ON A CONJECTURE FOR THE DISTRIBUTIONS OF PRIMES ASSOCIATED WITH ELLIPTIC CURVES

Jeremy Graham Porter

A Thesis

in

the Department

of

Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements

For the Degree of Master of Science (Mathematics) at

Concordia University

Montreal, Quebec, Canada

September 2009

Abstract

On a conjecture for the distributions of primes associated with elliptic curves

Jeremy Porter

For an elliptic curve E and fixed integer r, Lang and Trotter have conjectured an asymptotic estimate for the number of primes $p \leq x$ such that the trace of Frobenius $a_p(E) = r$. Using similar heuristic reasoning, Koblitz has conjectured an asymptotic estimate for the number of primes $p \leq x$ such that the order of the group of points of E over the finite field $\mathbb{F}_p$ is also prime. These estimates have been proven correct for elliptic curves "on average"; however, beyond this the conjectures both remain open.

In this thesis, we combine the condition of Lang and Trotter with that of Koblitz to conjecture an asymptotic for the number of primes $p \leq x$ such that both $|E(\mathbb{F}_p)|$ is prime, and $a_p(E) = r$. In the case where E is a Serre curve, we will give an explicit construction for the estimate. As support for the conjecture, we will also provide several examples of Serre curves for which we computed the number of primes $p \leq x$ such that $|E(\mathbb{F}_p)|$ is prime and $a_p(E) = r$, and compared this count with the conjectured estimates.

Acknowledgements

To begin with, I owe a great debt to Dr. Chantal David for her insights, advice, and boundless patience while supervising this thesis. I would also thank my family for their unwavering encouragement, and my good friends for reprieve and support even from afar. Finally and most importantly I thank my wife Carolyn, without whom I could accomplish nothing worthwhile.

Table of Contents

List of Tables

Introduction

In [HL23], Hardy and Littlewood posed a heuristic argument for asymptotically counting the number of twin primes less than a given upper bound. Their argument centered around probabilistic methods, treating the integers as random events and subsets thereof as occuring with given probability. For a fixed elliptic curve $E/\mathbb{Q}$ without complex multiplication and an integer r, Lang and Trotter used similar heuristics to propose in [LT76] an estimate for the number of primes $p \leq x$ such that $p + 1 - |E(\mathbb{F}_p)| = r$, where $E(\mathbb{F}_p)$ is the group of points of E over $\mathbb{F}_p$.

Lang-Trotter Conjecture ([LT76])**.** *Let E be an elliptic curve without complex multiplication, and r an integer. Let $\pi_r^{\mathrm{LT}}(x)$ be the number of primes p for which $p + 1 - |E(\mathbb{F}_p)| = r$. Then*

$$\pi_r^{LT}(x) = \#\{p \leq x : p + 1 - |E(\mathbb{F}_p)| = r\} \sim C_{E,r} \cdot \frac{\pi(\sqrt{x})}{\log(x)}$$

where $C_{E,r}$ is a constant depending on the curve E and the constant r.

Lang and Trotter employ the Tchebotarev Density Theorem and Sato-Tate Conjecture to express the approximate number of primes p as a density. This estimate also relies on the Galois representation discussed in [Ser71] arising from the automorphism groups on the torsion points of elliptic curves. Serre proved that for an elliptic curve E over the rationals without complex multiplication, the image of the map

$$\hat{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \prod_{\ell} \mathrm{GL}_2(\mathbb{Z}_\ell)$$

is a subgroup of finite index of $\prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$. This implies in particular that the reductions

$$\rho_m : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

are surjective for all integers m coprime to some finite value. Serre also noticed that the image of $\hat{\rho}$ is always contained in a subgroup of index 2 of $\prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$. This leads to the concept of a *Serre curve*, defined to be an elliptic curve for which the image of $\hat{\rho}$ is the full subgroup of index 2. In these cases the constant $C_{E,r}$ may be written explicitly.

Similar to Lang and Trotter, but motivated by applications to public-key cryptography, in [Kob88], Koblitz proposed an estimate for the number of primes p such that $|E(\mathbb{F}_p)|$ is also prime.

Koblitz Conjecture ([Kob88])**.** *Let E be an elliptic curve with no complex multiplication. Then the number of primes p of good reduction for which the number of points on the curve $E(\mathbb{F}_p)$ is also prime can be written asymptotically as*

$$\pi^K(x) = \#\{p \leq x : \ |E(\mathbb{F}_p)| \text{ is prime}\} \sim C_E \cdot \frac{x}{\log^2(x)},$$

where C_E depends on the curve E.

The description of C_E was later refined by Zywina in [Zyw09], who also provided strong computational evidence for the conjecture by comparing the predicted and actual number of primes p up to one billion for several distinct curves.

To this day, both conjectures remain widely open, and we do not even know whether $\pi^{\mathrm{LT}}(x)$ or $\pi^{\mathrm{K}}(x)$ are unbounded. But there has been considerable work toward analyzing both the Koblitz and Lang-Trotter conjectures on average, notably in [BCD07], [BJ09], [Bai06], [DP99], and [Jon]. As an intermediate result, the authors of [BCD07] were led to consider an average for a composite of the Lang-Trotter and Koblitz conjectures, which can be expressed as follows.

Mixed Conjecture. *Let E be an elliptic curve with no complex multiplication, and let r be an nonzero integer with $r \neq 1$. Then we can write asymptotically the number of primes of good reduction for which both $p + 1 - |E(\mathbb{F}_p)|$ is equal to the nonzero constant r and the number of points on the curve $|E(\mathbb{F}_p)|$ is also prime as*

$$\pi^{Mix}(x) = \#\left\{p \leq x : \ p + 1 - |E(\mathbb{F}_p)| = r, \ |E(\mathbb{F}_p)| \text{ is prime}\right\} \sim C_{E,r}^{\mathrm{Mix}} \cdot \frac{\sqrt{x}}{\log^2(x)},$$

where $C_{E,r}$ depends on both the curve E and the nonzero constant r.

This Mixed Conjecture is the primary focus of this thesis. It is based on the same probabilistic arguments which prompted both the Lang-Trotter and Koblitz conjectures. We will explain those

arguments, and give an explicit description of the constant $C_{E,r}^{\text{Mix}}$ when E is a Serre curve. We will also present computational evidence supporting the Mixed Conjecture, as well as giving further support for each of the parent conjectures individually.

In Chapter 1, we present the fundamentals of elliptic curves and basic language surrounding their study, as well as introduce some of their geometry as a context for matrix representations and the trace of Frobenius. Chapter 2 discusses the matrix representations in more depth and Serre's results on surjectivity. The Lang-Trotter and Koblitz conjectures are presented in Chapter 3, preceding the statement of the new Mixed Conjecture. The conjectural constant is described, and given explicitly for all Serre curves. Finally, Chapter 4 contains computer-generated data supporting our mixed conjecture for three Serre curves, and several examples of computing the constant are worked through.

Chapter 1

Elliptic curve preliminaries

1.1 Notation and terminology

An elliptic curve E defined over a field K is a cubic curve of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with all coefficients a_i elements of the field K, referred to in [Was03] as the *generalized Weierstrass equation* for the curve. With the technical restriction that $\mathrm{char}(K) \neq 2, 3$, there is a change of variable that allows the curve to be expressed in its *Weierstrass equation* as

$$E : y^2 = x^3 + Ax + B$$

with coefficients A, B elements of K. We first complete the square, so that

$$E : y^2 + y(a_1x + a_3) = x^3 + a_2x^2 + a_4x + a_6$$

is rewritten as

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right)$$

$$u^2 = x^3 + ax^2 + bx + c$$

if $\mathrm{char}(K) \neq 2$. Then if $\mathrm{char}(K) \neq 3$, we may write

$$\begin{aligned} u^2 &= \left(x + \frac{a}{3}\right)^3 + ax^2 + bx + c - \left(ax^2 + a^2x + \frac{a^3}{27}\right) \\ &= \left(x + \frac{a}{3}\right)^3 + \left(x + \frac{a}{3}\right)(b - a^2) + \left(c - \frac{a^3}{27} + \frac{a^3}{3} - \frac{ab}{3}\right) \\ &= v^3 + Av + B, \end{aligned}$$

which is the Weierstrass equation.

The equations above describe the affine part of the curve, however an elliptic curve is a *projective* curve. Points in the projective space $\mathbb{P}^n(K)$ over a field K are written as $(n+1)$-tuples $(a_1, a_2, \ldots, a_{n+1})$ with elements $a_i \in K$ not all 0. There is also an equivalence relation $\sim$ defined such that two points X, Y given as $(n+1)$-tuples satisfy $X \sim Y$ if there is a non-zero scalar $t \in K$ such that $(x_1, x_2, \ldots, x_{n+1}) = (ty_1, ty_2, \ldots, ty_{n+1})$. This is an equivalence relation since the underlying the scalars are taken from K which is a field. The relation is obviously reflexive ($P \sim P$) and transitive ($P \sim Q$, $Q \sim R \Rightarrow P \sim R$), and it is symmetric ($P \sim Q \Rightarrow Q \sim P$) since any scalar $t \neq 0$ from the field K must have a multiplicative inverse which will satisfy the second. Under this equivalence relation, projective n-space over K is defined explicitly as

$$\mathbb{P}^n(K) = \{(a_1, a_2, \ldots, a_{n+1}) \neq (0, 0, \ldots, 0)\} / \sim .$$

We denote by $[a : b : c]$ the equivalence classes of (a, b, c) in $\mathbb{P}^2(K)$. If $c \neq 0$, then $[\frac{a}{c} : \frac{b}{c} : 1]$ is the unique reduced representative of each class of homogeneous points. The only other type of equivalence is of course $[a : b : 0]$. The equivalence classes represented by the form $[a : b : 1]$ constitute the affine points of $\mathbb{A}^2(K)$, while the classes represented by $[a : b : 0]$ constitute the projective line $\mathbb{P}^1(K)$: the *points at infinity*.

These points in $\mathbb{P}^1$ can be thought of as the set of possible directions in $\mathbb{A}^2$. Every such direction corresponds to a unique line through the origin, which should therefore satisfy an equation of the form $y = mx$ for a unique m. It is natural to think of the slope m as a ratio, in which case this corresponds to the homogeneous coordinates $[a : b : 0]$ where the ratio $\frac{b}{a} = m$. The only class of point for which this ratio does not work is $[0 : 1 : 0]$, and this corresponds meaningfully with the direction of the vertical line through the origin.

1.1.1 Curves over $\mathbb{P}^2(K)$

Over the affine plane $\mathbb{A}^2(K)$, a curve is any set of solutions to a polynomial $f(x, y) = 0$ in two variables. Over the projective plane $\mathbb{P}^2(K) = \mathbb{A}^2(K) \cup \mathbb{P}^1(K)$ we obviously require three variables as the points are written as triples, so polynomials will be of the form $F(x, y, z) = 0$. Further, to satisfy the equivalence class on $\mathbb{P}^2(K)$, the equality $F(x, y, z) = F(tx, ty, tz)$ must hold in general for every non-zero scalar $t \in K$. Since $F(x, y, z) = 0$, this will only hold if $F(tx, ty, tz) = t^d \cdot F(x, y, z)$. Any polynomial F such that $F(tx, ty, tz) = t^d F(x, y, z)$ is called a *homogeneous polynomial* of degree d, and all curves on the projective plane $\mathbb{P}^2(K)$ are of this form. The affine solutions to the polynomial $F(x, y, z)$ are those points $[a : b : 1]$ satisfying $F(x, y, 1) = f(x, y) = 0$, and the projective solutions are those points $[a : b : 0]$ satisfying $F(x, y, 0) = 0$. Any curve may be written by giving its affine or projective polynomials, either $f(x, y)$ or $F(x, y, z)$.

Definition 1.1. An *elliptic curve* is denoted as E/K (or simply E if the underlying field K is understood), and defined to be the set of points (x, y) satisfying its associated Weierstrass or generalized Weierstrass equation, as well as the single *point at infinity* $\mathcal{O} = [0 : 1 : 0]$.

This is in fact the only point at infinity on an elliptic curve, which is readily seen by considering the polynomial $y^2 = x^3 + Ax + B$ in its homogeneous form, $y^2 z = x^3 + Axz^2 + Bz^3$. The points at infinity all have $z = 0$ in common, so the homogeneous form reduces to $0 = x^3$, so $x = 0$ as well. This leaves only $[0 : 1 : 0]$ as a possible point under the equivalence relation of $\mathbb{P}^2(K)$. Geometrically, the point at infinity is thought of as being at the "top" (or equivalently, at the "bottom") of the xy-plane.

Though an elliptic curve itself is defined over a field K, these affine points need not have coordinates defined there also. In this case, it makes sense to refer to points on the curve E/K as living in the algebraic closure $\bar{K}$, and specifying those points which do have coordinates in the underlying field K as being *K-rational*. For curves defined over the field $\mathbb{Q}$ then, the set of *rational points* are all those points on E which have coordinates also in $\mathbb{Q}$.

1.1.2 Addition of points and the group law

Theorem 1.2 (Bezout's Theorem)**.**
Let C_1, C_2 be two smooth, projective curves of degree d_1 and d_2 respectively. The number of points in the intersection of C_1 and C_2 is then $d_1 d_2$.

In order to define a group structure on the set of points on E, we will first define the operation of the group.

Definition 1.3. For two points P, Q lying on a curve E given by a generalized Weierstrass equation, let L be the straight line passing through both points. Theorem 1.2 states that L and E will intersect in a third point R. Let L' be the straight line connecting $\mathcal{O}$ with R, which will also have a third point of intersection R'. Then the addition of points on an elliptic curve is defined as $P + Q = R'$.

That the point $\mathcal{O}$ is the identity element of the group follows directly from this definition.

For any other point $P \neq \mathcal{O}$ on the curve E, let L be a vertical line through P so that L joins the point P with $\mathcal{O}$. This line intersects the curve in a third point $P' \neq \mathcal{O}$ (note that it is possible for P' and P to be equal) such that if P is written with coordinates (x_0, y_0), then $x_0' = x_0$. To find P', we use the generalized Weierstrass equation to write the polynomial for E as

$$\begin{aligned} y^2 + y(a_1x_0 + a_3) - (x_0^3 + a_2x_0^2 + a_4x_0 + a_6) &= 0 \\ &= c \cdot (y - y_0)(y - y_0'). \end{aligned}$$

Expanding and comparing coefficients, we find that y^2 has coefficient $c = 1$ and y has coefficient $(a_1x_0 + a_3)$, so

$$\begin{aligned} (-y_0 - y_0') &= a_1x_0 + a_3 \\ y_0' &= -y_0 - a_1x_0 - a_3. \end{aligned}$$

So given $P = (x_0, y_0)$, we can find a point $P' = (x_0', y_0') = (x_0, -y_0 - a_1x_0 - a_3)$ such that $P + P' = \mathcal{O}$. In other words, $-P = P'$ is the additive inverse of P. If the curve E is given by the simpler Weierstrass equation $y^2 = x^3 + Ax + B$, then $a_1 = a_3 = 0$ so finding $-P$ simply amounts to flipping the point P about the x-axis

The addition of points also becomes simpler if the curve is given as a Weierstrass equation (a full description for generalized Weierstrass equations is given in [Sil86], §III.2). The line L connecting the points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ has equation $y = \frac{y_Q - y_P}{x_Q - x_P}(x - x_P) + y_P$, and so intersects with the curve at the three points which solve the cubic equation

$$\left(\frac{y_Q - y_P}{x_Q - x_P}(x - x_P) + y_P\right)^2 = x^3 + Ax + B.$$

Re-arranging this will give an equation of the form $x^3 - m^2x^2 + A'x + B' = 0$, and the three roots will correspond to the three intersection points of the line with the curve E. As we already know

two of these intersection points, we therefore also know two of the roots, and can find the third point R by factoring the polynomial as $(x - x_P)(x - x_Q)(x - x_R) = 0$. Even simpler, note that the coefficient $-m^2$ corresponding to x^2 in the expanded polynomial will be the negation of the sum of the three roots. Therefore, $x_R = x_{R'} = m^2 - (x_P + x_Q)$ and $y_{R'} = -y_R$ can be found accordingly.

To show that Definition 1.3 does indeed result in a group, we must also show associativity and closure (we have already seen the existence of inverse elements and the identity). The closure of the set under this operation is obvious, which leaves only associativity. The proof of this is not complicated, although somewhat tedious, and can be found in either of [Was03, ST92].

We may of course add a point P to itself, in which case $P + P$ is found by taking L to be the line tangent to the curve at the point P, so L intersects the curve twice at P and at a third point Q. Then the point $-Q$ will be the sum of P with itself. Iterating this same procedure gives meaning to the notation $2P = P + P$, $3P = P + P + P$, and in general

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ times}}.$$

Any point P satisfying $mP = \mathcal{O}$ in this notation is called a *point of m-torsion*. The set of all points on the curve E for which $mP = \mathcal{O}$ is the *m-torsion subgroup* of $E(K)$, denoted by $E[m]$. To consider all points of finite order on the curve E, and not just those of a specific order m, the *torsion subgroup* is defined as

$$E_{\text{tors}} = \bigcup_m E[m]$$

across all values of m.

From the following theorem of Mordell and Weil, we see that understanding the torsion points gives a useful perspective on understanding the curve as a whole.

Theorem 1.4 (Mordell, Weil. [Was03], §8.3)**.**
The group of rational points of the curve E over the number field K is a finitely generated abelian group which can be written as

$$E(K) \cong E_{tors}(K) \times \mathbb{Z}^r.$$

1.1.3 Curve invariants: discriminant, j-invariant, c_4, singular points

Recall the generalized Weierstrass equation of a curve E/K

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

There are several associated values presented in [Sil86] that can be computed using this standard equation which will give useful information about the curve. If $\text{char}(\bar{K}) \neq 2$, replace y with $\frac{1}{2}(y - a_1x - a_3)$ to give

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where the coefficients b_i are defined as

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned} \tag{1.1.1}$$

We then define

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ c_6 &= b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= \frac{c_4^3}{\Delta} \end{aligned}$$

The last two values will be the most often used in describing and working with elliptic curves, and they are the discriminant (Δ) and j-invariant (j) respectively. In particular, we can classify an elliptic curve once we have its generalized Weierstrass equation.

Proposition 1.5 ([Sil86], §III.1)**.** *Given a curve E in its Weierstrass equation, and computing the values as given above, then the following cases classify the curve.*

- *E is **non-singular** if and only if $\Delta \neq 0$.*
- *E has a **node** if and only if $\Delta = 0$ and $c_4 \neq 0$.*
- *E has a **cusp** if and only if $\Delta = c_4 = 0$.*

Finally, two elliptic curves over $\bar{K}$ are isomorphic if they have the same j-invariant, and for every value $j_0 \in \bar{K}$ there exists an elliptic curve which has this as its j-invariant.

Remark 1.6. Only non-singular curves given by a Weierstrass equation are also elliptic curves.

Regardless of which equation we use, these values carry important and sometimes invariant information about the curve. For example, if E is instead given as the Weierstrass equation

$$E : y^2 = x^3 + Ax + B$$

then

$$\Delta = -16(4A^3 + 27B^2), \text{ and}$$
$$j = 1728\frac{(4A)^3}{\Delta}.$$

1.2 Points on the curve: torsion, rational, and integral

The m-torsion subgroup $E[m]$ of an elliptic curve E has a simple characterization.

Proposition 1.7 ([Was03], Theorem 3.2)**.** *Given an elliptic curve E over a field K, denote by $E(\bar{K})$ the group of points. If K has characteristic $p = 0$ or $p \nmid m$, then the subgroup of $E(\bar{K})$ of m-torsion for this curve can be written as*

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

If $p > 0$ and $p \mid m$, let $m = p^r m'$, $p \nmid m'$ then

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z} \qquad \text{or} \qquad E[m] \simeq \mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z}.$$

Proof. The first statement is an automatic result of the group of complex points on a curve E being isomorphic to the complex plane modulo a lattice $L = w_1\mathbb{Z} + w_2\mathbb{Z}$ which is uniquely determined by the curve itself. Roughly speaking:

$$E[m] \simeq (\mathbb{C}/L)[m] \simeq \{\mathbb{Z}w_1 + \mathbb{Z}w_2 : w_1, w_2 \in \mathbb{C}\}[m] \simeq \left\{\frac{1}{m}\mathbb{Z}w_1 + \frac{1}{m}\mathbb{Z}w_2 : w_1, w_2 \in \mathbb{C}\right\} \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$

This fact is discussed in most introductory texts on the subject of elliptic curves (see for instance §II.2 of [ST92] and §VI.5 of [Sil86]). The full details of this proof including the alternate cases are presented throughout §3.2 in [Was03]. □

We can find explicit formulae for computing the value of mP, however these are generally quite complicated. A simpler example is the *duplication formula*

$$x' = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6} \tag{1.2.1}$$

which gives the x-coordinate of the point $2P$ if $P = (x, y)$, and where the coefficients b_i are given in (1.1.1). The denominator may be 0, in which case $2P = \mathcal{O}$.

Theorem 1.8 ([Was03], Theorem 3.6)**.**
Let P be a point on an elliptic curve over K given by the Weierstrass equation $y^2 = x^3 + Ax + B$. Then the x coordinate of the point mP is given by

$$\frac{\phi_m(x)}{\psi_m^2(x)} = \frac{x^{m^2} + \dots}{m^2 x^{m^2-1} + \dots}$$

where both polynomials are elements of $K[x]$.

Note that $\psi_m(x)$ is not a polynomial in $K[x]$, and some simplification is needed to express the first term of $\psi_m^2(x)$ as above. In particular, Theorem 1.8 holds for all integers m, and not only when m is odd.

Although the coefficients of the Weierstrass equation for a curve may be given over a specific field, say over the rationals $\mathbb{Q}$, the solutions to this equation corresponding to points on the curve are not necessarily defined over the same field. Recall that the set of rational points on a curve are those points which do have coefficients in $\mathbb{Q}$, and more generally the set of K-rational points are those points having coefficients entirely in the field K.

Theorem 1.9 (Lutz, Nagell)**.**
If E is an elliptic curve over $\mathbb{Q}$ in Weierstrass form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$, then for any rational point $P = (x, y)$ of finite order, $x, y \in \mathbb{Z}$ and

$$y^2 \mid 4A^3 + 27B^2$$

so long as $y \neq 0$.

Corollary 1.9.1. *From this theorem come two important conclusions:*

a) any rational point of finite order $P \in E_{tors}(\mathbb{Q})$ in fact has integer coordinates, and further

b) the torsion subgroup of $E(\mathbb{Q})$ is necessarily finite.

Proof. We omit the proof of this theorem, which can be found in [Sil86], §VIII.7, as well as further discussion in each of [ST92], §II.5 and [Was03], Theorem 8.7. □

1.3 Maps between curves

The *function field* $F(E)$ of a curve E is the set of all fractions of polynomials (i.e., rational functions) which may act on the points of this curve. Let ϕ be a non-constant, rational homomorphism of curves

$\phi : E_1 \to E_2$ defined over the field K. This homomorphism then induces a particular injective mapping between the respective function fields

$$\phi^* : F(E_2) \to F(E_1)$$
$$\phi^*(f) \mapsto f \circ \phi.$$

In fact, $F(E_1)$ is a finite extension of the image of ϕ^* .

Definition 1.10. The *degree* of ϕ is defined to be the degree of this extension $[F(E_1) : \phi^* F(E_2)]$, or by convention 0 if the map is constant, and ϕ is called *separable* or *inseparable* if the field extension is separable or inseparable, accordingly.

There is an alternate and equally instructive way of viewing the separability of a map ϕ, which requires further terminology. To begin with, we observe a rational map at a single point on the curve.

Definition 1.11 ([Eng99], §2.1)**.** Given a curve E/K and a function $\phi \in F(E)$, the function is called *regular* at a point P if it is defined as $\phi(P) = \frac{f(P)}{g(P)}$ with $g(P) \neq 0$. Denote by $O_P(E)$ the ring of all functions ϕ which are regular at P. This is the *local ring* of E at P, with units

$$O_P(E)^\times = \{\phi \in O_P(E) : f(P), g(P) \neq 0\},$$

and it has a unique maximal ideal

$$m_P = \left\{ \phi = \frac{f(P)}{g(P)} \in O_P(E) : g(P) \neq 0, f(P) = 0 \right\}.$$

Proposition 1.12 ([Eng99], §2.5)**.** *Let u be a generator for the unique maximal ideal m_P of $O_P(E)$ for a given point P on the curve E. Then for any nonzero $s \in O_P(E)$, there is a unique non-negative integer d such that*

$$s = u^d r$$

for some unit $r \in O_P(E)^\times$.

For any non-zero rational polynomial ϕ, the integer d as in Proposition (1.12) is the *order* of ϕ at P, and is denoted $\mathrm{ord}_P(\phi)$. This can be extended from $O_P(E)$ to all of $F(E)$ by letting $\mathrm{ord}_P\left(\frac{f}{g}\right) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$.

Definition 1.13. The order of ϕ at P is used to determine the behaviour of the function at this point, as given in the following list.

- If $\mathrm{ord}_P(\phi) > 0$ then ϕ is regular at P, with a *zero* at P of multiplicity $|\mathrm{ord}_P(\phi)|$.
- If $\mathrm{ord}_P(\phi) < 0$ then ϕ has a *pole* at P of multiplicity $|\mathrm{ord}_P(\phi)|$.
- If $\mathrm{ord}_P(\phi) = 0$ then ϕ is regular at P.

From these statements comes the important notion of the *ramification index* e_ϕ of a non-constant, rational map $\phi \in F(E)$. This is defined to be $e_\phi(P) = \mathrm{ord}_P(\phi^* u)$, where $u \in m_P$ is a generator of the maximal ideal m_P. In fact, the value of the ramification index can be shown to be independent of the point P, for instance in [Eng99]. The map ϕ is called *unramified* if $e_\phi = 1$, and this corresponds exactly with the notion of separability in Definition 1.10.

As stated in [Sil86], §III.4, an *isogeny* is any rational homomorphism ϕ between the groups of points for two elliptic curves E_1, E_2, and any two curves are called *isogenous* if there exists a non-trivial isogeny between them.

Theorem 1.14 ([Eng99], §3.1)**.**
If ϕ is a homomorphism defined by

$$\phi : E/K \to E/K$$

for an elliptic curve E/K, then ϕ is either surjective, or constant.

As the only constant isogeny is the trivial map $\phi_0 : E_1 \mapsto [\infty]$, this theorem implies that all non-trivial isogenies are surjective, of finite degree, and may be classified as separable or inseparable according to the definitions given above. The set of all isogenies between two curves E_1, E_2 is written as $\mathrm{Hom}(E_1, E_2)$, and is a group under the operation of addition given as $(\phi_1 + \phi_2)(P) = \phi_1(P) + \phi_2(P)$.

Lemma 1.15 ([Sil86], §III.6)**.** *If ϕ is a non-constant isogeny of degree m between two curves E_1, E_2 defined over a field K, then there is a unique associated isogeny $\hat{\phi} : E_2 \to E_1$ which satisfies $\hat{\phi} \circ \phi(P) = [m]P$ for every point $P \in E_1(K)$, called the dual isogeny of ϕ. Similarly, $\phi \circ \hat{\phi}(Q) = [m]Q$ for all $Q \in E_2(K)$ and $\deg(\hat{\phi}) = \deg(\phi)$.*

An *endomorphism* of a group G is any homomorphism mapping G to itself which can be represented by a quotient of polynomials. Therefore an endomorphism of an elliptic curve is an isogeny $\phi : E(\bar{K}) \to E(\bar{K})$ of finite degree (hence non-trivial). The group $\mathrm{Hom}(E, E)$ is now a ring,

as the second operation can be defined using composition of functions, with $(\phi_1 \cdot \phi_2)(P) = \phi_1(\phi_2(P))$. This is referred to as the *endomorphism ring*, $\mathrm{End}(E) = \mathrm{Hom}(E, E)$.

Proposition 1.16 ([Eng99], §3.1)**.** *Given a non-zero endomorphism α of degree d as defined in Definition* (1.10)*, we have the following identity*

$$\deg(\alpha) = d = e_\alpha \cdot |\ker(\alpha)|.$$

Of particular interest is that for any separable endomorphism α, we have the relatively simple equality $\deg(\alpha) = |\ker(\alpha)|$.

Proposition 1.17 ([Sil86], §III.4)**.** *Let E be an elliptic curve over a field K and m be a nonzero integer. Then the multiplication by m map defined by*

$$\begin{aligned} [m] : E &\to E \\ P &\mapsto mP \end{aligned}$$

is a non-constant endomorphism, and $\mathrm{End}(E)$ *is an integral domain of characteristic* 0*.*

This leads to an important classification for all elliptic curves.

Definition 1.18. An elliptic curve E has no *complex multiplication* if $\mathrm{End}(E) \cong \mathbb{Z}$; otherwise, if $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, then E has complex multiplication.

Elliptic curves with complex multiplication have extra symmetry and other special properties, however we will not deal with them in any significant capacity in this thesis. Indeed, several of our main conjectures for elliptic curves will be conditional on those curves not having complex multiplication.

Theorem 1.19 ([Was03], §3.3 and [Sil86], §III.8)**.**
Let E be an elliptic curve defined over a field K and m a positive integer with char$(K) \nmid m$. There is a pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

which maps onto the m-th roots of unity μ_m called the Weil pairing, satisfying:

a) the bilinear condition:

$$e_m(S_1 + S_2, T) = e_m(S_1, T) e_m(S_2, T)$$

$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2)$$

$$e_m(S, T)^n = e_m([n]S, T).$$

b) the alternating condition:

$$e_m(S, T) = e_m(T, S)^{-1}.$$

c) the condition that an isogeny $\phi : E_1 \to E_2$ and its dual $\hat{\phi}$ are also dual with respect to e_m, in that:

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T).$$

Corollary 1.19.1. *For an endomorphism $\psi \in \mathrm{End}(E)$, let $\{S, T\}$ be a basis for $E[m]$ and e_m its Weil pairing. Then the action of ψ on $E[m]$ can be written as a matrix $\psi_m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries in $\mathbb{Z}/m\mathbb{Z}$, and*

$$\begin{aligned} e_m(S, T)^{\deg(\psi)} &= e_m([\deg(\psi)]S, T) \\ &= e_m(\hat{\psi}\psi(S), T) \\ &= e_m(\psi(S), \psi(T)) \qquad \textit{(by Lemma 1.15)} \\ &= e_m(aS + cT, bS + dT) \\ &= e_m(S, S)^{ab} e_m(S, T)^{ad} e_m(T, S)^{bc} e_m(T, T)^{cd} \\ &= e_m(S, T)^{ad-bc}. \end{aligned}$$

The exponent $(ad-bc)$ is equal to the determinant of the matrix ψ_m, so $\deg(\psi) \equiv \det(\psi_m) \pmod{m}$.

Corollary 1.19.2. *Let ψ be a separable endomorphism, r and s be integers, and I be the identity matrix of dimension 2. Then*

$$\begin{aligned} \deg(r\psi - s) &\equiv \det(r \cdot \psi_m - s \cdot I) \\ &\equiv \begin{vmatrix} ra - s & rb \\ rc & rd - s \end{vmatrix} = (ra - s)(rd - s) - r^2bc \\ &\equiv r^2(ad - bc) + rs(-a - d) + s^2 \\ &\equiv r^2(\det(\psi_m)) + rs(\det(\psi_m - I) - 1 - \det(\psi_m)) + s^2 \pmod{m}. \\ &= r^2(\deg(\psi)) + rs(\deg(\psi - 1) - 1 - \deg(\psi)) + s^2. \end{aligned}$$

The last line writes as an equality, as the previous congruences hold for all (infinitely many) m.

Lemma 1.20.

$$\mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

Proof. The automorphisms on $E[m]$ are just the invertible endomorphisms on $E[m]$. The action of each endomorphism on $E[m]$ is determined by its action on the basis elements, which gives a homomorphism onto the matrices of dimension 2 with entries in $\mathbb{Z}/m\mathbb{Z}$. The invertible endomorphisms must therefore correspond to the matrices with $\det \not\equiv 0 \pmod{m}$, which together make up the group $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. □

1.4 Elliptic curves over finite fields

Definition 1.21 ([Sil86], §VII.5)**.** For a prime p, we say that the curve E/K has

- *good reduction* if $E/\mathbb{F}_p$ is nonsingular: E is then an elliptic curve mod p, and this happens for all but finitely many primes.
- *additive reduction* if $E/\mathbb{F}_p$ has a cusp, so its cubic equation has a triple root mod p.
- *multiplicative reduction* if $E/\mathbb{F}_p$ has a node, so its cubic equation has a double root mod p. This may then be further classified as being *split* if the slopes of the tangent lines at the node are in $\mathbb{F}_p$; otherwise, it is *non-split*.

  The latter two cases are together referred to as *bad reduction*.

Using definition 1.5 as well, note that the primes p dividing Δ are exactly those for which $E/\mathbb{F}_p$ has bad reduction, since then $\Delta \equiv 0 \pmod{p}$.

Let E be an elliptic curve over the finite field $\mathbb{F}_p$ for prime p, and with $\Delta \neq 0$. We want to determine the order of the group $E(\mathbb{F}_p)$. There is of course a trivial bound on this order: a point $P \in E(\mathbb{F}_p)$ is written as $(x_P, y_P) \pmod{p}$ and there are finitely many choices for the coordinates x_P and y_P, so the total number of points in $E(\mathbb{F}_p)$ is bounded by $|E(\mathbb{F}_p)| \leq p^2$. Better bounds are available of course, and the most useful of these was conjectured by Artin, and later proven in two separate parts by Hasse and Weil.

Theorem 1.22 (Hasse, Weil. [Was03], §4.1)**.**
Let $E/\mathbb{F}_p$ be an elliptic curve defined over a finite field of p elements, and let

$$a_p(E) = p + 1 - \#E(\mathbb{F}_p).$$

Then the number of elements in the group $E(\mathbb{F}_q)$ will satisfy the inequality

$$|\#E(\mathbb{F}_p) - p - 1| = |a_p(E)| \leq 2\sqrt{p}.$$

Over a finite field $\mathbb{F}_p$ of characteristic p, the *Frobenius map* $\phi_p : x \mapsto x^p$ is defined for all $x \in \bar{\mathbb{F}}_p$. In particular, this map induces a non-separable endomorphism of the points on the curve $E(\bar{\mathbb{F}}_p)$. Thus $\phi_p(x, y) = (x^p, y^p)$. Since the characteristic of $\mathbb{F}_p$ is p, if $(x, y) \in E(\mathbb{F}_p)$ then $\phi_p(x, y) = (\phi_p(x), \phi_p(y)) = (x, y)$ by Fermat's Little Theorem over finite fields. The degree of ϕ_p can be shown to be p, as in [Sil86], §II.2.

Lemma 1.23 ([Was03], §2.8)**.** *If τ is a non-trivial, separable endomorphism of an elliptic curve E over a field K, then* $\deg(\tau)$ *is equal to the number of elements in the kernel of $\tau : E(\bar{K}) \to E(\bar{K})$.*

In order to use this lemma, we require a separable endomorphism. The Frobenius endomorphism is not separable, however the map

$$(\phi_p - 1) : x \mapsto \phi_p(x) - x$$

is separable over $\mathbb{F}_p$, and the kernel of this map is $E(\mathbb{F}_p)$. Therefore, $\deg(\phi_p - 1) = \#E(\mathbb{F}_p)$.

Proof of Theorem 1.22. To show that

$$|\#E(\mathbb{F}_p) - p - 1| = |a_p(E)| \leq 2\sqrt{p}$$

we will mostly follow the proof given in [Was03], §4.2. First, notice that

$$a_p(E) = p + 1 - \deg(\phi_p - 1).$$

Then from corollary 1.19.2, we know that for integers r and s,

$$\begin{aligned}
\deg(r\phi_p - s) &= r^2(\deg(\phi_p)) + rs(\deg(\phi_p - 1) - 1 - \deg(\phi_p)) + s^2 \\
&= r^2(p) + rs(\deg(\phi_p - 1) - 1 - p) + s^2 \\
&= s^2 \left(\frac{r^2 p}{s^2} - \frac{a_p(E) \cdot r}{s} + 1 \right).
\end{aligned}$$

The value of $p\left(\frac{r}{s}\right)^2 - a_p(E)\left(\frac{r}{s}\right) + 1$ is therefore non-negative, and as the rationals are dense in $\mathbb{R}$ the inequality

$$px^2 - a_p(E)x + 1 \geq 0$$

holds as well. Finally, this means this quadratic polynomial has at most one root, so $0 \geq \Delta = a_p(E)^2 - 4p$ which rearranges to give $|a_p(E)| \leq 2\sqrt{p}$. □

1.5 Algebraic number theory

Following the introduction given in chapter 4 of [Mar77], define the number fields L and K, with L a normal extension of degree n over K. Let $S \subset L$ and $R \subset K$ be the respective rings of integers. Given a prime $P \subset R$, define $Q_i \subset S$ to be the finite number of primes indexed by $i = 1, 2, \ldots$, lying over P. Recall that the extension L over K is *normal* if for every $\alpha \in L$, $\notin K$ which is the root of a monic polynomial in $K[x]$, L also contains all of the conjugates of α. That is, L is normal if it is the splitting field for the collection of polynomials $f(x) \in K[x]$ having at least one root in L. The *ramification index* $e(Q_i|P)$ is the highest power of Q_i which divides the prime decomposition of P in S, and the *inertial degree* $f(Q_i|P)$ is the degree of the extension of the *residue field* S/Q over the residue field R/P.

$$\begin{array}{ccc} L & S & Q_1^{e_i} \ldots Q_r^{e_r} \\ {\scriptstyle n}\,\big| & \big| & \vdots \\ K & R & P \end{array}$$

Elements of the Galois group G of a normal extension L permute the primes $Q_i \subset S$ lying above P, and both the ramification indices and inertial degrees of all the primes Q_i are equal. In general, the sum of the products of the inertial degrees and ramification indices of the r primes in S above a prime $P \in R$ is given by

$$\sum_{i=1}^{r} e_i f_i = n.$$

In the case where the extension is normal, we have $e_i = e_j$ and $f_i = f_j$ for all $1 \leq i, j \leq r$, so let $e = e_1$ and $f = f_1$, then

$$n = \sum_{i=1}^{r} e_i f_i = r \cdot ef.$$

For a single prime Q lying above P, there exist two special subgroups of the Galois group $G = \mathrm{Gal}(L/K)$. The *decomposition group* $D(Q|P)$ and the *inertia group* $E(Q|P)$, defined as

$$D(Q|P) = \{\sigma \in G : \sigma Q = Q\}, \qquad E(Q|P) = \{\sigma \in G : \sigma\alpha \equiv \alpha \pmod{Q}\ \forall\ \alpha \in S\}.$$

As subgroups of the Galois group, there are associated fixed fields called the *decomposition field* L^D and *inertia field* L^E respectively. The important feature of these fields is that they occur in a

straightforward way as extensions of K and subfields of L, forming the tower of field extensions

$$\begin{array}{c} L \\ | \, e \\ L^E \\ | \, f \\ L^D \\ | \, r \\ K \end{array}$$

which implies $e = |E(Q|P)|$ and $ef = |D(Q|P)|$.

Lemma 1.24. *Let $D = D(Q|P)$ and $E = E(Q|P)$ for fixed primes Q and P as already defined, and let $S(Q) = S/Q$ and $R(P) = R/P$ denote the respective residue fields. Then*

$$\mathrm{Gal}\left(S(Q)/R(P)\right) = D/E.$$

Proof. Under restriction, every $\sigma \in G$ is an automorphism of S. Further, if we take $\sigma \in D$ then σ fixes Q and so induces an automorphism $\bar{\sigma} : S(Q) \to S(Q)$ such that $\bar{\sigma}\left(s \pmod{Q}\right) = \sigma(s) \pmod{Q}$ for all $s \in S$. As σ fixes the field R then so must it fix the residue field $R(P)$, and it follows that $\bar{\sigma}$ also fixes $R(P)$. The automorphism $\bar{\sigma}$ is therefore an element of $\mathrm{Gal}(S(Q)/R(P))$. Composition in D corresponds to composition in $\mathrm{Gal}(S(Q)/R(P))$, so we therefore have a group homomorphism between D and $\mathrm{Gal}(S(Q)/R(P))$. If $\tau \in E$, then under the same restrictions there is an induced automorphism $\bar{\tau}$ on $S(Q)$, and by definition $\bar{\tau}$ must be the identity automorphism. Thus, the group homomorphism has kernel E. □

If P is unramified in a normal extension L, then $D(Q|P) \cong \mathrm{Gal}(S(Q)/R(P))$ as $e = 1$ and $E(Q|P)$ is trivial. There is a unique element $\phi \in D(Q|P)$ which generates the group, and has the property that $\phi(s) \equiv s^{|R(P)|} \pmod{Q}$ for all $s \in S$. The order of the element ϕ in the Galois group is $f(Q|P)$, so an unramified prime splits completely iff $\phi = 1$. When G is an abelian group, the Frobenius element is uniquely determined by the underlying prime P, and in these cases we will use the notation ϕ_P to emphasize this relation.

Theorem 1.25 (Tchebotarev Density Theorem. [Ser68], [Len])**.**
Let L be a finite extension of the number field K, of degree $n = [L : K]$, and with Galois group G. Fix a conjugacy class $C \subseteq G$, and recall that the class of the Frobenius automorphism $\phi(Q|P) \in G$

of Q over P is uniquely determined by the unramified prime P. Then

$$\#\{P \leq x : P \text{ unramified}, \ \phi(Q|P) \in C\} \sim \frac{|C|}{|G|}\ \pi(x) = \frac{|C|}{n}\ \pi(x)$$

Corollary 1.25.1 ([DS05])**.** *Every element in* $\mathrm{Gal}(L/\mathbb{Q})$ *is equal to the Frobenius automorphism* $\phi(Q|P)$ *for infinitely many primes* $Q \in L$*.*

Proposition 1.26 ([Kat80], Appendix)**.** *Let $E(K)$ be an elliptic curve defined over a number field K, and $e_{\mathfrak{p}}$ be the absolute ramification index of a prime $\mathfrak{p} \in K$ lying above the rational prime p. If $e_{\mathfrak{p}} < p - 1$, then the order of the torsion subgroup $E_{tors}(K)$ divides $|E(\mathbb{F}_{\mathfrak{p}})|$, the order of the curve mod $\mathfrak{p}$.*

Chapter 2

Galois representations of curves

A Galois representation is a type of group representation for which the group in question is Galois for an associated field extension. The representation allows elements of the group to be mapped to matrices, where the usual rules of linear algebra may there provide a more natural way of understanding the underlying structure of the group. In the case of elliptic curves, the field extension will be built around the group of m-torsion points $E[m]$ of a curve $E/\mathbb{Q}$ and the representation will follow thereafter.

We know from Proposition 1.7 that $E[m] \equiv \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ so points in $E[m]$ may be written in terms of two basis elements, call them P and Q. Then $E[m] = \{aP + bQ : a, b \in \mathbb{Z}/m\mathbb{Z}\}$. Any homomorphism $\sigma : E[m] \to E[m]$ can therefore be completely determined by its actions

$$\sigma(P) = \alpha_\sigma P + \beta_\sigma Q, \qquad \sigma(Q) = \gamma_\sigma P + \delta_\sigma Q$$

on the basis elements of $E[m]$ for appropriate constants $\alpha_\sigma, \beta_\sigma, \gamma_\sigma, \delta_\sigma \in \mathbb{Z}/m\mathbb{Z}$.

Lemma 1.20 states that each automorphism on $E[m]$ can be written as a matrix in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, so

$$\mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

These two groups were seen to be isomorphic simply because $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the group of automorphisms for the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. However we can also show this isomorphism explicitly. Using the above notation, every homomorphism σ on $E[m]$ is determined by the behaviour of $\sigma(P)$

and $\sigma(Q)$. The matrix

$$A = \begin{pmatrix} \alpha_\sigma & \gamma_\sigma \\ \beta_\sigma & \delta_\sigma \end{pmatrix}$$

clearly corresponds in a one-to-one manner to the automorphism $\sigma \in \mathrm{Aut}(E[m])$ since

$$A \cdot \begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} \alpha_\sigma P + \gamma_\sigma Q \\ \beta_\sigma P + \delta_\sigma Q \end{pmatrix} = \begin{pmatrix} \sigma(P) \\ \sigma(Q) \end{pmatrix}.$$

The kernel of the map taking $E[m]$ to $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the preimage of the identity matrix $I \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, which corresponds to the homomorphism σ with coefficients $\alpha_\sigma = \delta_\sigma = 1$ and $\beta_\sigma = \gamma_\sigma = 0$. The map σ is then necessarily the identity map, since $\sigma(P) = P$ and $\sigma(Q) = Q$, and thus the map is indeed one-to-one.

The group law is upheld, since for any two automorphisms $\sigma, \tau \in \mathrm{Aut}(E[m])$ the composition $(\tau \circ \sigma)$ is also determined by its action on the basis elements, and we may therefore write

$$\begin{aligned}
\tau(\sigma(P)) &= \tau(\alpha_\sigma P + \beta_\sigma Q) \\
&= \alpha_\sigma \tau(P) + \beta_\sigma \tau(Q) = (\alpha_\tau \alpha_\sigma + \beta_\sigma \gamma_\tau)P + (\alpha_\sigma \beta_\tau + \beta_\sigma \delta_\tau)Q, \\
\tau(\sigma(Q)) &= \tau(\gamma_\sigma P + \delta_\sigma Q) \\
&= \gamma_\sigma \tau(P) + \delta_\sigma \tau(Q) = (\gamma_\sigma \alpha_\tau + \delta_\sigma \gamma_\tau)P + (\gamma_\sigma \beta_\tau + \delta_\sigma \delta_\tau)Q.
\end{aligned}$$

This is easily recognizable by fully expanding the matrix multiplication

$$\begin{aligned}
(\tau \circ \sigma) \begin{pmatrix} P \\ Q \end{pmatrix} &= \begin{pmatrix} (\alpha_\tau \alpha_\sigma + \beta_\sigma \gamma_\tau)P + (\alpha_\sigma \beta_\tau + \beta_\sigma \delta_\tau)Q \\ (\gamma_\sigma \alpha_\tau + \delta_\sigma \gamma_\tau)P + (\gamma_\sigma \beta_\tau + \delta_\sigma \delta_\tau)Q \end{pmatrix} \\
&= \begin{pmatrix} \alpha_\tau \alpha_\sigma + \gamma_\tau \beta_\sigma & \alpha_\tau \gamma_\sigma + \gamma_\tau \delta_\sigma \\ \beta_\tau \gamma_\sigma + \delta_\tau \beta_\sigma & \beta_\tau \gamma_\sigma + \delta_\sigma \delta_\tau \end{pmatrix} \cdot \begin{pmatrix} P \\ Q \end{pmatrix} \\
&= \begin{pmatrix} \alpha_\tau & \gamma_\tau \\ \beta_\tau & \delta_\tau \end{pmatrix} \begin{pmatrix} \alpha_\sigma & \gamma_\sigma \\ \beta_\sigma & \delta_\sigma \end{pmatrix} \cdot \begin{pmatrix} P \\ Q \end{pmatrix} \\
&= A_\tau A_\sigma \cdot \begin{pmatrix} P \\ Q \end{pmatrix}.
\end{aligned}$$

We have thus shown that each automorphism of $E[m]$ can be uniquely represented by a 2x2 matrix with elements in $\mathbb{Z}/m\mathbb{Z}$. To see that in fact the possible matrix representations are limited to those in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, completing the proof that isomorphism holds, observe that each automorphism

σ is of course invertible. The matrix representation for each map in $\mathrm{Aut}(E[m])$ must therefore also be invertible, and this is equivalent to requiring that $\det(A) \not\equiv 0 \pmod{m}$.

Proposition 2.1 ([ST92], §VI.2)**.** *Let $\mathbb{Q}(E[m]) = \mathbb{Q}(x_1, y_1, \ldots, x_k, y_k\}$ be the field generated by the coordinates x_i, y_i of the m-torsion points in $E[m]$. Then $\mathbb{Q}(E[m])$ is a Galois extension of $\mathbb{Q}$, and $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ acts on the elements of $E[m]$ by*

$$\sigma(P) = \begin{cases} (\sigma(x), \sigma(y)) & \text{if } P = (x, y) \\ \mathcal{O} & \text{if } P = \mathcal{O}. \end{cases}$$

Proof. Let α be an embedding of $\mathbb{Q}(E[m])$ in $\mathbb{C}$ fixing $\mathbb{Q}$. Any point on the curve $P_i = (x_i, y_i)$ with $x_i, y_i \in \mathbb{Q}(E[m])$ is necessarily in $E[m]$, so $mP_i = \mathcal{O}$.

By Theorem 1.8, the x coordinate is algebraic as it is the root of a rational polynomial, and the y coordinate is algebraic as it can be written in terms of x. The following identity must therefore hold

$$\begin{aligned} \alpha(\mathcal{O}) &= \mathcal{O} \\ &= \alpha(mP_i) = m\alpha(P_i) = m(\alpha(x_i), \alpha(y_i)). \end{aligned}$$

The resulting point $(\alpha(x_i), \alpha(y_i))$ is therefore itself an element of $E[m]$, meaning its coordinates are already in the field extension $\mathbb{Q}(E[m])$ and $(\alpha(x_i), \alpha(y_i)) = (x_j, y_j)$ for some positive $j \leq k$. □

Definition 2.2. Given the group $E[m]$ of m-torsion points of the elliptic curve $E/\mathbb{Q}$, the homomorphism

$$\begin{aligned} \rho_m : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) &\hookrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \\ \sigma &\mapsto \begin{pmatrix} \alpha_\sigma & \gamma_\sigma \\ \beta_\sigma & \delta_\sigma \end{pmatrix} \end{aligned}$$

is a *Galois representation* associated to the field extension $\mathbb{Q}(E[m])$.

The integer m of a Galois representation may be a prime ℓ or prime power ℓ^n, and using these as in [LT76] we construct the ℓ-adic representation

$$\hat{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \prod_{\ell} \mathrm{GL}_2(\mathbb{Z}_\ell) \tag{2.0.1}$$

as a product over ℓ of the ℓ-adic integers $\mathbb{Z}_\ell$.

Definition 2.3. For an elliptic curve E and a prime ℓ, the associated *Tate module* is

$$T_\ell E = \varprojlim_r E[\ell^r]$$

defined by the inverse limit with respect to the multiplication-by-ℓ map: $E[\ell^{r+1}] \to E[\ell^r]$.

Using Proposition 1.7, it can be shown that $\mathrm{Aut}(T_\ell E) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$. This corresponds with the definition of $\hat{\rho}$ in (2.0.1). Reducing the representation $\hat{\rho}$ modulo a positive integer m then gives the original map ρ_m. As ρ maps into a product of spaces, there is a corresponding ℓ-th factor representation

$$\hat{\rho}_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

and equivalent factor representation

$$\hat{\rho}_m : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \prod_{\ell|m} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Following the exposition in [LT76], denote by K^ρ the fixed field of $\ker(\rho)$ over $\mathbb{Q}$, and let $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. The factor group $G(\ell) = \frac{G}{\ker(\rho_\ell)}$ is the Galois group over $\mathbb{Q}$ of K^{ρ_ℓ}, and the factor group $G(m) = \frac{G}{\ker(\rho_m)}$ is the Galois group of $K^{\rho_m} = \mathbb{Q}(E[m])/\mathbb{Q}$. Additionally, the factor groups $G_m = \frac{G}{\ker(\hat{\rho}_m)}$ and $G_\ell = \frac{G}{\ker(\hat{\rho}_\ell)}$ are the Galois groups of $K^{\ker(\hat{\rho}_m)}$ and $K^{\ker(\hat{\rho}_\ell)}$ respectively. Using this notation, the integer m is said to *split* the representation $\hat{\rho}$ if

$$\hat{\rho}(G) = \prod_{\ell \nmid m} \mathrm{GL}_2(\mathbb{Z}_\ell) \times G_m, \tag{2.0.2}$$

in other words if ρ is surjective on the ℓ-th factor if and only if $\ell \nmid m$. Define the reduction map $r_m : \prod_{\ell|m} \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. The integer m is *stable* if

$$r_m^{-1}(G(m)) = G_m.$$

Theorem 2.4.

Let p be an unramified prime in $\mathbb{Q}(E[m])/\mathbb{Q}$, and $\phi_p \in \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ be the Frobenius automorphism. Then $\rho_m(\phi_p)$ is a conjugacy class of matrices in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ satisfying

$$\det(\rho_m(\phi_p)) \equiv p \pmod{m}, \qquad \mathrm{tr}(\rho_m(\phi_p)) \equiv a_p \pmod{m}.$$

Corollary 2.4.1. *The degree of the Frobenius automorphism as in definition 1.10 is given by $\deg(\phi_p) \equiv \det(\rho_m(\phi_p)) \pmod{m}$ for an unramified prime p, as evidenced in the statement of corollary 1.19.1. Lemma 1.23 implied that $\deg(\phi_p - 1) = \#E(\mathbb{F}_p)$, and this is in turn equivalent to*

$$\#E(\mathbb{F}_p) = \deg(\phi_p - 1) \equiv \det(\rho_m(\phi_p - 1)) \equiv \det(\rho_m(\phi_p) - I) \pmod{m}.$$

As these matrices all have two rows and columns, $\det(A) = \det(-A)$ and so the previous statement can be rewritten as

$$\#E(\mathbb{F}_p) = \det(\rho_\ell(I - \phi_p)) \pmod{m}.$$

2.1 Serre curves

Theorem 2.5 ([Ser71], Théorème 2)**.**
If the elliptic curve E does not have complex multiplication, then the image of the representation

$$\hat{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \prod_\ell \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

has finite index in $\prod_\ell \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Corollary 2.5.1. *In particular, Serre's theorem implies all of the following statements:*

1. *The image of*

   $$\rho_\ell : \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

   is surjective for all but finitely many primes ℓ.

2. *The image of*

   $$\rho_m : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

   is surjective for all integers m coprime to some integer M.

3. *For an elliptic curve E, there is always an integer $M = m_E$ which splits and stabilizes the representation $\hat{\rho}$, so*

   $$\hat{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to G(m_E) \times \prod_{\ell \nmid m_E} \mathrm{GL}_2(\mathbb{Z}_\ell)$$

   and the image of $\hat{\rho}$ in $\prod_{\ell | m_E} \mathrm{GL}_2(\mathbb{Z}_\ell)$ is the full inverse image of $G(m_E)$ under the reduction map modulo m_E.

Serre also proved that

Theorem 2.6 ([Ser71], Théorème 3)**.**
For an elliptic curve $E/\mathbb{Q}$ without complex multiplication, the image of the map

$$\hat{\rho} : G \to \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$$

is always contained in a subgroup of index 2.

We now write an explicit description of this subgroup of order 2 for any given curve E, following Serre and Zywina.

The symmetric group on 3 letters S_3 is isomorphic to $\mathrm{GL}_2(\mathbb{F}_2)$, so

$$\mathrm{Aut}(E[2]) \cong S_3.$$

If we write the three affine points of order 2 on an elliptic curve E as $\{(e_1, 0), (e_2, 0, (e_3, 0)\}$, then the symmetric group operates on $\{e_1, e_2, e_3\}$ by permuting the indices. A permutation is called even or odd respectively if it can be written as the composition of an even or odd number of transpositions of two elements. If N_σ is the number of transpositions for the permutation $\sigma \in S_3$, then define the character

$$\begin{aligned} \epsilon : \mathrm{Aut}(E[2]) &\to \{\pm 1\} \\ \epsilon(\sigma) &\mapsto (-1)^{N_\sigma} \end{aligned} \tag{2.1.1}$$

which is consistent with the existing notions of even and odd.

Recall from (1.2.1) that the three points of order 2 must satisfy the equation

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 0,$$

which has discriminant

$$\Delta = a_n^{2n-2} \prod_{i<j} (e_i - e_j)^2 = 4^4 \prod_{i<j} (e_i - e_j)^2.$$

Obviously

$$\sqrt{\Delta} = \pm 16(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$$

so the field extension $\mathbb{Q}(\sqrt{\Delta})$ is contained in $\mathbb{Q}(E[2])$. Define the character

$$\chi_\Delta(\sigma) = (\epsilon \circ \rho_2)(\sigma) : \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \to \{\pm 1\}$$

to be the composition of the maps ϵ and ρ_2 for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Lemma 2.7. *The character χ_Δ corresponds to a field extension of degree ≤ 2, namely $\mathbb{Q}(\sqrt{\Delta})$.*

We now define this homomorphism.

Definition 2.8. Let Δ be the discriminant of an elliptic curve E, then $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(E[2])$.

Define the character χ_Δ to be

$$\chi_\Delta : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\},$$

and such that $\chi_\Delta(a) = \epsilon(\rho_2(a))$ for all $a \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. In particular, this equality holds for all $a \in \mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q})$.

The extension $\mathbb{Q}(\sqrt{\Delta})$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_{d_\Delta})$, where the minimal d_Δ is

$$d_\Delta = \begin{cases} |\Delta_{\mathrm{sf}}| & \text{if } \Delta_{\mathrm{sf}} \equiv 1 \pmod 4 \\ 4|\Delta_{\mathrm{sf}}| & \text{if } \Delta_{\mathrm{sf}} \not\equiv 1 \pmod 4. \end{cases} \tag{2.1.2}$$

Here Δ_{sf} denotes the square-free part of $\Delta \in \mathbb{Z}$, in other words the largest factor $\Delta_{\mathrm{sf}} \mid \Delta$ such that $\frac{\Delta}{\sqrt{\Delta_{\mathrm{sf}}}} \in \mathbb{Z}$. Lemma 2.7 can now be restated to claim that

$$\epsilon(\rho_2(a)) = \chi_\Delta(a)$$

for all $a \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

The character χ_Δ can also be factored as a composition of the canonical homomorphism $G \to \mathrm{Gal}(\mathbb{Q}(\zeta_{d_\Delta})/\mathbb{Q})$ with the character

$$\alpha_\Delta : (\mathbb{Z}/d_\Delta\mathbb{Z})^\times \to \{\pm 1\},$$

which is the Kronecker symbol for modulus d_Δ. This leads to the equality

$$\chi_\Delta(a) = \alpha_\Delta(\det(\rho_{d_\Delta}(a)))$$

and so Lemma 2.7 can again be restated as requiring

$$\epsilon(\rho_2(a)) = \alpha_\Delta(\det(\rho_{d_\Delta}(a)))$$

for all $a \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Definition 2.9. Let $r_m : \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ be the usual reduction modulo m map, and define

$$H_\Delta = \left\{ s \in \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell) : \epsilon(r_2(s)) = \alpha_\Delta(\det(r_{d_\Delta}(s))) \right\}.$$

Then H_Δ is a subgroup of $\prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$ of index 2.

This states that for an elliptic curve as in Theorem 2.6 with discriminant Δ, $\mathrm{Im}(\hat{\rho}) \subseteq H_\Delta$, so in general the index of $\mathrm{Im}(\hat{\rho})$ in H_Δ is ≥ 2.

Definition 2.10. A *Serre curve* is an elliptic curve without complex multiplication and with discriminant Δ, such that

$$\mathrm{Im}(\hat{\rho}) = H_\Delta.$$

In other words, the image of $\hat{\rho}$ in $\prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$ is as large as possible.

The third statement of Corollary 2.5.1 is that for an elliptic curve E there is always an integer m_E such that

$$\hat{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to G(m_E) \times \prod_{\ell \nmid m_E} \mathrm{GL}_2(\mathbb{Z}_\ell)$$

and

$$r_{m_E}^{-1}(G(m_E)) = G_{m_E}.$$

If E is a Serre curve, define

$$M_\Delta = \mathrm{lcm}(2, d_\Delta) \tag{2.1.3}$$

where d_Δ is as defined in (2.1.2). Then $m_E = M_\Delta$ for the curve E. In [Jon06], Jones has proven that almost all elliptic curves are Serre curves, so non-Serre curves may be thought of as being somewhat exceptional.

Chapter 3

Conjectures on distributions of primes associated with elliptic curves

3.1 Notions of probability and the Twin-Prime Conjecture

The original twin prime conjecture posits that there are infinitely many primes p such that $p+2$ is also prime. In [HL23], Hardy and Littlewood refine this slightly to conjecture that the asymptotic relations

$$N_r(x) = \#\{p \leq x : p,\ p+r \text{ both prime}\} \sim 2 \cdot \prod_{\ell \neq 2} \left(1 - \frac{1}{(\ell-1)^2}\right) \prod_{\substack{\ell \mid r \\ \ell \neq 2}} \frac{(\ell-1)}{(\ell-2)} \cdot \frac{x}{\log^2(x)},$$

$$\#\{p \leq x : p, p+2 \text{ both prime}\} \sim 2 \cdot \prod_{\ell \neq 2} \frac{\ell(\ell-2)}{(\ell-1)^2} \cdot \frac{x}{\log^2(x)} \tag{3.1.1}$$

hold as x tends to infinity. The reasoning behind this conjecture is a heuristic argument, that treats the distribution of the primes among the positive integers as if it were a probability distribution. In this sense, the "probability" that a random integer n is a prime is

$$\text{Prob}(n \text{ prime}) = \frac{1}{\log(n)}$$

by the prime number theorem. Similarly then, if the twin prime candidates n and $n+2$ are chosen randomly and independently, the probability of both these integers being a twin prime pair should

be

$$\text{Prob}(n \text{ prime}) \cdot \text{Prob}(n+2 \text{ prime})$$

so counting the twin primes less than an upper bound x should give

$$\pi^{\text{twin}}(x) = \sum_{n \leq x} \frac{1}{\log(n)} \cdot \frac{1}{\log(n+2)} \sim \frac{x}{\log^2(x)}. \tag{3.1.2}$$

While mostly sensible, this approximation is immediately seen to be inaccurate. Obviously, it does not account for the non-independent nature of the divisibility of n and $n+2$ - namely that once we are given n, the value of $n+2$ follows automatically and is thus fully dependent on the initial choice of n. To compensate for this inaccuracy, it will be necessary to introduce a correcting factor.

To derive this factor, we will begin by considering an alternate heuristic argument for computing the probability of $n, n+2$ being twin primes, this time using divisibility conditions. Requiring that n and $n+2$ both be prime is equivalent to requiring that $\ell \nmid n(n+2)$ for all primes ℓ. The probability $\text{Prob}(\ell \nmid n(n+2)$ for a single odd prime ℓ is found from a simple counting argument to be

$$\begin{aligned}
\text{Prob}(\ell \nmid n(n+2)) &= \frac{\#\{n \pmod{\ell} : n(n+2) \not\equiv 0 \pmod{\ell}\}}{\#\{n \pmod{\ell}\}} \\
&= \frac{\#\{n \pmod{\ell} : n \not\equiv 0 \pmod{\ell},\ (n+2) \not\equiv 0 \pmod{\ell}\}}{\ell} \\
&= \frac{\ell - 2}{\ell},
\end{aligned}$$

and for $\ell = 2$ the same argument gives

$$\begin{aligned}
\text{Prob}(2 \nmid n(n+2)) &= \frac{\#\{n \pmod 2 : n(n+2) \not\equiv 0 \pmod 2\}}{2} \\
&= \frac{1}{2}.
\end{aligned}$$

These divisibility conditions cannot be used to themselves represent the asymptotic number of twin primes. Although the number of twin primes less than an upper bound x is given by

$$\frac{1}{2} \prod_{\substack{\ell < x \\ \ell \neq 2}} \left(\frac{\ell - 2}{\ell} \right) = \frac{1}{2} \prod_{\substack{\ell < x \\ \ell \neq 2}} \left(1 - \frac{2}{\ell} \right),$$

taking the limit as $x \to \infty$ gives the divergent product

$$\lim_{x \to \infty} \frac{1}{2} \prod_{\substack{\ell < x \\ \ell \neq 2}} \left(1 - \frac{2}{\ell} \right) = \frac{1}{2} \prod_{\ell \neq 2} \left(1 - \frac{2}{\ell} \right) \to \infty.$$

The problem enters in when taking the limit of the product across all primes: before this point, the argument is sound. So instead of trying to use this model to compute the probability, we can instead

employ it to account for the dependent relationship between n and $n+2$. We can express the finite ratio of the probability that $n, n+2$ are prime to the probability that a, b are prime where these latter two are chosen in a truly random fashion. The probability that $\ell \nmid a$ and $\ell \nmid b$ for independent integers a and b is

$$\text{Prob}(\ell \nmid a,\ \ell \nmid b) = \text{Prob}(\ell \nmid a) \cdot \text{Prob}(\ell \nmid b) = \left(\frac{(\ell-1)}{\ell}\right)^2,$$

so the ratio of probabilities is

$$\begin{aligned}\frac{\text{Prob}(\ell \nmid n(n+2))}{\text{Prob}(\ell \nmid a,\ \ell \nmid b)} &= \frac{1/2}{(1/2)^2} \cdot \prod_{\ell \neq 2} \frac{\left(\frac{\ell-2}{\ell}\right)}{\left(\frac{\ell-1}{\ell}\right)^2} \\ &= 2 \cdot \prod_{\ell \neq 2} \frac{\ell(\ell-2)}{(\ell-1)^2} = 2 \cdot \prod_{\ell \neq 2} \left(1 - \frac{1}{\ell^2 - 2\ell + 1}\right).\end{aligned}$$

This ratio does not require the taking of limits, and so does not introduce any errors: indeed, this infinite product can be seen to converge. In some sense, the value of this ratio accounts for the part of $\text{Prob}(\ell \nmid n(n+2))$ which results from n and $n+2$ having non-independent divisibility conditions, so multiplying this by the estimate of (3.1.2) should correct for its inability to account for this non-independent divisibility, and this is the product given in (3.1.1).

The same approach will be used later for the Lang-Trotter and Koblitz conjectures, to compute a ratio of probabilities consisting of the naive probability as the denominator, and the desired probability condition as the numerator.

Theorem 3.1 (Sato-Tate. [ST92], IV.2)**.** *Let E be an elliptic curve without complex multiplication, with discriminant Δ_E, and using the Hasse bound define $z = \frac{a_p(E)}{2\sqrt{p}} \in [-1, 1]$. Then the distribution of primes $p \leq x$ such that z lies in the interval $[\alpha, \beta] \subseteq [-1, 1]$ is given asymptotically by*

$$\lim_{x \to \infty} \frac{\{p \leq x : \alpha \leq z \leq \beta\}}{\pi(x)} \sim \int_\alpha^\beta \psi_E(t)dt = \int_\alpha^\beta \frac{2}{\pi}\sqrt{1-t^2}dt.$$

Equivalently, this gives a $\sin^2$ distribution of the angle θ_p defined by $\cos(\theta_p) = \frac{a_p(E)}{2\sqrt{p}}$ in the interval $[0, \pi]$.

Formerly the Sato-Tate Conjecture, this was proven by Richard Taylor in [Tay08].

Theorem 3.2. *Let $\Omega(m) \subseteq G(m)$ be a union of conjugacy classes in the image of ρ_m, and*

$$D_m = \{p : \rho_m(\sigma_p) \in \Omega(m) \subseteq G(m)\}$$

be a subset of the primes p. Then

$$\#\{p \leq x : p \in D_m\} \sim \delta_m \pi(x)$$

as a consequence of the Tchebotarev Density Theorem (Theorem 1.25), where

$$\delta_m = \frac{|\Omega(m)|}{|G(m)|}.$$

3.2 The Lang-Trotter Conjecture

Definition 3.3. For the Lang-Trotter conjecture, we define the following notation.

$$G(\ell) = \mathrm{Im}(\rho_\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \qquad G(m) = \mathrm{Im}(\rho_m) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

where $\mathrm{Im}(\rho_m) = \prod_{\ell|m} \mathrm{Im}(\rho_\ell)$ if $\ell \nmid m_E$, and

$$G_r(m) = \{g \in G(m) : \mathrm{tr}(g) \equiv r \pmod{m}\}.$$

Conjecture 3.4 (Lang-Trotter Conjecture. [LT76])**.** *Let E be an elliptic curve with no complex multiplication, and m_E an integer which splits and stabilizes the curve's representation $\hat{\rho}$ of 2.0.1. Then the number of primes p for which the trace of Frobenius $a_p(E)$ is equal to a nonzero constant r satisfying $|r| \leq 2\sqrt{p}$ can be expressed asymptotically as*

$$\pi_r^{LT}(x) = \#\{p \leq x : a_p(E) = r\} \sim C_{E,r} \cdot \frac{\pi(\sqrt{x})}{2}$$

where

$$\frac{\pi(\sqrt{x})}{2} = \sum_{p \leq x} \frac{1}{2\sqrt{p}} \sim \frac{\sqrt{x}}{2\log(\sqrt{x})} = \frac{\sqrt{x}}{\log(x)},$$

and

$$C_{E,r} = \psi_E(0) \cdot \frac{m_E |G_r(m_E)|}{|G(m_E)|} \cdot \prod_{\ell \nmid m_E} \frac{\ell |G_r(\ell)|}{|G(\ell)|}.$$

The function $\psi_E(x)$ is from Theorem 3.1 and $\psi_E(0) = \frac{2}{\pi}$. This constant can be 0 and the asymptotic is then interpreted to mean that there are finitely many such primes.

Lemma 3.5.

$$\#\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}(A) \equiv r \pmod{\ell}\} = \begin{cases} \ell(\ell^2 - \ell - 1) & \text{if } r \not\equiv 0 \pmod{\ell} \\ \ell^2(\ell - 1) & \text{if } r \equiv 0 \pmod{\ell} \end{cases}$$

Proof. Observe that this can be further broken up as

$$\begin{aligned} &\#\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}(A) \equiv r \pmod{\ell}\} \\ &\quad = \#\{A \in M_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}(A) \equiv r \pmod{\ell}\} - \#\{A \in M_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}(A) \equiv r, \det(A) \equiv 0 \pmod{\ell}\}. \end{aligned}$$

Working modulo ℓ: there are clearly ℓ^3 possible matrices of the form $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2 \pmod{\ell}$ with a fixed trace $a + b \equiv r$, so we have only to compute the number of these which also have a determinant of 0.

If $r \equiv 0$, then $\det(A) = ad - bc = a(r-a) - bc \equiv 0$. If $a \equiv 0, r$ then there are $2\ell - 1$ choices for combinations of b and c. If $a \not\equiv 0, r$ then there are $(\ell - 2)$ choices for a, and $(\ell - 1)$ choices for combinations of b and c. In total then,

$$\#\{A \in M_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}(A) \equiv 0, \det(A) \equiv 0 \pmod{\ell}\} = 2(2\ell - 1) + (\ell - 2)(\ell - 1) = \ell^2 + \ell,$$

so there are $\ell^3 - \ell^2 - \ell$ matrices with nonzero determinant.

If $r \not\equiv 0$, then $\det(A) = ad - bc = -a^2 - bc \equiv 0$. If $a \equiv 0$ then there are $(2\ell - 1)$ choices for combinations of b and c. If $a \not\equiv 0$ then there are $(\ell - 1)$ choices for a and $(\ell - 1)$ choices for combinations of b and c. In total then, there are

$$\#\{A \in M_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}(A) \not\equiv 0, \det(A) \equiv 0 \pmod{\ell}\} = (2\ell + 1) + (\ell - 1)^2 = \ell^2,$$

so there are $\ell^3 - \ell^2$ matrices with nonzero determinant. □

Lemma 3.6. *The constant $C_{E,r}$ from Conjecture 3.4 is given by*

$$\begin{aligned} C_{E,r} &= \psi_E(0) \cdot \frac{|G_r(m_E)|}{|G(m_E)|} \left(\frac{1}{m_E}\right)^{-1} \cdot \prod_{\ell \nmid m_E} \left(\frac{1}{\ell}\right)^{-1} \frac{|G_r(\ell)|}{|G(\ell)|} \\ &= \frac{2}{\pi} \cdot \frac{m_E |G_r(m_E)|}{|G(m_E)|} \prod_{\substack{\ell \nmid m_E \\ \ell \mid r}} \left(\frac{\ell^2}{\ell^2 - 1}\right) \prod_{\substack{\ell \nmid m_E \\ \ell \nmid r}} \frac{\ell(\ell^2 - \ell - 1)}{(\ell - 1)(\ell^2 - 1)} \\ &= \frac{2}{\pi} \cdot \frac{m_E |G_r(m_E)|}{|G(m_E)|} \prod_{\substack{\ell \nmid m_E \\ \ell \mid r}} \left(1 - \frac{1}{\ell^2}\right)^{-1} \cdot \prod_{\substack{\ell \nmid m_E \\ \ell \nmid r}} \left(1 - \frac{1}{(\ell - 1)(\ell^2 - 1)}\right). \end{aligned}$$

Proof. The naive probability that a random integer a will be equivalent to $r \pmod{m}$ is $\frac{1}{m}$ for any integer m, which explains the factors of $\left(\frac{1}{\ell}\right)^{-1}$ and $\left(\frac{1}{m_E}\right)^{-1}$ present in the constant. Then for all $\ell \nmid m_E$, by Corollary 2.5.1

$$G_r(\ell) \simeq \{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}(A) \equiv r \pmod{\ell}\}, \qquad \text{and } G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

so $|G_r(\ell)|$ is given by Lemma 3.5 and

$$\frac{\ell|G_r(\ell)|}{|G(\ell)|} = \begin{cases} \dfrac{\ell^3(\ell-1)}{\ell(\ell-1)^2(\ell+1)} & \text{if } r \equiv 0 \pmod{\ell} \\ \\ \dfrac{\ell^2(\ell^2-\ell-1)}{\ell(\ell-1)^2(\ell+1)} & \text{if } r \not\equiv 0 \pmod{\ell}. \end{cases}$$

□

3.3 The Koblitz Conjecture

Definition 3.7. For the Koblitz conjecture, the sets

$$G(\ell) = \mathrm{Im}(\rho_\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \qquad \text{and } G(m) = \mathrm{Im}(\rho_m) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

are defined the same as in the Lang-Trotter conjecture. Again, $\mathrm{Im}(\rho_m) = \prod_{\ell|m} \mathrm{Im}(\rho_\ell)$ if $\ell \nmid m_E$. We also define

$$\Omega(m) = \{g \in G(m) : (\det(g) + 1 - \mathrm{tr}(g), m) = 1\}.$$

Notice that if $m = \ell$ is a prime, then

$$\Omega(\ell) = \{g \in G(\ell) : \ell \nmid (\det(g) + 1 - \mathrm{tr}(g))\}.$$

Conjecture 3.8 (Koblitz Conjecture. [Kob88], [Zyw09])**.** *Let E be an elliptic curve with no complex multiplication. Then the number of primes $p \nmid \Delta$ for which the number of points on the curve $E \pmod{p}$ is also prime can be written asymptotically as*

$$\pi^K(x) = \#\{p \le x : p \nmid \Delta,\ |E \pmod{p}| \text{ is prime}\} \sim C_E \cdot \frac{x}{\log^2(x)},$$

where

$$\frac{x}{\log^2(x)} \sim \sum_{p \le x} \frac{1}{\log(p+1)}$$

and

$$C_E = \frac{|\Omega(m_E)|}{|G(m_E)|} \prod_\ell \left(\frac{\ell}{\ell-1}\right) \prod_{\ell \nmid m_E} \frac{|\Omega(\ell)|}{|G(\ell)|}.$$

The constant C_E may be 0, in which case the conjecture is interpreted to mean there are finitely many primes. The sum

$$\sum_{p \le x} \frac{1}{\log(p+1)} \sim \sum_{p \le x} \frac{1}{\log(|E \pmod{p}|)}$$

is based on the naive probability that $|E(\text{mod } p)|$ is prime. This in turn comes from the prime number theorem which states that

$$\frac{\#\{p \leq x : p \text{ is prime}\}}{x} \sim \frac{1}{\log(x)}.$$

The absolute value of $(|E \pmod p| - (p+1))$ is bounded by $|2\sqrt{p}|$, so we use $\frac{1}{\log(p+1)}$ in the sum instead of $\frac{1}{|E(\text{mod } p)|}$.

Lemma 3.9. *Given a matrix $A \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ where m is a positive integer, the following two conditions are equivalent:*

$$\det(A) + 1 - \mathrm{tr}(A) \in (\mathbb{Z}/m\mathbb{Z})^\times$$

$$\det(I - A) \in (\mathbb{Z}/m\mathbb{Z})^\times$$

Proof. A straightforward computation reveals

$$\begin{aligned}\det(I - A) &= \left| \begin{pmatrix} 1-a & b \\ c & 1-d \end{pmatrix} \right| \\ &= (1-a)(1-d) - bc \\ &= 1 - (a+d) + ad - bc \\ &= \det(A) + 1 - \mathrm{tr}(A).\end{aligned}$$

□

Obviously if m is a prime, then both conditions simplify to requiring non-zero elements. This allows us to use notation interchangeably for the set

$$\left\{A \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \det(A) + 1 - \mathrm{tr}(A) \in (\mathbb{Z}/m\mathbb{Z})^\times\right\} = \left\{A \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \det(I - A) \in (\mathbb{Z}/m\mathbb{Z})^\times\right\}.$$

Lemma 3.10. *Let q be a fixed unit in the finite field $\mathbb{Z}/\ell\mathbb{Z}$ with ℓ elements, and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Then*

$$\#\{A : A \textit{ has eigenvalues } 1 \textit{ and } q\} = \begin{cases} \ell^2 + \ell & \textit{if } q \neq 1 \\ \ell^2 & \textit{if } q = 1 \end{cases}$$

Proof. If $q = 1$, then A has only $\lambda = 1$ as an eigenvalue so $\mathrm{tr}(A) = 2$ and $\det(A) = 1$. If $ad = 1$ then bc must equal 0 giving $(2\ell - 1)$ combinations, and this happens exactly when $a = 1$ regardless of the

modulus ℓ, as $\det(A) = a(2-a) = 1$ is equivalent to the polynomial $(a-1)^2 = 0$ which has only the one solution. There are then $(\ell - 1)$ possible combinations remaining for ad, and for each of these there are exactly $(\ell - 1)$ combinations for $bc = 1 - ad$. We sum these two values to find that there are $(2\ell - 1) + (\ell - 1)^2 = \ell^2$ matrices if $q = 1$.

If $q \neq 1$, then A has both $\lambda = 1, q$ as eigenvalues so $\mathrm{tr}(A) = q+1$ and $\det(A) = q$. Counting the matrices with both conditions amounts to solving the polynomial $a(q+1-a) - bc - q = 0$, which is equivalent to $(1-a)(q-a) + bc = 0$. If $a = 1$ or q then $bc = 0$ which can be written in $(2\ell - 1)$ different ways. If $a \neq 1, q$ then $bc = -(1-a)(q-a) \neq 0$ which can be written in $(\ell - 1)$ different ways. Together then, we have $2(2\ell - 1) + (\ell - 1)(\ell - 2) = \ell + \ell^2$ different matrices if $q \neq 1$. □

Corollary 3.10.1.

$$|\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(I - A) = 0\}| = \left(\ell^2 + (\ell - 2)(\ell^2 + \ell)\right)$$

Proof. Recall that by writing $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$$\begin{aligned} \det(\lambda I - A) &= \begin{vmatrix} \lambda - a & b \\ c & \lambda - d \end{vmatrix} = (\lambda - a)(\lambda - d) - bc \\ &= \lambda^2 - (a+d)\lambda + ad - bc = \lambda^2 - \mathrm{tr}(A)\lambda + \det(A) = (\lambda - 1)(\lambda - q) \\ &= \lambda^2 - (q+1)\lambda + q. \end{aligned}$$

So $\mathrm{tr}(A) = (q+1)$ and $\det(A) = q$, the sum and product of the eigenvalues. Clearly, $\det(A) \neq 0$ so $q \neq 0$. The value of q is therefore either itself 1, or else $q \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, $q \neq 0, 1$, leaving $(\ell - 2)$ possible values. Applying Lemma 3.10 then gives the desired result. □

Lemma 3.11. *The constant C_E from Conjecture 3.8 is given by*

$$\begin{aligned} C_E &= \frac{|\Omega(m_E)|}{|G(m_E)|} \prod_{\ell \mid m_E} \left(1 - \frac{1}{\ell}\right)^{-1} \prod_{\ell \nmid m_E} \left(1 - \frac{1}{\ell}\right)^{-1} \frac{|\Omega(\ell)|}{|G(\ell)|} \\ &= \frac{|\Omega(m_E)|}{|G(m_E)|} \prod_{\ell \mid m_E} \left(\frac{\ell}{\ell - 1}\right) \prod_{\ell \nmid m_E} \left(\frac{\ell}{\ell - 1}\right) \left(1 - \frac{\ell^2 - 2}{(\ell - 1)^2(\ell + 1)}\right) \\ &= \frac{|\Omega(m_E)|}{|G(m_E)|} \prod_{\ell \mid m_E} \left(\frac{\ell}{\ell - 1}\right) \prod_{\ell \nmid m_E} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}\right) \end{aligned}$$

Proof. The naive probability that a random integer a will satisfy $a \not\equiv 0 \pmod{\ell}$ is $\frac{\ell-1}{\ell}$, justifying the factors of $\left(\frac{1}{\ell}\right)^{-1}$ in C_E. Since $\ell \nmid m_E$, then by Corollary 2.5.1

$$\Omega(\ell) = \{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(I - A) \not\equiv 0 \pmod{\ell}\}, \qquad \text{and } G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

so

$$\frac{|\Omega(\ell)|}{|G(\ell)|} = 1 - \frac{|\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(I - A) = 0 (\mathrm{mod} \ell)\}|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}$$

which by Corollary 3.10.1 is

$$\begin{aligned} &= 1 - \frac{\left(\ell^2 + (\ell-2)(\ell^2+\ell)\right)}{\ell(\ell-1)^2(\ell+1)} \\ &= 1 - \left(\frac{\ell^2 - 2}{(\ell-1)^2(\ell+1)}\right) \end{aligned}$$

□

3.4 The Mixed Conjecture

Combining the conditions of the Lang-Trotter and Koblitz conjectures amounts to finding the distribution of primes p such that $p + 1 - a_p(E)$ is also prime, for a fixed value of $a_p(E) = r$. We are then looking for an asymptotic estimate for

$$\pi_r^{\mathrm{mix}}(x) = \#\{p \leq x : a_p(E) = r,\ p + 1 - a_p(E) \text{ is prime}\}$$

where r is a fixed integer. This value must clearly be odd, since otherwise $p+1-a_p(E)$ will be even and necessarily composite, and if $r = 1$ then the condition of $p + 1 - a_p(E)$ being prime becomes redundant. Unless explicitly stated otherwise, we will henceforth assume that $r \neq 1$ and is odd. Clearly, $\pi_r^{\mathrm{mix}}(x)$ is finite in these cases. Note also that the $\pi_r^{\mathrm{mix}}(x) = \pi_r^{\mathrm{LT}}(x)$ if (and only if) $r = 1$.

So given an elliptic curve E with no complex multiplication and an integer r with $|r| \leq 2\sqrt{p}$, we wish to count the primes $p \leq x$ which have $a_p(E) = r$ and such that $|E(\mathbb{F}_p)| = p + 1 - r$ is also prime. Under a product over all primes ℓ, we will use the well defined trace and determinant maps

$$\mathrm{tr}(\rho_\ell(\phi_p)) \equiv a_p(E) \pmod{\ell}, \qquad \det(\rho_\ell(\phi_p)) \equiv p \pmod{\ell}$$

for primes $p \neq \ell$ of good reduction.

Definition 3.12. For the mixed conjecture, the sets

$$G(\ell) = \mathrm{Im}(\rho_\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \qquad \text{and } G(m) = \mathrm{Im}(\rho_m) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

are defined the same as in the Lang-Trotter conjecture. Once again, $\mathrm{Im}(\rho_m) = \prod_{\ell \mid m} \mathrm{Im}(\rho_\ell)$ if $\ell \nmid m_E$. We also define

$$\Omega_r(m) = \{g \in G(m) : (\det(g) + 1 - \mathrm{tr}(g), m) = 1,\ \mathrm{tr}(g) \equiv r \pmod m\} \tag{3.4.1}$$

for an integer m.

Conjecture 3.13 (Mixed Conjecture)**.** *Let E be an elliptic curve with no complex multiplication. Then we can write asymptotically the number of primes $p \nmid \Delta$ for which both the trace of Frobenius $a_p(E)$ is equal to a nonzero constant r and the number of points on the curve $E \pmod p$ is also prime as*

$$\pi^{\mathrm{mix}}(x) = \#\{p \le x : p \nmid \Delta,\ p + 1 - |E(\mathbb{F}_p)| = r,\ |E(\mathbb{F}_p)| \text{ is prime}\} \sim C_{E,r} \cdot \frac{\sqrt{x}}{\log^2(x)},$$

where

$$C_{E,r} = \frac{2}{\pi} \frac{m_E^2}{\phi(m_E)} \cdot \frac{|\Omega_r(m_E)|}{|G(m_E)|} \cdot \prod_{\ell \nmid m_E} \left(\frac{\ell^2}{\ell - 1}\right) \frac{|\Omega_r(\ell)|}{|G(\ell)|}$$

and $\phi(m_E)$ is just Euler's totient function at m_E.

The constant $C_{E,r}$ is derived using the naive probability of $\frac{\phi(m)}{m^2} = \frac{\phi(m)}{m} \cdot \frac{1}{m}$ that the random integers a and b will satisfy both $a \not\equiv 0 \pmod m$ and $b \equiv r \pmod m$, for any integer m. This gives a correcting factor of

$$\frac{\frac{|\Omega_r(\ell)|}{|G(\ell)|}}{\left(\frac{\ell-1}{\ell^2}\right)}$$

for each prime $\ell \nmid m_E$, and a correcting factor of

$$\frac{\frac{|\Omega_r(m_E)|}{|G(m_E)|}}{\left(\frac{\phi(m_E)}{m_E^2}\right)}$$

to account for the primes $\ell \nmid m_E$. From the definitions of $\Omega_r(m)$ and $G(m)$ in (3.4.1), the constant $C_{E,r}$ must split into factors according to the divisibility of the integer m_E as

$$\begin{aligned} C_{E,r} &= \psi_E(0) \cdot \left(\frac{m_E^2}{\phi(m_E)}\right) \prod_{\ell \nmid m_E} \left(\frac{\ell^2}{\ell - 1}\right) \cdot \delta_{m_E} \prod_{\ell \nmid m_E} \delta_\ell \\ &= \frac{2}{\pi} \cdot \delta_{m_E} \left(\frac{m_E^2}{\phi(m_E)}\right) \cdot \prod_{\ell \nmid m_E} \left(\delta_\ell \cdot \frac{\ell^2}{(\ell - 1)}\right). \end{aligned}$$

The function δ is multiplicative whenever $\hat{\rho}$ is surjective (which is for all primes $\ell \nmid m_E$), so we write

$$= \frac{2}{\pi} \frac{|\Omega_r(m_E)|}{|G(m_E)|} \left(\frac{m_E^2}{\phi(m_E)}\right) \cdot \prod_{\ell \nmid m_E} \left(\frac{|\Omega_r(\ell)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} \cdot \frac{\ell^2}{(\ell - 1)}\right). \tag{3.4.2}$$

This constant may be equal to 0, in which case this is interpreted as meaning there are finitely many primes in the set

$$\{p : p \nmid \Delta,\ p+1-|E(\mathbb{F}_p)| = r,\ |E(\mathbb{F}_p)| \text{ is prime}\}.$$

The most obvious case in which the constant is zero occurs whenever the value of the trace r is even (since then $p+1-r$ is also even) so $C_{E,r}$ is zero or non-zero based on the value of $r \pmod 2$. Perhaps less obviously, $C_{E,r}$ is also zero if the curve E has any rational points of torsion, since by Proposition 1.26 this will give a non-trivial divisor for $|E(\mathbb{F}_p)|$. Finally, there may be other divisibility conditions which give rise to additional constraints on $C_{E,r}$. For instance, we will see an elliptic curve in chapter 4 for which the constant is zero or non-zero based on the value of $r \pmod 6$ instead of just mod 2.

In order to compute $C_{E,r}$ and give a precise description of the factors $|\Omega_r(m_E)|$ and $|\Omega_r(\ell)|$, we will deal with the terms of this expression in two parts by writing

$$C_{E,r} = \frac{2}{\pi} \cdot C_1(E,r) \cdot C_2(E,r)$$

where

$$\begin{aligned} C_1(E,r) &= \prod_{\ell \nmid m_E} \left(\frac{|\Omega_r(\ell)|}{|\mathrm{GL}_2(\ell)|} \cdot \frac{\ell^2}{(\ell-1)} \right) \\ C_2(E,r) &= \frac{|\Omega_r(m_E)|}{|G(m_E)|} \cdot \frac{m_E^2}{\phi(m_E)}. \end{aligned} \tag{3.4.3}$$

We will need several lemmas before we can write these explicitly.

Lemma 3.14. *For ℓ an odd prime,*

$$\#\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(I-A) \equiv 0 \pmod \ell,\ \mathrm{tr}(A) \equiv r \pmod \ell\} = \begin{cases} \ell^2+\ell & \text{if } r \equiv 0 \pmod \ell \\ 0 & \text{if } r \equiv 1 \pmod \ell \\ \ell^2 & \text{if } r \equiv 2 \pmod \ell \\ \ell^2+\ell & \text{otherwise.} \end{cases} \tag{3.4.4}$$

Proof. To count the matrices $A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with both $\det(I-A) \equiv 0 \pmod \ell$ and $\mathrm{tr}(A) \equiv r \pmod \ell$, we observe that the condition $\det(I-A) \equiv 0$ implies that $\lambda = 1$ is an eigenvalue for A, and as A can have at most one other eigenvalue, its characteristic polynomial is either $(\lambda-1)(\lambda-q) =$

$\lambda^2-(q+1)\lambda+q$ or simply $(\lambda-1)^2$, corresponding respectively to whether it has another eigenvalue $q \not\equiv 0,1 \pmod{\ell}$ or not. Recall from Lemma 3.9 that $\det(I-A) = 1-\operatorname{tr}(A)+\det(A)$. We want both $\det(I-A)$ and $\det(A)$ to be coprime to the prime ℓ.

Write $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then the characteristic polynomial of A is

$$\begin{aligned} \det(\lambda I - A) &= \begin{vmatrix} \lambda-a & b \\ c & \lambda-d \end{vmatrix} = (\lambda-a)(\lambda-d)-bc \\ &= \lambda^2-(a+d)\lambda+ad-bc \\ &= \lambda^2-\operatorname{tr}(A)\lambda+\det(A). \end{aligned} \tag{3.4.5}$$

Of course, $\lambda \equiv 1 \pmod{\ell}$ is a root by the Lemma's assumption that $\det(I-A) \equiv 0 \pmod{\ell}$. This lets us factor the polynomial as

$$\begin{aligned} \lambda^2-\operatorname{tr}(A)\lambda+\det(A) &= (\lambda-1)(\lambda-q) \\ &= \lambda^2-(q+1)\lambda+q \end{aligned} \tag{3.4.6}$$

where $\lambda = q \in \mathbb{Z}/\ell\mathbb{Z}$ is the second root.

As the respective sum and product of the eigenvalues, we see that $\operatorname{tr}(A) = (q+1)$ and $\det(A) = q$. Then using Lemma 3.10 we have the following list:

- if $r \equiv 0 \pmod{\ell}$ then $q \equiv -1$ so there are $\ell^2+\ell$ matrices
- if $r \equiv 1 \pmod{\ell}$ then $q \equiv 0$ so there are no matrices
- if $r \equiv 2 \pmod{\ell}$ then $q \equiv 1$ so there are ℓ^2 matrices
- if $r \not\equiv 0,1,2 \pmod{\ell}$ then there are $\ell^2+\ell$ matrices

Putting these conditions together, the stated result follows immediately. □

Theorem 3.15. *For ℓ an odd prime,*

$$\#\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(I-A) \not\equiv 0 \pmod{\ell}, \operatorname{tr}(A) \equiv r \pmod{\ell}\} = \begin{cases} \ell^3-2\ell^2-\ell & \text{if } r \equiv 0 \pmod{\ell} \\ \ell^3-\ell^2-\ell & \text{if } r \equiv 1 \pmod{\ell} \\ \ell^3-2\ell^2-\ell & \text{if } r \equiv 2 \pmod{\ell} \\ \ell^3-2\ell^2-2\ell & \text{otherwise} \end{cases}$$

Proof. For odd ℓ, this is a simple sum using Lemmas 3.5 and 3.14:

$$\#\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(I-A) \in (\mathbb{Z}/\ell\mathbb{Z})^\times, \mathrm{tr}(A) \equiv r \pmod{\ell})\} = \begin{cases} \ell^2(\ell-1) - (\ell^2+\ell) & \text{if } r \equiv 0 \pmod{\ell} \\ \ell(\ell^2-\ell-1) \ - \ 0 & \text{if } r \equiv 1 \pmod{\ell} \\ \ell(\ell^2-\ell-1) - \ell^2 & \text{if } r \equiv 2 \pmod{\ell} \\ \ell(\ell^2-\ell-1) - (\ell^2+\ell) & \text{otherwise} \end{cases}$$

□

We can now give an explicit statement of $C_1(E,r)$.

Theorem 3.16.

$$C_1(E,r) = \prod_{\ell \nmid m_E} \frac{\ell^2(\ell^2-2\ell-2)}{(\ell-1)^3(\ell+1)} \cdot \prod_{\substack{\ell \mid (r-1) \\ \ell \nmid m_E}} \frac{(\ell^2-\ell-1)}{(\ell^2-2\ell-2)} \cdot \prod_{\substack{\ell \mid r(r-2) \\ \ell \nmid m_E}} \frac{(\ell^2-2\ell-1)}{(\ell^2-2\ell-2)}$$

Proof. For $\Omega_r(\ell)$ as defined in (3.4.1), let r be odd and ℓ an odd prime not dividing m_E, then

$$\frac{\dfrac{|\Omega_r(\ell)|}{|\mathrm{GL}_2(\mathbb{F}_\ell)|}}{\left(\dfrac{\ell-1}{\ell^2}\right)} = \frac{\ell|\Omega_r(\ell)|}{(\ell-1)^3(\ell+1)},$$

and

$$|\Omega_r(\ell)| = \begin{cases} \ell(\ell^2-2\ell-1) & r \equiv 0 \\ \ell(\ell^2-\ell-1) & r \equiv 1 \\ \ell(\ell^2-2\ell-1) & r \equiv 2 \\ \ell(\ell^2-2\ell-2) & \text{otherwise} \end{cases}$$

by Theorem 3.15. So

$$\begin{aligned} \frac{\dfrac{|\Omega_r(\ell)|}{|\mathrm{GL}_2(\mathbb{F}_\ell)|}}{\left(\dfrac{\ell-1}{\ell^2}\right)} &= |\Omega_r(\ell)| \cdot \frac{\ell}{(\ell-1)^3(\ell+1)} \\ &= \frac{\ell^2}{(\ell-1)^3(\ell+1)} \cdot \begin{cases} \ell^2-2\ell-1 & r \equiv 0 \\ \ell^2-\ell-1 & r \equiv 1 \\ \ell^2-2\ell-1 & r \equiv 2 \\ \ell^2-2\ell-2 & \text{otherwise} \end{cases} \end{aligned}$$

and re-phrasing this in terms of products over all the primes $\ell \nmid m_E$ gives

$$\begin{aligned} C_1(E,r) &= \prod_{\ell \nmid m_E} \left(\frac{|\Omega_r(\ell)|}{|\mathrm{GL}_2(\ell)|} \cdot \frac{\ell^2}{(\ell-1)} \right) \\ &= \prod_{\ell \nmid m_E} \frac{\ell^2}{(\ell-1)^3(\ell+1)} \cdot \prod_{\substack{\ell \nmid r(r-1)(r-2) \\ \ell \nmid m_E}} (\ell^2 - 2\ell - 2) \cdot \prod_{\substack{\ell \mid (r-1) \\ \ell \nmid m_E}} (\ell^2 - \ell - 1) \cdot \prod_{\substack{\ell \mid r(r-2) \\ \ell \nmid m_E}} (\ell^2 - 2\ell - 1) \\ &= \prod_{\ell \nmid m_E} \frac{\ell^2(\ell^2-2\ell-2)}{(\ell-1)^3(\ell+1)} \cdot \prod_{\substack{\ell \mid (r-1) \\ \ell \nmid m_E}} \frac{(\ell^2-\ell-1)}{(\ell^2-2\ell-2)} \cdot \prod_{\substack{\ell \mid r(r-2) \\ \ell \nmid m_E}} \frac{(\ell^2-2\ell-1)}{(\ell^2-2\ell-2)} \end{aligned} \tag{3.4.7}$$

□

The constant $C_1(E,r)$ also appears in the work of [BCD07], where the authors show that the Koblitz conjecture is true on average over all elliptic curves over $\mathbb{Q}$. One cannot hope to prove a similar average result for this conjecture on the distribution of $\pi^{\mathrm{mix}}(x)$, as the error term in the average computation would be the error term of the twin prime conjecture (for p and $p+1-r$ prime). This error term cannot be controlled as the twin prime conjecture is still open, however it is true on average over r which allows the authors of [BCD07] to prove the Koblitz conjecture on average. In doing so, they are lead to an intermediate step where they compute the main term of the mixed conjecture as an average. The resulting constant

$$C_r = \frac{4}{3} \prod_{\ell \neq 2} \frac{\ell^2(\ell^2-2\ell-2)}{(\ell-1)^3(\ell+1)} \cdot \prod_{\substack{\ell \mid (r-1) \\ \ell \neq 2}} \frac{(\ell^2-\ell-1)}{(\ell^2-2\ell-2)} \cdot \prod_{\substack{\ell \mid r(r-2) \\ \ell \neq 2}} \frac{(\ell^2-2\ell-1)}{(\ell^2-2\ell-2)} \tag{3.4.8}$$

of their paper matches the constant $C_1(E,r)$ when $\ell \nmid m_E$, as it should.

The second part $C_2(E,r)$ of the constant $C_{E,r} = \frac{2}{\pi} C_1(E,r) C_2(E,r)$ is much simpler to describe in detail when the curve E is a Serre curve, so from this point on we will restrict our attention to this class of curves.

3.5 Computing the Mixed constant for Serre curves

The second part of the constant we want to compute is written as

$$C_2(E,r) = \frac{|\Omega_r(m_E)|}{|G(m_E)|} \cdot \frac{m_E^2}{\phi(m_E)}.$$

Since $m_E = M_\Delta$ for a Serre curve by (2.1.3), the constant can be written as

$$C_2(E,r) = \frac{|\Omega_r(M_\Delta)|}{|G(M_\Delta)|} \cdot \frac{M_\Delta^2}{\phi(M_\Delta)}.$$

Definitions 2.9 and 2.10 imply that

$$|G(M_\Delta)| = \frac{1}{2}\left|\mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z})\right|,$$

and $\Omega_r(M_\Delta)$ is the set

$$\left\{A \in \mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z}) :\ \alpha_\Delta((\det(A_{d_\Delta}))) = \epsilon(A_2),\ \det(I-A) \in (\mathbb{Z}/M_\Delta\mathbb{Z})^\times,\ \mathrm{tr}(A) \equiv r \pmod{M_\Delta}\right\},$$

where α_Δ is a real non-trivial character, so the Legendre symbol, and A_{d_Δ} and A_2 denote the matrix A reduced modulo d_Δ and modulo 2, respectively.

Lemma 3.17. *For any $A \in \Omega_r(M_\Delta)$, $\epsilon(A \pmod 2) = 1$.*

Proof. The character ϵ is defined in Lemma 2.7 based on an isomorphism with the symmetric group on three letters, and it was earlier established that each $A \in \Omega_r(M_\Delta)$ must have trace $\equiv 1 \pmod 2$. Of the six matrices in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, only $\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$ have non-zero traces. Neither of these matrices are their own inverses in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, and one can verify that

$$\epsilon\left(\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)\right) = \epsilon\left(\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)\right) = 1.$$

□

A simpler statement of $\Omega_r(M_\Delta)$ is thus

$$\left\{A \in \mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z}) :\ \alpha_\Delta((\det(A_{d_\Delta}))) = 1,\ \det(I-A) \in (\mathbb{Z}/M_\Delta\mathbb{Z})^\times,\ \mathrm{tr}(A) \equiv r \pmod{M_\Delta}\right\}.$$

Since M_Δ may or may not be squarefree according to which power of 2 it has as a divisor, we should consider both cases. Either $M_\Delta \equiv 0 \pmod 4$ and $d_\Delta \equiv 0 \pmod 4$, or $M_\Delta \equiv 2 \pmod 4$ and $d_\Delta \not\equiv 0 \pmod 4$.

We can break up the set $\Omega_r(M_\Delta)$ into subsets for each prime $\ell \mid M_\Delta$ corresponding to whether α_Δ is positive or negative, a process which mirrors the steps taken in [Zyw09], as

$$\beta^{\pm}_{\ell,r} = \left\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell^{v_\ell(M_\Delta)}\mathbb{Z}) :\ \alpha^\ell_\Delta(\phi_\ell(\det(A))) = \pm 1,\ \det(I-A) \in (\mathbb{Z}/\ell\mathbb{Z})^\times,\ \mathrm{tr}(A) \equiv r \pmod{\ell}\right\}$$

where $v_\ell(M_\Delta)$ is just the ℓ-adic order of M_Δ, satisfying $\ell^{v_\ell(M_\Delta)} \mid\mid M_\Delta$.

Using the obvious isomorphism

$$\mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z}) \cong \prod_{\ell \mid M_\Delta} \mathrm{GL}_2(\mathbb{Z}/\ell^{v_\ell(M_\Delta)}\mathbb{Z})$$

and applying the Chinese Remainder Theorem across the divisors $\ell^{v_\ell(M_\Delta)}$, we have

$$\{A \in \mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z}) : \mathrm{tr}(A) \equiv r \pmod{M_\Delta}\} \cong \prod_{\ell \mid M_\Delta} \left\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell^{v_\ell(M_\Delta)}\mathbb{Z}) : \mathrm{tr}(A) \equiv r \pmod{\ell^{v_\ell(M_\Delta)}}\right\}.$$

Now we recall that $\alpha_\Delta(\det A_{d_\Delta}) = 1$ yet this may factor across the dividing primes ℓ as $\alpha_\Delta^\ell(\det A_\ell) = \left(\frac{\det(A \bmod \ell)}{\ell}\right) = \pm 1$. We can therefore take the disjoint union

$$\bigcup_{\substack{D \subseteq \{\ell : \ell \mid M_\Delta\} \\ 2 \mid\mid D\mid}} \prod_{\ell \in D} \beta_{\ell,r}^- \times \prod_{\substack{\ell \notin D \\ \ell \mid M_\Delta}} \beta_{\ell,r}^+ = \Omega_r(M_\Delta)$$

which groups together subsets $\beta_{\ell,r}^+$ which have a positive character, and pairs of subsets $\beta_{\ell,r}^-$ which have negative characters. This relies on the character $\alpha_\Delta = \prod_{\ell \mid M_\Delta} \alpha_\Delta^\ell$ being multiplicative and $\alpha_\Delta(\det(A)) = 1$, then α_Δ is a product of $+1$ and an even power of (-1). This gives us the identity

$$\begin{aligned} |\Omega_r(M_\Delta)| &= \sum_{d \mid \mathrm{rad}(M_\Delta)} \frac{1+\mu(d)}{2} \prod_{\ell \mid d} |\beta_{\ell,r}^-| \prod_{\ell \mid \frac{\mathrm{rad}(M_\Delta)}{d}} |\beta_{\ell,r}^+| \\ &= \frac{1}{2} \prod_{\ell \mid M_\Delta} (|\beta_{\ell,r}^+| + |\beta_{\ell,r}^-|) + \frac{1}{2} \prod_{\ell \mid M_\Delta} (|\beta_{\ell,r}^+| - |\beta_{\ell,r}^-|) \end{aligned} \tag{3.5.1}$$

We can begin to compute this value directly, however it will be beneficial to first make the following observation.

Lemma 3.18. *For odd r,*

$$|\beta_{2,r}^+| - |\beta_{2,r}^-| = \begin{cases} 2 & \text{if } M_\Delta \equiv 2 \pmod 4 \\ 0 & \text{if } M_\Delta \equiv 0 \pmod 4. \end{cases}$$

Proof. For $\ell = 2$, we can easily verify these results through direct calculation, specifically that $|\beta_{2,r}^+| - |\beta_{2,r}^-| = 2$ if $v_2(M_\Delta) = 1$, and $|\beta_{2,r}^+| = |\beta_{2,r}^-|$ if $v_2(M_\Delta) = 2, 3$. □

This suggests a simpler expression for the value of $|\Omega_r(M_\Delta)|$. If we define both of

$$a_r(\ell) = \left(|\beta_{\ell,r}^+| + |\beta_{\ell,r}^-|\right), \qquad b_r(\ell) = \left(|\beta_{\ell,r}^+| - |\beta_{\ell,r}^-|\right),$$

then

$$|\Omega_r(M_\Delta)| = \begin{cases} \frac{1}{2}\prod_{\ell|M_\Delta} a_r(\ell) + \frac{1}{2}\prod_{\ell|M_\Delta} b_r(\ell) & \text{if } M_\Delta \equiv 2 \pmod 4 \\ \frac{1}{2}\prod_{\ell|M_\Delta} a_r(\ell) & \text{if } M_\Delta \equiv 0 \pmod 4. \end{cases}$$

In turn, the value of $C_2(E,r)$ can be written as

$$\begin{aligned} \frac{|\Omega_r(M_\Delta)|}{|G(M_\Delta)|}\frac{M_\Delta^2}{\phi(M_\Delta)} &= \left(\frac{M_\Delta^2}{\phi(M_\Delta)}\right)\cdot\left(\frac{2}{|\mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z})|}\right)\cdot\left(\frac{1}{2}\prod_{\ell|M_\Delta} a_r(\ell) + \frac{1}{2}\prod_{\ell|M_\Delta} b_r(\ell)\right) \\ &= \frac{M_\Delta^2}{\phi(M_\Delta)}\cdot\frac{\prod_{\ell|M_\Delta} a_r(\ell)}{|\mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z})|}\left(1+\prod_{\ell|M_\Delta}\frac{b_r(\ell)}{a_r(\ell)}\right) \\ &= \begin{cases} \frac{M_\Delta^2\cdot\prod_{\ell|M_\Delta} a_r(\ell)}{\phi(M_\Delta)\cdot|\mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z})|}\cdot\left(1+\prod_{\ell|M_\Delta}\frac{b_r(\ell)}{a_r(\ell)}\right) & \text{if } M_\Delta \equiv 2 \pmod 4 \\ \frac{M_\Delta^2\cdot\prod_{\ell|M_\Delta} a_r(\ell)}{\phi(M_\Delta)\cdot|\mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z})|} & \text{if } M_\Delta \equiv 0 \pmod 4. \end{cases} \end{aligned} \tag{3.5.2}$$

It still remains to compute explicit values for $a_r(\ell)$ in terms of ℓ, and $b_r(\ell)$ in terms of odd ℓ.

Proposition 3.19. *Let $e = v_2(M_\Delta)$. If r is odd, then*

$$a_r(2) = |\beta_{2,r}^+| + |\beta_{2,r}^-| = 2^{3e-2} = \begin{cases} 2 & \text{if } e = 1 \\ 16 & \text{if } e = 2 \\ 128 & \text{if } e = 3. \end{cases}$$

If r is even, $|\beta_{2,r}^+| + |\beta_{2,r}^-| = 0$.

For ℓ odd,

$$\begin{aligned} a_r(\ell) = |\beta_{\ell,r}^+| + |\beta_{\ell,r}^-| &= \#\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(I-A) \in (\mathbb{Z}/\ell\mathbb{Z})^\times, \mathrm{tr}(A) \equiv r \pmod \ell\} \\ &= \begin{cases} \ell^3 - 2\ell^2 - \ell & \text{if } r \equiv 0 \pmod \ell \\ \ell^3 - \ell^2 - \ell & \text{if } r \equiv 1 \pmod \ell \\ \ell^3 - 2\ell^2 - \ell & \text{if } r \equiv 2 \pmod \ell \\ \ell^3 - 2\ell^2 - 2\ell & \text{otherwise.} \end{cases} \end{aligned}$$

Proof. For $\ell = 2$, we observe that

$$\begin{aligned}
|\beta^+_{2,r}| + |\beta^-_{2,r}| &= \#\left\{A \in \mathrm{GL}_2(\mathbb{Z}/2^e\mathbb{Z}) : \det(I-A) \in (\mathbb{Z}/2^e\mathbb{Z})^\times,\ \mathrm{tr}(A) \equiv r \pmod{2^e}\right\} \\
&= \#\left\{B \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : \det(I-B) = 1,\ \mathrm{tr}(B) \equiv 1 \pmod 2\right\} \cdot (2^{e-1})^4 \cdot (2^{e-1})^{-1} \\
&= (2) \cdot (2^{e-1})^3 \\
&= 2^{3e-2} = \begin{cases} 2 & \text{if } e = 1 \\ 16 & \text{if } e = 2 \\ 128 & \text{if } e = 3. \end{cases}
\end{aligned}$$

This can also be confirmed simply through explicit computation.

For odd ℓ, this is the same result as Theorem 3.15. In particular, note that the factors $a_r(\ell)$ match exactly with the factors of (3.4.7), such that

$$\prod_{\ell \nmid M_\Delta} \frac{\ell^2 \cdot a_r(\ell)}{(\ell-1) \cdot |\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} = C_1(E, r). \tag{3.5.3}$$

□

We now have $|\beta^+_{\ell,r}| + |\beta^-_{\ell,r}| = a_r(\ell)$ for a fixed trace r, so we want to find $|\beta^-_{\ell,r}|$ which will give the value of $|\beta^+_{\ell,r}| - |\beta^-_{\ell,r}|$. Obviously,

$$\begin{aligned}
|\beta^-_{\ell,r}| = \#\left\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \alpha^\ell_\Delta(\det(A)) = -1, \mathrm{tr}(A) \equiv r \pmod \ell\right\} \\
- \#\left\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \alpha^\ell_\Delta(\det(A)) = -1, \det(I-A) \equiv 0, \mathrm{tr}(A) \equiv r \pmod \ell\right\},
\end{aligned} \tag{3.5.4}$$

so we can compute the cardinality of these two sets separately in order to find $|\beta^-_{\ell,r}|$ for a fixed trace.

Lemma 3.20.

$$\begin{aligned}
&\#\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \alpha^\ell_\Delta(\det(A)) = -1, \mathrm{tr}(A) \equiv r \pmod \ell\} \\
&= \begin{cases} \frac{1}{2}\ell(\ell^2 - 2\ell + 1) & \text{if } r \equiv 0 \pmod \ell,\ \ell \equiv 1 \pmod 4 \\ \frac{1}{2}\ell(\ell^2 - 1) & \text{if } r \equiv 0 \pmod \ell,\ \ell \equiv 3 \pmod 4 \\ \frac{1}{2}\ell^2(\ell - 1) & \text{if } r \not\equiv 0 \pmod \ell,\ \ell \equiv 1 \pmod 4 \\ \frac{1}{2}\ell(\ell^2 - \ell - 2) & \text{if } r \not\equiv 0 \pmod \ell,\ \ell \equiv 3 \pmod 4 \end{cases}
\end{aligned}$$

Proof. Consider as usual a generic matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with trace $a + d \equiv r$ and determinant $ad - bc \not\equiv 0 \pmod{\ell}$.

If $bc \not\equiv 0 \pmod{\ell}$, then there are $(\ell - 1)$ ways to write the product bc (i.e., every nonzero choice of b has only one associated choice of c).

We want to count the choices of a, b, c, d under the conditions that $\det(A) = ad - bc \not\equiv 0 \pmod{\ell}$ and $ad - bc$ is a non-quadratic residue $\bmod\ \ell$. As the trace $a + d = r$ is fixed, the expression $ad - bc = a(r - a) - bc \pmod{\ell}$ may be used instead.

The first term $a(r - a)$ may be a quadratic residue, or a non-quadratic residue (at least one, but not both), and there are $\frac{\ell-1}{2}$ congruence classes of each category $\bmod\ \ell$. If we know the behaviour of $a(r - a)$, then we may use the following two facts:

1. There are $\frac{1}{2}(\ell^2 - 2\ell + 1)$ combinations of a, b, c, d if $a(r - a)$ is a quadratic residue $(\bmod\ \ell)$, or if $a(r - a) \equiv 0 \pmod{\ell}$.

2. There are $\frac{1}{2}(\ell^2 + 1)$ combinations of a, b, c, d if $a(r - a)$ is a non-quadratic residue $(\bmod\ \ell)$.

If $a(r - a)$ is a quadratic residue or $a(r - a) \equiv 0 \pmod{\ell}$, then bc may not be equivalent to 0 $(\bmod\ \ell)$, and there are $\frac{\ell-1}{2}$ possible non-zero values for $\det(A) \pmod{\ell}$. Each of these values fixes a non-zero value for bc which may then be written in $(\ell - 1)$ ways. Therefore, there are

$$\frac{1}{2}(\ell - 1)(\ell - 1) = \frac{1}{2}(\ell^2 - 2\ell + 1)$$

different ways to write $\det(A) = a(r - a) - bc$ if $a(r - a)$ is a quadratic residue, and the same number of ways if $a(r - a) \equiv 0 \pmod{\ell}$. This is the first fact.

If $a(r - a)$ is a non-quadratic residue, then bc may be either $\equiv 0 \pmod{\ell}$ or $\not\equiv 0 \pmod{\ell}$. If $bc \not\equiv 0 \pmod{\ell}$, there are $\frac{\ell-3}{2}$ possible non-zero values for $\det(A)$. Each of these fixes a non-zero value for bc, which may then be expressed in $(\ell - 1)$ ways, as before. If, on the other hand, $bc \equiv 0 \pmod{\ell}$, then obviously $\det(A) = a(r - a)$, and there are $(2\ell - 1)$ ways of writing $bc \equiv 0$. Taking the sum of both conditions $bc \equiv 0,\ bc \not\equiv 0 \pmod{\ell}$, we have

$$\frac{1}{2}(\ell - 3)(\ell - 1) + (2\ell - 1) = \frac{1}{2}(\ell^2 + 1)$$

ways to write $\det(A)$ if $a(r - a)$ is a non-quadratic residue. This is the second fact.

We now turn to determining when $a(r-a)$ is a quadratic residue (modℓ). Assume $r \not\equiv 0 \pmod{\ell}$, then we can factor

$$a(r-a) = -a^2 + ra \equiv -\left(a + \frac{\ell-1}{2}r\right)^2 + \frac{r^2}{4} \equiv -\left(a - 2^{-1}r\right)^2 + r^2 4^{-1} \pmod{\ell}.$$

Obviously, this only has the two roots $a = 0, r$. Denote by χ_ℓ the Legendre symbol modulo the prime ℓ, and let $x = (a - 2^{-1}r)$. Since x runs over all the values mod ℓ, the behaviour of $\chi_\ell(-a^2 + ra)$ is identical to the behaviour of

$$\chi_\ell(-x^2 + r^2 4^{-1}) = \chi_\ell(-1)\chi_\ell(x + 2^{-1}r)\chi_\ell(x - 2^{-1}r) = \chi_\ell(-1)\chi_\ell(y)\chi_\ell(y + r),$$

where $y = (x - 2^{-1}r)$ is simply a change of variable.

Construct an ℓ-tuple $(c_0, c_1, \ldots, c_{\ell-1})$, where each $c_i \in \mathbb{F}_2$ is 1 if $\chi_\ell(i) = 1$ and 0 otherwise. The set of tuples generated by successive right-shifts of the elements c_i is isomorphic to the set of tuples constructed by letting

$$c_i = \begin{cases} 1 & \text{if } \chi_\ell(i + r) = 1 \\ 0 & \text{otherwise} \end{cases}$$

for each value of $r \pmod{\ell}$. Thinking of these as belonging to a linear code of length ℓ, each element has a Hamming distance of $\frac{\ell+1}{2}$ between every other element.

We therefore have

$$\begin{aligned} &\#\left\{a \not\equiv 0 \pmod{\ell} : \chi_\ell(-a^2 + ra) = 1,\ r \in (\mathbb{Z}/\ell\mathbb{Z})^\times\right\} \\ &\qquad = \#\left\{y \pmod{\ell} : \chi_\ell(-1)\chi_\ell(y)\chi_\ell(y + r) = 1,\ r \in (\mathbb{Z}/\ell\mathbb{Z})^\times\right\} \\ &\qquad = \begin{cases} \left(\frac{\ell-3}{2}\right) & \text{if } \ell \equiv 1 \pmod 4 \\ \left(\frac{\ell-1}{2}\right) & \text{if } \ell \equiv 3 \pmod 4. \end{cases} \end{aligned}$$

The polynomial $a(r-a)$ is zero twice, and by the above is a quadratic residue for $\left(\frac{\ell-3}{2}\right)$ non-zero values of a if $\ell \equiv 1 \pmod 4$, or for $\left(\frac{\ell-1}{2}\right)$ non-zero values of a if $\ell \equiv 3 \pmod 4$. So knowing this behaviour of $\chi_\ell(a(r-a))$ and using the two facts from the beginning of the proof, the number of matrices with elements a, b, c, d is given by

$$\begin{cases} 2 \cdot \frac{1}{2}(\ell^2 - 2\ell + 1) + \left(\frac{\ell-3}{2}\right) \cdot \frac{1}{2}(\ell^2 - 2\ell + 1) + \left(\frac{\ell-1}{2}\right) \cdot \frac{1}{2}(\ell^2 + 1) & \text{if } \ell \equiv 1 \pmod 4 \\ 2 \cdot \frac{1}{2}(\ell^2 - 2\ell + 1) + \left(\frac{\ell-1}{2}\right) \cdot \frac{1}{2}(\ell^2 - 2\ell + 1) + \left(\frac{\ell-3}{2}\right) \cdot \frac{1}{2}(\ell^2 + 1) & \text{if } \ell \equiv 3 \pmod 4 \end{cases}$$

and simplifying these sums gives

$$\#\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \alpha_\Delta^\ell(\det(A)) = -1, \mathrm{tr}(A) \equiv r \pmod{\ell}\} = \begin{cases} \frac{1}{2}\ell^2(\ell-1) & \text{if } \ell \equiv 1 \pmod 4 \\ \frac{1}{2}\ell(\ell^2-\ell-2) & \text{if } \ell \equiv 3 \pmod 4 \end{cases}$$

whenever $r \not\equiv 0 \pmod{\ell}$.

The case of $r \equiv 0 \pmod{\ell}$ gives $a(r-a) = -a^2$, the non-zero values of which are always quadratic residues if $\ell \equiv 3 \pmod 4$, or never quadratic residues if $\ell \equiv 1 \pmod 4$. Therefore

$$\begin{aligned}\#\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \alpha_\Delta^\ell(\det(A)) = -1, \mathrm{tr}(A) \equiv 0 \pmod{\ell}\} &= \begin{cases} (\ell-1)\cdot\frac{1}{2}(\ell^2-2\ell+1) & \text{if } \ell \equiv 1 \pmod 4 \\ (\ell-1)\cdot\frac{1}{2}(\ell^2+1) & \text{if } \ell \equiv 3 \pmod 4. \end{cases} \\ &= \begin{cases} \frac{1}{2}\ell(\ell^2-2\ell+1) & \text{if } \ell \equiv 1 \pmod 4 \\ \frac{1}{2}\ell(\ell^2-1) & \text{if } \ell \equiv 3 \pmod 4. \end{cases}\end{aligned}$$

These combine to give the statement of the lemma. □

Theorem 3.21. *For ℓ is odd, let*

$$B_1 = \begin{cases} \frac{1}{2}\ell(\ell^2-2\ell+1) & \text{if } r \equiv 0 \pmod{\ell},\ \ell \equiv 1 \pmod 4 \\ \frac{1}{2}\ell(\ell^2-1) & \text{if } r \equiv 0 \pmod{\ell},\ \ell \equiv 3 \pmod 4 \\ \frac{1}{2}\ell^2(\ell-1) & \text{if } r \not\equiv 0 \pmod{\ell},\ \ell \equiv 1 \pmod 4 \\ \frac{1}{2}\ell(\ell^2-\ell-2) & \text{if } r \not\equiv 0 \pmod{\ell},\ \ell \equiv 3 \pmod 4 \end{cases}$$

$$B_2 = \begin{cases} 0 & \text{if } \alpha_\Delta^\ell(r-1) \neq -1 \\ \ell^2+\ell & \text{if } \alpha_\Delta^\ell(r-1) = -1. \end{cases}$$

Then

$$|\beta_{\ell,r}^-| = B_1 - B_2.$$

Proof. We work from the identity given in (3.5.4). The value of B_1 is given by Lemma 3.20, so we need only compute

$$B_2 = \#\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \alpha_\Delta^\ell = -1, \det(I-A) \equiv 0, \mathrm{tr}(A) \equiv r \pmod{\ell}\}$$

to find $|\beta_{\ell,r}^-|$. Recall that $r = \mathrm{tr}(A) \equiv q+1 \pmod{\ell}$ if A has both 1 and q as eigenvalues, so that fixing the trace when $\det(I-A) \equiv 0$ also fixes the second eigenvalue $q \not\equiv 1$. Using Lemma 3.10, it

is then an obvious result that

$$B_2 = \begin{cases} 0 & \text{if } \alpha_\Delta^\ell(r-1) \neq -1 \\ \ell^2 + \ell & \text{if } \alpha_\Delta^\ell(r-1) = -1 \end{cases}.$$

□

Remark 3.22. When considered across all possible values for $r \pmod{\ell}$, Theorem 3.21 is equivalent to the results obtained in [Zyw09]. There, the author computes the cardinality of

$$Y_\ell^- = \left\{ A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \left(\frac{\det(A)}{\ell}\right) = -1,\ \det(I-A) \not\equiv 0 \pmod{\ell} \right\}.$$

Clearly,

$$|Y_\ell^-| = \sum_{r=0}^{\ell-1} |\beta_{\ell,r}^-|$$

and we can use this relation to check that our computation matches.

If $\ell \equiv 1 \pmod 4$, this gives

$$\begin{aligned} |\beta_\ell^-| &= \frac{1}{2}\left(\ell(\ell^2 - 2\ell + 1) + \sum_{r=1}^{\ell-1} \ell^2(\ell-1)\right) - \sum_{\substack{r \pmod \ell \\ \alpha_\Delta^\ell(r-1)=-1}} (\ell^2+\ell) \\ &= \frac{1}{2}\left(\ell(\ell^2-2\ell+1) + (\ell-1)\ell^2(\ell-1)\right) - \left(\frac{\ell-1}{2}\right)(\ell^2+\ell) \\ &= \frac{1}{2}\left(\ell^4 - 2\ell^3 - \ell^2 + 2\ell\right) = \frac{1}{2}\left(|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})| - (\ell^3-\ell)\right) \end{aligned}$$

and if $\ell \equiv 3 \pmod 4$, then

$$\begin{aligned} |\beta_\ell^+| &= \frac{1}{2}\left(\ell(\ell^2 - 1) + \sum_{r=1}^{\ell-1} \ell^2(\ell-1)\right) - \sum_{\substack{r \pmod \ell \\ \alpha_\Delta^\ell(r-1)=-1}} (\ell^2+\ell) \\ &= \frac{1}{2}\left(\ell(\ell^2-1) + (\ell-1)\ell(\ell^2-\ell-2)\right) - \left(\frac{\ell-1}{2}\right)(\ell^2+\ell) \\ &= \frac{1}{2}\left(\ell^4 - 2\ell^3 - \ell^2 + 2\ell\right) = \frac{1}{2}\left(|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})| - (\ell^3-\ell)\right). \end{aligned}$$

In both cases, this confirms that our value is in accordance with that of Zywina.

We now have the pieces to calculate $b_r(\ell) = |\beta_{\ell,r}^+| - |\beta_{\ell,r}^-|$ for odd ℓ, which gives the following theorem.

Theorem 3.23. *If r is odd, then*

$$b_2(\ell) = |\beta_{2,r}^+| - |\beta_{2,r}^-| = \begin{cases} 2 & \text{if } v_2(M_\Delta) = 1 \\ 0 & \text{if } v_2(M_\Delta) = 2 \\ 0 & \text{if } v_2(M_\Delta) = 3 \end{cases}$$

and $|\beta_{2,r}^+| - |\beta_{2,r}^-| = 0$ if r is even.

For odd ℓ, if $\ell \equiv 1 \pmod 4$ then

$$b_r(\ell) = |\beta_{\ell,r}^+| - |\beta_{\ell,r}^-| = \begin{cases} -2\ell & \text{if } r \equiv 0 \pmod \ell \\ -\ell & \text{if } r \equiv 1 \pmod \ell \\ -\ell^2 - \ell & \text{if } r \equiv 2 \pmod \ell \\ \ell^2 - 2\ell & \text{if } \alpha_\Delta^\ell(r-1) \neq -1,\ r \not\equiv 0,1,2 \pmod \ell \\ \ell^2 & \text{if } \alpha_\Delta^\ell(r-1) = -1,\ r \not\equiv 0,1,2 \pmod \ell, \end{cases}$$

and otherwise if $\ell \equiv 3 \pmod 4$, then

$$b_r(\ell) = |\beta_{\ell,r}^+| - |\beta_{\ell,r}^-| = \begin{cases} 2\ell & \text{if } r \equiv 0 \pmod \ell \\ \ell & \text{if } r \equiv 1 \pmod \ell \\ -\ell^2 + \ell & \text{if } r \equiv 2 \pmod \ell \\ -\ell^2 & \text{if } \alpha_\Delta^\ell(r-1) \neq -1,\ r \not\equiv 0,1,2 \pmod \ell \\ \ell^2 + 2\ell & \text{if } \alpha_\Delta^\ell(r-1) = -1,\ r \not\equiv 0,1,2 \pmod \ell. \end{cases}$$

Proof. For $\ell = 2$, this is a restatement of Lemma 3.18.

For ℓ odd, since

$$|\beta_{\ell,r}^+| - |\beta_{\ell,r}^-| = (|\beta_{\ell,r}^+| + |\beta_{\ell,r}^-|) - 2|\beta_{\ell,r}^-|$$

we use the results of Theorems 3.19 and 3.21 to find

$$
\begin{aligned}
&|\beta^+_{\ell,r}| - |\beta^-_{\ell,r}| \\
&\quad = \begin{cases} \ell^3 - 2\ell^2 - \ell & \text{if } r \equiv 0 \pmod{\ell} \\ \ell^3 - \ell^2 - \ell & \text{if } r \equiv 1 \pmod{\ell} \\ \ell^3 - 2\ell^2 - \ell & \text{if } r \equiv 2 \pmod{\ell} \\ \ell^3 - 2\ell^2 - 2\ell & \text{o/wise} \end{cases} - 2 \cdot \begin{cases} \frac{1}{2}\ell(\ell^2 - 2\ell + 1) & \text{if } r \equiv 0 \pmod{\ell},\ \ell \equiv 1 \pmod 4 \\ \frac{1}{2}\ell(\ell^2 - 1) & \text{if } r \equiv 0 \pmod{\ell},\ \ell \equiv 3 \pmod 4 \\ \frac{1}{2}\ell^2(\ell - 1) & \text{if } r \not\equiv 0 \pmod{\ell},\ \ell \equiv 1 \pmod 4 \\ \frac{1}{2}\ell(\ell^2 - \ell - 2) & \text{if } r \not\equiv 0 \pmod{\ell},\ \ell \equiv 3 \pmod 4 \end{cases} \\
&\qquad + 2 \cdot \begin{cases} 0 & \text{if } \alpha^\ell_\Delta(r-1) \neq -1 \\ \ell^2 + \ell & \text{if } \alpha^\ell_\Delta(r-1) = -1. \end{cases}
\end{aligned}
$$

So if $\ell \equiv 1 \pmod 4$ this becomes

$$
= \begin{cases} (\ell^3 - 2\ell^2 - \ell) - (\ell^3 - 2\ell^2 + \ell) + (0) & \text{if } r \equiv 0 \pmod{\ell} \\ (\ell^3 - \ell^2 - \ell) - (\ell^3 - \ell^2) + (0) & \text{if } r \equiv 1 \pmod{\ell} \\ (\ell^3 - 2\ell^2 - \ell) - (\ell^3 - \ell^2) + (0) & \text{if } r \equiv 2 \pmod{\ell} \\ (\ell^3 - 2\ell^2 - 2\ell) - (\ell^3 - \ell^2) + (0) & \text{if } \alpha^\ell_\Delta(r-1) \neq -1,\ r \neq 0,1,2 \pmod{\ell} \\ (\ell^3 - 2\ell^2 - 2\ell) - (\ell^3 - \ell^2) + (2\ell^2 + 2\ell) & \text{if } \alpha^\ell_\Delta(r-1) = -1,\ r \neq 0,1,2 \pmod{\ell} \end{cases}
$$

and if $\ell \equiv 3 \pmod 4$ it becomes

$$
= \begin{cases} (\ell^3 - 2\ell^2 - \ell) - (\ell^3 - \ell) + (2\ell^2 + 2\ell) & \text{if } r \equiv 0 \pmod{\ell} \\ (\ell^3 - \ell^2 - \ell) - (\ell^3 - \ell^2 - 2\ell) + (0) & \text{if } r \equiv 1 \pmod{\ell} \\ (\ell^3 - 2\ell^2 - \ell) - (\ell^3 - \ell^2 - 2\ell) + (0) & \text{if } r \equiv 2 \pmod{\ell} \\ (\ell^3 - 2\ell^2 - 2\ell) - (\ell^3 - \ell^2 - 2\ell) + (0) & \text{if } \alpha^\ell_\Delta(r-1) \neq -1,\ r \neq 0,1,2 \pmod{\ell} \\ (\ell^3 - 2\ell^2 - 2\ell) - (\ell^3 - \ell^2 - 2\ell) + (2\ell^2 + 2\ell) & \text{if } \alpha^\ell_\Delta(r-1) = -1,\ r \neq 0,1,2 \pmod{\ell}, \end{cases}
$$

which sums to give our result. □

Combining these conditions to write the product $\prod_{\ell | M_\Delta}(|\beta^+_{\ell,r}| - |\beta^-_{\ell,r}|) = \prod_{\ell | M_\Delta} b_r(\ell)$ when $M_\Delta \equiv 2 \pmod 4$, we write

$$
\prod_{\ell | M_\Delta} b_r(\ell) = \begin{cases} 2\gamma_1\gamma_3 & \text{if } M_\Delta \equiv 2 \pmod 4 \\ 0 & \text{if } M_\Delta \equiv 0 \pmod 4 \end{cases} \tag{3.5.5}
$$

where

$$\gamma_1 = \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | r}} (-2\ell) \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | (r-1)}} (-\ell) \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | (r-2)}} (-\ell^2 - \ell) \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \alpha_\Delta^\ell(r-1) \neq -1 \\ \ell \nmid r(r-1)(r-2)}} (\ell^2 - 2\ell) \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \alpha_\Delta^\ell(r-1) = -1 \\ \ell \nmid r(r-1)(r-2)}} (\ell^2)$$

is taken as a product across only the primes $\ell \equiv 1 \pmod 4$, and

$$\gamma_3 = \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | r}} (2\ell) \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | (r-1)}} (\ell) \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | (r-2)}} (-\ell^2 + \ell) \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \alpha_\Delta^\ell(r-1) \neq -1 \\ \ell \nmid r(r-1)(r-2)}} (-\ell^2) \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \alpha_\Delta^\ell(r-1) = -1 \\ \ell \nmid r(r-1)(r-2)}} (\ell^2 + 2\ell)$$

is taken only across the primes $\ell \equiv 3 \pmod 4$.

Remark 3.24. When considered across all possible values for $r \pmod \ell$, Theorem 3.23 is equivalent to the results obtained in [Zyw09]. There, the author computes the cardinality of

$$Y_\ell^+ = \left\{ A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \left(\frac{\det(A)}{\ell}\right) = 1,\ \det(I - A) \not\equiv 0 \pmod \ell \right\}.$$

Clearly,

$$|Y_\ell^+| = \sum_{r=0}^{\ell-1} |\beta_{\ell,r}^+|$$

and we can use this relation to check that our computation matches.

Each of $r \equiv 0, 1, 2 \pmod \ell$ corresponds to $r - 1 \equiv -1, 0, 1$, so computing $\alpha_\Delta^\ell(r-1)$ can be done explicitly in these instances. For all other values, we must look at the prime modulus. If $\ell \equiv 1 \pmod 4$, then both 1 and -1 are quadratic residues, leaving $\left(\frac{\ell-5}{2}\right)$ other values of $r-1$ which are also quadratic residues, and $\left(\frac{\ell-1}{2}\right)$ which are not. If $\ell \equiv 3 \pmod 4$, then 1 is a quadratic residue but -1 is not, leaving $\left(\frac{\ell-3}{2}\right)$ other values which are quadratic residues, and $\left(\frac{\ell-3}{2}\right)$ which are non-quadratic residues.

This lets us use a sum over all fixed traces of the value which we computed above, to find

$$|Y_\ell^+| - |Y_\ell^-| = \sum_{r=0}^{\ell-1} |\beta_{\ell,r}^+| - |\beta_{\ell,r}^-|.$$

So if $\ell \equiv 1 \pmod 4$ this gives

$$\begin{aligned} |Y_\ell^+| - |Y_\ell^-| &= (-2\ell) + (-\ell) + (-\ell^2 - \ell) + \sum_{\substack{2 \leq r \leq (\ell-1) \\ \alpha_\Delta^\ell(r-1) \neq -1}} (\ell^2 - 2\ell) + \sum_{\substack{2 \leq r \leq (\ell-1) \\ \alpha_\Delta^\ell(r-1) = -1}} (\ell^2) \\ &= -\ell^2 - 4\ell + \left(\frac{\ell-5}{2}\right)(\ell^2 - 2\ell) + \left(\frac{\ell-1}{2}\right)(\ell^2) \\ &= -\ell^2 - 4\ell + \frac{1}{2}\left(2\ell^2 + 10\ell\right) = \ell \end{aligned}$$

and if $\ell \equiv 3 \pmod 4$ then

$$|Y_\ell^+| - |Y_\ell^-| = \sum_{r=0}^{\ell-1} |\beta_{\ell,r}^+| - |\beta_{\ell,r}^-| = (2\ell) + (\ell) + (-\ell^2+\ell) + \sum_{\substack{2\le r\le(\ell-1)\\ \alpha_\Delta^\ell(r-1)\neq -1}} (-\ell^2) + \sum_{\substack{2\le r\le(\ell-1)\\ \alpha_\Delta^\ell(r-1)= -1}} (\ell^2+2\ell)$$
$$= -\ell^2 + 4\ell + \left(\frac{\ell-3}{2}\right)(-\ell^2) + \left(\frac{\ell-3}{2}\right)(\ell^2+2\ell)$$
$$= -\ell^2 + 4\ell + \frac{1}{2}\left(2\ell^2 - 6\ell\right) = \ell,$$

and the result is the same as expected, since the value $|Y_\ell^+| - |Y_\ell^-|$ does not depend on the nature of the odd prime ℓ.

From (3.5.2), we can rewrite the identity for $C_2(E,r)$ as

$$\frac{|\Omega_r(M_\Delta)|}{|G(M_\Delta)|}\frac{M_\Delta^2}{\phi(M_\Delta)} = \begin{cases} \displaystyle\prod_{\ell\mid M_\Delta} \frac{\ell^2\cdot a_r(\ell)}{(\ell-1)\cdot|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\cdot\left(1+\prod_{\ell\mid M_\Delta}\frac{b_r(\ell)}{a_r(\ell)}\right) & \text{if } M_\Delta\equiv 2 \pmod 4 \\ \dfrac{M_\Delta^2\cdot\prod_{\ell\mid M_\Delta} a_r(\ell)}{\phi(M_\Delta)\cdot|\mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z})|} & \text{if } M_\Delta\equiv 0 \pmod 4 \end{cases}$$
$$= \begin{cases} \dfrac{4}{3}\displaystyle\prod_{\substack{\ell\mid M_\Delta\\ \ell\neq 2}} \frac{\ell^2\cdot a_r(\ell)}{(\ell-1)\cdot|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\cdot\left(1+\prod_{\ell\mid M_\Delta}\frac{b_r(\ell)}{a_r(\ell)}\right) & \text{if } M_\Delta\equiv 2 \pmod 4 \\ \dfrac{M_\Delta^2}{\phi(M_\Delta)\cdot|\mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z})|}\cdot a_r(2)\displaystyle\prod_{\substack{\ell\mid M_\Delta\\ \ell\neq 2}} a_r(\ell) & \text{if } M_\Delta\equiv 0 \pmod 4. \end{cases}$$

and we will now treat these cases separately.

3.5.1 Case 1: $M_\Delta \equiv 2 \pmod 4$

From (3.5.3) in the proof of Theorem 3.19, we have the equality

$$\prod_{\ell\mid M_\Delta}\frac{a(\ell)}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} = \frac{4}{3}\prod_{\ell\mid M_\Delta}\frac{1}{(\ell-1)^2(\ell+1)\ell}\prod_{\substack{\ell\mid M_\Delta\\ \ell\mid r(r-2)}}(\ell^3-2\ell^2-\ell)\prod_{\substack{\ell\mid M_\Delta\\ \ell\mid(r-1)}}(\ell^3-\ell^2-\ell)\prod_{\substack{\ell\mid M_\Delta\\ \ell\nmid r(r-1)(r-2)}}(\ell^3-2\ell^2-2\ell)$$

if $M_\Delta \equiv 2 \pmod 4$. We now need an expression for $\prod_{\ell\mid M_\Delta}\frac{b_r(\ell)}{a_r(\ell)}$ which requires (3.5.5) in order to write

$$\prod_{\ell\mid M_\Delta}\frac{b_r(\ell)}{a_r(\ell)} = 2\gamma_1\gamma_3\prod_{\ell\mid M_\Delta}\frac{1}{a_r(\ell)}$$
$$= \gamma_1\gamma_3\prod_{\substack{\ell\mid M_\Delta,\ \ell\neq 2\\ \ell\mid r(r-2)}}(\ell^3-2\ell^2-\ell)^{-1}\prod_{\substack{\ell\mid M_\Delta,\ \ell\neq 2\\ \ell\mid(r-1)}}(\ell^3-\ell^2-\ell)^{-1}\prod_{\substack{\ell\mid M_\Delta,\ \ell\neq 2\\ \ell\nmid r(r-1)(r-2)}}(\ell^3-2\ell^2-2\ell)^{-1}$$
$$= \gamma_1'\gamma_3'$$

where

$$\gamma_1' = \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | r}} \frac{-2\ell}{\ell^3 - 2\ell^2 - \ell} \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | (r-1)}} \frac{-\ell}{\ell^3 - \ell^2 - \ell} \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | (r-2)}} \frac{-\ell^2 - \ell}{\ell^3 - 2\ell^2 - \ell}$$
$$\cdot \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \alpha_\Delta^\ell(r-1) \neq -1 \\ \ell \nmid r(r-1)(r-2)}} \frac{\ell^2 - 2\ell}{\ell^3 - 2\ell^2 - 2\ell} \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \alpha_\Delta^\ell(r-1) = -1 \\ \ell \nmid r(r-1)(r-2)}} \frac{\ell^2}{\ell^3 - 2\ell^2 - 2\ell}$$

is a product taken across only the primes $\ell \equiv 1 \pmod 4$, and

$$\gamma_3' = \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | r}} \frac{2\ell}{\ell^3 - 2\ell^2 - \ell} \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | (r-1)}} \frac{\ell}{\ell^3 - \ell^2 - \ell} \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \ell | (r-2)}} \frac{-\ell^2 + \ell}{\ell^3 - 2\ell^2 - \ell}$$
$$\cdot \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \alpha_\Delta^\ell(r-1) \neq -1 \\ \ell \nmid r(r-1)(r-2)}} \frac{-\ell^2}{\ell^3 - 2\ell^2 - 2\ell} \prod_{\substack{\ell | M_\Delta,\ \ell \neq 2 \\ \alpha_\Delta^\ell(r-1) = -1 \\ \ell \nmid r(r-1)(r-2)}} \frac{\ell^2 + 2\ell}{\ell^3 - 2\ell^2 - 2\ell}$$

is taken across only the primes $\ell \equiv 3 \pmod 4$.

Combining these expressions with (3.4.7) and using (3.4.8), if $M_\Delta \equiv 2 \pmod 4$ then

$$\begin{aligned} C_{E,r} &= \frac{2}{\pi} C_1(E,r) C_2(E,r) \\ &= \frac{8}{3\pi} \prod_{\ell \neq 2} \frac{\ell^2(\ell^2 - 2\ell - 2)}{(\ell-1)^3(\ell+1)} \cdot \prod_{\substack{\ell | (r-1) \\ \ell \neq 2}} \frac{(\ell^2 - \ell - 1)}{(\ell^2 - 2\ell - 2)} \cdot \prod_{\substack{\ell | r(r-2) \\ \ell \neq 2}} \frac{(\ell^2 - 2\ell - 1)}{(\ell^2 - 2\ell - 2)} \cdot \left(1 + \prod_{\ell | M_\Delta} \frac{b_r(\ell)}{a_r(\ell)}\right) \\ &= \frac{2}{\pi} \cdot C_r \cdot \left(1 + \prod_{\ell | M_\Delta} \frac{b_r(\ell)}{a_r(\ell)}\right). \end{aligned}$$

3.5.2 Case 2: $M_\Delta \equiv 0 \pmod 4$

Recall from Theorem 3.19 the value e such that $2^e \mid\mid M_\Delta$. We will need the identity

$$|\mathrm{GL}_2(\mathbb{Z}/2^e\mathbb{Z})| = 3 \cdot 2^{4e-3}$$

which can be easily verified, and

$$a_r(2) = 2^{3e-2}$$

which is also stated in Theorem 3.19.

So then

$$\begin{aligned}\frac{M_\Delta^2}{\phi(M_\Delta)\cdot|\mathrm{GL}_2(\mathbb{Z}/M_\Delta\mathbb{Z})|}\cdot a_r(2)\prod_{\substack{\ell\mid M_\Delta\\ \ell\neq 2}} a_r(\ell) &= \frac{2^{2e}\cdot 2^{3e-2}}{\phi(2^e)\cdot 3\cdot 2^{4e-3}}\cdot\prod_{\substack{\ell\mid M_\Delta\\ \ell\neq 2}}\left(\frac{\ell^2}{(\ell-1)}\cdot\frac{1}{(\ell-1)^2(\ell+1)\ell}\cdot a_r(\ell)\right)\\ &= \frac{2^{5e-2}}{3\cdot 2^{5e-4}}\cdot\prod_{\substack{\ell\mid M_\Delta\\ \ell\neq 2}}\left(\frac{\ell}{(\ell-1)^3(\ell+1)}\cdot a_r(\ell)\right)\\ &= \frac{4}{3}\cdot\prod_{\substack{\ell\mid M_\Delta\\ \ell\neq 2}}\left(\frac{\ell\cdot a_r(\ell)}{(\ell-1)^3(\ell+1)}\right).\end{aligned}$$

Using (3.5.3), it is then an obvious conclusion that

$$\begin{aligned}C_{E,r} &= \frac{2}{\pi}C_1(E,r)C_2(E,r)\\ &= \frac{2}{\pi}\cdot\prod_{\substack{\ell\nmid M_\Delta\\ \ell\neq 2}}\left(\frac{\ell\cdot a_r(\ell)}{(\ell-1)^3(\ell+1)}\right)\cdot\frac{4}{3}\cdot\prod_{\substack{\ell\mid M_\Delta\\ \ell\neq 2}}\left(\frac{\ell\cdot a_r(\ell)}{(\ell-1)^3(\ell+1)}\right)\\ &= \frac{2}{\pi}\cdot C_r.\end{aligned}$$

Chapter 4

Data tables and specific examples

The primary motivation for this section is to present lists of actual values for the Mixed Conjecture value $\pi^{\mathrm{Mix}}(x)$ for various Serre curves, as found by computer calculation. These calculations were performed in large part on the Caedmon cluster at the Université de Montreal, running a program written in C and making extensive use of the PARI library for all number theoretic functions. This program iterated over the primes $p \leq 4 \times 10^{10}$ for each curve, counting the number of primes found for which $a_p(E) = r$ for every fixed value of r within the range given by Hasse's bound, and for which $p + 1 - a_p(E)$ was also prime. The data files generated by this program would be far too large to present in a non-digital format, so instead we will limit ourselves to viewing a small segment of the data generated around the median $r = 0$. Each table of data for the Mixed Conjecture is divided into five columns, one each for the value of r, the resulting count of $\pi_r^{\mathrm{LT}}(x)$, the count of $\pi^{\mathrm{Mix}}(x)$, the expected value of $\pi^{\mathrm{Mix}}(x)$, and finally the percentage error in the expected value from the actual count. The expected value for $\pi^{\mathrm{Mix}}(x)$ is computed separately for each r for each curve, as the product of $C_{E,r}$ and

$$\sum_{\substack{p \leq x \\ p \nmid \Delta}} \frac{1}{2\sqrt{p}\log(p+1)} \approx \int_2^x \frac{1}{2\sqrt{u}\log(u+1)} \frac{du}{\log(u)},$$

where $x = 4 \times 10^{10}$.

r	$\pi_r^{\mathrm{LT}}(x)$	$=\pi^{\mathrm{Mix}}(x)$	$\sim\pi^{\mathrm{Mix}}(x)$	$\%_{\mathrm{err}}$	r	$\pi_r^{\mathrm{LT}}(x)$	$=\pi^{\mathrm{Mix}}(x)$	$\sim\pi^{\mathrm{Mix}}(x)$	$\%_{\mathrm{err}}$
-99	2787	418	428.76	2.57	1	4247	4247	–	–
-95	4544	488	470.52	3.58	3	2846	326	290.34	10.94
-93	2721	358	321.13	10.3	7	4323	497	483.22	2.77
-89	4348	677	660.54	2.43	9	2804	290	299.14	3.15
-87	2788	321	326.72	1.78	13	4184	421	443.12	5.25
-83	4258	620	585.1	5.63	15	2949	419	391.23	6.63
-81	2933	316	298.02	5.69	19	4304	411	438.59	6.71
-77	4273	485	498.43	2.77	21	2952	473	438.56	7.28
-75	3015	350	345.75	1.21	25	4459	474	469.99	0.85
-71	4302	433	435.68	0.62	27	2841	320	343.72	7.41
-69	2789	527	528.42	0.27	31	4293	622	638.04	2.58
-65	4439	536	530.89	0.95	33	2835	315	293.66	6.77
-63	2934	342	324.43	5.14	37	4265	479	483.6	0.96
-59	4297	668	636.88	4.66	39	2829	299	310.86	3.97
-57	2801	268	302.52	12.88	43	4263	507	541.73	6.85
-53	4228	482	474.02	1.66	45	2962	371	351.55	5.24
-51	2849	332	320.55	3.45	49	4427	459	448.92	2.2
-47	4253	464	448.92	3.25	51	2832	437	438.93	0.44
-45	3001	302	328.43	8.75	55	4585	492	474.02	3.65
-41	4205	538	541.73	0.69	57	2804	378	393.7	4.15
-39	2845	410	427.62	4.3	61	4127	616	636.88	3.39
-35	4606	471	483.6	2.67	63	2830	309	309.9	0.29
-33	2923	349	348.63	0.11	67	4190	542	530.89	2.05
-29	4091	616	638.04	3.58	69	2771	300	311.71	3.9
-27	2862	349	361.19	3.49	73	4198	434	435.68	0.39
-23	4209	440	469.99	6.81	75	2966	315	321.93	2.2
-21	2835	355	336.84	5.11	79	4246	492	498.43	1.31
-17	4227	432	438.59	1.53	81	2779	434	424.41	2.21
-15	3013	289	313.91	8.62	85	4537	557	585.1	5.04
-11	4303	407	443.12	8.87	87	2788	293	322.16	9.95
-9	2883	445	428.72	3.66	91	4371	677	660.54	2.43
-5	4376	514	483.22	5.99	93	2854	339	316.64	6.59
-3	2879	328	312.67	4.67	97	4247	474	470.52	0.73

Table 4.1: Mixed Conjecture data for the curve $A : y^2 = x^3 + 6x - 2$ up to 4×10^{10}

r	$\pi_r^{\mathrm{LT}}(x)$	$=\pi^{\mathrm{Mix}}(x)$	$\sim\pi^{\mathrm{Mix}}(x)$	$\%_{\mathrm{err}}$	r	$\pi_r^{\mathrm{LT}}(x)$	$=\pi^{\mathrm{Mix}}(x)$	$\sim\pi^{\mathrm{Mix}}(x)$	$\%_{\mathrm{err}}$
-99	1763	280	288.08	2.88	1	2749	2749	–	–
-95	2870	328	316.14	3.62	3	1815	224	195.07	12.91
-93	1770	244	215.76	11.57	7	2824	340	324.67	4.51
-89	2784	461	443.8	3.73	9	1787	198	200.99	1.51
-87	1783	224	219.52	2	13	2719	305	297.72	2.39
-83	2753	442	393.12	11.06	15	1878	276	262.86	4.76
-81	1906	210	200.23	4.65	19	2779	269	294.68	9.55
-77	2757	323	334.88	3.68	21	1921	337	294.66	12.56
-75	1904	233	232.3	0.3	25	2834	326	315.77	3.14
-71	2734	302	292.73	3.07	27	1806	223	230.94	3.56
-69	1840	347	355.03	2.32	31	2786	430	428.69	0.31
-65	2816	372	356.7	4.11	33	1841	210	197.3	6.05
-63	1889	234	217.98	6.85	37	2736	328	324.92	0.94
-59	2781	456	427.91	6.16	39	1780	212	208.86	1.48
-57	1753	177	203.26	14.84	43	2726	338	363.98	7.69
-53	2742	342	318.49	6.88	45	1908	254	236.2	7.01
-51	1811	228	215.37	5.54	49	2815	328	301.62	8.04
-47	2687	302	301.62	0.13	51	1843	282	294.91	4.58
-45	1943	202	220.67	9.24	55	3007	338	318.49	5.77
-41	2644	357	363.98	1.96	57	1758	244	264.52	8.41
-39	1837	277	287.31	3.72	61	2701	423	427.91	1.16
-35	2963	325	324.92	0.02	63	1858	211	208.21	1.32
-33	1866	241	234.24	2.81	67	2645	354	356.7	0.76
-29	2607	401	428.69	6.9	69	1787	196	209.44	6.85
-27	1859	252	242.67	3.7	73	2695	297	292.73	1.44
-23	2626	287	315.77	10.03	75	1863	203	216.3	6.55
-21	1816	234	226.32	3.28	79	2651	337	334.88	0.63
-17	2735	295	294.68	0.11	81	1747	292	285.15	2.34
-15	1903	199	210.91	5.98	85	2873	356	393.12	10.43
-11	2787	260	297.72	14.51	87	1790	203	216.46	6.63
-9	1847	307	288.05	6.17	91	2786	477	443.8	6.96
-5	2838	360	324.67	9.81	93	1797	239	212.75	10.98
-3	1881	219	210.08	4.07	97	2748	324	316.14	2.43

Table 4.2: Mixed Conjecture data for the curve $A : y^2 = x^3 + 6x - 2$ up to 15×10^9

r	$= \pi_r^{\mathrm{LT}}(x)$	$\sim \pi_r^{\mathrm{LT}}(x)$	$\%_{\mathrm{err}}$	r	$= \pi_r^{\mathrm{LT}}(x)$	$\sim \pi_r^{\mathrm{LT}}(x)$	$\%_{\mathrm{err}}$
-99	2787	2851.14	2.3	1	4247	4237.84	0.22
-95	4544	4473.96	1.54	3	2846	2825.22	0.73
-93	2721	2828.27	3.94	7	4323	4341.2	0.42
-89	4348	4238.38	2.52	9	2804	2825.22	0.76
-87	2788	2828.71	1.46	13	4184	4265.18	1.94
-83	4258	4238.46	0.46	15	2949	2973.92	0.85
-81	2933	2825.22	3.67	19	4304	4250.26	1.25
-77	4273	4381.03	2.53	21	2952	2894.13	1.96
-75	3015	2973.92	1.36	25	4459	4460.88	0.04
-71	4302	4238.69	1.47	27	2841	2825.22	0.56
-69	2789	2830.82	1.5	31	4293	4242.4	1.18
-65	4439	4489.66	1.14	33	2835	2851.14	0.57
-63	2934	2894.13	1.36	37	4265	4241.02	0.56
-59	4297	4239.07	1.35	39	2829	2843.45	0.51
-57	2801	2833.51	1.16	43	4263	4240.18	0.54
-53	4228	4239.37	0.27	45	2962	2973.92	0.4
-51	2849	2835.65	0.47	49	4427	4341.2	1.94
-47	4253	4239.8	0.31	51	2832	2835.65	0.13
-45	3001	2973.92	0.9	55	4585	4501.81	1.81
-41	4205	4240.42	0.84	57	2804	2833.51	1.05
-39	2845	2843.45	0.05	61	4127	4238.99	2.71
-35	4606	4569.68	0.79	63	2830	2894.13	2.27
-33	2923	2851.14	2.46	67	4190	4238.79	1.16
-29	4091	4243.06	3.72	69	2771	2830.82	2.16
-27	2862	2825.22	1.28	73	4198	4238.64	0.97
-23	4209	4246.23	0.88	75	2966	2973.92	0.27
-21	2835	2894.13	2.09	79	4246	4238.52	0.18
-17	4227	4253.47	0.63	81	2779	2825.22	1.66
-15	3013	2973.92	1.3	85	4537	4477.34	1.31
-11	4303	4276.72	0.61	87	2788	2828.71	1.46
-9	2883	2825.22	2	91	4371	4369.21	0.04
-5	4376	4460.88	1.94	93	2854	2828.27	0.9
-3	2879	2825.22	1.87	97	4247	4238.29	0.21

Table 4.3: Lang-Trotter data for the curve $A : y^2 = x^3 + 6x - 2$ up to 4×10^{10}

4.1 $A : y^2 = x^3 + 6x - 2$

The elliptic curve given by $A : y^2 = x^3 + 6x - 2$ is a Serre curve (proven in [LT76], §I.7) with $\Delta_A = -15552 = -1 \cdot 2^6 \cdot 3^5$ and $\Delta_{\text{sf}} = -3 \equiv 1 \pmod 4$. The value of d_Δ is then $|\Delta_{\text{sf}}| = 3$, so $M_\Delta = 6$. With such a small value for M_Δ, we can list all of the possible cases for $r \pmod{M_\Delta}$. In fact, since the trace must be odd, there are only the three cases $r \equiv 1, 3, 5 \pmod 6$ to consider in order to find

$$|\Omega_r(6)| = \left|\left\{A \in \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) : \alpha_\Delta(3) = 1, \mathrm{tr}(A) \equiv r \pmod 6, \det(A) + 1 - \mathrm{tr}(A) \in (\mathbb{Z}/6\mathbb{Z})^\times\right\}\right|.$$

- If $r \equiv 5 \pmod 6$ then

  $$\det(A) + 1 - \mathrm{tr}(A) \equiv \det(A) + 2 \pmod 3,$$

  so $\det(A) \not\equiv 1 \pmod 3$. Thus $\alpha_\Delta(A) \neq 1$ so $|\Omega_r(6)| = 0$ when $r \equiv 5 \pmod 6$.

- If $r \equiv 3 \pmod 6$ then

  $$\det(A) + 1 - \mathrm{tr}(A) \equiv \det(A) + 1 \pmod 3,$$

  so $\det(A) \not\equiv 2 \pmod 3$ which is a redundant condition. Counting we find 6 matrices with both determinant $\equiv 1 \pmod 3$ and trace $\equiv 0 \pmod 3$, and thus $|\Omega_r(6)| = 12$ when $r \equiv 3 \pmod 6$.

- If $r \equiv 1 \pmod 6$ then

  $$\det(A) + 1 - \mathrm{tr}(A) \equiv \det(A) \pmod 3,$$

  so $\det(A) \not\equiv 0 \pmod 3$ which is a redundant condition of $A \in \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$. Counting we find 9 matrices having both determinant $\equiv 1 \pmod 3$ and trace $\equiv 1 \pmod 3$, so $|\Omega_r(6)| = 18$ when $r \equiv 1 \pmod 6$.

We will show the computation of each part of the constant $C = C_1(A, r)C_2(A, r)$ separately for a fixed trace r up to an upper limit of $x \leq 4 \times 10^{10}$.

Let $r = 13 \equiv 1 \pmod 6$. From computer calculation, the infinite part of the product converges relatively rapidly to

$$\begin{aligned} C_r = C_{13} &= \frac{4}{3} \prod_\ell \frac{\ell^2(\ell^2 - 2\ell - 2)}{(\ell - 1)^3(\ell + 1)} \cdot \prod_{\ell | (r-1)} \frac{(\ell^2 - \ell - 1)}{(\ell^2 - 2\ell - 2)} \cdot \prod_{\ell | r(r-2)} \frac{(\ell^2 - 2\ell - 1)}{(\ell^2 - 2\ell - 2)} \\ &\approx 0.892917729503\ldots \end{aligned}$$

The finite part, while complicated to express over every possible r, is simpler for a single value.

$$1+\prod_{\ell|6}\frac{b_r(\ell)}{a_r(\ell)} = 1+\prod_{\ell|6}\frac{b_{(13)}(\ell)}{a_{(13)}(\ell)} = 1+\gamma_1'\gamma_3'$$
$$= \frac{6}{5}.$$

Computer calculation also yields

$$\int_2^{4\times 10^{10}} \frac{1}{2\sqrt{u}\log(u+1)}\frac{du}{\log(u)} \approx 413.550661685\ldots$$

and the product of these three values gives

$$C_{13}\cdot\left(1+\prod_{\ell|6}\frac{b_{(13)}(\ell)}{a_{(13)}(\ell)}\right)\cdot\int_2^{4\times 10^{10}} \frac{1}{2\sqrt{u}\log(u+1)}\frac{du}{\log(u)} \approx 443.12\ldots,$$

while the computer generated count over the same range $x \le 4\times 10^{10}$ shows 421 as the actual value.

As another example, let $r = -75 \equiv 3 \pmod 6$. Then

$$C_r = C_{-75} = \frac{4}{3}\prod_{\ell}\frac{\ell^2(\ell^2-2\ell-2)}{(\ell-1)^3(\ell+1)}\cdot\prod_{\ell|(r-1)}\frac{(\ell^2-\ell-1)}{(\ell^2-2\ell-2)}\cdot\prod_{\ell|r(r-2)}\frac{(\ell^2-2\ell-1)}{(\ell^2-2\ell-2)}$$
$$\approx 0.418023996502\ldots$$

and the finite part is

$$1+\prod_{\ell|6}\frac{b_r(\ell)}{a_r(\ell)} = 1+\prod_{\ell|6}\frac{b_{(-75)}(\ell)}{a_{(-75)}(\ell)} = 1+\gamma_1'\gamma_3'$$
$$= 2.$$

This gives the final product of

$$C_{-75}\cdot\left(1+\prod_{\ell|6}\frac{b_r(\ell)}{a_r(\ell)}\right)\cdot\int_2^{4\times 10^{10}} \frac{1}{2\sqrt{u}\log(u+1)}\frac{du}{\log(u)} \approx 345.75\ldots$$

which is quite close to the actual count of 350.

Remark 4.1. As a check that this data is reliable, we will also compute expected value associated to the Koblitz conjecture.

The Koblitz constant C_E is already computed for this curve in [Zyw09] as

$$C_E = \prod_{\ell}\left(1-\frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right)\cdot\left(1+\prod_{\ell|\Delta_{\mathrm{sf}}}\frac{1}{\ell^3-2\ell^2-\ell+3}\right)$$
$$\approx 0.561295742488...$$

so rounded to the nearest integer, we can compute the expected value

$$C_E \cdot \int_2^{4\times 10^{10}} \frac{1}{\log(u+1)} \frac{du}{\log(u)} \approx 41219014.$$

Although impossible to fully display in the format of Table 4.1, the actual count (taken as a sum across all values of r) was 41219800.

As a point of comparison, Table 4.2 contains data for the same curve, however only for primes up to 15×10^9. Since the number of primes for any given r is so small relative to either of the Koblitz or Lang-Trotter counts, it may not be apparent whether the estimates are improving with more data. However the average percentage error was 5.40% for the data presented in Table 4.2, while the average percentage error for Table 4.1 was only 4.07%. This suggests that an improvement does take place.

4.2 $B : y^2 = x^3 + x^2 - y$

The elliptic curve given by $B : y^2 = x^3 + x^2 - y$ is a Serre curve (given in [Kob88]) with $\Delta_B = -43 = \Delta_{\text{sf}} \equiv 1 \pmod 4$. The value of d_Δ is then $|\Delta_{\text{sf}}| = 43$, so $M_\Delta = 86$.

Let $r = 45$, then

$$\begin{aligned} C_r = C_{45} &= \frac{4}{3} \prod_{\ell} \frac{\ell^2(\ell^2 - 2\ell - 2)}{(\ell-1)^3(\ell+1)} \cdot \prod_{\ell \mid (r-1)} \frac{(\ell^2 - \ell - 1)}{(\ell^2 - 2\ell - 2)} \cdot \prod_{\ell \mid r(r-2)} \frac{(\ell^2 - 2\ell - 1)}{(\ell^2 - 2\ell - 2)} \\ &= 0.425044005447\ldots \end{aligned}$$

and the finite part is

$$\begin{aligned} 1 + \prod_{\ell \mid 86} \frac{b_r(\ell)}{a_r(\ell)} = 1 + \prod_{\ell \mid 86} \frac{b_{(43)}(\ell)}{a_{(43)}(\ell)} &= 1 + \gamma_1' \gamma_3' \\ &= 1 + \frac{-1892}{75766} \\ &= \frac{860}{881}. \end{aligned}$$

This gives the final product of

$$C_{45} \cdot \left(1 + \prod_{\ell \mid 86} \frac{b_r(\ell)}{a_r(\ell)} \right) \cdot \int_2^{4\times 10^{10}} \frac{1}{2\sqrt{u}\log(u+1)} \frac{du}{\log(u)} \approx 171.59\ldots$$

while the actual count over $x \leq 4 \times 10^{10}$ is 169.

r	$\pi_r^{\mathrm{LT}}(x)$	$=\pi^{\mathrm{Mix}}(x)$	$\sim\pi^{\mathrm{Mix}}(x)$	$\%_{\mathrm{err}}$	r	$\pi_r^{\mathrm{LT}}(x)$	$=\pi^{\mathrm{Mix}}(x)$	$\sim\pi^{\mathrm{Mix}}(x)$	$\%_{\mathrm{err}}$
-67	3642	156	159.84	2.46	1	3576	3576	–	–
-65	3682	414	453.72	9.59	3	4282	170	148.88	12.42
-63	4247	168	166.36	0.98	5	3756	159	152.52	4.08
-61	3603	172	151.16	12.11	7	3591	427	392.85	8
-59	3529	555	544.3	1.93	9	4249	155	153.39	1.04
-57	4208	140	155.13	10.8	11	3559	195	209.12	7.24
-55	3896	208	201.88	2.94	13	3575	364	378.7	4.04
-53	3546	413	405.11	1.91	15	4475	207	190.84	7.81
-51	4256	135	164.37	21.76	17	3489	156	153.12	1.84
-49	3672	217	214.11	1.33	19	3501	335	374.83	11.89
-47	3569	369	364.96	1.09	21	4313	200	224.89	12.44
-45	4464	155	160.21	3.36	23	3487	183	172.73	5.61
-43	3480	201	175.98	12.45	25	3717	404	382.09	5.42
-41	3549	418	440.68	5.43	27	4244	198	176.25	10.98
-39	4256	210	219.27	4.42	29	3503	189	185.21	2.01
-37	3370	151	159.4	5.56	31	3420	499	545.29	9.28
-35	3841	392	413.3	5.43	33	4265	161	150.58	6.47
-33	4298	177	170.06	3.92	35	3881	200	178.77	10.62
-31	3529	158	143.24	9.34	37	3551	363	393.16	8.31
-29	3640	510	518.72	1.71	39	4182	156	151.63	2.8
-27	4135	154	176.18	14.41	41	3534	201	208.59	3.78
-25	3748	180	167.66	6.85	43	3415	428	451.96	5.6
-23	3529	403	401.66	0.33	45	4411	169	171.59	1.53
-21	4239	159	164.31	3.34	47	3503	151	168.41	11.53
-19	3453	217	213.93	1.42	49	3541	371	383.66	3.41
-17	3456	348	356.57	2.46	51	4221	227	225.07	0.85
-15	4505	169	160.97	4.75	53	3511	149	156.36	4.94
-13	3599	205	200.61	2.14	55	3687	380	385.37	1.41
-11	3575	344	360.25	4.72	57	4351	199	192.04	3.5
-9	4276	236	219.84	6.85	59	3496	159	147.57	7.19
-7	3672	146	145.92	0.06	61	3643	493	517.77	5.03
-5	3708	377	412.98	9.54	63	4313	161	158.91	1.3
-3	4247	164	160.33	2.24	65	3755	134	158.26	18.1
-1	3615	174	141.63	18.61	67	3568	462	431.61	6.58

Table 4.4: Mixed Conjecture data for the curve $B : y^2 = x^3 + x^2 - y$ up to 4×10^{10}

Remark 4.2. The Koblitz constant C_E is found using computer calculation to be

$$C_E = \prod_{\ell} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)}\right) \cdot \left(1 + \prod_{\ell | \Delta_{\text{sf}}} \frac{1}{\ell^3 - 2\ell^2 - \ell + 3}\right)$$
$$\approx 0.505172861299\ldots$$

so rounded to the nearest integer, we can compute the expected value

$$C_E \cdot \int_2^{4\times 10^{10}} \frac{1}{\log(u+1)} \frac{du}{\log(u)} \approx 37097602.$$

The actual count from the full data set for this curve over $x \leq 4 \times 10^{10}$ is 37093490.

4.3 $C : y^2 = x^3 - x^2 - xy - y$

The elliptic curve given by $C : y^2 = x^3 - x^2 - xy - y$ is a Serre curve (given in [Kob88]) with $\Delta_C = -53 = \Delta_{\text{sf}} \equiv 3 \pmod 4$. The value of d_Δ is then $4|\Delta_{\text{sf}}| = 212$, so $M_\Delta = 212$.

Let $r = -47$, then

$$C_r = C_{-47} = \frac{4}{3} \prod_{\ell} \frac{\ell^2(\ell^2 - 2\ell - 2)}{(\ell-1)^3(\ell+1)} \cdot \prod_{\ell | (r-1)} \frac{(\ell^2 - \ell - 1)}{(\ell^2 - 2\ell - 2)} \cdot \prod_{\ell | r(r-2)} \frac{(\ell^2 - 2\ell - 1)}{(\ell^2 - 2\ell - 2)}$$
$$= 0.904603725791\ldots$$

and since $M_\Delta \equiv 0 \pmod 4$, this is in fact the whole of $C_{E,r}$. This gives the final product of

$$C_{-47} \cdot \int_2^{4\times 10^{10}} \frac{1}{2\sqrt{u}\log(u+1)} \frac{du}{\log(u)} \approx 374.10\ldots$$

while the actual count over $x \leq 4 \times 10^{10}$ is 391.

Remark 4.3. The Koblitz constant C_E is found using computer calculation to be

$$C_E = \prod_{\ell} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)}\right) \cdot \left(1 + \prod_{\ell | \Delta_{\text{sf}}} \frac{1}{\ell^3 - 2\ell^2 - \ell + 3}\right)$$
$$\approx 0.505166194110\ldots$$

so rounded to the nearest integer, we can compute the expected value

$$C_E \cdot \int_2^{4\times 10^{10}} \frac{1}{\log(u+1)} \frac{du}{\log(u)} \approx 37097112.$$

The actual count for the full data set for this curve over $x \leq 4 \times 10^{10}$ is 37112431.

r	$\pi_r^{\mathrm{LT}}(x)$	$=\pi^{\mathrm{Mix}}(x)$	$\sim\pi^{\mathrm{Mix}}(x)$	$\%_{\mathrm{err}}$	r	$\pi_r^{\mathrm{LT}}(x)$	$=\pi^{\mathrm{Mix}}(x)$	$\sim\pi^{\mathrm{Mix}}(x)$	$\%_{\mathrm{err}}$
-67	3473	138	155.86	12.94	1	3528	3528	–	–
-65	3610	410	442.41	7.9	3	4326	142	145.17	2.23
-63	4364	153	162.22	6.02	5	3727	147	156.34	6.35
-61	3521	172	154.95	9.91	7	3559	394	402.69	2.2
-59	3527	517	530.73	2.66	9	4209	154	149.57	2.88
-57	4239	148	151.26	2.2	11	3482	216	214.36	0.76
-55	3788	198	196.85	0.58	13	3618	350	369.27	5.5
-53	3505	373	395.02	5.9	15	4519	210	195.61	6.85
-51	4262	152	160.27	5.44	17	3602	155	156.95	1.26
-49	3520	198	219.46	10.84	19	3605	367	365.49	0.41
-47	3562	391	374.1	4.32	21	4325	224	219.28	2.11
-45	4404	177	164.22	7.22	23	3549	167	168.42	0.85
-43	3468	193	175.78	8.92	25	3683	392	391.65	0.09
-41	3371	424	451.45	6.47	27	4155	145	171.86	18.52
-39	4227	219	213.81	2.37	29	3498	175	180.59	3.2
-37	3465	169	155.43	8.03	31	3612	553	531.7	3.85
-35	3900	412	403	2.19	33	4354	165	146.83	11.01
-33	4195	185	174.31	5.78	35	3847	170	174.31	2.54
-31	3481	140	146.83	4.88	37	3513	400	403	0.75
-29	3621	534	531.7	0.43	39	4209	136	155.43	14.29
-27	4263	193	180.59	6.43	41	3387	213	213.81	0.38
-25	3670	163	171.86	5.44	43	3478	433	451.45	4.26
-23	3506	355	391.65	10.33	45	4538	189	175.78	7
-21	4395	174	168.42	3.21	47	3504	155	164.22	5.95
-19	3536	232	219.28	5.48	49	3646	373	374.1	0.29
-17	3575	364	365.49	0.41	51	4195	240	219.46	8.56
-15	4549	150	156.95	4.64	53	3662	157	160.27	2.09
-13	3600	204	195.61	4.11	55	3741	412	395.02	4.12
-11	3440	364	369.27	1.45	57	4187	206	196.85	4.44
-9	4280	208	214.36	3.06	59	3533	146	151.26	3.6
-7	3732	161	149.57	7.1	61	3458	528	530.73	0.52
-5	3695	400	402.69	0.67	63	4306	159	154.95	2.55
-3	4254	144	156.34	8.57	65	3718	169	162.22	4.01
-1	3524	141	145.17	2.96	67	3540	457	442.41	3.19

Table 4.5: Mixed Conjecture data for the curve $C : y^2 = x^3 - x^2 - xy - y$ up to 4×10^{10}

Bibliography

[Bai06] S. Baier. The Lang-Trotter conjecture on average. *Arxiv preprint math.NT/0609095*, 2006.

[BCD07] A. Balog, A. Cojocaru, and C. David. Average twin prime conjecture for elliptic curves. *Arxiv preprint arXiv:0709.1461*, 2007.

[BJ09] S. Baier and N. Jones. A refined version of the Lang-Trotter Conjecture. *International Mathematics Research Notices*, 2009(3):433, 2009.

[DP99] C. David and F. Pappalardi. Average Frobenius distributions of elliptic curves. *International Mathematics Research Notices*, 1999(4):165, 1999.

[DS05] F. Diamond and J.M. Shurman. *A first course in modular forms*. Springer Verlag, 2005.

[Eng99] A. Enge. *Elliptic curves and their applications to cryptography: an introduction*. Springer, 1999.

[HL23] G.H. Hardy and J.E. Littlewood. Some problems of Partitio Numerorum; III: On the expression of a number as a sum of primes. *Acta Mathematica*, 44(1):1–70, 1923.

[Jon] N. Jones. Averages of elliptic curve constants. *Mathematische Annalen*, pages 1–26.

[Jon06] N. Jones. Almost all elliptic curves are Serre curves. *Arxiv preprint math.NT/0611096*, 2006.

[Kat80] N.M. Katz. Galois properties of torsion points on abelian varieties. *Inventiones Mathematicae*, 62(3):481–502, 1980.

[Kob88] N. Koblitz. Primality of the number of points on an elliptic curve over a finite field. *Pacific J. Math*, 131(1):157–165, 1988.

[Len] H.W. Lenstra. The Chebotarev Density Theorem. *URL: http://math.berkeley.edu/jvoight/notes/oberwolfach/Lenstra-Chebotarev.pdf*.

[LT76] S. Lang and H. Trotter. *Frobenius Distributions in GL2-extensions*. Springer, 1976.

[Mar77] D.A. Marcus. *Number fields*. Springer, 1977.

[Ser68] J.P. Serre. Abelian l-adic representations and elliptic curves. 1968.

[Ser71] J.P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae*, 15(4):259–331, 1971.

[Sil86] J.H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, 1986.

[ST92] J.H. Silverman and J.T. Tate. *Rational points on elliptic curves*. Springer, 1992.

[Tay08] R. Taylor. Automorphy for some l-adic lifts of automorphic mod l Galois representations. II. *Publications Mathématiques de L'IHÉS*, 108(1):183–239, 2008.

[Was03] L.C. Washington. *Elliptic curves*. Chapman & Hall/CRC, 2003.

[Zyw09] D. Zywina. A refinement of Koblitz's conjecture. *preprint*, 2009.