) \equiv \chi(\frac{b}{a}) (\text{mod } N)$$

and,

$$\frac{b}{a} \equiv 1 (\text{mod } t).$$

Thus $\chi(x) \equiv 1 (\text{mod } N)$ for all $x \equiv 1 (\text{mod } t)$. This gives us that χ is periodic $(\text{mod } t)$, and so the conductor of χ must divide t as desired.

$\diamond$

Suppose $\mathcal{A}_N(E) = \{p_1, ..., p_r\}$ (possibly empty). Then we would wish to find a character $\chi_D = \left(\frac{D}{\cdot}\right)$ so that $\chi_D(a) \equiv -1 (\text{mod } N)$ for any $a \equiv p_i (\text{mod } \tilde{s})$ for some i. By the lemma, we see that the conductor of χ_D must divide $\tilde{s}$. However, this is not enough. Suppose that $\{q_0, ..., q_k\}$ are the set of congruences $(\text{mod } m)$ so that

$a_{q_j}(E) \equiv -1 (\text{mod } N)$. Then, we must also guarantee that $\chi_D(b) \equiv 1 (\text{mod } N)$ for any $b \equiv q_j (\text{mod } m)$ for some j. Otherwise, we might flip the sign of one of those non-anomalous values making it anomalous for the twist. If we could successfully do this, we would have found a twist E_D of E which is finitely anomalous, as $\mathcal{A}_N(E_D)$ would now be empty.

We illustrate this via the following example:

Let E be the curve of conductor 50, class 2, curve 1 which has a 15-isogeny. From the table of a_p values (appendix A), we see that the curve is finitely anomalous since $\mathcal{A}_{15}(E) = \emptyset$. However, for $p \equiv 13 (\text{mod } 15)$, we have $a_p(E) \equiv -1 (\text{mod } 15)$. We are looking for a D so that $(\frac{D}{13}) = 1$, so that the twist of the curve by χ_D will remain finitely anomalous. We know that

$$\text{cond}(\chi_D) = \begin{cases} |D| & \text{if } D \equiv 1 (\text{mod } 4) \\ 4|D| & \text{if } D \equiv 2, 3 (\text{mod } 4) \end{cases}$$

.

Thus for this example we have that $D = -3, 5, \text{or} -15$. If $D = -3$, $(\frac{-3}{13}) = 1$. Therefore twisting by -3 gives us another finitely anomalous curve. However, $(\frac{5}{13}) = (\frac{-15}{13}) = -1$. Either of these would flip the -1 to 1, and thus those twists would be infinitely anomalous.

The table containing the finitely anomalous curves and their twists is given in chapter 1 and again in appendix A.

CHAPTER 3

SPLIT CARTAN SUBGROUP

3.1 Split Cartan Subgroups

In the split Cartan case we consider $N = \ell$, prime. In general, a split Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is conjugate to one of the form

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \text{ such that } a, b \in (\mathbb{Z}/\ell\mathbb{Z})^* \right\}.$$

In the normalizer N of C, we also include the off-diagonal matrices. Given C, a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we have the following sequence

$$1 \longrightarrow C \longrightarrow N \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1.$$

For a given curve $E/\mathbb{Q}$, if we could find a subgroup $G \subset N$ so that $\rho_{E,\ell}$ has image contained in G, we would need the determinant map from G to $(\mathbb{Z}/\ell\mathbb{Z})^*$ to be surjective (because of the Weil pairing [7]). If we could then show that G was trace 1 free, and not a strict subset of C (as this is already handled in the Borel case), we would have $\ell \in \mathcal{O}_S(E)$. Thus, we are looking for subgroups $G \subset N$ with

- G is trace 1 free.
- $|det(G)| = \ell - 1$.

- $G \not\subset C$.

G is not easy to get a handle on, so we first look at $H = G \cap C$. Consider the following sequence:

$$G \xrightarrow{\psi} N \xrightarrow{\phi} N/C \cong \mathbb{Z}/2\mathbb{Z}$$

Then $ker(\phi \circ \psi) = G \cap C = H$, and $G/H \hookrightarrow \mathbb{Z}/2\mathbb{Z}$. Thus we have that $[G : H] \leq 2$. If $[G : H] = 1$, we would have $G \subset C$. Therefore we need $[G : H] = 2$. This gives us

$$1 \longrightarrow H \longrightarrow G \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

Then, we try to find an appropriate G which extends such an H.

Now, we consider $H \subset C$ such that

- H is trace 1 free.
- $|det(H)| = (\ell - 1)$ or $\frac{(\ell-1)}{2}$.

Since $H \subset C$, we know that $h \in H$ has the form

$$\begin{pmatrix} h_1 & 0 \\ 0 & h_2 \end{pmatrix}$$

.

If we take $\gamma \in N\ C$, then

$$\gamma h \gamma^{-1} = \begin{pmatrix} h_2 & 0 \\ 0 & h_1 \end{pmatrix} = h_{\text{flip}}$$

.

Let

$$\begin{aligned} \sigma : H &\longrightarrow H \\ h &\longrightarrow h_{\text{flip}} \end{aligned}$$

.

This gives us an action of $\mathbb{Z}/2\mathbb{Z}$ on H, where $0 = id$ and $1 = \sigma$. Through this action we are able to further break down H so that we may search for obstructions.

3.2 The Subgroup H'

Define

$$H^+ = \{h|\sigma(h) = h\} = \{h|h_1 = h_2\}$$

$$H^- = \{h|\sigma(h) = h^{-1}\} = \{h|h_1 = h_2^{-1}\},$$

where σ is the action from the previous section. We would like to have $H = H^+H^-$, however we cannot always guarantee this. We thus define $H' = H^+H^-$. We can then define a map

$$\begin{array}{ccc} H' & \stackrel{\phi}{\rightarrow} & H \\ (h_1, h_2) & \rightarrow & h_1h_2^{-1} \end{array}$$

Now, we wish to see which elements of H are actually in the image of ϕ. In other words, we wish to find $h_1 \in H^+$ and $h_2 \in H^-$ so that $h = h_1h_2^{-1}$. Consider the following maps:

$$h \longrightarrow h\sigma(h)$$

$$h \longrightarrow h^{-1}\sigma(h)$$

If $h = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, then

$$h\sigma(h) = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} \in H^+$$

and

$$h^{-1}\sigma(h) = \begin{pmatrix} a^{-1}b & 0 \\ 0 & b^{-1}a \end{pmatrix} \in H^-$$

We can now construct a map

$$\begin{array}{ccc} H & \xrightarrow{\psi} & H' \\ h & \longrightarrow & (h\sigma(h), h^{-1}\sigma(h)) \end{array}$$

Now consider

$$\phi \circ \psi(h) = \phi(h\sigma(h), h^{-1}\sigma(h)) = h\sigma(h)\sigma^{-1}(h)h = h^2$$

Moreover

$$\psi \circ \phi(h_1, h_2) = \psi(h_1 h_2^{-1}) = (h_1 h_2^{-1}\sigma(h_1 h_2^{-1}), h_2 h_1^{-1}\sigma(h_1 h_2^{-1})) = (h_1^2, h_2^2)$$

This gives us that the squares are contained in the image of ϕ.

Now, we have that

$$H/H' \subset H/H^2,$$

and H/H^2 is isomorphic to one of $1, \mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This gives us that $[H : H'] = 1$, 2, or 4. We saw above that the determinants of H are either all of $(\mathbb{Z}/\ell\mathbb{Z})^*$ or the squares inside of it. We can then look at the determinants of H', which are either the squares or fourth powers in $(\mathbb{Z}/\ell\mathbb{Z})^*$.

Now, since $H^+ \subset C \cong (\mathbb{Z}/\ell\mathbb{Z})^* \times (\mathbb{Z}/\ell\mathbb{Z})^*$, and we have that the diagonal elements are equal, we can take $H^+ = \left\langle \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \right\rangle$. Similarly we can take $H^- = \left\langle \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \right\rangle$. Then we have

$$H' = \left\langle \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \right\rangle$$

3.3 Main Results

Theorem 3.1 *Let E be an elliptic curve whose $(\mathrm{mod}\ \ell)$ Galois representation has image G contained in the normalizer N of a split Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*

1. *If $\ell \equiv 3 (\mathrm{mod}\ 4)$, then $\ell \notin \mathcal{O}_S(E)$.*

2. *If $H' \subset H = G \cap C$ has determinants equal to the squares in $(\mathbb{Z}/\ell\mathbb{Z})^*$, then $\ell \notin \mathcal{O}_S(E)$.*

3. *If $\ell \equiv 1 (\mathrm{mod}\ 8)$, then $\ell \notin \mathcal{O}_S(E)$.*

Proof.

1. We have that

$$X_0^+(\ell^2)(\mathbb{Q}) \cong X_0^+(\ell^2)/\omega \cong X_{\mathrm{split}}(\ell),$$

where $X_{\mathrm{split}}(\ell)$ is the set of all elliptic curves E whose (mod ℓ) Galois representations have their image contained inside the normalizer of a split Cartan subgroup and ω is the Artin-Lehrer involution.

Parent[3] tells us that if ℓ is not a square (mod 4), that $X_{\mathrm{split}}(\ell)$ is trivial. Therefore there are no elliptic curves whose (mod ℓ) Galois representations have images contained inside the normalizer of a split Cartan subgroup when $\ell \equiv 3 (\mathrm{mod}\ 4)$.

2. For a general element $h \in H'$, we have

$$h = \begin{pmatrix} a^i & 0 \\ 0 & a^i \end{pmatrix} \begin{pmatrix} b^j & 0 \\ 0 & b^{-j} \end{pmatrix} = \begin{pmatrix} a^i b^j & 0 \\ 0 & a^i b^{-j} \end{pmatrix}$$

Then we have that $\det(h) = a^{2i}$.

Suppose that the determinants of H' are the squares, and suppose $a = g^k$ where g is a generator for $(\mathbb{Z}/\ell\mathbb{Z})^*$. We know that $\left(k, \frac{(\ell-1)}{2}\right) = 1$ because a^2 must generate the squares. Then we have

$$\text{ord}(a) = \text{ord}(g^k) = \frac{(\ell-1)}{(k, \ell-1)} = (\ell-1) \text{ or } \frac{\ell-1}{2}$$

If $\text{ord}(a) = \frac{\ell-1}{2}$, then $(k, \ell-1) = 2$, and thus k is even and $\frac{\ell-1}{2}$ is odd. That would give that $\ell \equiv 3 (\text{mod } 4)$, which is taken care of by the Parent[3] paper.

Thus, $\text{ord}(a) = \ell - 1$, and a is a generator. Then we have that

$$H' = \left\langle \begin{pmatrix} g & 0 \\ 0 & g \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \right\rangle \subset H$$

Then

$$h \in H' = \begin{pmatrix} g^i & 0 \\ 0 & g^i \end{pmatrix} \begin{pmatrix} b^j & 0 \\ 0 & b^{-j} \end{pmatrix} = \begin{pmatrix} g^i b^j & 0 \\ 0 & g^i b^{-j} \end{pmatrix}$$

.

Then we have $\text{trace}(h) = g^i(b^j + b^{-j})$. Then for $j = 0$, we have that $\text{trace}(h) = g^i$. Since g is a generator we are guaranteed that we can find an element of H with trace 1. Thus, there are no trace 1 free subgroups where the determinants of H' are contained in the squares.

3. If the determinants of H' are the squares, this is handled by the previous statement. Suppose that the determinants of H' are the fourth powers. Using a similar argument as above, we see that $\text{ord}(a^2) = \frac{l-1}{4}$ which gives us that $\text{ord}(a) = \frac{l-1}{2}$. Take $a = g^2$ and $b = g^k$, where g is a generator for $(\mathbb{Z}/\ell\mathbb{Z})^*$. Now, we have that for a general element $h \in H'$, $\text{trace}(h) = g^{2i}(g^{ki} + g^{-kj})$. When $j = 0$, we get that the trace is $g^{2i}(2) (\text{mod } \ell)$. Now, as i goes from 1 to $\ell - 1$, g^{2i} goes through all of the squares. If $\ell \cong 1 (\text{mod } 8)$, we have that 2

is a square $(\mathrm{mod}\ \ell)$, and therefore we would have that for some i, the trace will be $1(\mathrm{mod}\ \ell)$.

$\diamond$

Conjecture 3.2 *Let E be an elliptic curve whose $(\mathrm{mod}\ \ell)$ Galois representation has image contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Then $\ell \notin \mathcal{O}_S(E)$.*

The only thing left to prove is the case where $\ell \equiv 5(\mathrm{mod}\ 8)$ and the determinants of H' are the fourth powers in $(\mathbb{Z}/\ell\mathbb{Z})^*$, as then we will have dealt with all primes ℓ which are either 1 or $3(\mathrm{mod}\ 4)$. Again, there could potentially be some composite obstructions, but the theory is still being developed to handle this case.

A P P E N D I X A

DATA FOR BOREL CURVES

This appendix contains various tables containing the data for curves whose (mod N) Galois representations have images contained in a Borel subgroup. As outlined in the example in chapter 1, the a_p(mod N) values were computed for congruences (mod $\tilde{s}$), where $\tilde{s}$ is the least common multiple of the isogeny, N, and s, the conductor of the cyclotomic field where the torsion point lives. However, for the sake of condensing the tables of a_p values, we take the congruences (mod $\tilde{s}$) and reduce them to give congruences (mod N). Then, rather than a single value for a_p for that congruence, we have a list of all of the a_p values whose p(mod $\tilde{s}$) reduce to that congruence (mod N). The table of finitely anomalous curves and their finitely anomalous twists is given again for completeness.

The reader may also note that we had to deviate from the standard Cremona notation for elliptic curves. The first number is the conductor of the curve. The second number corresponds to its isomorphism class, which is classically given as a letter of the alphabet. However, since some of these curves had classes beyond the number 26, it was necessary to refer to them by number instead of letter. The third number is the curve from that isomorphism class. The reader will note that we always chose the first curve in the class. As an example, E:121-A is referred to as E:121,1,1 in our notation.

Table 4. a_p Table For Curves With An 11-Isogeny

E:121,1,1		E:121,2,1		E:121,3,1	
$p(\text{mod } 11)$	a_p values	$p(\text{mod } 11)$	a_p values	$p(\text{mod } 11)$	a_p values
1	2	1	2	1	2
2	-1	2	0	2	1
3	2	3	10	3	2
4	8	4	7	4	8
5	1	5	8	5	1
6	6	6	0	6	6
7	9	7	0	7	9
8	6	8	0	8	6
9	9	9	6	9	9
10	0	10	0	10	0

Table 5. a_p Table For Curves With A 15-Isogeny

E:50,1,1		E:50,2,1	
$p(\text{mod } 15)$	a_p values	$p(\text{mod } 15)$	a_p values
1	2	1	2
2	12	2	3
4	5	4	5
7	2	7	8
8	6	8	9
11	12	11	12
13	11	13	14
14	0	14	0

Table 6. a_p Table For Curves With An 17-Isogeny

E:14450,14,1		E:14450,16,1	
$p(\text{mod } 17)$	a_p values	$p(\text{mod } 17)$	a_p values
1	$0, 2, 15$	1	$0, 2, 15$
2	$3, 4, 13, 14$	2	$3, 4, 13, 14$
3	$2, 5, 12, 15$	3	$2, 5, 12, 15$
4	$5, 12$	4	$5, 12$
5	$2, 4, 13, 15$	5	$2, 4, 13, 15$
6	$4, 5, 12, 13$	6	$4, 5, 12, 13$
7	$3, 6, 11, 14$	7	$3, 6, 11, 14$
8	$6, 8, 9, 11$	8	$6, 8, 9, 11$
9	$2, 7, 10, 15$	9	$2, 7, 10, 15$
10	$5, 7, 10, 12$	10	$5, 7, 10, 12$
11	$1, 3, 14, 16$	11	$1, 3, 14, 16$
12	$1, 8, 9, 16$	12	$1, 8, 9, 16$
13	$3, 14$	13	$3, 14$
14	$3, 8, 9, 14$	14	$3, 8, 9, 14$
15	$1, 5, 12, 16$	15	$1, 5, 12, 16$
16	$0, 8, 9$	16	$0, 8, 9$
E:14450,37,1		E:14450,38,1	
$p(\text{mod } 17)$	a_p values	$p(\text{mod } 17)$	a_p values
1	$0, 2, 15$	1	$0, 2, 15$
2	$3, 4, 13, 14$	2	$3, 4, 13, 14$
3	$2, 5, 12, 15$	3	$2, 5, 12, 15$
4	$5, 12$	4	$5, 12$
5	$2, 4, 13, 15$	5	$2, 4, 13, 15$
6	$4, 5, 12, 13$	6	$4, 5, 12, 13$
7	$3, 6, 11, 14$	7	$3, 6, 11, 14$
8	$6, 8, 9, 11$	8	$6, 8, 9, 11$
9	$2, 7, 10, 15$	9	$2, 7, 10, 15$
10	$5, 7, 10, 12$	10	$5, 7, 10, 12$
11	$1, 3, 14, 16$	11	$1, 3, 14, 16$
12	$1, 8, 9, 16$	12	$1, 8, 9, 16$
13	$3, 14$	13	$3, 14$
14	$3, 8, 9, 14$	14	$3, 8, 9, 14$
15	$1, 5, 12, 16$	15	$1, 5, 12, 16$
16	$0, 8, 9$	16	$0, 8, 9$

Table 7. a_p **Table For Curves With A 19-Isogeny**

E:361,1,1	
$p(\text{mod } 19)$	a_p values
1	2
2	0
3	0
4	15
5	18
6	10
7	3
8	0
9	13
10	0
11	14
12	0
13	0
14	0
15	0
16	8
17	12
18	0

Table 8. a_p **Table For Curves With A 21-Isogeny**

E:162,2,1		E:162,3,1	
$p(\text{mod } 21)$	a_p values	$p(\text{mod } 21)$	a_p values
1	2, 20	1	2, 20
2	3, 15	2	6, 18
4	5, 11	4	5, 11
5	0, 6, 15	5	0, 6, 15
8	6, 9	8	12, 15
10	11, 14, 17	10	11, 14, 17
11	12, 18	11	3, 9
13	2, 5, 14	13	2, 5, 14
16	8, 17	16	8, 17
17	0, 3, 18	17	0, 3, 18
19	8, 14, 20	19	8, 14, 20
20	0, 9, 12	20	0, 9, 12

Table 9. a_p Table For Curves With An 37-Isogeny

E:1225,5,1		E:1225,6,1	
$p \pmod{37}$	a_p values	$p \pmod{37}$	a_p values
1	0, 22, 1, 35, 2, 36, 15	1	0, 22, 1, 35, 2, 36, 15
2	34, 1, 36, 3, 6, 7, 25, 9, 28, 12, 30, 31	2	34, 1, 36, 3, 6, 7, 25, 9, 28, 12, 30, 31
3	1, 18, 36, 19, 4, 23, 24, 25, 12, 13, 14, 33	3	1, 18, 36, 19, 4, 23, 24, 25, 12, 13, 14, 33
4	34, 18, 19, 3, 5, 8, 9, 27, 10, 28, 29, 32	4	34, 18, 19, 3, 5, 8, 9, 27, 10, 28, 29, 32
5	17, 35, 2, 20, 4, 6, 24, 8, 29, 13, 31, 33	5	17, 35, 2, 20, 4, 6, 24, 8, 29, 13, 31, 33
6	12, 25, 7, 18, 30, 19	6	12, 25, 7, 18, 30, 19
7	1, 36, 4, 22, 5, 7, 8, 29, 30, 15, 32, 33	7	1, 36, 4, 22, 5, 7, 8, 29, 30, 15, 32, 33
8	33, 4, 5, 28, 9, 32	8	33, 4, 5, 28, 9, 32
9	22, 5, 23, 25, 26, 27, 10, 11, 12, 14, 32, 15	9	22, 5, 23, 25, 26, 27, 10, 11, 12, 14, 32, 15
10	0, 17, 20, 22, 26, 11, 15	10	0, 17, 20, 22, 26, 11, 15
11	0, 23, 12, 14, 25, 28, 9	11	0, 23, 12, 14, 25, 28, 9
12	29, 1, 2, 35, 36, 8, 9, 11, 13, 24, 26, 28	12	29, 1, 2, 35, 36, 8, 9, 11, 13, 24, 26, 28
13	35, 2, 5, 22, 23, 7, 8, 29, 30, 14, 15, 32	13	35, 2, 5, 22, 23, 7, 8, 29, 30, 14, 15, 32
14	33, 22, 4, 15, 18, 19	14	33, 22, 4, 15, 18, 19
15	4, 21, 23, 7, 9, 27, 10, 28, 30, 14, 33, 16	15	4, 21, 23, 7, 9, 27, 10, 28, 30, 14, 33, 16
16	17, 1, 18, 36, 19, 20, 21, 6, 27, 10, 31, 16	16	17, 1, 18, 36, 19, 20, 21, 6, 27, 10, 31
17	35, 18, 2, 19, 22, 24, 8, 26, 11, 29, 13, 15	17	35, 18, 2, 19, 22, 24, 8, 26, 11, 29, 13, 15
18	34, 18, 1, 36, 19, 3, 21, 9, 27, 10, 28, 16	18	34, 1, 18, 19, 36, 3, 21, 9, 27, 10, 28, 16
19	31, 3, 34, 6, 14, 15, 17, 18, 19, 20, 22, 23	19	31, 3, 34, 6, 14, 15, 17, 18, 19, 20, 22, 23
20	29, 3, 4, 33, 34, 8, 11, 12, 16, 21, 25, 26	20	29, 3, 4, 33, 34, 8, 11, 12, 16, 21, 25, 26
21	34, 1, 36, 3, 22, 23, 6, 9, 28, 14, 31, 15	21	34, 1, 36, 3, 22, 23, 6, 9, 28, 14, 31, 15
22	17, 20, 22, 5, 23, 24, 27, 10, 13, 14, 32, 15	22	17, 20, 22, 5, 23, 24, 27, 10, 13, 14, 15, 32
23	34, 13, 24, 3, 16, 21	23	34, 13, 24, 3, 16, 21
24	21, 5, 7, 25, 26, 27, 10, 11, 12, 30, 32, 16	24	21, 5, 7, 25, 26, 27, 10, 11, 12, 30, 32, 16
25	17, 20, 4, 6, 25, 8, 26, 11, 29, 12, 31, 33	25	17, 20, 4, 6, 25, 8, 26, 11, 12, 29, 31, 33
26	0, 2, 35, 27, 17, 20, 10	26	0, 2, 35, 27, 17, 20, 10
27	0, 16, 28, 29, 8, 9, 21	27	0, 16, 28, 29, 8, 9, 21
28	35, 2, 21, 23, 7, 8, 27, 10, 29, 30, 14, 16	28	35, 2, 21, 23, 7, 8, 27, 10, 29, 30, 14, 16
29	24, 13, 17, 7, 30, 20	29	24, 13, 17, 7, 30, 20
30	21, 5, 6, 24, 7, 26, 11, 13, 30, 31, 32, 16	30	21, 5, 6, 24, 7, 26, 11, 13, 30, 31, 32, 16
31	34, 35, 2, 3, 5, 32	31	34, 35, 2, 3, 5, 32
32	1, 36, 4, 24, 25, 26, 9, 11, 28, 12, 13, 33	32	1, 36, 4, 24, 25, 26, 9, 11, 28, 12, 13, 33
33	34, 17, 18, 19, 3, 20, 23, 7, 26, 11, 30, 14	33	34, 17, 18, 19, 3, 20, 23, 7, 26, 11, 30, 14
34	34, 35, 2, 3, 4, 6, 24, 27, 10, 13, 31, 33	34	34, 35, 2, 3, 4, 6, 24, 27, 10, 13, 31, 33
35	1, 2, 31, 32, 5, 35, 6, 36, 17, 18, 19, 20	35	1, 2, 31, 32, 5, 35, 6, 36, 17, 18, 19, 20
36	0, 12, 25, 16, 6, 31, 21	36	0, 12, 25, 16, 6, 31, 21
E:14450,37,1		E:14450,38,1	
$p \pmod{37}$	a_p values	$p \pmod{37}$	a_p values
1	0, 22, 1, 35, 2, 36, 15	1	0, 22, 1, 35, 2, 36, 15
2	34, 1, 36, 3, 6, 7, 25, 9, 28, 12, 30, 31	2	34, 1, 36, 3, 6, 7, 25, 9, 28, 12, 30, 31
3	1, 18, 36, 19, 4, 23, 24, 25, 12, 13, 14, 33	3	1, 18, 36, 19, 4, 23, 24, 25, 12, 13, 14, 33
4	34, 18, 19, 3, 5, 8, 9, 27, 10, 28, 29, 32	4	34, 18, 19, 3, 5, 8, 9, 27, 10, 28, 29, 32
5	17, 35, 2, 20, 4, 6, 24, 8, 29, 13, 31, 33	5	17, 35, 2, 20, 4, 6, 24, 8, 29, 13, 31, 33
6	12, 25, 7, 18, 30, 19	6	12, 25, 7, 18, 30, 19
7	1, 36, 4, 22, 5, 7, 8, 29, 30, 15, 32, 33	7	1, 36, 4, 22, 5, 7, 8, 29, 30, 15, 32, 33
8	33, 4, 5, 28, 9, 32	8	33, 4, 5, 28, 9, 32
9	22, 5, 23, 25, 26, 27, 10, 11, 12, 14, 32, 15	9	22, 5, 23, 25, 26, 27, 10, 11, 12, 14, 32, 15
10	0, 17, 20, 22, 26, 11, 15	10	0, 17, 20, 22, 26, 11, 15
11	0, 23, 12, 14, 25, 28, 9	11	0, 23, 12, 14, 25, 28, 9
12	29, 1, 2, 35, 36, 8, 9, 11, 13, 24, 26, 28	12	29, 1, 2, 35, 36, 8, 9, 11, 13, 24, 26, 28
13	35, 2, 5, 22, 23, 7, 8, 29, 30, 14, 15, 32	13	35, 2, 5, 22, 23, 7, 8, 29, 30, 14, 15, 32
14	33, 22, 4, 15, 18, 19	14	33, 22, 4, 15, 18, 19
15	4, 21, 23, 7, 9, 27, 10, 28, 30, 14, 33, 16	15	4, 21, 23, 7, 9, 27, 10, 28, 30, 14, 33, 16
16	17, 1, 18, 36, 19, 20, 21, 6, 27, 10, 31, 16	16	17, 1, 18, 36, 19, 20, 21, 6, 27, 10, 31
17	35, 18, 2, 19, 22, 24, 8, 26, 11, 29, 13, 15	17	35, 18, 2, 19, 22, 24, 8, 26, 11, 29, 13, 15
18	34, 18, 1, 36, 19, 3, 21, 9, 27, 10, 28, 16	18	34, 1, 18, 19, 36, 3, 21, 9, 27, 10, 28, 16
19	31, 3, 34, 6, 14, 15, 17, 18, 19, 20, 22, 23	19	31, 3, 34, 6, 14, 15, 17, 18, 19, 20, 22, 23
20	29, 3, 4, 33, 34, 8, 11, 12, 16, 21, 25, 26	20	29, 3, 4, 33, 34, 8, 11, 12, 16, 21, 25, 26
21	34, 1, 36, 3, 22, 23, 6, 9, 28, 14, 31, 15	21	34, 1, 36, 3, 22, 23, 6, 9, 28, 14, 31, 15
22	17, 20, 22, 5, 23, 24, 27, 10, 13, 14, 32, 15	22	17, 20, 22, 5, 23, 24, 27, 10, 13, 14, 15, 32
23	34, 13, 24, 3, 16, 21	23	34, 13, 24, 3, 16, 21
24	21, 5, 7, 25, 26, 27, 10, 11, 12, 30, 32, 16	24	21, 5, 7, 25, 26, 27, 10, 11, 12, 30, 32, 16
25	17, 20, 4, 6, 25, 8, 26, 11, 29, 12, 31, 33	25	17, 20, 4, 6, 25, 8, 26, 11, 12, 29, 31, 33
26	0, 2, 35, 27, 17, 20, 10	26	0, 2, 35, 27, 17, 20, 10
27	0, 16, 28, 29, 8, 9, 21	27	0, 16, 28, 29, 8, 9, 21
28	35, 2, 21, 23, 7, 8, 27, 10, 29, 30, 14, 16	28	35, 2, 21, 23, 7, 8, 27, 10, 29, 30, 14, 16
29	24, 13, 17, 7, 30, 20	29	24, 13, 17, 7, 30, 20
30	21, 5, 6, 24, 7, 26, 11, 13, 30, 31, 32, 16	30	21, 5, 6, 24, 7, 26, 11, 13, 30, 31, 32, 16
31	34, 35, 2, 3, 5, 32	31	34, 35, 2, 3, 5, 32
32	1, 36, 4, 24, 25, 26, 9, 11, 28, 12, 13, 33	32	1, 36, 4, 24, 25, 26, 9, 11, 28, 12, 13, 33
33	34, 17, 18, 19, 3, 20, 23, 7, 26, 11, 30, 14	33	34, 17, 18, 19, 3, 20, 23, 7, 26, 11, 30, 14
34	34, 35, 2, 3, 4, 6, 24, 27, 10, 13, 31, 33	34	34, 35, 2, 3, 4, 6, 24, 27, 10, 13, 31, 33
35	1, 2, 31, 32, 5, 35, 6, 36, 17, 18, 19, 20	35	1, 2, 31, 32, 5, 35, 6, 36, 17, 18, 19, 20
36	0, 12, 25, 16, 6, 31, 21	36	0, 12, 25, 16, 6, 31, 21

Table 10. a_p Table For Curves With A 43-Isogeny

E:1849,1,1			
$p(\text{mod } 43)$	a_p values	$p(\text{mod } 43)$	a_p values
1	2	22	0
2	0	23	7
3	0	24	28
4	39	25	33
5	0	26	0
6	29	27	0
7	0	28	0
8	0	29	0
9	37	30	0
10	30	31	34
11	42	32	0
12	0	33	0
13	3	34	0
14	20	35	22
15	19	36	12
16	8	37	0
17	5	38	18
18	0	39	0
19	0	40	26
20	0	41	32
21	27	42	0

Table 11. a_p Table For Curves With A 67-Isogeny

E:4489,1,1					
p(mod 67)	a_p values	p(mod 67)	a_p values	p(mod 67)	a_p values
1	2	23	5	45	0
2	0	24	30	46	0
3	0	25	57	47	11
4	63	26	39	48	0
5	0	27	0	49	53
6	52	28	0	50	0
7	0	29	7	51	0
8	0	30	0	52	0
9	61	31	0	53	0
10	43	32	0	54	45
11	0	33	20	55	32
12	0	34	0	56	31
13	0	35	41	57	0
14	18	36	12	58	0
15	44	37	58	59	13
16	8	38	0	60	46
17	66	39	42	61	0
18	0	40	48	62	28
19	3	41	0	63	0
20	0	42	0	64	51
21	34	43	0	65	27
22	50	44	0	66	0

Table 12. Finitely Anomalous Borel Curves

Conductor	Class	Curve	Finitely Anomalous Twists
121	2	1	No Twists
50	1	1	All Twists
50	2	1	Twist by -3
361	1	1	Twist by -19
162	2	1	Twist by -3
162	3	1	Twisty by -3
1849	1	1	Twist by -43
4489	1	1	Twist by -67

A P P E N D I X B

ELLIPTIC CURVE CRYPTOGRAPHY

In the mid 1980's, Neal Koblitz and Victor Miller proposed a variation of the discrete logarithm problem (as is used in the Diffie-Hellman algorithm), which used elliptic curves as the main tool of the system.

Consider the process of taking an element $a \in \mathbb{F}_p$ and raising it to the n^{th} power, ie, $a^n (\mathrm{mod} p)$. For a particular $b \in \langle a \rangle$, the cyclic subgroup generated by a, we have the $b \equiv a^k (\mathrm{mod}\ p)$ for some $k < \mathrm{ord(a)}$. The key observation which made this a good tool for a cryptosystem is that computing $a^k (\mathrm{mod} p)$ is very easy if we have a and k, but given only a and b, finding the power k such that $b \equiv a^k (\mathrm{mod}\ p)$ is very difficult when p and k are sufficiently large. This is the discrete logarithm problem over $\mathbb{F}_p$.

For the elliptic curve systems, the idea is very similar. In this paper we look at elliptic curve cryptosystems when the new base field of the curve is taken to be $\mathbb{F}_p$ and p is a prime number. Other systems use base fields $\mathbb{F}_q$ where q is a prime power or a power of 2. Given an elliptic curve over $\mathbb{Q}$ with equation $y^2 = x^3 + ax + b$, we can then look at the curve over $\mathbb{F}_p$. That is, we have the points (x, y) where $x, y \in \mathbb{F}_p$, remembering to include the base point (or point at infinity) $\mathcal{O}$. We denote the set of points of E living in $\mathbb{F}_p$ by $E(\mathbb{F}_p)$. Under the special addition of

points on elliptic curves, we define for a positive integer n,

$$[n]P = \underbrace{P + P + ... + P}_{\text{n times}}$$

.

Now, for a point P on the curve E, we can take the cyclic subgroup of $E(\mathbb{F}_p)$ generated by P. For a point $Q \in \langle P \rangle$, we have that $Q = [k]P$ for some k. Similar to the discrete log problem above, it is easy to compute $[k]P$ given P and k, but it is extremely difficult to find k if we are simply given Q and P if the order of the point P and k are sufficiently large.

However, these systems, like all cryptosystems, are subject to certain attacks. We will call a pair (E, p) an anomalous pair if p is an anomalous prime for the curve E. Nigel Smart, in 1999 wrote [9], showing that if the cryptosystem used such an anomalous pair, the elliptic curve discrete logarithm problem can be solved in linear time. For this reason, using a finitely anomalous elliptic curve and avoiding its set of anomalous primes gives a much more secure system. Thus, finding such curves is important for computer scientists and cryptographers.

BIBLIOGRAPHY

[1] H.P.F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms. Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), Lecture Notes in Math., Vol. 350, Springer, Berlin, (1973),1-55*

[2] J.P. Serre, *Proprietes galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972), 259-331*

[3] Pierre J.R. Parent, *Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$. (English summary) Compos. Math. 141 (2005), no. 3, 561-572*

[4] B. Mazur, *Rational isogenies of prime degree, Inventiones Math. 44 (1978), 129-162.*

[5] B. Mazur, *Rational points of abelian varieties with values in towers of number fields, Invent. Math., 18 (1972), 183-266*

[6] Serge Lang, Hale Trotter, *Frobenius distributions in* GL_2*-extensions. Distribution of Frobenius automorphisms in* GL_2*-extensions of the rational numbers. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976. iii+274 pp*

[7] J. Silverman, *The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp*

[8] Kenneth Ireland, Michael Rosen, *A classical introduction to modern number theory. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990. xiv+389 pp*

[9] Nigel P. Smart, *The Discrete Logarithm Problem on Elliptic Curves of Trace One. J. Cryptology 12(3): 193-196 (1999)*

[10] Tom Weston, *Unobstructed modular deformation problems. (English Summary) Amer. J. Math. 126 (2004), no. 6, 1237–1252*