Elliptic Curves over Finite Fields and their ℓ-Torsion Galois Representations

by

Michael Baker

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2015

© Michael Baker 2015

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Let q and ℓ be distinct primes. Given an elliptic curve E over $\mathbf{F}_q$, we study the behaviour of the 2-dimensional Galois representation of $\mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q) \cong \widehat{\mathbf{Z}}$ on its ℓ-torsion subgroup $E[\ell]$. This leads us to the problem of counting elliptic curves with prescribed ℓ-torsion Galois representations, which we answer for small primes ℓ by counting rational points on suitable modular curves. The resulting exact formulas yield expressions for certain sums of Hurwitz class numbers.

Acknowledgements

I would like to sincerely thank my supervisor Dr. David McKinnon for the opportunity to work with him. David is a person who always goes out of his way to help others. I benefited greatly from his knowledge and guidance, and being in his company was always enjoyable.

Next, I would like to thank my thesis readers Dr. Wentang Kuo and Dr. Cameron Stewart. Their constructive feedback was very useful in the preparation of this thesis.

I am also very indebted to my good friends Hanci Chi, Erik Crevier, Chenfei Du, Jimmy He, Jason Lin, Kevin Matthews, Ritvik Ramkumar, Samin Riasat, Steven Scott, Mackie Tucciarone, Adam Venis, George Wen, Philip Xiao, Harmony Zhan, and Jimmy Zhu, for all the invaluable discussions they shared with me, mathematical or otherwise. Their impact on my growth as a person cannot be overstated.

Finally, although they have no idea what I do, I thank my parents and family for their endless support. Without their love, I would not be where I am today.

Table of Contents

Chapter 1

Introduction

The problem of counting rational points on algebraic varieties has a long and intriguing history. Perhaps the first nontrivial example is the investigation of the behaviours of the traces of Frobenius $a_q \in \mathbf{Z}$ of the $\mathbf{F}_q$-reductions of an elliptic curve E over $\mathbf{Q}$. These should be thought of as "error terms" to a point-counting problem; they appear as Fourier coefficients of cusp forms. As another example, the values $\tau(n)$ of the Ramanujan tau function, which famously appear as the Fourier coefficients of the modular discriminant Δ, give the error involved in trying to count the number of ways a given integer can be represented as a sum of four squares; see Mazur [23]. Hence the conjecture that $\tau(n) \neq 0$ for all n amounts to saying that our approximation is never exact.

The residues $a_q \bmod m$ of the traces of Frobenius have also been studied; see [5]. In this thesis, we consider an elliptic curve E over the finite field $\mathbf{F}_q$ (for q a prime) and study the Galois representation

$$\rho_\ell = \rho_\ell(E) : \mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q) \to \mathrm{GL}(2,\ell) := \mathrm{GL}_2(\mathbf{F}_\ell)$$

attached to the group of ℓ-torsion points of E. This representation encodes the algebraic complexity of the coordinates of the ℓ-torsion points of E, i.e. the manner in which these points are distributed among the various field extensions of $\mathbf{F}_q$. Since we are only concerned with representations up to equivalence, we view ρ_ℓ as a conjugacy class in $\mathrm{GL}(2,\ell)$.

Often, the representation ρ_ℓ is completely determined by the residues of q and a_q modulo ℓ. The existence of scalar (central) conjugacy classes in $\mathrm{GL}(2,\ell)$, however, causes this to fail in general. In this sense, ρ_ℓ is a slightly finer invariant of E than is the residue of a_q modulo ℓ. We are therefore lead to consider the problem of counting the number of curves with prescribed ρ_ℓ.

In Section 2, we collect some standard facts about elliptic curves over finite fields, providing references to the literature for their proofs.

In Section 3, we completely handle the case when $\ell = 2$.

In Section 4, we discuss modular curves and their interpretation as moduli spaces, recording information on their genera and number of cusps.

In Section 5, we apply the Hasse-Weil bound to derive explicit formulas for the number of curves with any prescribed ρ_ℓ when $\ell = 3$. We then move on to the cases $\ell = 5$ and $\ell = 7$, obtaining similar formulas for certain choices of ρ_ℓ. Our method does not likely extend to larger primes ℓ, as it relies on the existence of relevant modular curves with genus zero. As a byproduct, we deduce identities involving certain sums of Hurwitz class numbers, as in the paper [2]; the reader is strongly advised to compare the results and methods contained therein to those that follow.

In Section 6, we conclude the thesis by stating some conjectures.

Chapter 2

Background on elliptic curves

In this section we review standard material on elliptic curves. No attempt is made at generality; we immediately restrict our attention to finite fields. Our primary reference for this section is Silverman [33, Chap. V]. For further reading, one can consult the excellent texts by Husemöller [15], Knapp [18], Koblitz [17], and McKean-Moll [24].

2.1 Basic notions

We loosely follow the treatment in Menezes [25]. Let q be a prime number, and denote by $\mathbf{F}_q$ and $\overline{\mathbf{F}_q}$ the finite field of order q and its algebraic closure, respectively. Recall that an *elliptic curve* E over $\mathbf{F}_q$ is the set of all solutions $(X : Y : Z)$ in the projective plane $\mathbf{P}^2(\overline{\mathbf{F}_q})$ of a smooth *Weierstrass equation*, which in general takes the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

for $a_1, a_2, a_3, a_4, a_6 \in \mathbf{F}_q$. The point $O = (0:1:0)$ is called the *point at infinity*; it behaves as the identity element for the group law on E. Define the quantities

$$\begin{aligned} d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1 a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \\ c_4 &= d_2^2 - 24 d_4 \\ \Delta &= -d_2^2 d_8 - 8 d_4^3 - 27 d_6^2 + 9 d_2 d_4 d_6 \\ j(E) &= c_4^3 / \Delta. \end{aligned}$$

We call Δ the *discriminant* of the Weierstrass equation. The Weierstrass equation is smooth if and only if $\Delta \neq 0$, in which case the quantity $j(E)$ is referred to as the *j-invariant* of E. Its role in classifying elliptic curves will be discussed shortly. Under the heading of "monstrous moonshine", the j-invariant has also recently been connected to a diverse host of objects, including the representation theory of sporadic groups, vertex operator algebras, and conformal field theory; see Gannon [12].

For convenience, we typically dehomogenize, that is, we take $x = X/Z$ and $y = Y/Z$ and work instead with the affine equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

When $q \neq 2, 3$, by means of a change of variables, the curve E can be brought into *short Weierstrass form*,

$$y^2 = x^3 + ax + b.$$

In this case we have the simpler formulas $\Delta = -16(4a^3 + 27b^2)$ and $j(E) = -1728(4a)^3/\Delta$.

For the definition of the trace of Frobenius, see [33, Remark V.2.6].

2.2 Torsion points

Let $E[m] = E[m](\overline{\mathbf{F}_q})$ denote the set of $P \in E(\overline{\mathbf{F}_q})$ with $m \cdot P = O$; we refer to $E[m]$ as the *m-torsion subgroup* of E. The smallest integer $d > 0$ such that $E[m](\mathbf{F}_{q^d}) = E[m]$ shall be called the *m-torsion depth* of E. See [33, Cor. III.6.4] for the following result:

Proposition 1. *Let E be an elliptic curve and let $m \in \mathbf{Z}$ with $m \neq 0$.*

(a) If $q \nmid m$, then $E[m] \cong (\mathbf{Z}/m\mathbf{Z})^2$.

(b) If $q \mid m$, one of the following holds:

(i) $E[q^e] = \{O\}$ for $e = 1, 2, 3, \ldots$

(ii) $E[q^e] = \mathbf{Z}/q^e\mathbf{Z}$ for $e = 1, 2, 3, \ldots$

Now fix a prime $\ell \neq q$. The absolute Galois group $\mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$, being topologically generated by the Frobenius automorphism $x \mapsto x^q$, is isomorphic to the profinite completion of the integers $\widehat{\mathbf{Z}}$. It acts on the homogeneous coordinates of points in the projective plane $\mathbf{P}^2(\overline{\mathbf{F}_q})$, and this action preserves $E[\ell]$. We therefore obtain a representation[1]

$$\rho_\ell = \rho_\ell(E) : \mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q) \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}(2, \ell)$$

which we will identify with the conjugacy class of $\mathrm{GL}(2, \ell)$ determined by the image of the Frobenius under ρ_ℓ. Thus by abuse of language, we will for example refer to the multiplicative order of ρ_ℓ. For a full description of the conjugacy class structure of $\mathrm{GL}(2, \ell)$, see Lang [20, XVIII.12].

Let d and t be elements of $\mathbf{F}_\ell$ with $d \neq 0$. The number of conjugacy classes having trace t and determinant d is 2 or 1 according as d is, or is not, a quadratic residue modulo ℓ. Thus there are precisely $\ell^2 - 1$ conjugacy classes in total. Furthermore, it can be shown [33] that ρ_ℓ has trace a_q and determinant q. As a consequence, ρ_ℓ is determined completely by q and a_q modulo ℓ whenever the pair (q, a_q) is not of the form $(q, \pm 2\sqrt{q})$.

Definition 2. Let q be a prime. A conjugacy class C of $\mathrm{GL}(2, \ell)$ shall be called *admissible for q* if matrices in C have determinant q mod ℓ, and have trace t mod ℓ for some t in the Hasse interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$.

Proposition 3. *Suppose the conjugacy class C of $\mathrm{GL}(2, \ell)$ is admissible for q, and q is a quadratic nonresidue modulo ℓ. Then there exists an elliptic curve E over $\mathbf{F}_q$ with $\rho_\ell(E) = C$.*

The proof is immediate from the following result, which we quote from Waterhouse [36]. Here $(\frac{a}{b})$ denotes the Jacobi symbol while $H(N)$ denotes the Hurwitz class number; see §2.5 below.

[1] Note that all homomorphisms from $\widehat{\mathbf{Z}}$ to a finite group are continuous.

Theorem 4 (Deuring)**.** *Let p be a prime and $q = p^m$. Let t be an integer with $|t| \leq 2\sqrt{q}$. Then the number of isomorphism classes of elliptic curves over $\mathbf{F}_q$ with $a_q(E) = t$, that is, with $\#E(\mathbf{F}_q) = q + 1 - t$, is*

$$\begin{cases} H(t^2 - 4q) & \text{if } t^2 < 4q \text{ and } p \nmid t \\ H(-4p) & \text{if } t = 0, \ m \text{ odd} \\ 1 & \text{if } t^2 = 2q, \ p = 2, \ m \text{ odd} \\ 1 & \text{if } t^2 = 3q, \ p = 3, \ m \text{ odd} \\ \frac{1}{12}(p + 6 - 4(\frac{-3}{p}) - 3(\frac{-4}{p})) & \text{if } t^2 = 4q \text{ and } m \text{ even} \\ 1 - (\frac{-3}{p}) & \text{if } t^2 = q \text{ and } m \text{ even} \\ 1 - (\frac{-4}{p}) & \text{if } t = 0 \text{ and } m \text{ even} \\ 0 & \text{otherwise.} \end{cases}$$

Conjecture 5. *Proposition 3 holds even when q is a quadratic residue modulo ℓ, as long as q is sufficiently large.*

Proposition 6. *The multiplicative order of $\rho_\ell(E)$ in $\mathrm{GL}(2, \ell)$ is precisely the ℓ-torsion depth of E.*

Proof. Write k for the order and d for the depth. The Galois representation descends to a map $\mathbf{Z}/d\mathbf{Z} \cong \mathrm{Gal}(\mathbf{F}_{q^d}/\mathbf{F}_q) \to \mathrm{GL}(2, \ell)$. Clearly $k \leq d$, then, but we claim that in fact $k = d$. Suppose instead that $k < d$. Then we have that $\mathrm{Frob}^k(P) = P$, meaning that the coordinates of P are all fixed by $x \mapsto x^{q^k}$, therefore the coordinates all lie in $\mathbf{F}_{q^k}$, so that P lies in $\mathbf{F}_{q^k}$, so that $d \leq k < d$, which is a contradiction. □

We attach to each conjugacy class C of $\mathrm{GL}(2, \ell)$ two invariants $r_1(C)$ and $r_2(C)$ as follows. If A is a matrix in C, then we define $r_1(C)$ to be the least integer $k > 0$ such that A^k admits 1 as an eigenvalue, and $r_2(C)$ to be the least integer $k > 0$ such that A^k is the identity matrix, i.e. $r_2(C)$ is the multiplicative order of A.

Remark 7. The existence of nontrivial $\mathbf{F}_q$-rational ℓ-torsion on E is equivalent to the linear algebraic condition that 1 be an eigenvalue of $\rho_\ell(E)$. If r_1 denotes the least positive integer k such that $E[\ell](\mathbf{F}_{q^k}) \neq \{O\}$, and r_2 denotes the least positive integer k such that $E[\ell](\mathbf{F}_{q^k}) = (\mathbf{Z}/\ell\mathbf{Z})^2$, then $r_1 = r_1(\rho_\ell)$ and $r_2 = r_2(\rho_\ell)$. Hence the spectral properties of $\mathrm{GL}(2, \ell)$ control the possible behaviours of the ℓ-torsion of an elliptic curve over $\mathbf{F}_q$ (knowledge of this structure can be used to write a fast algorithm for determining ℓ-torsion depth).

2.3 Local zeta function

Let $N_m := \#E(\mathbf{F}_{q^m}) = q^m + 1 - a_{q^m}$. Then the *local zeta function* of E is defined by

$$Z(t) = \exp\left(\sum_{m=1}^{\infty} N_m \frac{t^m}{m}\right).$$

The same definition can be used for any smooth projective variety over a finite field. The terminology is intended to contrast $Z(t)$ with the "global", or *Hasse-Weil zeta function*, attached to a variety over a number field (for example $\mathbf{Q}$), which (ignoring issues at primes of bad reduction) is obtained by taking an Euler product over all local zeta functions. In this context one takes $t = q^{-s}$ for $s \in \mathbf{C}$, but for our purposes it will suffice to view $Z(t)$ as a formal power series in t.

It turns out that the integers N_m $(m > 1)$ are uniquely determined by N_1. There are, unfortunately, elliptic curves E over $\mathbf{F}_q$ with the same number of $\mathbf{F}_q$-rational points (and hence the same zeta function), whose corresponding ρ_ℓ do not coincide. In view of the above remarks, this occurs if and only if the traces and determinants agree, but one of them is a scalar conjugacy class while the other is not.

The Weil conjectures were proven in full generality by Deligne in [7] and [8]. The portions relevant for us are stated below.

Theorem 8. *Let X be a smooth projective variety of dimension n defined over $\mathbf{F}_q$, and let $Z(t)$ be the local zeta function of X. Then we have:*

1. *$Z(t)$ is a rational function of t. More precisely, we can write*

$$Z(t) = \frac{P_1(t) \cdots P_{2n-1}(t)}{P_0(t) \cdots P_{2n}(t)}$$

   where each $P_i(t)$ is a polynomial with integral coefficients. Furthermore, $P_0(t) = 1-t$, $P_{2n}(t) = (1 - q^n t)$, and for $1 \leq i \leq 2n-1$, $P_i(t)$ factors over $\mathbf{C}$ as $\prod_j (1 - \alpha_{ij} t)$ for some $\alpha_{ij} \in \mathbf{C}$.

2. *$|\alpha_{ij}| = q^{i/2}$ for all $1 \leq i \leq 2n-1$ and all j.*

Taking X to be an elliptic curve E, we obtain the following.

Corollary 9. *Let E be an elliptic curve defined over $\mathbf{F}_q$, and let $Z(t)$ be its zeta function. Then*

$$Z(t) = \frac{1 - a_q t + qt^2}{(1-t)(1-qt)} = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)}.$$

We have $a_q = \alpha + \beta \leq 2\sqrt{q}$ by Hasse's theorem, and $\alpha\beta = q$, so $|\alpha| = |\beta| = \sqrt{q}$.

Since a_{q^m} is the trace of the mth power of the Frobenius endomorphism $x \mapsto x^q$, the Newton-Girard identities for expressing power sums in terms of elementary symmetric polynomials yield the following formula:

$$N_m = q^m + 1 - a_{q^m} = q^m + 1 - (\alpha^m + \beta^m) = q^m + 1 - \begin{vmatrix} a_q & 1 & 0 & \dots & 0 \\ 2q & a_q & 1 & \dots & 0 \\ \vdots & q & a_q & \ddots & 0 \\ \vdots & 0 & \ddots & a_q & 1 \\ 0 & \dots & \dots & q & a_q \end{vmatrix}.$$

Here, as above, $\alpha, \beta \in \mathbf{C}$ denote the Frobenius eigenvalues.

2.4 Isomorphism classes

Let q be a prime. The number of pairs $(a, b) \in \mathbf{F}_q \times \mathbf{F}_q$ such that $y^2 = x^3 + ax + b$ defines a nonsingular curve is $q^2 - q$, since there are precisely q such pairs with discriminant Δ equal to zero. First we discuss $\mathbf{F}_q$-isomorphism classes of elliptic curves over $\mathbf{F}_q$; denote the collection of such by $\mathcal{E}_q$. It is mentioned in [14] that

$$|\mathcal{E}_q| := \sum_{[E] \in \mathcal{E}_q} 1 = \begin{cases} 2q+6 & q \equiv 1 \bmod 12 \\ 2q+2 & q \equiv 5 \bmod 12 \\ 2q+4 & q \equiv 7 \bmod 12 \\ 2q & q \equiv 11 \bmod 12. \end{cases}$$

However, this is a somewhat vulgar way of counting curves; to accommodate curves with unusually large automorphism groups, we should really take a weighted count as follows:

$$|\mathcal{E}_q|' := \sum_{[E] \in \mathcal{E}_q} \frac{1}{|\mathrm{Aut}(E)|} = q.$$

Here, $\mathrm{Aut}(E)$ denotes the group of $\mathbf{F}_q$-automorphisms of E. The group of $\overline{\mathbf{F}_q}$-automorphisms of E, on the other hand, will be denoted $\overline{\mathrm{Aut}}(E)$. One should always be careful to not confuse the notion of $\mathbf{F}_q$-isomorphism with that of $\overline{\mathbf{F}_q}$-isomorphism, as much of the literature glosses over this subtlety. Unless explicitly mentioned, by "number of isomorphism classes" below we always mean the unweighted count.

Isomorphic elliptic curves have the same j-invariant, and over an algebraically closed field, the converse is true (that is, the j-invariant classifies elliptic curves up to isomorphism). The story over $\mathbf{C}$ is classical and beautiful; in that setting, the connection between lattices and complex tori shows that the isomorphism classes correspond to the orbits of the Poincaré upper half-plane $\mathcal{H} = \{\tau \in \mathbf{C} : \mathrm{Im}\ \tau > 0\}$ under the action of the modular group $\mathrm{PSL}(2, \mathbf{Z})$. The j-invariant then turns out to be a holomorphic function on the upper half-plane which surjects onto $\mathbf{C}$ and is invariant under this action.

Unfortunately, finite fields are not algebraically closed, so there are non-isomorphic elliptic curves over $\mathbf{F}_q$ with the same j-invariant. However, such curves must be twists of one another. The following characterization of twists can be found in [33, X.5.4].

Proposition 10. *If K is a field of characteristic not equal to 2 or 3, then the twists of an elliptic curve E/K are in one-to-one correspondence with K^*/K^{*n} where*

$$n = \begin{cases} 2 & j(E) \neq 0, 1728 \\ 4 & j(E) = 1728 \\ 6 & j(E) = 0. \end{cases}$$

Corollary 11. *Write $|j^{-1}(x)|$ for the number of isomorphism classes of elliptic curves with $j = x \in \mathbf{F}_q$. Then for any $x \neq 0, 1728$ we have $|j^{-1}(x)| = 2$ (quadratic twists), while*

$$|j^{-1}(0)| = \begin{cases} 6 & q \equiv 1, 7 \bmod 12 \\ 2 & q \equiv 5, 11 \bmod 12, \end{cases} \qquad |j^{-1}(1728)| = \begin{cases} 4 & q \equiv 1, 5 \bmod 12 \\ 2 & q \equiv 7, 11 \bmod 12. \end{cases}$$

Proof. Note that $|K^*/K^{*2}| = 2$ while $|K^*/K^{*4}| = 2$ if $q \equiv 3 \bmod 4$ and 4 if $q \equiv 1 \bmod 4$. Also, $|K^*/K^{*6}| = 2$ if $q \equiv 2 \bmod 3$ and 6 if $q \equiv 1 \bmod 3$. □

Remark 12. Suppose $q \neq 2, 3$. If a value of $j = j(z)$ is given it is possible to write an equation for a representative curve in the isomorphism class, namely [4, §6]

- If $j \neq 0, 1728$, then $y^2 = x^3 - ax \pm 2a$, where $a = 27j/(j - 1728)$.
- If $j = 0$, then $y^2 = x^3 + a_6$.

- If $j = 1728$, then $y^2 = x^3 + a_4 x$.

a_6 should be chosen from the sixth roots of unity and a_4 from the fourth roots of unity. This is very useful for computational purposes.

We now describe the number of automorphisms of an elliptic curve E over $\mathbf{F}_q$.

Proposition 13. *Assume $q \neq 2, 3$. If E is an elliptic curve in the isomorphism class $C \in \mathcal{E}_q$ with j-invariant j, then the number of $\overline{\mathbf{F}_q}$-automorphisms of E is*

$$|\overline{\mathrm{Aut}}(E)| = \begin{cases} 6 & \text{if } j = 0 \\ 4 & \text{if } j = 1728 \\ 2 & \text{otherwise.} \end{cases}$$

The number of $\mathbf{F}_q$-automorphisms is [29, Cor. 3.3.6]

$$|\mathrm{Aut}(E)| = \begin{cases} 2 & \text{if } j \neq 0, 1728 \\ 4 & \text{if } j = 1728 \quad \text{and } q \equiv 1 \bmod 4 \\ 2 & \text{if } j = 1728 \quad \text{and } q \equiv 3 \bmod 4 \\ 6 & \text{if } j = 0 \quad \text{and } q \equiv 1 \bmod 6 \\ 2 & \text{if } j = 0 \quad \text{and } q \equiv 5 \bmod 6. \end{cases}$$

The number of elliptic curves over $\mathbf{F}_q$ which are $\mathbf{F}_q$-isomorphic to E is

$$|C| = \frac{q-1}{|\mathrm{Aut}(E)|}.$$

An elliptic curve E over a field of characteristic q is said to be *supersingular* when $E[q]$ is trivial, that is, when no points of order q exist, even in $E(\overline{\mathbf{F}_q})$. We note the following facts about supersingular curves. For their proofs, see [35, Sec. 4.6].

Proposition 14. *Let E be an elliptic curve over $\mathbf{F}_q$, where $q \geq 5$ is a prime. Then E is supersingular if and only if $a_q(E) = 0$, that is, if and only if $\#E(\mathbf{F}_q) = q + 1$.*

Proposition 15. *Let $q \geq 5$ be prime. Then the elliptic curve $y^2 = x^3 + 1$ over $\mathbf{F}_q$ is supersingular if and only if $q \equiv 2 \bmod 3$, and the elliptic curve $y^2 = x^3 + x$ over $\mathbf{F}_q$ is supersingular if and only if $p \equiv 3 \bmod 4$.*

2.5 Hurwitz class numbers

The Hurwitz class number $H(N)$ is a modification of the class number of positive definite binary quadratic forms of discriminant $-N$. For an integer $N \geq 0$, $H(N)$ is defined as follows. $H(0) = -1/12$. If $N \equiv 1, 2 \bmod 4$ then $H(N) = 0$. Otherwise, $H(N)$ is the number of classes of not necessarily primitive positive definite quadratic forms of discriminant $-N$, except that those classes which have a representative which is a multiple of the form $x^2 + y^2$ (respectively $x^2 + xy + y^2$) are weighted by $1/2$ (respectively $1/3$).

Results similar to Theorem 4 involving curves with prescribed torsion can be found in [6].

For this reason, we will see later that formulas counting curves naturally yield formulas for evaluating certain sums of Hurwitz class numbers. A trivial example of this is:

Corollary 16. *If q is prime,*

$$\frac{1}{2} \sum_{|r|<2\sqrt{q}} H(4q - r^2) = q.$$

In other words, if one sums over all possible values of $a_q(E)$, one obtains the weighted number of isomorphism classes.

Chapter 3

The case $\ell = 2$

3.1 The case $q = 2$

The general Weierstrass form for the elliptic curve C in this case is

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

We denote by $O = (0 : 1 : 0)$ the point at infinity (the identity element for the group law). Noting that $P + Q + R = O$ in group law iff P, Q, R are collinear, we see that $2P = O$ iff P, P, O are collinear, iff the tangent line at P contains O, iff the tangent line at P is vertical. Differentiating the equation of the curve, we obtain

$$a_1x\ dy + a_1y\ dx + a_3\ dy = 3x^2\ dx + a_4\ dx \quad \Rightarrow \quad \frac{dy}{dx} = \frac{3x^2 + a_4 - a_1y}{a_1x + a_3}$$

so in order for this to be infinite, we need $x = a_3/a_1$. Certainly this cannot hold if $a_3 = 1$ and $a_1 = 0$. On the other hand, if $a_1 = a_3 = 0$ then C is singular, so it is not an elliptic curve. So assume $a_1 = 1$. Then for all 2-torsion points (x_0, y_0), $x_0 = a_3$. This means

$$y_0^2 + a_3y_0 + a_3y_0 = a_3^3 + a_2a_3^2 + a_4a_3 + a_6 \quad \Rightarrow \quad y_0 = a_3^3 + a_2a_3^2 + a_4a_3 + a_6$$

and so there is exactly *one* nontrivial 2-torsion point

$$(x_0, y_0) = (a_3, a_3^3 + a_2a_3^2 + a_4a_3 + a_6).$$

Hence $E[2]$ is a 1-dimensional $\mathbf{F}_2$-vector space, upon which the Galois group must act trivially, since the above point (x_0, y_0) has both coordinates in $\mathbf{F}_2$.

3.2 The case $q = 3$

Now the general Weierstrass form for the elliptic curve C is

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

Performing a similar analysis to the case $q = 2$, we obtain

$$2y\ dy = 2b_2x\ dx + 2b_4\ dx \quad \Rightarrow \quad \frac{dy}{dx} = \frac{b_2x + b_4}{y}$$

so we need $y = 0$. In this case x can be any root of the cubic $4x^3 + b_2x^2 + 2b_4x + b_6$ and it will be 2-torsion. Hence $E[2]$ is a 2-dimensional $\mathbf{F}_2$-vector space. This case now reduces to the case treated next.

3.3 The case $q \neq 2, 3$

Now suppose $q \neq 2$, so that $E[2]$ is a 2-dimensional $\mathbf{F}_q$-vector space, and $q \neq 3$, so that the short Weierstrass form

$$y^2 = x^3 + ax + b, \qquad a, b \in \mathbf{F}_q$$

can be used. Let E be the elliptic curve defind by this equation. Then the 2-torsion points of E all satisfy $y = 0$, so that

$$E[2] = \{O, \quad P_1 = (\alpha_1, 0), \quad P_2 = (\alpha_2, 0), \quad P_3 = P_1 + P_2 = (\alpha_3, 0)\}$$

where $\alpha_1, \alpha_2, \alpha_3 \in \overline{\mathbf{F}}_q$ are the distinct roots of the cubic $x^3 + ax + b$, and O is the point at infinity (the identity element for the group law on the elliptic curve).

If G is a finite group, we are interested in the possible continuous group homomorphisms $\phi : \widehat{\mathbf{Z}} \to G$. First of all, note that any such homomorphism must factor through the projection map $\pi_n : \widehat{\mathbf{Z}} \twoheadrightarrow \mathbf{Z}/n\mathbf{Z}$ for some n. Indeed, $1 \in \widehat{\mathbf{Z}}$ is sent by ϕ to some element $a \in G$ with order n dividing $|G|$. However this means we can define a homomorphism $\psi : \mathbf{Z}/n\mathbf{Z} \to G$ by declaring $\psi(1) = a$, but then $\phi(1) = (\psi \circ \pi_n)(1)$, which implies $\phi = \psi \circ \pi_n$ as any continuous homomorphism out of $\widehat{\mathbf{Z}}$ is determined by where it sends 1 (note π_n is continuous by the very definition of $\widehat{\mathbf{Z}}$ as an inverse limit in the category of topological groups, and any homomorphism coming out of a discrete group, such as ψ, is automatically continuous).

Now, we are interested in the case $G = \mathrm{GL}(2,2) \cong S_3$; this group has 3 elements of order 2 (the "transpositions"):

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

2 elements of order 3 (the "3-cycles"):

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

and 1 element of order 1 (the identity):

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Moreover, these are precisely the three conjugacy classes. Hence, since we are merely trying to show that every possible mod 2 representation of $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ is *equivalent* to a representation attached to the 2-torsion of an elliptic curve, it suffices to hit one matrix from each conjugacy class in this manner. The foregoing remarks therefore reduce our problem to understanding the nontrivial homomorphisms $\mathbf{Z}/n\mathbf{Z} \to \mathrm{GL}(2,2)$ for $n = 2, 3$. However, this is simple: when $n = 2$, the element $1 \in \mathbf{Z}/2\mathbf{Z}$ can be sent to any of the elements of order 2. When $n = 3$, the element $1 \in \mathbf{Z}/3\mathbf{Z}$ can be sent to any of the elements of order 3. As was just remarked, the actual matrix it is sent to is immaterial (only its order in $\mathrm{GL}(2,2)$ matters), so we only have three elliptic curves to exhibit:

- For the trivial representation $\widehat{\mathbf{Z}} \to \mathrm{GL}(2,2)$, it suffices to choose three distinct elements $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{F}_q$ and form the cubic $(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Then the Galois group acts trivially on the roots, so the representation attached to the corresponding elliptic curve is the trivial representation.

- For the unique equivalence class of representation $\widehat{\mathbf{Z}} \to \mathrm{GL}(2,2)$ wherein the element $1 \in \widehat{\mathbf{Z}}$ is sent to a linear operator of order 2, it suffices to choose $\alpha_1 \in \mathbf{F}_q$ and an irreducible quadratic $f \in \mathbf{F}_q[x]$ with distinct roots $\alpha_2, \alpha_3 \notin \mathbf{F}_q$, and form the cubic $(x - \alpha_1) \cdot f(x)$. Then the generator of the Galois group acts on the roots by fixing α_1 and swapping the roots of f, so the representation attached to the corresponding elliptic curve is in the aforementioned equivalence class. Indeed, choosing the basis $\{P_1, P_2\}$ where $P_i = (\alpha_i, 0)$, the representation obtained from the 2-torsion is the one

where $1 \in \widehat{\mathbf{Z}}$ acts by the transformation defined by $P_1 \mapsto P_1$, $P_2 \mapsto P_1 + P_2$, in other words, the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

which has order 2.

- For the unique equivalence class of representation $\widehat{\mathbf{Z}} \to \mathrm{GL}(2,2)$ wherein the element $1 \in \widehat{\mathbf{Z}}$ is sent to a linear operator of order 3, it suffices to choose an irreducible cubic $f \in \mathbf{F}_q[x]$ with distinct roots $\alpha_1, \alpha_2, \alpha_3 \notin \mathbf{F}_q$. Then the generator of the Galois group acts by cycling the roots of f (that is, $\alpha_i \mapsto \alpha_{i+1}$ where we put $\alpha_4 := \alpha_1$), so the representation attached to the corresponding elliptic curve is in the aforementioned equivalence class. Indeed, choosing the basis $\{P_1, P_2\}$ where $P_i = (\alpha_i, 0)$, the representation obtained from the 2-torsion is the one where $1 \in \widehat{\mathbf{Z}}$ acts by the transformation determined by $P_1 \mapsto P_2$ and $P_2 \mapsto P_1 + P_2$, in other words, the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

which has order 3.

Chapter 4

Modular curves

To count elliptic curves with prescribed Galois representations ρ_ℓ, we will make use of modular curves. These are moduli spaces whose non-cuspidal points parameterize "enhanced" elliptic curves over $\mathbf{F}_q$. A thorough treatment of these objects in the language of modern algebraic geometry can be found in the Katz-Mazur book [16] or the paper of Deligne-Rapoport [9]. The Hasse-Weil bound, which is equivalent to the determination of the absolute values of the roots of the local zeta function (see §2.3), will be of key importance:

Theorem 17. *Let X be a smooth, absolutely irreducible projective curve of genus g over $\mathbf{F}_q$. Then*

$$|\#X(\mathbf{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

The following corollary is the main tool we will use to deduce exact formulas.

Corollary 18. *Let X be a smooth, absolutely irreducible projective curve of genus 0 over $\mathbf{F}_q$. Then $\#X(\mathbf{F}_q) = q + 1$.*

4.1 Moduli problems

We will be most interested in the $\mathbf{F}_q$-reductions of the (compactified) modular curves $X(N)$, $X_1(N)$, and $X_0(N)$ arising from the congruence subgroups $\Gamma(N)$, $\Gamma_1(N)$, and $\Gamma_0(N)$ of $\mathrm{SL}(2, \mathbf{Z}) = \Gamma(1)$. These act as moduli spaces for the moduli problems of classifying $\overline{\mathbf{F}_q}$-isomorphism classes of:

- pairs (E, B) where B is an ordered basis for $E[N]$ whose value under the Weil pairing is $\zeta_N = e^{2\pi i/N}$.
- pairs (E, P) where P is a point of exact order N.
- pairs (E, C) where C is a cyclic subgroup of order N.

4.2 Cusps and genera

Denote by $g(N)$, $g_1(N)$ and $g_0(N)$ the genera of the modular curves $X(N)$, $X_1(N)$ and $X_0(N)$ respectively. Then when $N \leq 10$, we have $g_0(N) = g_1(N) = 0$. On the other hand, $g(N) = 0$ when $N \leq 5$, but $g(7) = 3$. In fact, $X(7)$ is a Hurwitz surface known as the *Klein quartic*.

It will be important for us to know which cusps of these curves are defined over $\mathbf{F}_q$. The algebraic curve $X_1(N)$ has half of its $N-1$ cusps defined over $\mathbf{Q}$ and the rest over the maximal real subfield of $\mathbf{Q}(\zeta_N)$, which is $\mathbf{Q}(\zeta_N + \overline{\zeta_N})$, an extension of degree $(N-1)/2$. Hence, for example, $X_1(7)$ has 6 cusps defined over $\mathbf{F}_q$ when $q \equiv \pm 1 \bmod 7$ and 3 cusps otherwise. See also [26, Cor. 5.10.1] for an explicit formula for $\#X_0(N)(\mathbf{F}_q)$ in terms of traces of Hecke operators.

Let $Y(N)$ denote the non-compactified modular curve of full level N structures, let c_N denote the number of cusps and g_N denote its genus. Then the Hasse-Weil bound says

$$|\#Y(N)(\mathbf{F}_q) - (q + 1 - c_N)| = |\#X(N)(\mathbf{F}_q) - (q+1)| \leq 2g_N\sqrt{q}.$$

For $N \leq 5$, we have $g_N = 0$, so this implies that $\#Y(N)(\mathbf{F}_q) = q + 1 - c_N$. Suppose $N = \ell$ is a prime different from q. The number of cusps is, according to [10, p. 101],

$$\epsilon_\infty(\Gamma(\ell)) = c_\ell = \frac{1}{2}(\ell^2 - 1).$$

Thus $c_3 = 4$ while $c_5 = 12$. We conclude that $\#Y(3)(\mathbf{F}_q) = q + 1 - 4 = q - 3$ while $\#Y(5)(\mathbf{F}_q) = q + 1 - 12 = q - 11$.

Chapter 5

Counting curves with given Galois representation

5.1 Introduction

If C denotes a conjugacy class of $\mathrm{GL}(2,\ell)$, we write $N_q(C)$ for the number of (short Weierstrass equations of) elliptic curves over $\mathbf{F}_q$ with $\rho_\ell = C$; the prime ℓ is omitted from the notation since it will always be fixed. Henceforth, we denote by $C_{d,t}$ (resp. $C^*_{d,t}$) the non-scalar (resp. scalar, if it exists) conjugacy class of $\mathrm{GL}(2,\ell)$ with determinant d and trace t. Since $a_q(E) = -a_q(E')$ where E' denotes the quadratic twist of E, we deduce the symmetries $N_q(C_{d,t}) = N_q(C_{d,-t})$ and $N_q(C^*_{d,t}) = N_q(C^*_{d,-t})$. For brevity of notation, we set

$$\widetilde{N}_q(C) = \frac{N_q(C)}{q-1} = \sum_E \frac{1}{|\mathrm{Aut}(E)|},$$

the sum being taken over a complete set of representatives E for the isomorphism classes of elliptic curves over $\mathbf{F}_q$ with $\rho_\ell = C$. The quantities $\widetilde{N}_q(C)$ are related to sums of Hurwitz class numbers as follows:

$$\frac{1}{2}\sum_{\substack{|r|<2\sqrt{q}\\ r\equiv t \bmod \ell}} H(4q-r^2) = \begin{cases} \widetilde{N}_q(C_{q,\pm t}) + \widetilde{N}_q(C^*_{q,\pm t}) & \text{if } t^2 \equiv 4q \bmod \ell, \\ \widetilde{N}_q(C_{q,\pm t}) & \text{otherwise.} \end{cases} \tag{5.1}$$

For the small ℓ we consider, the right-hand side turns out to simply be a linear polynomial in q with constant coefficients. Note that the trace of ρ_ℓ must be $a_q \bmod \ell$, while its

determinant must be $q \bmod \ell$. Furthermore, d is a quadratic residue mod ℓ if and only if there exist scalar (central) conjugacy classes in $\mathrm{GL}(2,\ell)$ of determinant d.

There are a few choices for how to go about counting curves. We could simply sample the curve $y^2 = x^3 + ax + b$ with (a,b) chosen uniformly at random from $\mathbf{F}_q^2 \setminus S$ where S is the set of (a,b) with discriminant zero. On the other hand, we could count $\mathbf{F}_q$-*isomorphism classes* instead. Finally, we could count isomorphism classes weighted by the reciprocal of the size of their automorphism groups. Methods 1 and 3 turn out to give the same answer; see [13].

5.2 The case $\ell = 3$

The purpose of this section is to prove the following theorem. It will be proved in several pieces, and in most cases, we will also give the number of isomorphism classes with $j = 0$ and $j = 1728$ which contribute to each conjugacy class.

Theorem 19. *Let q be a prime. Then for any conjugacy class C of $\mathrm{GL}(2,3)$,*

$$\widetilde{N}_q(C) = \frac{|C|}{|\mathrm{SL}(2,3)|}(q - a_C) = \frac{|C|}{24}(q - a_C)$$

where a_C is the integer corresponding to C in the below table[1]*, where each cell contains the information*

$$a_C \ (|C|)\text{: } (r_1(C), r_2(C)).$$

We first treat the case $q \equiv 1 \bmod 3$. Corollary 11 says that $|j^{-1}(0)| = 6$ and $|j^{-1}(1728)| = 4$ or 2 depending on whether $q \equiv 1$ or $7 \bmod 12$.

Proposition 20. *When $q \equiv 1 \bmod 3$,*

$$\widetilde{N}_q(C^*_{1,\pm 1}) = \frac{q-3}{24}.$$

Precisely one isomorphism class with $j = 0$ contributes. The number of classes with $j = 1728$ which contribute is 1 (respectively 0) when $q \equiv 1 \bmod 12$ (respectively $q \equiv 7 \bmod 12$).

[1]The class function on $\mathrm{GL}(2,3)$ defined by $C \mapsto a_C$ is in fact an irreducible character.

Proof. Let S_3 denote the collection of isomorphism classes of elliptic curves over $\mathbf{F}_q$ with complete rational 3-torsion. Using the moduli interpretation of $Y(3)(\mathbf{F}_q)$ previously mentioned,

$$\frac{q-3}{24} = \frac{\#Y(3)(\mathbf{F}_q)}{|\mathrm{SL}(2,3)|} = \sum_{E \in S_3} \frac{1}{|\mathrm{Aut}(E)|}.$$

To establish the second statement, note that when $q \equiv 1 \bmod 12$, we have $|\mathrm{Aut}(E)| \in \{2,4,6\}$ for all E, so

$$q - 3 = 12m_{\mathrm{ord}} + 6m_{1728} + 4m_0$$

with $0 \leq 2m_{1728} \leq 4$ and $0 \leq 2m_0 \leq 6$, hence $0 \leq m_{1728} \leq 2$ and $0 \leq m_0 \leq 3$. We claim $m_0 = m_{1728} = 1$. Reducing the above equation we obtain $2 \equiv 2m_{1728} \bmod 4$ while $1 \equiv m_0 \bmod 3$, and the claim follows. On the other hand, when $q \equiv 7 \bmod 12$, we have $|\mathrm{Aut}(E)| \in \{2,6\}$ for all E, so

$$q - 3 = 12m_{\mathrm{ord}} + 4m_0$$

with $0 \leq m_0 \leq 3$. Reducing gives $m_0 \equiv 1 \bmod 3$, so $m_0 = 1$. The final statement then follows from Proposition 15. □

Let us now turn our attention to the non-scalar classes $C_{1,\pm 1}$, which have size 8.

Proposition 21. *When $q \equiv 1 \bmod 3$,*

$$\widetilde{N}_q(C_{1,\pm 1}) = \frac{8q}{24}.$$

Precisely 2 classes with $j = 0$ contribute, and none with $j = 1728$ contribute.

Proof. A generic isomorphism class with rank 1 rational 3-torsion should contribute exactly 1 point to $Y_1(3)(\mathbf{F}_q)$ because $\mathbf{Z}/3\mathbf{Z}$ only has one possible cyclic 3-subgroup. On the other hand each generic isomorphism class with full (rank 2) rational 3-torsion should contribute $|\mathbf{P}^1(\mathbf{F}_3)| = 4$ points to $Y_1(3)(\mathbf{F}_q)$. Therefore,

$$q - 1 = \#Y_1(3)(\mathbf{F}_q) = 8 \sum_{\text{rank } 2} \frac{1}{|\mathrm{Aut}(E)|} + 2 \sum_{\text{rank } 1} \frac{1}{|\mathrm{Aut}(E)|} = 8\widetilde{N}_q(C^*_{1,-1}) + 2\widetilde{N}_q(C_{1,-1})$$

and so

$$\widetilde{N}_q(C_{1,-1}) = \frac{q-1}{2} - \frac{q-3}{6} = \frac{3q - 3 - q + 3}{6} = \frac{q}{3}.$$

To establish the remaining statements, note that when $q \equiv 1 \bmod 12$, by the same techniques as above we obtain

$$4q = 6m_{\text{ord}} + 3m_{1728} + 2m_0$$

with $0 \leq m_{1728} \leq 1$ and $0 \leq m_0 \leq 2$. Reducing we get $0 \equiv m_{1728} \bmod 2$ so $m_{1728} = 0$. Similarly $1 \equiv 2m_0 \bmod 3$ so $m_0 = 2$. Otherwise if $q \equiv 7 \bmod 12$, the same technique shows $m_0 = 2$, but we must have $m_{1728} = 0$ again by Proposition 15. □

To conclude our analysis of the $q \equiv 1 \bmod 3$ case, we deduce the count for the remaining conjugacy class $C_{1,0}$ of size 6.

Proposition 22. *When $q \equiv 1 \bmod 3$,*

$$\widetilde{N}_q(C_{1,0}) = \frac{6(q+1)}{24}.$$

No classes with $j = 0$ contribute, while 2 with $j = 1728$ contribute.

Proof. This is immediate: since every elliptic curve over $\mathbf{F}_q$ has $\det \rho_\ell = q \in \mathbf{F}_3$, we certainly have

$$\sum_C \widetilde{N}_q(C) = q,$$

the sum taken over all conjugacy classes C in $\mathrm{GL}(2,3)$ of determinant $q \bmod 3$. Hence, using the previous two results, we have

$$\widetilde{N}_q(C_{1,0}) = q - 2 \cdot \frac{8q}{24} - 2 \cdot \frac{q-3}{24} = \frac{3(q+1)}{12}.$$

For the remaining statements, note that all 6 classes with $j = 0$ have already been accounted for above. If $q \equiv 1 \bmod 4$, only 2 of the 4 with $j = 1728$ have been accounted for. On the other hand, if $q \equiv 3 \bmod 4$, there are 2 classes with $j = 1728$ in total, and we haven't accounted for either of them yet (in fact Proposition 15 says they are supersingular anyway). □

Now consider $q \equiv 2 \bmod 3$. In this case, Corollary 11 says $|j^{-1}(0)| = 2$, and $|j^{-1}(1728)| = 4$ or 2 depending on whether $q \equiv 5$ or $11 \bmod 12$. By Proposition 15, those with $j = 0$ are always supersingular, and when $q \equiv 11 \bmod 12$, those with $j = 1728$ are as well.

Proposition 23. *When $q \equiv 2 \bmod 3$,*

$$\widetilde{N}_q(C_{2,0}) = \frac{12(q-1)}{24}.$$

Both isomorphism classes with $j = 0$ contribute. The number of classes with $j = 1728$ which contribute is 2 when $q \equiv 11 \bmod 12$.

Proof. The strategy is identical to the above; count the $\mathbf{F}_q$-rational points on $Y_1(3)$. The statement about the $j = 0$ contribution follows from remarks above. For the $j = 1728$ contribution, note that if $q \equiv 11 \bmod 12$ then Proposition 15 implies the result. □

Proposition 24. *When $q \equiv 2 \bmod 3$,*

$$\widetilde{N}_q(C_{2,1}) = \widetilde{N}_q(C_{2,2}) = \frac{6(q+1)}{24}.$$

No classes with $j = 0$ contribute. If $q \equiv 11 \bmod 12$, then no classes with $j = 1728$ contribute.

Proof. The count formula itself follows from subtracting from the total, as in Proposition 22. That is, we note

$$\widetilde{N}_q(C_{2,1}) + \widetilde{N}_q(C_{2,2}) = q - \widetilde{N}_q(C_{2,0}) = \frac{2q-(q-1)}{2} = \frac{q+1}{2}$$

and both terms on the left-hand side are equal. The statement about the $j = 0$ contribution is clear, since all of these isomorphism classes were already accounted for above. For the $j = 1728$ contribution, note that if $q \equiv 11 \bmod 12$, the same is true. □

5.3 The case $\ell = 5$

In this section we will prove certain cases of the following conjecture. Note that since 5 does not divide 12, the analysis required to give information about the $j = 0$ and $j = 1728$ contributions is significantly more involved; we therefore remain silent on this question.

Conjecture 25. *Let q be a prime. Then for any conjugacy class C of $\mathrm{GL}(2,5)$,*

$$\widetilde{N}_q(C) = \frac{|C|}{|\mathrm{SL}(2,5)|}(q - a_C) = \frac{|C|}{120}(q - a_C)$$

where, as before, a_C is the integer corresponding to C in the table.

We first assume $q \equiv 1 \bmod 5$. The following proposition gives the number of elliptic curves with complete $\mathbf{F}_q$-rational 5-torsion.

Proposition 26. *When $q \equiv 1 \bmod 5$,*

$$\widetilde{N}_q(C^*_{1,\pm 2}) = \frac{q-11}{120}.$$

Proof. We consider the modular curve $X(5)$ which has genus 0 and 12 cusps. Hence $\#Y(5)(\mathbf{F}_q) = q + 1 - 12 = q - 11$, so we obtain, as desired, that

$$q - 11 = 120 \sum_{E \in S_5} \frac{1}{|\mathrm{Aut}(E)|},$$

where S_5 denotes the collection of isomorphism classes of elliptic curves over $\mathbf{F}_q$ with complete rational 5-torsion. □

As before, we seek to take care of the nonscalar conjugacy class of these same traces. Looking at the values of (r_1, r_2) listed in the table, we see that another modular curve can help.

Proposition 27. *When $q \equiv 1 \bmod 5$,*

$$\widetilde{N}_q(C_{1,\pm 2}) = \frac{24(q-1)}{120}.$$

Proof. Consider the modular curve $X_1(5)$, which has 4 cusps and genus 0. We have $\#Y_1(5)(\mathbf{F}_q) = q + 1 - 4 = q - 3$, so that

$$q - 3 = 4 \sum_{\text{rank 1}} \frac{1}{|\mathrm{Aut}(E)|} + 24 \sum_{\text{rank 2}} \frac{1}{|\mathrm{Aut}(E)|}.$$

The second ("rank 2") summation was calculated above, so

$$q - 3 = 4 \sum_{\text{rank 1}} \frac{1}{|\mathrm{Aut}(E)|} + \frac{q-11}{5}$$

and hence

$$\frac{q-1}{5} = \sum_{\text{rank 1}} \frac{1}{|\mathrm{Aut}(E)|}.$$

□

To complete the analysis of the $q \equiv 1 \bmod 5$ case, it would be necessary to prove Conjecture 25 either for $C = C_{1,1}$ or for $C_{1,0}$; the rest of the claims would follow from the quadratic twist symmetry and subtraction from the total.

The relation (5.1) to sums of Hurwitz class numbers immediately establishes the following conjecture made in [2, Table 1].

Corollary 28. *When $q \equiv 1 \bmod 5$, we have that for $c \equiv \pm 2 \bmod 5$,*

$$\sum_{\substack{|r|<2\sqrt{q} \\ r \equiv c \bmod 5}} H(4q - r^2) = \frac{5q - 7}{12}.$$

The conjecture stated there for $q \equiv 4 \bmod 5$ and $c \equiv \pm 1 \bmod 5$ would follow in the same manner if we could prove our predictions for $\widetilde{N}_q(C_{4,\pm 1})$ and $\widetilde{N}_q(C^*_{4,\pm 1})$.

The following two propositions are equivalent to [2, Theorem 4] and can be proved by counting points on $X_1(5)$. Recall that the number of cusps of $X_1(5)$ defined over $\mathbf{F}_q$ is 4 when $q \equiv \pm 1 \bmod 5$, and otherwise is 2. This explains the slight difference between the following two formulas.

Proposition 29. *When $q \equiv \pm 2 \bmod 5$,*

$$\widetilde{N}_q(C_{q,\pm(q+1)}) = \frac{30(q-1)}{120}.$$

Proposition 30. *When $q \equiv 4 \bmod 5$,*

$$\widetilde{N}_q(C_{4,0}) = \frac{30(q-3)}{120}.$$

5.4 The case $\ell = 7$ and the Klein quartic

It is tempting to believe that there exists a single class function $C \mapsto a_C \in \mathbf{Z}$ on each of the groups $\mathrm{GL}(2, \ell)$, such that a result analogous to the ones mentioned for $\ell = 3$ and $\ell = 5$ would hold. After all, were this true, perhaps there would be some fruitful representation-theoretic interpretation of this information. In Table 3, we have tabulated values of a_C that agree with computational evidence. Sizes of conjugacy classes are also shown in brackets, although the invariants (r_1, r_2) have been omitted due to space constraints. For

each prime q, if we evaluate $\widetilde{N}_q(C)$ by computation, we can then calculate $a_C = a_C(q)$ using the relation

$$\widetilde{N}_q(C) = \frac{|C|}{|\mathrm{SL}(2,\ell)|} \cdot (q - a_C).$$

We then see that in the case $\ell = 7$, for some conjugacy classes C, the values $a_C(q)$ are no longer constant as q runs through the relevant arithmetic progression modulo ℓ. In our table these are denoted by "?". Indeed, the mere congruence conditions that such putative integers would have to satisfy appear to preclude them from existing. Hence we can no longer assign a single $a_C \in \mathbf{Z}$ to each conjugacy class C of $\mathrm{GL}(2,\ell)$, having to resort instead (as will be elaborated shortly) to the assignment of an infinite family of integers to each conjugacy class. Moreover, the sets indexing these families, for conjugacy classes of varying determinant, appear to be different, thereby slashing any hopes of packaging this information together into a family of class functions on $\mathrm{GL}(2,\ell)$, in general. Thus, without substantial modification, such a result cannot be true.

Proposition 31. *When $q \not\equiv \pm 1 \bmod 7$, we have*

$$\widetilde{N}_q(C_{q,\pm(q+1)}) = \frac{56(q-2)}{336}.$$

Proof. As we mentioned above, only 3 of the 6 cusps of $X_1(7)$ are defined over $\mathbf{F}_q$ when $q \not\equiv \pm 1 \bmod 7$. Note that the maximal real subfield of $\mathbf{Q}(\zeta_7)$ is the cubic extension $\mathbf{Q}(\zeta_7 + \overline{\zeta_7})$. The result now follows by emulating the proof of Proposition 27. □

We would like to draw attention to the conjectures in the table [2, Table 2]. Since the Klein quartic $X(7)$ has genus 3, any exact formula for $\widetilde{N}_q(C^*_{1,\pm 2})$ and $\widetilde{N}_q(C_{1,\pm 2})$ will have to depend on further properties of the prime q. It is mentioned in [26, Section 5.7.5] that $\#X(7)(\mathbf{F}_q)$ is related to how the prime q splits in the ring $\mathbf{Z}[\sqrt{-7}]$; note this is not a Dedekind domain. By Eichler-Shimura and the fact that the Jacobian of $X(7)$ decomposes as a product of three elliptic curves, the numbers $\#X(7)(\mathbf{F}_q)$ are related to the Fourier coefficients b_n of the unique cusp form for $\Gamma_0(49)$ by the formula $\#X(7)(\mathbf{F}_q) = q + 1 - 3b_q$; see [22, Elliptic curve 49.a4] and the Master's thesis [31, p. 67]. In [19, Cor. 11.4] the numbers $\#X(7)(\mathbf{F}_q)$ are shown, in some cases, to satisfy certain congruences.

However, we have the following weaker result, which shows that if one takes an appropriate linear combination of $\widetilde{N}_q(C^*_{1,\pm 2})$ and $\widetilde{N}_q(C_{1,\pm 2})$, the behaviour is once again straightforward.

Proposition 32. *When $q \equiv 1 \bmod 7$,*

$$\widetilde{N}_q(C_{1,\pm 2}) + 8\widetilde{N}_q(C^*_{1,\pm 2}) = \frac{56(q-5)}{336}.$$

Proof. $X_1(7)(\mathbf{F}_q)$ has 6 cusps and genus 0, so we obtain

$$q + 1 - 6 = 6\widetilde{N}_q(C_{1,\pm 2}) + 48\widetilde{N}_q(C^*_{1,\pm 2}). \qquad \square$$

Note the 56 in the numerator is no mistake, as $|C_{1,\pm 2}| + 8 \cdot |C^*_{1,\pm 2}| = 56$.

Here are some other results proved in [2, Theorem 6], using other tools such as the Eichler-Selberg trace formula.

Proposition 33. *When $q \equiv 3 \bmod 7$,*

$$\widetilde{N}_q(C_{3,0}) = \widetilde{N}_q(C_{5,0}) = \frac{56(q+1)}{336}, \qquad \widetilde{N}_q(C_{6,0}) = \frac{56(q-5)}{336}, \qquad \widetilde{N}_q(C_{6,\pm 2}) = \frac{56(q+1)}{336}.$$

To end this section, we discuss some auxiliary patterns we noticed in our computations of $\widetilde{N}_q(C^*_{4,\pm 1})$. It appears that all of the values $a_C(q)$ do become constant when we restrict the prime q to lie in certain fixed *quadratic progressions*. For example, one should obtain formulas just as simple and explicit as in the $\ell = 3$ case upon restriction to primes of the form $q = 28n^2 - 28n + A$ for $A \in \{11, 53, 151, 263, \ldots\}$. This seems to be due to the fact that the elliptic curve appearing in the decomposition of the Jacobian mentioned above admits complex multiplication; see the main result of [27].

GL(2, 3)	**1**	2
0	-1 (6): $(4, 4)$	1 (12): $(1, 2)$
1	0 (8): $(2, 6)$ 3 (1): $(2, 2)$	-1 (6): $(8, 8)$
2	0 (8): $(1, 3)$ 3 (1): $(1, 1)$	-1 (6): $(8, 8)$

GL(2, 5)	**1**	2	3	**4**
0	-1 (30): $(4, 4)$	-1 (20): $(8, 8)$	-1 (20): $(8, 8)$	3 (30): $(1, 2)$
1	-1 (20): $(6, 6)$	-1 (20): $(24, 24)$	1 (30): $(2, 4)$	-1 (24): $(4, 20)$ -1 (1): $(4, 4)$
2	1 (24): $(1, 5)$ 11 (1): $(1, 1)$	1 (30): $(2, 4)$	-1 (20): $(24, 24)$	-1 (20): $(12, 12)$
3	1 (24): $(2, 10)$ 11 (1): $(2, 2)$	1 (30): $(1, 4)$	-1 (20): $(24, 24)$	-1 (20): $(12, 12)$
4	-1 (20): $(3, 3)$	-1 (20): $(24, 24)$	1 (30): $(1, 4)$	-1 (24): $(4, 20)$ -1 (1): $(4, 4)$

GL(2, 7)	**1**	**2**	3	**4**	5	6
0	? (42)	? (42)	-1 (56)	? (42)	-1 (56)	5 (56)
1	-1 (56)	? (48) ? (1)	-1 (42)	? (42)	2 (56)	-1 (42)
2	? (48) ? (1)	? (42)	-1 (42)	2 (56)	-1 (42)	-1 (56)
3	? (42)	2 (56)	2 (56)	? (48) ? (1)	-1 (42)	-1 (42)
4	? (42)	2 (56)	2 (56)	? (48) ? (1)	-1 (42)	-1 (42)
5	? (48) ? (1)	? (42)	-1 (42)	2 (56)	-1 (42)	-1 (56)
6	-1 (56)	? (48) ? (1)	-1 (42)	? (42)	2 (56)	-1 (42)

Chapter 6

Concluding remarks

For a fixed prime ℓ and conjugacy class C of $\mathrm{GL}(2,\ell)$, it is natural to ask about the asymptotic behaviour of $\widetilde{N}_q(C)$, that is, as $q \to \infty$. The genera of modular curves increase fairly rapidly, and the error terms in the Hasse-Weil bound appear in many cases to be related to well-guarded arithmetic data, such as the traces of Hecke operators on spaces of cusp forms (Eichler-Shimura). Although this makes it likely that any exact formulas for $\widetilde{N}_q(C)$ will be complicated, the Hasse-Weil bound and the general idea that we should be able to express $\widetilde{N}_q(C)$ in terms of point counts of modular curves suggests the following equidistribution conjecture.

Conjecture 34. *For a conjugacy class C of $\mathrm{GL}(2,\ell)$,*

$$\frac{\widetilde{N}_q(C)}{q} = \frac{|C|}{|\mathrm{SL}(2,\ell)|} + O(q^{-1/2}).$$

That is, the (suitably weighted) proportion of elliptic curves E over $\mathbf{F}_q$ with $\rho_\ell(E) = C$ should approach the proportion of matrices in $\mathrm{GL}(2,\ell)$ admissible for q which lie in C.

By looking at Table 3, we see that the conjugacy classes $C = C_{3,0}$ and $C' = C_{3,\pm 3}$ of $\mathrm{GL}(2,7)$ both have order 56, and multiplicative order 6, but $a_C \neq a_{C'}$. Thus, the coincidence of these properties alone will not suffice to ensure $\widetilde{N}_q(C) = \widetilde{N}_q(C')$.

We conclude with the remark that even where strong computational evidence suggests that exact formulas exist, some such formulas seem to remain just beyond the reach of these methods. For example, as stated at the end of [2], all conjugacy classes of $\mathrm{GL}(2,5)$, as well as many conjugacy classes of $\mathrm{GL}(2,7)$ (namely, the cells in the table where no "?"

is found) should admit simple formulas, and it seems likely that the remaining conjugacy classes of the latter group (or at least those with determinant 1) can all be connected to the Klein quartic. The reader is referred to [3] for recent progress.

References

[1] T.E. Venkata Balaji. *An Introduction to Families, Deformations and Moduli*. Universitatsverlag Gottingen, 2010.

[2] B. Brown, N.J. Calkin, T.B. Flowers, K. James, E. Smith, and A. Stout. Elliptic curves, modular forms, and sums of Hurwitz class numbers. J. Number Theory. **128**, 1847-1863 (2008).

[3] K. Bringmann, B. Kane. Sums of class numbers and mixed mock modular forms. arXiv:1305.0112, to appear in Math. Proc. Cambridge Philos. Soc. (2013).

[4] N.A. Carella. Topics in Elliptic Curve Cryptography. `http://arxiv.org/pdf/1103.4560.pdf`.

[5] W. Castryck and H. Hubrechts. The distribution of the number of points modulo an integer on elliptic curves over finite fields. The Ramanujan Journal, **30** (2), 223-242.

[6] V. Chandee, C. David, D. Koukoulopoulos, and E. Smith. The frequency of elliptic curve groups over prime finite fields. Available at `http://www.dms.umontreal.ca/~koukoulo/documents/publications/CDKS2.pdf`.

[7] P. Deligne. La conjecture de Weil, I. Pub. Math. I.H.E.S **43**, 273-307 (1974).

[8] P. Deligne. La conjecture de Weil, II. Pub. Math. I.H.E.S **56**, 137-252 (1980).

[9] P. Deligne and M. Rapoport. Schémas de modules de courbes elliptiques. In *Modular Functions of One Variable II*. Lectures Notes in Mathematics **349**, Springer-Verlag, New York, 1973.

[10] F. Diamond and J. Shurman. *A first course in modular forms*. Graduate Texts in Mathematics **228**, Springer-Verlag, New York, 2005.

[11] J. Fuselier. Hypergeometric functions over finite fields and relations to modular forms and elliptic curves. Ph.D. thesis, Texas A&M University, 2007.

[12] T. Gannon. *Moonshine Beyond the Monster: The Bridge Connecting Algebra, Modular Forms and Physics*. Cambridge University Press, Cambridge, 2006.

[13] S. Galbraith and J. McKee. The probability that the number of points on an elliptic curve is prime. J. London Math. Soc. (2) **62** N°3 (2000), 671-684.

[14] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer Professional Computing, Springer-Verlag, New York, 2004.

[15] D. Husemöller. *Elliptic Curves*, second Edition. Graduate Texts in Mathematics **111**, Springer-Verlag, New York, 2003.

[16] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*. Annals of Mathematics Studies **108**, Princeton University Press, Princeton, NJ, 1985.

[17] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Graduate Texts in Mathematics **97**, Springer-Verlag, New York, 1993.

[18] A. Knapp. *Elliptic Curves*. Mathematical Notes **40**, Princeton University Press, Princeton, NJ, 1992.

[19] G. Lachaud. Ramanujan modular forms and the Klein quartic. Mosc. Math. J., **5** (4), 829856, 972973 (2005).

[20] S. Lang. *Algebra*, third edition. Addison-Wesley, 1983.

[21] H. W. Lenstra, Jr. Factoring integers with elliptic curves. Ann. Math. **126**, 649-673, 1987.

[22] The LMFDB Collaboration, The L-functions and Modular Forms Database, `http://www.lmfdb.org`, 2015, [Online; accessed 27 August 2015].

[23] B. Mazur. Finding meaning in error terms. Bull. Am. Math. Soc. **45**, 185-228 (2008).

[24] H. McKean and V. Moll. *Elliptic Curves*. Cambridge University Press, Cambridge, 1997.

[25] A. Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, Boston, 1993.

[26] C. Moreno. *Algebraic Curves over Finite Fields*. Cambridge Tracts in Math. **97**, Cambridge University Press, Cambridge, 1991.

[27] L. D. Olson. The trace of Frobenius for elliptic curves with complex multiplication. Lecture Notes in Mathematics **732**, 454-476. Springer-Verlag, New York, 1979.

[28] B. Tran, M. Trinh and P. Wertheimer. *On the distribution of traces of Frobenius of rational elliptic curves*. 2012 Clemson University REU Report, available at `http://www.math.clemson.edu/~kevja/REU/2012/2012ClemsonREUReport_Tran-Trinh-Wertheimer.pdf`.

[29] M.A. Tsfasman, S.G. Vlădut, and D. Nogin. *Algebraic geometry codes: basic notions*. American Mathematical Society, Providence, RI, 2007.

[30] M.A. Tsfasman and S.G. Vlădut. *Algebraic-Geometric Codes*. Kluwer Academic Publishers, Dordrecht, 1991.

[31] A. van Tuyl. The Field of N-Torsion Points of an Elliptic Curve over a Finite Field. M. Sc. Thesis, McMaster University, 1997.

[32] R. Schoof. Nonsingular plane cubic curves over finite fields. J. Combin. Theory, A **46** (2), 183-211 (1987).

[33] J. Silverman. *The arithmetic of elliptic curves*. Graduate Texts in Mathematics **106**. Springer-Verlag, New York, 1986.

[34] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publ. Math. Soc. Japan, No. 11, Iwanami Shoten and Princeton University Press, 1971.

[35] L. C. Washington. *Elliptic curves: number theory and cryptography*, second edition. Chapman & Hall/CRC, London/West Palm Beach, 2008.

[36] E. Waterhouse. Abelian varieties over finite fields. Ann. Sc. Ec. Norm. Sup. **2**, 521-560 (1969).