Average Cyclicity for Elliptic Curves in Torsion Families

Luke Fredericks
January 18, 2021

Abstract

We prove asymptotic formulas for cyclicity of reductions of elliptic curves over the rationals in a family of curves having specified torsion. These results agree with established conditional results and with average results taken over larger families. As a key tool, we prove an analogue of a result of Vlăduţ that estimates the number of elliptic curves over a finite field with a specified torsion point and cyclic group structure.

1 Introduction

Let $E$ be an elliptic curve over $\mathbb{Q}$. Then $E$ is defined by a Weierstrass equation

$$E : y^2 + a_1 xy + a_3 y^2 = x^3 + a_2 x^2 + a_4 x + a_6, \ a_i \in \mathbb{Q}.$$  

By an admissible changes of variable and after clearing denominators, $E$ can be given by a short Weierstrass equation

$$E_{(a,b)} : y^2 = x^3 + ax + b, \ a, b \in \mathbb{Z}.$$  

It is well-known that given an elliptic curve $E$ over a field $K$, the set $E(K)$ of $K$-rational points of $E$ has the structure of an abelian group. When $K$ is a number field, the Mordell-Weil theorem says that $E(K)$ is finitely generated, and Mazur’s torsion theorem classifies the possibilities for $E(\mathbb{Q})_{\text{tors}}$. If $K = \mathbb{F}_q$ is the finite field of $q$ elements, then $E(\mathbb{F}_q)$ is a finite abelian group of rank at most 2; that is,

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z} \text{ where } n_2 \mid n_1.$$  

Denote by $a_q(E) = \#E(\mathbb{F}_q) - q - 1$; then the Hasse bound states that $|a_q(E)| \leq 2\sqrt{q}$.

For all but finitely many primes $p$, we obtain an elliptic curve $E_p/\mathbb{F}_p$ by reducing the coefficients of a Weierstrass model of $E$ modulo $p$. It is natural to ask how how the properties of $E_p$ vary with $p$. Given $E/\mathbb{Q}$, denote by

$$\pi^t_E(x) = \#\{p \leq x : a_p(E) = t\}$$
\[ \pi^c_E(x) = \#\{p \leq x : E_p(\mathbb{F}_p) \text{ is cyclic}\}. \]

The asymptotic growth of these functions are the subjects of the Lang-Trotter conjecture and the cyclicity conjecture, respectively.

**Conjecture 1** (Lang-Trotter). Let \( E/\mathbb{Q} \) be an elliptic curve, and let \( r \in \mathbb{Z} \) with \( r \neq 0 \) if \( E \) has complex multiplication. Then

\[ \pi^r_E(x) \sim C_{E,r} \sqrt{x} \log x, \]

where \( C_{E,r} \) is an explicit constant depending only on \( E \) and \( r \).

Denote by \( \mathbb{Q}(E[k]) \) the field obtained by adjoining to \( \mathbb{Q} \) the coordinates of all points in the \( k \)-torsion subgroup \( E[k] \) of \( E \), and by \( \text{li}(x) \) the logarithmic integral.

**Conjecture 2** (Cyclicity). Let \( E/\mathbb{Q} \) be a non-CM elliptic curve. Then

\[ \pi^c_E(x) \sim \left( \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]} \right) \text{li}(x). \]

The study of \( \pi^c_E \) goes back to the work of Borosh, Moreno and Porta [3] who suggested that for certain chosen examples of \( E/\mathbb{Q} \), \( E_p(\mathbb{F}_p) \) is cyclic for infinitely many \( p \). Serre formulated and proved the cyclicity conjecture conditional on the Generalized Riemann Hypothesis for the division fields of \( E \) [15]. The best result to date is the following conditional theorem of Cojocaru and Murty.

**Theorem 1.** [5, Theorem 1.1] Let \( E \) be a non-CM elliptic curve defined over \( \mathbb{Q} \) of conductor \( N \). Assuming GRH for the Dedekind zeta functions of the division fields of \( E \), we have that

\[ \pi^c_E(x) = \hat{f}_E \text{li}(x) + O_N \left( x^{5/6} (\log x)^{2/3} \right) \]

where

\[ \hat{f}_E = \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]} \]

Unconditionally, we cannot prove that the asymptotic in (1) or (2) holds for a single elliptic curve \( E \). However, starting with the work of Fouvry and Murty [7], average versions of Conjectures 1 and 2 have been obtained. These average results provide strong unconditional evidence for the corresponding conjectures.

Let

\[ \pi_{1/2}(X) = \int_2^X \frac{dt}{2\sqrt{t} \log t} \sim \frac{\sqrt{X}}{\log X}. \]

In the case of the Lang-Trotter conjecture we have
Theorem 2. [6, Corollary 1.3] Let \( E(a, b) : y^2 = x^3 + ax + b \), and let \( \epsilon > 0 \). If \( A, B > X^{1+\epsilon} \) then we have as \( X \to \infty \)

\[
\frac{1}{4AB} \sum_{|a| \leq A \atop |b| \leq B} \pi_{E(a,b)}^r(X) \sim D_r \pi_{1/2}(X) \tag{6}
\]

where

\[
D_r = \frac{2}{\pi} \prod_{\ell \mid r} \frac{\ell(\ell^2 - \ell - 1)}{(\ell + 1)(\ell - 1)^2} \prod_{\ell \not| r} \frac{\ell^2}{\ell^2 - 1} \tag{7}
\]

Here and throughout the paper, \( \ell \) denotes a prime number, and a product over \( \ell \) is taken over all primes satisfying the given conditions.

In the case of the cyclicity conjecture, Banks and Shparlinski proved

Theorem 3. [1, Theorem 17] Let \( \epsilon > 0 \) and \( K > 0 \) be fixed. Then, for all integers \( A \) and \( B \) satisfying \( AB \geq x^{1+\epsilon} \), \( A, B \leq x^{1-\epsilon} \), we have

\[
\frac{1}{4AB} \sum_{|a| \leq A \atop |b| \leq B} \pi_{cyc}^E(a,b)(x) = C_{\text{cyc}} \pi(x) + O(\pi(x)/(\log x)^K),
\]

where

\[
C_{\text{cyc}} = \prod_{\ell \text{ prime}} \left( 1 - \frac{1}{\ell(\ell - 1)(\ell^2 - 1)} \right),
\]

and the constant implied by \( O \) depends only on \( \epsilon \) and \( K \).

The average asymptotics described above provide strong evidence for the conjectures in each case. In particular, the constants \( f_E \) and \( C_{\text{cyc}} \) and \( C_{E,r} \) and \( D_r \) are clearly closely related. We view \( C_{\text{cyc}} \) and \( D_r \) as idealized constants where the variation of individual curves are averaged out. Furthermore, Jones [11] proved that the average of the constants predicted by the respective conjectures is indeed the constant seen in the average results.

Jones proof leveraged the fact (also due to Jones) that almost all elliptic curves are what are known as Serre curves [12]. However, there are interesting families which consist entirely of elliptic curves that are not Serre curves. These curves are essentially invisible in the prior average results cited above; it is therefore of interest to study the averages of the functions \( \pi^t_E \) and \( \pi_{\text{cyc}}^E \) as \( E \) varies over such a family.

One class of such families are the torsion families – the family of elliptic curves some specified torsion structure. It follows from Mazur’s theorem that if \( E \) has a point of order \( m \geq 2 \), then \( m \in \{ 2, 3, 4, 5, 6, 7, 8, 9, 10, 12 \} \). The elliptic curves \( E/\mathbb{Q} \) that have a rational point of order \( m \geq 4 \) lie in a one-parameter family; these were obtained by Kubert [14] and are given in Table 1.
Table 1: Parameterizations for elliptic curves with $m$-torsion.

| $m$ | $E_m(a)$ |
|-----|----------|
| 4   | $y^2 + xy - ay = x^3 - ax^2$ |
| 5   | $y^2 + (1 - a) xy - ay = x^3 - ax^2$ |
| 6   | $y^2 + (1 - a) xy - (a^2 + a) y = x^3 - (a^2 + a)x^2$ |
| 7   | $y^2 + (1 + a - a^2) xy + (a^2 - a^3) y = x^3 + (a^2 - a^3)x^2$ |
| 8   | $y^2 + \left(\frac{-2a^5 + 3a^4 - a^3}{a^3 - 3a^2 + 3a - 1}\right) xy + \left(\frac{-2a^5 + 3a^4 - a^3}{a^4 - 6a^3 + 11a^2 - 6a + 1}\right) y$ $= x^3 + \left(\frac{-2a^5 + 3a^4 - a^3}{a^4 - 6a^3 + 11a^2 - 6a + 1}\right) x^2$ |
| 9   | $y^2 + (1 + a^2 - a^3) xy + (a^2 - 2a^3 + 2a^4 - a^5) y = x^3 + (a^2 - 2a^3 + 2a^4 - a^5)x^2$ |
| 10  | $y^2 + \left(\frac{2a^3 - 2a^2 - 2a + 1}{a^3 - 2a^2 + 3a - 1}\right) xy + \left(\frac{-2a^5 + 3a^4 - a^3}{a^4 - 6a^3 + 11a^2 - 6a + 1}\right) y$ $= x^3 + \left(\frac{-2a^5 + 3a^4 - a^3}{a^4 - 6a^3 + 11a^2 - 6a + 1}\right) x^2$ |
| 12  | $y^2 + \left(\frac{6a^4 - 8a^3 + 2a^2 + 2a - 1}{a^3 - 2a^2 + 3a - 1}\right) xy + \left(\frac{-12a^6 + 30a^5 - 34a^4 + 21a^3 - 7a^2 + a}{a^4 - 4a^3 + 6a^2 - 4a + 1}\right) y$ $= x^3 + \left(\frac{-12a^6 + 30a^5 - 34a^4 + 21a^3 - 7a^2 + a}{a^4 - 4a^3 + 6a^2 - 4a + 1}\right) x^2$ |

The discriminant $\Delta_m(a)$ of the curve with $m$-torsion given above is

- $\Delta_4(a) = (16a + 1)a^4$
- $\Delta_5(a) = a^5(a^2 - 11a - 1)$
- $\Delta_6(a) = (9a + 1)(a + 1)^3a^6$
- $\Delta_7(a) = (a - 1)^7a^7(a^3 - 8a^2 + 5a + 1)$
- $\Delta_8(a) = a^{-4}(2a - 1)^4(a - 1)^8(8a^2 - 8a + 1)$
- $\Delta_9(a) = (a - 1)^9a^9(a^2 - a + 1)^3(a^3 - 6a^2 + 3a + 1)$
- $\Delta_{10}(a) = (2a - 1)^5(a - 1)^{10}(a^2 - 3a + 1)^{-10}(4a^2 - 2a - 1)$
- $\Delta_{12}(a) = (a - 1)^{-24}(2a - 1)^6a^{12}(6a^2 - 6a + 1)(2a^2 - 2a + 1)^3(3a^2 - 3a + 1)^4$.

James [10] gave the first results in this direction when he obtained an asymptotic for the Lang-Trotter conjecture on average over the family of curves with a point of order 3. Battista, Bayless, Ivnaov, and James [2] extended this investigation over the family of elliptic curves which possess a $\mathbb{Q}$-rational point of order $m$ for $m = 5, 7$ or 9. They prove

**Theorem 4.** [2] Let $E_m(a)$ be the parameterization of elliptic curves which have a rational point of order $m \in \{5, 7, 9\}$. Then for any $c > 0$, we have

$$\frac{1}{\mathcal{C}(N)} \sum_{|a| \leq N}^\prime \pi_{E_m(a)}(X) = \frac{2}{\pi} C_{r,m} \pi_{1/2}(X) + O \left(\frac{X^{3/2}}{N} + \frac{\sqrt{X}}{\log^c X}\right),$$

where $\sum^\prime$ represents the sum over non-singular curves, $\mathcal{C}(N)$ represents the number of curves
in the sum, and

\[ C_{r,m} = C_r(m) \prod_{\ell \mid m} \ell \left( \frac{\ell}{\ell + 1} \right) \prod_{\ell \nmid m} \left( \frac{\ell^2}{\ell^2 - 1} \right), \]

where

\[ C_r(m) = \begin{cases} 
5/4 & \text{if } m = 5 \text{ and } r \equiv 0, 3, 4 \pmod{5}, \\
7/6 & \text{if } m = 7 \text{ and } r \equiv 0, 3, 4, 5, 6 \pmod{7}, \\
3/2 & \text{if } m = 9 \text{ and } r \equiv 0, 3, 6 \pmod{9}.
\]

The main result in this paper is to establish an average cyclicity result over torsion families of elliptic curves. More precisely, we prove

**Theorem 5.** Let \( \epsilon > 0 \), \( A > x^{1+\epsilon} \). Let \( E_m(a) \) denote the parameterization of elliptic curves over \( \mathbb{Q} \) which have a rational \( m \)-torsion point for \( m \neq 2, 3 \). Then

\[ \frac{1}{2A} \sum_{|a| \leq A} \pi_{cyc}(E_m(a))(x) = C_m \prod_{\ell \mid m} \left( 1 - \frac{1}{\ell(\ell - 1)(\ell^2 - 1)} \right) \pi(x) + O \left( \frac{x^{1-\epsilon}}{\log x} \right) \]

where \( C_m \) summarized in Table 2.

| \( m \) | \( 4 \) | \( 5 \) | \( 6 \) | \( 7 \) | \( 8 \) | \( 9 \) | \( 10 \) | \( 12 \) |
|---|---|---|---|---|---|---|---|---|
| \( C_m \) | \( \frac{1}{2} \) | \( \frac{10}{20} \) | \( \frac{3}{12} \) | \( \frac{31}{42} \) | \( \frac{1}{2} \) | \( \frac{3}{6} \) | \( \frac{19}{30} \) | \( \frac{3}{12} \) |

Table 2:

**Remark 1.** The effect of the presence of \( m \)-torsion is apparent; we interpret the constant \( C_{cyc} \) as a product of local factors, each of which is the probability that \( E_p \) has cyclic \( \ell \)-torsion. The presence of a point of order \( m \) should have some influence on these probabilities for \( \ell \mid m \). Indeed, a curve with a point of order \( \ell \) over \( \mathbb{Q} \) need only acquire a single linearly independent point of order \( \ell \) for cyclicity of the reduction to fail. Compared to the generic case of a curve without a point of order \( \ell \), we expect it to be much less likely that the reductions of these curves are cyclic. Our result quantifies this heuristic reasoning.

**Remark 2.** The family of curves with a point of order \( m \) for \( m = 4 \) or 8 includes curves with full 2-torsion. Since the torsion points of \( E(\mathbb{Q}) \) injects into \( E_p(\mathbb{F}_p) \), the reductions of these curves never have cyclic group of \( \mathbb{F}_p \)-rational points. It would be interesting to obtain a similar result where the average is taken only over curves with cyclic 2-torsion. Furthermore, we note that we have not treated all torsion families; instead we have focused on curves in one-parameter families. The two-parameter families (curves with 2-torsion or 3-torsion points) will be the subject of future work.
Remark 3. The proof broadly follows the steps of [11]; however, we note that an important feature of that work was the use of character sums to reduce the size of the family over which the average is taken. The torsion families over which we average in the current paper are each a one-parameter family, and it is unclear how to adapt the character sum estimates to this context. Consequently, we average over curves in a larger family than we would prefer. Reducing the size of the family will be the subject of subsequent work.

A key ingredient for the argument in [1] was the fixed-field count of Vlăduţ [17] which, for a finite field of \( q \) elements, estimates the number of \( E/\mathbb{F}_q \) which have cyclic group structure. Our proof requires the following analogous fixed field count which takes into account the additional torsion data.

It is frequently convenient to express counts of elliptic curves over finite fields as weighted cardinalities where we weight each curve by the size of its automorphism group. We indicate weighted cardinalities by \( \#$' \).

For a prime number \( \ell \), denote by \( v_\ell(n) \) the \( \ell \)-adic valuation of \( n \). Concretely, any positive integer \( n \) can be written \( n = \ell^e m \) where \( \ell \nmid m \). Then \( v_\ell(n) = e \).

Theorem 6. Denote by

\[ C_q(m) = \{ E/\mathbb{F}_q : E(\mathbb{F}_q) \text{ is cyclic and contains a point of order } m \}/\sim_{\mathbb{F}_q}. \]

Then

\[
\#C_q(m) = q \prod_{\ell|m} \frac{1}{\ell^v_\ell(m)} \prod_{\ell|m \mid q \not\equiv 1 \pmod{\ell}} \frac{1}{\varphi(v_\ell(m))} \prod_{\ell|m \mid q \equiv 1 \pmod{\ell}} (1 - \frac{1}{\ell(\ell^2 - 1)}) + O(q^{1/2}).
\]

The structure of this paper is as follows. In Section 2, we give the proof of Theorem 6. In Section 3, we describe the isomorphism classes of \( E/\mathbb{F}_p \) in the torsion families described above. In Section 4, we give the proof of Theorem 5.

2 Fixed Field Counts

There has been significant recent interest in counting problems for elliptic curves over a fixed finite field \( \mathbb{F}_q \) with specified conditions on their group of \( \mathbb{F}_q \)-rational points. See for example Howe, [8], Vlăduţ [17], Castryck and Hubrechts [11] and Kaplan and Petrow [13].

Our goal is to generalize Vlăduţ’s result giving the number of elliptic curves \( E/\mathbb{F}_q \) such that \( E(\mathbb{F}_q) \) is cyclic to obtain a count of the number of \( E/\mathbb{F}_q \) such that for some fixed \( m \in \mathbb{Z} \), \( E(\mathbb{F}_q) \) has a point of order \( m \) and is cyclic. We begin by recalling the various fixed field counts we will require.

Denote by \( \varphi \) the Euler totient function, and define \( \psi(n) = n \prod_{l|n} (1 + 1/l) \). For \( a | b \), denote by \( W(a,b) = \{ E/\mathbb{F}_q : E[b](\mathbb{F}_q) \cong (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}) \}/\sim_{\mathbb{F}_q} \). Estimates for the size of \( W(a,b) \) are given by Howe [8]. Howe shows that

\[ |\#W(a,b) - \hat{w}(a,b)| < Cq^{1/2} \]
for an explicit constant $C$ where
\[ \hat{w}(a, b) = \frac{g \psi(b/a)}{a \varphi(b) \psi(b)} \prod_{l \text{ prime}} \left( 1 - \frac{1}{l} \right). \]

It will be convenient to define $\check{w}(a, b) = \hat{w}(a, b)/q$. Howe notes that $\check{w}(a, b)$ is a multiplicative function of both arguments simultaneously.

Vlăduţ observes the 'obvious' cyclicity condition: $E(\mathbb{F}_q)$ is cyclic if and only if for any prime $l \mid q - 1$, $E \not\in W(l, l)$. Assuming that our curve $E$ has a point of order $m$, we observe that $E(\mathbb{F}_q)$ is cyclic if and only if for all $l \mid q - 1$,
\[
\begin{cases}
E \not\in W(l, m) & \text{(in the case where } l \mid m),
E \not\in W(l, lm) & \text{(in the case where } l \nmid m).
\end{cases}
\]

For $q = p^n$, define $r'_q(m)$ by the following conditions:

(a) $r'_q$ is multiplicative.

(b) For $l$ prime, $l \neq p$, we have
\[
r'_q(p^n) = \begin{cases}
1/(l^n - l^{n-2}) & \text{if } v \geq n,
(l^{2v+1} + 1)/(l^{n+2v-1}(l^2 - 1)) & \text{if } v < n,
\end{cases}
\]
where $v = v_l(q - 1)$.

(c) $r'_q(p^e) = 1/(p^e - p^{e-1})$.

Denote by $T_q(m) = \{E/\mathbb{F}_q : E \text{ has a point of order } m\}/\sim_{\mathbb{F}_q}$. It follows from Theorem 3 of [4] that
\[
| #T_q(m) - qr'_q(m) | \leq Cm^2 \log \log(m)q^{1/2}
\]
for an absolute and explicitly computable $C \in \mathbb{R}_{>0}$.

Applying these estimates and the inclusion/exclusion principle, we obtain the estimate
\[
#C_q(m) = qr'_q(m) - \sum_{d|m, d > 1} \hat{w}(d, m) + \sum_{t|(q-1)} \mu(t) \hat{w}(t, mt) + O \left(q^{1/2}\right). \tag{8}
\]

Note that we have
\[
\hat{w}(1, m) = \prod_{l|m} \hat{w}(1, l^{v_l(m)}) = \prod_{l|m} \frac{1}{\varphi(l^{v_l(m)})} \prod_{l|m} \frac{1}{l^{v_l(m)}}.
\]
Equating the right hand side of (8) to the right hand side of the equation in Theorem 6 and dividing through by \( q \), we see that it is sufficient to show that

\[
 r'_q(m) - \sum_{d|m, \ d > 1} \tilde{w}(d, m) + \sum_{t | q - 1 \text{ gcd}(t, m) = 1} \mu(t)\tilde{w}(t, mt) = \tilde{w}(1, m) \prod_{t | q - 1 \text{ gcd}(t, m) = 1} \left(1 - \frac{1}{\ell(t^2 - 1)}\right) + O\left(q^{-1/2}\right).
\]

Furthermore, since \( \tilde{w}(t, mt) = \tilde{w}(t, t)\tilde{w}(1, m) \) for \( t \) relatively prime to \( m \), it suffices to show that

\[
 r'_q(m) = \sum_{d|m} \tilde{w}(d, m).
\]

Indeed, in this case, we have

\[
 C_q(m) = qr'_q(m) - \sum_{d|m, \ d > 1} \tilde{w}(d, m) + \sum_{t | q - 1 \text{ gcd}(t, m) = 1} \mu(t)\tilde{w}(t, mt) + O(q^{1/2})
\]

\[
 = qr'_q(m) - q \sum_{d|m, \ d > 1} \tilde{w}(d, m) + q \sum_{t | q - 1 \text{ gcd}(t, m) = 1} \mu(t)\tilde{w}(t, t)\tilde{w}(1, m) + O(q^{1/2})
\]

\[
 = q\tilde{w}(1, m) \left(1 + \sum_{t | q - 1 \text{ gcd}(t, m) = 1} \frac{\mu t}{t\varphi(t)\psi(t)}\right) + O(q^{1/2})
\]

\[
 = q \prod_{v|\varphi(lv(m))} \frac{1}{\varphi(lv(m))} \prod_{v|\psi(lv(m))} \frac{1}{\psi(lv(m))} \prod_{v | q - 1 \text{ gcd}(m, l) = 1} \left(1 - \frac{1}{l(l^2 - 1)}\right) + O(q^{1/2}).
\]

We will prove (9) by induction on the number of prime factors of \( m \). The following lemma provides the base of induction.

**Lemma 1.** Denote by \( v \) the \( \ell \)-adic valuation of \( q - 1 \). Then

\[
 r'_q(\ell^e) = \sum_{k=0}^{t} \tilde{w}(\ell^k, \ell^e) \quad (10)
\]

where

\[
t = \begin{cases} v & \text{if } v < e \\ e & \text{if } v \geq e. \end{cases}
\]

**Proof.** Suppose that \( v = 0 \). Then

\[
 \sum_{k=0}^{v} \tilde{w}(\ell^k, \ell^e) = \tilde{w}(1, \ell^e) = \frac{\psi(\ell^e)}{\varphi(\ell^e)} = r'_q(\ell^e).
\]
Now suppose that $0 < v < e$. Then we have

$$\sum_{k=0}^{v} \tilde{w}(\ell^k, \ell^e) = \frac{\psi(\ell^{e-v})}{\ell^v \varphi(\ell^e) \psi(\ell^e)} + \sum_{k=0}^{v-1} \frac{\psi(\ell^{e-k})(\ell - 1)}{\ell^{k+1} \varphi(\ell^e) \psi(\ell^e)}$$

$$= \frac{\ell^{e-v-1}(\ell + 1)}{\ell^v \varphi(\ell^e) \psi(\ell^e)} + \sum_{k=0}^{v-1} \frac{\ell^{e-k-1}(\ell^2 - 1)}{\ell^{k+1} \varphi(\ell^e) \psi(\ell^e)}$$

$$= \frac{1}{\ell^e \varphi(\ell^e) \psi(\ell^e)} \left( \ell^{2e-2v} + \ell^{2e-2v-1} + \sum_{k=0}^{v-1} (\ell^{2e-2k} - \ell^{2e-2k-2}) \right).$$

The sum above telescopes to $\ell^{2e} - \ell^{2e-2v}$, and we are left with

$$\frac{\ell^{2e} + \ell^{2e-2v-1}}{\ell^e \varphi(\ell^e) \psi(\ell^e)} = \frac{\ell^{2e-2v-1}(\ell^{2v+1} + 1)}{\ell^{3e-2}(\ell^2 - 1)}$$

$$= \frac{\ell^{2v+1} + 1}{\ell^{2v-1}(\ell^2 - 1)} = r'_q(\ell^e),$$

as needed.

Finally, suppose $v \geq e$. we have

$$\sum_{k=0}^{e} \tilde{w}(\ell^k, \ell^e) = \frac{1}{\ell^e \varphi(\ell^e) \psi(\ell^e)} + \sum_{k=0}^{e-1} \frac{\psi(\ell^{e-k})(\ell - 1)}{\ell^{k+1} \varphi(\ell^e) \psi(\ell^e)}$$

$$= \frac{1}{\ell^e \varphi(\ell^e) \psi(\ell^e)} + \sum_{k=0}^{e-1} \frac{\ell^{e-k-1}(\ell^2 - 1)}{\ell^{k+1} \varphi(\ell^e) \psi(\ell^e)}$$

$$= \frac{1}{\ell^e \varphi(\ell^e) \psi(\ell^e)} \left( 1 + \sum_{k=0}^{e-1} (\ell^{2e-2k} - \ell^{2e-2k-2}) \right).$$

As above, this sum telescopes, leaving $\ell^{2e} - 1$. We are left with

$$\frac{\ell^{2e}}{\ell^e \varphi(\ell^e) \psi(\ell^e)} = \frac{\ell^{2e}}{\ell^{3e-2}(\ell^2 - 1)} = \frac{1}{\ell^e - \ell^{e-2}} = r'_q(\ell^e).$$

\[ \Box \]

**Proof of Theorem** Assume for induction that for some $m > 1$ we have

$$r'_q(m) = \sum_{d|m} \tilde{w}(d, m).$$

Let $\ell$ be a prime that does not divide $m$ and let $e \geq 1$. Let $t$ be as in the statement of Lemma. We have
\[
\sum_{d|\ell^e} \tilde{w}(d, m\ell^e) = \sum_{k=0}^{t} \sum_{d|m} \tilde{w}(\ell^k d, \ell^e m) = \sum_{k=0}^{t} \tilde{w}(\ell^k, \ell^e) \sum_{d|m} \tilde{w}(d, m) = r'_q(\ell^e) r'_q(m) = r'_q(\ell^e m)
\]

by Lemma \(\text{II}\) and the induction hypothesis.

\[\square\]

### 3 Isomorphisms of \(m\)-torsion Curves

The parameterizations given in Table \(\text{I}\) were derived by Kubert by studying the modular curve \(X_1(m)\). A point of \(X_1(m)\) corresponds to an elliptic curve \(E\) together with a point of order \(m\) up to action by automorphisms of \(E\). For example, if \((E, P)\) represents a point of \(X_1(m)\) and \(#\text{Aut}(E) = 2\), then \((E, -P)\) represents the same point. We will be concerned with which parameter values yield isomorphic curves over \(\mathbb{F}_q\) where \(q = p^n\) and \(p > 3\). With at most 10 exceptions, an isomorphism class of elliptic curves over \(\mathbb{F}_q\) consists of curves whose automorphism group has cardinality 2. If \(#\text{Aut}(E) = 2\) and \(E\) has cyclic \(m\)-torsion, then there are \(\phi(m)/2\) parameters in \(\mathbb{F}_q\) that yield an isomorphic curve. These correspond to the \(\phi(m)\) points of order \(m\) on \(E_m(a)\), up to the action of \(\text{Aut}(E_m(a))\).

If \(#\text{Aut}(E) > 2\), the number of parameters yielding an isomorphic curve will vary depending on the size of the automorphism group and the number of \(m\)-torsion points of \(E\); in general, the number of parameters which yield an isomorphic curve will not be \(\phi(m)/2\). However, these \(O(1)\) isomorphism classes can be absorbed into the ‘unweighted’ version of Theorem \(6\).

**Corollary 1** (to Theorem \(6\)).

\[
C_q(m) = 2q \prod_{\ell|m} \frac{1}{\ell^{\nu(m)}} \prod_{q \equiv 1 \pmod{\ell}} \frac{1}{\varphi(\ell^{\nu(m)})} \prod_{q \equiv 1 \pmod{\ell}} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) + O(q^{1/2}).
\]

**Proof.** Denote by \(C_q(m, n) = \{E \in C_q(m): \#\text{Aut}(E) = n\}\). Then

\[
C_q(m) = C_q(m, 2) + C_q(m, 4) + C_q(m, 6).
\]

We then have

\[
\#C_q(m, 2)/2 = \#C_q(m) - \#C_q(m, 4)/4\#C_q(m, 6)/6.
\]

Multiplying by 2 and observing that \(\#C_q(m, 4)/2 + \#C_q(m, 6)/3 = O(1)\), we have

\[
\#C_q(m, 2) = 2q \prod_{\ell|m} \frac{1}{\ell^{\nu(m)}} \prod_{q \equiv 1 \pmod{\ell}} \frac{1}{\varphi(\ell^{\nu(m)})} \prod_{q \equiv 1 \pmod{\ell}} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) + O(q^{1/2})
\]

as required. \(\square\)
Given an $m$-torsion curve $E_m(a)$, we can perform a change of variables to obtain a short Weierstrass equation $y^2 = x^3 + Ax + B$. In order for $E_m(a)$ to have more than two automorphisms, the $j$-invariant must be 0 or 1728. In terms of the short Weierstrass equation, this means that $A = 0$ or $B = 0$, respectively. The coefficients $A$ and $B$ will be polynomials or rational functions in the parameter $a$. Since such functions have finitely many zeros, we deduce the following

**Lemma 2.** Each torsion family $E_m(a)$ contains finitely many curves with $j$-invariant 0 or 1728. The parameters which yield curves with these $j$-invariants are roots of a polynomial that depends only on $m$.

Using explicit change of variables, it is possible to specify precisely which parameter values yield isomorphic curves. We summarize this below for curves with $\# \text{Aut}(E) = 2$.

| $m$ | Parameters               |
|-----|--------------------------|
| 4   | $a$                      |
| 5   | $a$ $-a^{-1}$            |
| 6   | $a$                      |
| 7   | $a (1 - a)a^{-1}$ $-(1 - a)^{-1}$ |
| 8   | $a$ $-a + 1$             |
| 9   | $a (a - 1)a^{-1}$ $-(a - 1)^{-1}$ |
| 10  | $a (a - 1)(2a - 1)^{-1}$ |
| 12  | $a$ $-a + 1$             |

Table 3: Parameters yielding isomorphic curves.

### 4 Proof of Theorem 5

The fixed field counts of $E/\mathbb{F}_p$ which have an $m$-torsion point and cyclic group of $\mathbb{F}_p$-points depends on the value of $p$ modulo the prime divisors of $m$. For one-parameter torsion families over $\mathbb{Q}$, we are concerned with $m \in \{4, 5, 6, 7, 8, 9, 10, 12\}$. In this case, $m$ has at most two prime divisors, and if $m$ is not a prime power, then one of its prime factors is 2. Since all odd primes are 1 (mod 2), the number of curves we are counting varies according to the value of $p$ (mod $\ell$) where $\ell$ is the unique odd prime divisor of $m$.

Let $m \in \{4, 5, 6, 7, 8, 9, 10, 12\}$, and denote by

$$\mathcal{E}_m(A) = \{E_m(a) : -A \leq a \leq A\}$$

the family of elliptic curves over $\mathbb{Q}$ with an $m$-torsion point given above. Write the prime factorization of $m$ as $m = 2^k\ell_0^n$ where we take $n = \ell_0 = 1$ if $m$ is a power of 2. Let $A \geq x^{1+\epsilon}$ for $x, \epsilon \geq 0$. 

11
We have
\[ \sum_{|a| \leq A} \pi^{\text{cyc}}_{E_m(a)}(x) = \sum_{p \leq x} \sum_{\substack{b \in \mathbb{F}_p \\ E_m(b) \neq 0}} \# \{ a \in [-A, A] : E_m(a)_p \cong E_m(b) \}. \]

There are \(2A/p + O(1)\) values of \(a\) which yield a particular Weierstrass model modulo \(p\). Thus the expression above becomes

\[
\sum_{p \leq x} \left( \frac{2A}{p} + O(1) \right) \left( \frac{\varphi(m)}{2} \sum_{\substack{b \in \mathbb{F}_p \\ \Delta_m(b) \neq 0 \text{ cyclic} \atop \# \text{ Aut}(E_m(b)) = 2}} 1 + \frac{\varphi(m)}{4} \sum_{\substack{b \in \mathbb{F}_p \\ \Delta_m(b) \neq 0 \text{ cyclic} \atop \# \text{ Aut}(E_m(b)) = 4}} 1 + \frac{\varphi(m)}{6} \sum_{\substack{b \in \mathbb{F}_p \\ \Delta_m(b) \neq 0 \text{ cyclic} \atop \# \text{ Aut}(E_m(b)) = 6}} 1 \right). \]

Applying the estimate obtained in Corollary 1 and Lemma 2, this is equal to

\[
\sum_{p \leq x} \left( \frac{2A}{p} + O(1) \right) \left( \frac{\varphi(m)}{2} \sum_{\substack{b \in \mathbb{F}_p \\ \Delta_m(b) \neq 0 \text{ cyclic} \atop \# \text{ Aut}(E_m(b)) = 2}} \frac{2p}{m} \prod_{\ell \mid p-1, \gcd(\ell, m) = 1} \left( 1 - \frac{1}{\ell^2} \right) + O(p^{1/2}) \right) + \sum_{p \leq x} \left( \frac{2A}{p} + O(1) \right) \left( \frac{\varphi(m)}{2} \frac{2p}{\varphi(p_{0}^m)} \prod_{\ell \mid p-1, \gcd(\ell, m) = 1} \left( 1 - \frac{1}{\ell^2} \right) + O(p^{1/2}) \right). \]

Simplifying and applying the trivial estimate

\[
\frac{\varphi(m)p}{2^k \varphi(p_{0}^m)} \prod_{\ell \mid p-1, \gcd(\ell, m) = 1} \left( 1 - \frac{1}{\ell^2} \right) < p,
\]

we have

\[
\sum_{p \leq x} \frac{2A \varphi(m)}{m} \prod_{\ell \mid p-1, \gcd(\ell, m) = 1} \left( 1 - \frac{1}{\ell^2} \right) + \sum_{p \not\equiv 1 (\text{mod } \ell_0)} \frac{2A \varphi(m)}{2^k \varphi(p_{0}^m)} \prod_{\ell \mid p-1} \left( 1 - \frac{1}{\ell^2} \right) + O \left( \sum_{p \leq x} p \right). \tag{11}
\]

Note that according to Lemma 3.4 of [16], we have

\[
\sum_{p \leq x} p = O \left( \frac{x^2}{2 \log x} \right).
\]
We analyze these two sums individually following [1]. A main input to this analysis is a theorem on averages of multiplicative functions due to [9, Theorem 3].

Assume first that \( m \) is not a power of 2, so that \( \ell_0 > 1 \). For any integer \( n \), define

\[
\chi_{\ell_0}(n) = \begin{cases} 
1 & \text{if } \ell_0 \nmid n \\
0 & \text{if } \ell_0 | n,
\end{cases}
\]

\[
F(n) = \prod_{\ell | n \atop \ell \neq m} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right),
\]

and

\[
F'(n) = \prod_{\ell | n \atop \ell \neq m} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) \chi_{\ell_0 h}(n).
\]

Note that \( \chi_{\ell_0} \) and \( F \) are multiplicative (whence \( F' \) is multiplicative as well). We compute

\[
\sum_{p \leq x} \prod_{\ell | p-1 \atop \ell \neq \ell_0} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right)
= \sum_{p \leq x} \prod_{\ell | p-1 \atop \gcd(\ell, m) = 1} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) - \sum_{p \leq x} \prod_{\ell | p-1 \atop p \not\equiv \ell_0 \pmod{\ell_0} \atop \gcd(\ell, m) = 1} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right)
\]

\[
= \sum_{p \leq x} \prod_{\ell | p-1 \atop \gcd(\ell, m) = 1} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) - \sum_{p \leq x} \prod_{\ell | p-1 \atop \gcd(\ell, m) = 1} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) \chi_{\ell_0}(p - 1)
\]

\[
= \sum_{p \leq x} F(p - 1) + \sum_{p \leq x} F'(p - 1).
\]

Denote by \( G \) and \( G' \) the Dirichlet convolution of the Möbius \( \mu \) function with \( F, F' \), respectively. Explicitly, \( G \) and \( G' \) are multiplicative functions defined on prime powers by

\[
G(\ell^k) = \begin{cases} 
\frac{-1}{\ell(\ell^2 - 1)} & \text{if } \ell \nmid m, k = 1 \\
0 & \text{if } \ell | m, k = 1 \\
0 & \text{if } k > 1,
\end{cases}
\]

and

\[
G'(\ell^k) = \begin{cases} 
\frac{-1}{\ell(\ell^2 - 1)} & \text{if } \ell \nmid m, k = 1 \\
-1 & \text{if } \ell = \ell_0, k = 1 \\
0 & \text{if } \ell = 2 | m, k = 1 \\
0 & \text{if } k > 1.
\end{cases}
\]
Both pairs of functions $F, G$ and $F', G'$ satisfy the hypotheses of [9, Theorem 3]. It follows that

$$\frac{1}{\pi(x)} \sum_{p \leq x} F(p - 1) = \sum_{d=1}^{\infty} \frac{G(d)}{\varphi(d)} + O_B(\log^{-B} x)$$

holds for any $B > 0$, and similarly for $F', G'$. Now we have

$$\sum_{d=1}^{\infty} \frac{G(d)}{\varphi(d)} = \prod_{\ell \parallel m} \left(1 - \frac{1}{\ell(\ell^2 - 1)(\ell - 1)}\right),$$

and

$$\sum_{d=1}^{\infty} \frac{G'(d)}{\varphi(d)} = \frac{\ell_0 - 2}{\ell_0 - 1} \prod_{\ell \parallel m} \left(1 - \frac{1}{\ell(\ell^2 - 1)(\ell - 1)}\right).$$

Thus,

$$\sum_{p \equiv 1 (\text{mod } \ell_0)} \frac{2A\varphi(m)}{m} \prod_{\ell \parallel m, \ell \parallel p-1} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) \pi(x) + O\left(A x \log B + 1\right).$$

Similarly, we write

$$\sum_{p \leq x} \prod_{\ell \parallel p-1} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) = \sum_{p \leq x} \prod_{\ell \parallel p-1} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) \chi_{\ell_0}(p - 1) = \sum_{p \leq x} F'(p - 1)$$

so that, again by [9, Theorem 3], we have

$$\frac{1}{\pi(x)} \sum_{p \leq x} F'(p - 1) = \sum_{d=1}^{\infty} \frac{G'(d)}{\varphi(d)} + O_B(\log^{-B} x)$$

$$= \frac{\ell_0 - 2}{\ell_0 - 1} \prod_{\ell \parallel m, \ell_0} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) + O_B(\log^{-B} x)$$

holds for any $B > 0$. Thus,

$$\sum_{p \equiv 1 (\text{mod } \ell_0)} \frac{2A\varphi(m)}{2k\varphi(\ell_0^n)} \prod_{\ell \parallel p-1} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right)$$

$$= \frac{2A\varphi(m)}{2k\varphi(\ell_0^n)} \frac{\ell_0 - 2}{\ell_0 - 1} \prod_{\ell \parallel m} \left(1 - \frac{1}{\ell(\ell - 1)(\ell^2 - 1)}\right) \pi(x) + O\left(A x \log B + 1\right).$$
Combining (11), (12), and (13), we have
\[ \sum_{|a| \leq A} \pi_{E(a)}^{\text{cyc}}(x) = \left( \frac{2A\varphi(m)}{2^k \varphi(l_0^n) l_0 - 1} + \frac{2A\varphi(m)}{m} \frac{1}{l_0 - 1} \right) \prod_{\ell \mid m} \left( 1 - \frac{1}{\ell(\ell - 1)(\ell^2 - 1)} \right) \pi(x) \]
\[ + O \left( A \frac{x}{\log B + 1} \right) + O \left( \frac{x^2}{2 \log x} \right). \]

If \( m \) is a power of 2, the sum over \( p \not\equiv 1 \pmod{\ell_0} \) is empty. In this case, \( \varphi(m)/m = 1/2 \), and we are left to evaluate
\[ \frac{1}{2} \sum_{p \leq x} \prod_{\ell p - 1 \gcd(\ell, m) = 1} \left( 1 - \frac{1}{\ell(\ell^2 - 1)} \right). \]

An argument analogous to the above shows
\[ \sum_{|a| \leq A} \pi_{E(a)}^{\text{cyc}}(x) = A \prod_{\ell \neq 2} \left( 1 - \frac{1}{\ell(\ell - 1)(\ell^2 - 1)} \right) \pi(x) + O \left( A \frac{x}{\log B + 1} \right) + O \left( \frac{x^2}{2 \log x} \right). \]

Computing
\[ C_m = \left( \frac{2A\varphi(m)}{2^k \varphi(l_0^n) l_0 - 1} + \frac{2A\varphi(m)}{m} \frac{1}{l_0 - 1} \right) \]
for \( m \in \{4, 5, 6, 7, 8, 9, 10, 12\} \), we complete the proof.

References

[1] William D. Banks and Igor E. Shparlinski. Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height. *Israel J. Math.*, 173:253–277, 2009.

[2] Jonathan Battista, Jonathan Bayless, Dmitriy Ivanov, and Kevin James. Average Frobenius distributions for elliptic curves with nontrivial rational torsion. *Acta Arith.*, 119(1):81–91, 2005.

[3] I. Borosh, C. J. Moreno, and H. Porta. Elliptic curves over finite fields. II. *Math. Comput.*, 29:951–964, 1975.

[4] Wouter Castryck and Hendrik Hubrechts. The distribution of the number of points modulo an integer on elliptic curves over finite fields. *Ramanujan J.*, 30(2):223–242, 2013.

[5] Alina Carmen Cojocaru and M. Ram Murty. Cyclicity of elliptic curves modulo \( p \) and elliptic curve analogues of Linnik’s problem. *Math. Ann.*, 330(3):601–625, 2004.
[6] Chantal David and Francesco Pappalardi. Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices*, (4):165–183, 1999.

[7] Etienne Fouvry and M. Ram Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.

[8] Everett W. Howe. On the group orders of elliptic curves over finite fields. *Compositio Math.*, 85(2):229–247, 1993.

[9] K.-H. Indlekofer, S. Wehmeier, and L. G. Lucht. Mean behaviour and distribution properties of multiplicative functions. *Comput. Math. Appl.*, 48(12):1947–1971, 2004.

[10] Kevin James. Average Frobenius distributions for elliptic curves with 3-torsion. *J. Number Theory*, 109(2):278–298, 2004.

[11] Nathan Jones. Averages of elliptic curve constants. *Math. Ann.*, 345(3):685–710, 2009.

[12] Nathan Jones. Almost all elliptic curves are Serre curves. *Trans. Amer. Math. Soc.*, 362(3):1547–1570, 2010.

[13] Nathan Kaplan and Ian Petrow. Elliptic curves over a finite field and the trace formula. *Proc. Lond. Math. Soc. (3)*, 115(6):1317–1372, 2017.

[14] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Compositio Math.*, 38(1):121–128, 1979.

[15] Jean P. Serre. Résumé des cours de 1977-1978. *Annuaire du Collège de France*, 67-70, 1978.

[16] Enrique Treviño. The least inert prime in a real quadratic field. *Math. Comp.*, 81(279):1777–1797, 2012.

[17] S. G. Vlăduț. Cyclicity statistics for elliptic curves over finite fields. *Finite Fields Appl.*, 5(1):13–25, 1999.