

LOCAL TORSION ON ELLIPTIC CURVES AND THE DEFORMATION THEORY OF GALOIS REPRESENTATIONS

CHANTAL DAVID AND TOM WESTON

1. INTRODUCTION

Let E be an elliptic curve over \mathbf{Q} . Our primary goal in this paper is to investigate for how many primes p the elliptic curve E possesses a p -adic point of order p . Simple heuristics suggest the following conjecture.

Conjecture 1.1. *Assume that E does not have complex multiplication. Fix $d \geq 1$. Then there are finitely many primes p such that there exists an extension K/\mathbf{Q}_p of degree at most d with $E(K)[p] \neq 0$.*

We expect this conjecture to be false (for sufficiently large d) when E does have complex multiplication. Nevertheless, our main result is that Conjecture 1.1 at least holds on average. For $A, B > 0$, let $\mathcal{S}_{A,B}$ denote the set of elliptic curves with Weierstrass equations $y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Z}$, $|a| \leq A$ and $|b| \leq B$. For an elliptic curve E and $x > 0$, let $\pi_E^d(x)$ denote the number of primes $p \leq x$ such that E possesses a point of order p over an extension of \mathbf{Q}_p of degree at most d .

Theorem 1.2. *Fix $d \geq 1$. Assume $A, B \geq x^{\frac{7}{4}+\varepsilon}$ for some $\varepsilon > 0$. Then*

$$\frac{1}{\#\mathcal{S}_{A,B}} \sum_{E \in \mathcal{S}_{A,B}} \pi_E^d(x) \ll d^2$$

as $x \rightarrow \infty$.

Our proof is essentially a precise version of the heuristic alluded to above. We explain this heuristic for $d = 1$; in this case we say that a prime p is a *local torsion prime* for E if $E(\mathbf{Q}_p)[p] \neq 0$. One sees easily that for a local torsion prime $p \geq 7$ of good reduction for E one must have $a_p(E) = 1$. By the Riemann hypothesis, $a_p(E)$ lies in an interval of length approximately $4\sqrt{p}$, so that naively one expects $a_p(E) = 1$ to occur with a probability of $\frac{1}{4\sqrt{p}}$. A comparison of the reduction exact sequence with an analysis of extension classes suggests that when $a_p(E) = 1$, p is a local torsion prime with probability $\frac{1}{p}$. Combining these estimates, one expects

$$\sum_p \frac{1}{4\sqrt{p}} \cdot \frac{1}{p} < \infty$$

local torsion primes for E , hence the conjecture.

We especially like this heuristic as each of the two parts sometimes fail. Specifically, for some elliptic curves one has $a_p(E) = 1$ for only finitely many primes; in these cases, the conjecture (for $d = 1$) follows immediately. Furthermore, for CM

The first author was partially supported by a NSERC Individual Research Grant; the second author was supported by NSF grant DMS-0440708.

elliptic curves one finds that $a_p(E) = 1$ in fact forces p to be a local torsion prime; this explains the CM exception in the conjecture.

Although we believe that Conjecture 1.1 is of fundamental and independent interest in the arithmetic of elliptic curves, our motivation for its study originated in questions in the deformation theory of Galois representations. For any prime p let

$$\bar{\rho}_{E,p} : \text{Gal}(\mathbf{Q}_{S \cup \{p\}}/\mathbf{Q}) \rightarrow \text{GL}_2(\mathbf{F}_p)$$

be the Galois representation on the p -torsion points of E ; here $\mathbf{Q}_{S \cup \{p\}}$ is the maximal extension of \mathbf{Q} unramified away from p and the set S of places of bad reduction for E . When $\bar{\rho}_{E,p}$ is absolutely irreducible, one can associate to $\bar{\rho}_{E,p}$ its *universal deformation ring* $R_{E,p}^{\text{univ}}$, parameterizing all lifts of $\bar{\rho}_{E,p}$ to artinian local rings with residue field \mathbf{F}_p . Mazur [10] asked if the deformation theory of $\bar{\rho}_{E,p}$ is *unobstructed* (so that $R_{E,p}^{\text{univ}}$ is non-canonically isomorphic to a power series ring in three variables over \mathbf{Z}_p) for all but finitely many primes p . Using work of Flach [4], he showed that this is the case so long as one excludes those primes p such that E possesses a point of order p over a quadratic extension of \mathbf{Q}_p . Theorem 1.2 with $d = 2$ thus guarantees that this last condition holds, on average, for only finitely many primes p .

Unfortunately, we can not state a deformation theoretic analogue of Theorem 1.2, as the other reasons for obstructions do not satisfy as strong of a bound. Nevertheless, we do show that Mazur's question has an affirmative answer for elliptic curves admitting rational 2-isogenies (which is basically trivial) or 15-isogenies (which is an amusing computation).

For another application, recall that the newform $f_E := \sum a_n(E)q^n$ associated to E is said to possess a *companion form* modulo p if there is a mod p eigenform $g = \sum b_n q^n$ of weight $p - 1$ satisfying

$$n^2 b_n \equiv n a_n \pmod{p}$$

for all $n \geq 1$. For $d \geq 1$, let $\pi_E^{\text{cf}}(x)$ denote the number of primes $p \leq x$ such that $a_p(E)$ equals ± 1 and f_E possesses a companion form modulo p . Using a deep result of Gross [5], Theorem 1.2 yields the following.

Theorem 1.3. *Assume $A, B \geq x^{\frac{7}{4} + \varepsilon}$ for some $\varepsilon > 0$. Then*

$$\frac{1}{\#\mathcal{S}_{A,B}} \sum_{E \in \mathcal{S}_{A,B}} \pi_E^{\text{cf}}(x) \ll d^2$$

as $x \rightarrow \infty$.

It would be interesting to remove the assumption that $a_p(E) = \pm 1$ above, although it is not immediately clear to the authors how to adapt these methods to that question.

We present some data and simple results on Conjecture 1.1 in the case $d = 1$ in Section 2. In Section 3, we show that over the unramified extension of \mathbf{Q}_p of degree d , residual p -torsion points lift to p -adic p -torsion points with a frequency of $\frac{1}{p^d}$. In Section 4 we use this result and analytic methods to deduce Theorem 1.2. Finally, in Section 5 we discuss the applications to deformation theory and companion forms.

Acknowledgments. The authors would like to thank Hershy Kisilevsky, Siman Wong and Hui June Zhu for useful discussions during the preparation of this paper.

2. LOCAL TORSION PRIMES

Fix an elliptic curve E over \mathbf{Q} . We call a prime p a *local torsion prime* for E if E possesses a point of order p over \mathbf{Q}_p . For $x > 0$ let $\pi_E(x)$ denote the number of local torsion primes $p \leq x$ for E . Using the Magma Computational Algebra System we computed $\pi_E(10^6)$ for the 5113 elliptic curves E with conductor at most 1000. (Note that π_E is not isogeny-invariant, so that these computations were done over isomorphism classes rather than isogeny classes.)

Curves	# curves	# E such that $\pi_E(10^6) =$						
		0	1	2	3	4	5+	
All curves	5113	568	3687	828	15	1	14	
Curves with no torsion	1364	484	733	117	15	1	14	

The 14 curves E with $\pi_E(10^6) \geq 5$ were all CM curves and had between 22 and 36 local torsion primes in this range. (In fact, they all had CM by $\mathbf{Q}(\sqrt{-3})$, although this presumably is an artifact of the small conductors we considered.) Thus only one elliptic curve without complex multiplication and conductor at most 1000 had as many as four local torsion primes less than one million: the elliptic curve 774D1, for which 2, 3, 5, 7 are local torsion primes.

We remark that the precise ratios reported here should not be taken too seriously, as elliptic curves of small conductor are not at all representative of all elliptic curves. Nevertheless, this data certainly supports Conjecture 1.1. Indeed, large local torsion primes p were quite rare: 99.1% of the local torsion primes occurring were 2, 3, 5, 7. The only two elliptic curves in this sample with local torsion primes > 1000 were 131A1 (with local torsion primes 59 and 4723) and 775A1 (with local torsion prime 26993).

We now record some simple results on local torsion primes. Although some of the proofs rely on results in the next section, we find it most convenient to state them here.

Proposition 2.1. *Let E be an elliptic curve over \mathbf{Q} .*

- (1) *If $E(\mathbf{Q})_{\text{tors}} \neq 0$, then E has finitely many local torsion primes. (More precisely, if $E(\mathbf{Q})_{\text{tors}} \neq 0$, then any prime $p \geq 7$ of good reduction for E is not a local torsion prime for E unless $E(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/p$.)*
- (2) *For any finite set of primes \mathcal{P} , there exists an elliptic curve E such that each element of \mathcal{P} is a local torsion prime for E .*
- (3) *If E has complex multiplication, then a prime $p > 3$ of good reduction is a local torsion prime for E if and only if $a_p(E) = 1$.*

Proof.

- (1) Suppose that $p \geq 7$ is a local torsion prime of E at which E has good reduction. Since $p \geq 3$, the formal group of E over \mathbf{Z}_p is torsion-free, so that the natural map

$$E(\mathbf{Q}_p)_{\text{tors}} \rightarrow E(\mathbf{F}_p)$$

is injective. In particular, p divides $\#E(\mathbf{F}_p)$; since $p \geq 7$, it now follows from the Riemann hypothesis that $E(\mathbf{F}_p)$ must have exactly p elements. Since $E(\mathbf{Q})_{\text{tors}}$ is non-trivial and injects into $E(\mathbf{F}_p)$, we conclude that $E(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/p$, as desired.

- (2) For each $p \in \mathcal{P}$, fix $a_p, b_p \in \mathbf{F}_p$ so that the elliptic curve E_{a_p, b_p} with Weierstrass equation $y^2 = x^3 + a_p x + b_p$ has precisely p points over \mathbf{F}_p . (The existence of such a curve is guaranteed by Deuring's Theorem which gives an exact formula for the number of elliptic curves over \mathbf{F}_p with $p + 1 - r$ points for $|r| \leq 2\sqrt{p}$; see for example [8] for a statement of Deuring's Theorem.) Let $(A_p, B_p) \in \mathbf{Z}/p^2 \times \mathbf{Z}/p^2$ be one of the pairs lifting (a_p, b_p) in Corollary 3.5. Let $A, B \in \mathbf{Z}$ be such that $A \equiv A_p \pmod{p^2}$, $B \equiv B_p \pmod{p^2}$ for all $p \in \mathcal{P}$. Then by Corollary 3.5 each $p \in \mathcal{P}$ is a local torsion prime for $E_{A, B}$.
- (3) This is clear from Lemma 3.2 as a CM elliptic curve is a canonical lift of each of its reductions. Alternately, it follows from the fact that for an ordinary prime p the mod p Galois representation of a CM elliptic curve is abelian when restricted to a decomposition group at p . \square

3. LOCAL TORSION ON ELLIPTIC CURVES

Fix a prime $p > 3$ and a finite extension k of \mathbf{F}_p of degree d . Let W denote the ring of Witt vectors over k ; we write K for the field of fractions of W . Note that $k = W/pW$; we set $W_2 = W/p^2W$.

Let E be an elliptic curve over W ; that is, E is an elliptic curve over K with good reduction. The next lemma gives a criterion for E to possess a K -rational point of order p . For a finite abelian group M we write $\text{rank}_p M$ for the p -rank of M (that is, for the \mathbf{F}_p -dimension of $M \otimes_{\mathbf{Z}} \mathbf{F}_p$ or equivalently of the p -torsion subgroup $M[p]$).

Lemma 3.1. *Let E be an elliptic curve over W . Then:*

$$\text{rank}_p E(W_2) = \begin{cases} d & \text{if } E(K)[p] = 0; \\ d + 1 & \text{if } E(K)[p] \neq 0. \end{cases}$$

Proof. Consider the diagram (with exact rows)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_0(pW) & \longrightarrow & E(K) & \longrightarrow & E(k) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \parallel & & \\ 0 & \longrightarrow & E_0(pW/p^2) & \longrightarrow & E(W_2) & \longrightarrow & E(k) & \longrightarrow & 0 \end{array}$$

with E_0 the formal group of E over \mathcal{O}_K . Since W is unramified over \mathbf{Z}_p , it follows from [11, Theorem IV.6.4b] that the reduction map $E_0(pW) \rightarrow E_0(pW/p^2)$ can be identified with the natural map $\mathbf{Z}_p^d \rightarrow (\mathbf{Z}/p)^d$. In particular, taking p -torsion and applying the snake lemma we obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & E(K)[p] & \longrightarrow & E(k)[p] & \longrightarrow & (\mathbf{Z}/p)^d \\ & & \downarrow & & \downarrow & & \parallel & & \parallel \\ 0 & \longrightarrow & (\mathbf{Z}/p)^d & \longrightarrow & E(W_2)[p] & \longrightarrow & E(k)[p] & \longrightarrow & (\mathbf{Z}/p)^d \end{array}$$

It follows that

$$\text{rank}_p E(W_2) = d + \text{rank}_p E(K)[p].$$

Since the field $K(E[p])$ contains $K(\mu_p)$ and thus is ramified over \mathbf{Q}_p , $E(K)[p]$ is at most one-dimensional and the lemma follows. \square

We fix now an elliptic curve E over k such that $E(k)[p] \neq 0$. We first determine how many lifts of E to W_2 have p -rank $d + 1$.

Lemma 3.2. *Let E be an elliptic curve over k such that $E(k)$ has a non-trivial p -torsion point. Then precisely one of the p^d isomorphism classes of lifts of E to an elliptic curve \tilde{E} over W_2 satisfies $\text{rank}_p \tilde{E}(W_2) = d + 1$.*

Proof. Since E is necessarily ordinary, there is a canonical exact sequence of finite flat group schemes

$$0 \rightarrow \mu_p \rightarrow E[p] \rightarrow \mathbf{Z}/p \rightarrow 0$$

over \bar{k} . In fact, since $E(k)$ has a point of order p , it follows that this exact sequence exists already over k and is split; that is, $E[p] \cong \mu_p \times \mathbf{Z}/p$ as k -group schemes.

By the Serre–Tate theorem (see [6, Theorem 1.2.1], for example), the lifts of E to elliptic curves over W_2 are parameterized by the lifts of the p -divisible group $E[p^\infty]$ to a p -divisible group over W_2 . Any such lift is an extension of $\mathbf{Q}_p/\mathbf{Z}_p$ by μ_{p^∞} , so that these lifts correspond to elements of

$$\varprojlim_n \text{Ext}^1(\mathbf{Z}/p^n, \mu_{p^n})$$

where the extensions are computed in the category of finite flat group schemes over W_2 . It is equivalent to compute these extensions under the flat topology, so that

$$\text{Ext}^1(\mathbf{Z}/p^n, \mu_{p^n}) \cong H_{\mathbb{A}^1}^1(\text{Spec } W_2, \mu_{p^n}) \cong W_2^\times / W_2^{\times p^n} \cong p \cdot W_2 \cong (\mathbf{Z}/p)^d.$$

Therefore the natural map

$$(1) \quad \varprojlim_n \text{Ext}^1(\mathbf{Z}/p^n, \mu_{p^n}) \rightarrow \text{Ext}^1(\mathbf{Z}/p, \mu_p)$$

is an isomorphism, and these groups have order p^d . In particular, this proves that E has precisely p^d isomorphism classes of lifts to W_2 .

Let \tilde{E} be a lift of E to W_2 . One sees immediately from the proof of Lemma 3.1 that $\tilde{E}(W_2)$ has p -rank $d + 1$ if and only if the canonical exact sequence

$$0 \rightarrow \mu_p \rightarrow \tilde{E}[p] \rightarrow \mathbf{Z}/p \rightarrow 0$$

splits. By (1), this occurs for precisely one lift \tilde{E} , as claimed. (This lift is usually called the *canonical lift* of E to W_2 .) \square

Remark 3.3. We note that it follows from the above proof that the isomorphism class of an elliptic curve over W_2 is determined by its j -invariant and the isomorphism class of its reduction to k . This fact can certainly be proven in for more elementary ways.

For a, b elements of some ring R , we write $E_{a,b}$ for the projective plane curve with affine Weierstrass equation $y^2 = x^3 + ax + b$. The next lemma applies Lemma 3.2 to obtain a lifting result for these cubics.

Proposition 3.4. *Let $E_{a,b}$ be an elliptic curve over k such that $j(E_{a,b}) \neq 0, 1728$. Assume that $E_{a,b}(k)$ has an element of order p . Then there are exactly p^d distinct pairs $(A_i, B_i) \in W_2 \times W_2$ such that $(A_i, B_i) \equiv (a, b) \pmod{p}$ and*

$$\text{rank}_p E_{A_i, B_i}(W_2) = d + 1.$$

Proof. Consider the closed subscheme S of $\mathbf{A}_{W_2}^3$ (with coordinates j, A, B) defined by the j -invariant equation

$$j = 6912 \cdot \frac{A^3}{4A^3 + 27B^2}.$$

The surface $S \times_{W_2} k$ is smooth away from $j = 0, 1728$, so that it follows from Hensel's lemma that for each of the p^d lifts \tilde{j} of $j(E_{a,b})$ to W_2 , there are precisely p^d lifts of (a, b) to $W_2 \times W_2$ such that the corresponding elliptic curve over W_2 has j -invariant \tilde{j} . In particular, each of the p^d possible j -invariants lifting $j(E)$ to W_2 occurs for some $E_{A,B}$ with $(A, B) \in W_2 \times W_2$. Since by Lemma 3.2 there are precisely p^d isomorphism classes of lifts of $E_{a,b}$ to W_2 , it follows that the isomorphism class of a lift of E is determined by its j -invariant. (Alternately, since the twists of an elliptic curve E over a ring R are parameterized by $H_{\mathfrak{H}}^1(\text{Spec } R, \text{Aut } E)$ and one has $p \nmid \# \text{Aut } E_{a,b}$ since $p \geq 5$, one can deduce this from the fact that the categories of étale sheaves on $\text{Spec } k$ and $\text{Spec } W$ are equivalent.) In particular, each isomorphism class occurs for precisely p^d values of A, B . By Lemma 3.2 precisely one of these isomorphism classes has p -rank $d + 1$, which yields the proposition. \square

For our analytic arguments we will be interested only in elliptic curves over \mathbf{Z}_p . In this case Proposition 3.4 yields the following.

Corollary 3.5. *Let $E_{a,b}$ be an ordinary elliptic curve over \mathbf{F}_p such that $j(E_{a,b}) \neq 0, 1728$. Let k be an extension of \mathbf{F}_p of degree d such that $E(k)[p] \neq 0$; set $W_2 = W/p^2$ with W the ring of Witt vectors of k . Then there are exactly p distinct pairs $(A_i, B_i) \in \mathbf{Z}/p^2 \times \mathbf{Z}/p^2$ such that $(A_i, B_i) \equiv (a, b) \pmod{p}$ and*

$$\text{rank}_p E_{A_i, B_i}(W_2) = d + 1.$$

Proof. The canonical lift of $E_{a,b}$ to W_2 has j -invariant in \mathbf{Z}/p^2 . Thus by Hensel's lemma as before there are precisely p pairs lying in $\mathbf{Z}/p^2 \times \mathbf{Z}/p^2$ among the p^d pairs of Proposition 3.4. The corollary follows. \square

4. ANALYTIC ARGUMENTS

Fix $d \geq 1$ and as before let W_2 denote the Witt vectors of length two over a finite field k of order p^d .

Definition 4.1. We write $\nu_p(d)$ for the number of pairs $(a, b) \in \mathbf{Z}/p^2 \times \mathbf{Z}/p^2$ such that $E_{a,b}$ is an elliptic curve with $\text{rank}_p E_{a,b}(W_2) = d + 1$.

The following estimates will be used in our main result.

Lemma 4.2. *We have*

$$\sum_{p \leq x} \nu_d(p) \ll dx^{7/2} \log x;$$

$$\sum_{p \leq x} \frac{\nu_d(p)}{p^2} \ll dx^{3/2} \log x;$$

$$\sum_{p \leq x} \frac{\nu_d(p)}{p^4} \ll d.$$

Proof. Write $\nu_d(p) = \nu'_d(p) + \nu_d^0(p) + \nu_d^{1728}(p)$ where $\nu'_d(p)$ (resp. $\nu_d^0(p)$, resp. $\nu_d^{1728}(p)$) denotes the number of pairs $(a, b) \in \mathbf{Z}/p^2 \times \mathbf{Z}/p^2$ such that $E_{a,b}(W_2)$ has p -rank $d+1$ and $E_{a,b}$ does not have j -invariant 0 or 1728 (resp. has j -invariant 0, resp. has j -invariant 1728). It suffices to prove the lemma separately for each of these three functions.

We begin with $\nu'_d(p)$. Since an elliptic curve E over \mathbf{F}_p has a point of order p over \mathbf{F}_{p^d} if and only if $a_p(E)^d \equiv 1 \pmod{p}$ (see Lemma 4.3 below), by Corollary 3.5 we have

$$\begin{aligned} \nu'_d(p) &= p \cdot \#\{(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times; a_p(E_{a,b})^d \equiv 1 \pmod{p}\} \\ &= p \cdot \sum_{\substack{|r| < 2\sqrt{p} \\ r^d \equiv 1 \pmod{p}}} (p-1)H(r^2 - 4p) \end{aligned}$$

by Deuring's theorem; see for example [8]. (Note that restricting to $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$ has eliminated those elliptic curves with j -invariant 0 or 1728.) The class number formula together with the trivial bound $L(1, \chi_D) \ll \log D$ yields $H(r^2 - 4p) \ll \sqrt{p} \log^2 p$. As (for large enough p) there are at most d such r , it follows that

$$\nu'_d(p) \ll dp^{5/2} \log^2 p.$$

The asserted bounds for $\nu'_d(p)$ all follow easily from this.

Consider now $\nu_d^0(p)$. An elliptic curve E over \mathbf{Z}/p^2 with j -invariant 0 is always the canonical lift of its reduction, so that by the proof of Lemma 3.2 it has p -rank $d+1$ over W precisely when

$$a_p(E \times_{\mathbf{Z}/p^2} \mathbf{F}_p)^d \equiv 1 \pmod{p}.$$

(Note that in this case Corollary 3.5 does not apply.) Since a curve $E_{a,b}$ over \mathbf{F}_p has j -invariant 0 if and only if $b = 0$ and each such curve over \mathbf{F}_p has p^2 lifts to \mathbf{Z}/p^2 , we obtain

$$\nu_d^0(p) = p^2 \cdot \sum_{\substack{|r| < 2\sqrt{p} \\ r^d \equiv 1 \pmod{p}}} \#\{a \in \mathbf{F}_p^\times; a_p(E_{a,0}) = r\}.$$

Thus

$$\sum_{p \leq x} \frac{\nu_d^0(p)}{p^2} = \sum_{p \leq x} \sum_{\substack{|r| < 2\sqrt{p} \\ r^d \equiv 1 \pmod{p}}} \sum_{a \in \mathbf{F}_p^\times} \chi_{E_{a,0}}^r(p)$$

where $\chi_E^r(p)$ is 1 if $a_p(E) = r$ and 0 otherwise. Reversing the order of summation, we obtain

$$\begin{aligned} \sum_{p \leq x} \frac{\nu_d^0(p)}{p^2} &= \sum_{a \leq x} \sum_{a \leq p \leq x} \sum_{\substack{|r| < 2\sqrt{p} \\ r^d \equiv 1 \pmod{p}}} \chi_{E_{a,0}}^r(p) \\ &\ll d \cdot \max_r \left(\sum_{a \leq x} \#\{p \leq x; a_p(E_{a,0}) = r\} \right). \end{aligned}$$

An elementary argument using the description of $a_p(E_{a,0})$ in terms of the quadratic form $X^2 + Y^2$ shows that

$$\#\{p \leq x; a_p(E_{a,0}) = r\} \ll \sqrt{x}$$

so that we obtain

$$\begin{aligned} \sum_{p \leq x} \frac{\nu_d^0(p)}{p^2} &\ll d \cdot \sum_{a \leq x} \sqrt{x} \\ &\ll dx^{3/2}. \end{aligned}$$

Applying partial summation one now easily obtains

$$\begin{aligned} \sum_{p \leq x} \frac{\nu_d^0(p)}{p^4} &\ll d \\ \sum_{p \leq x} \nu_d^0(p) &\ll dx^{7/2} \end{aligned}$$

which suffice for the lemma. An entirely similar argument gives the same bounds for ν_d^{1728} . \square

The next lemma was used in the preceding proof. There are of course many proofs; we give one in the spirit of Section 3. Alternately, one could use the Weil conjectures and look at the p -divisibility of $\#E(\mathbf{F}_{p^d}) = p^d + 1 - (\alpha_p^d + \beta_p^d)$, where α_p, β_p are the roots of the characteristic polynomial $x^2 - a_p(E)x + p$ over \mathbf{F}_p .

Lemma 4.3. *Let E be an elliptic curve over \mathbf{F}_p . Then $E(\mathbf{F}_{p^d})[p] \neq 0$ if and only if $a_p(E)^d \equiv 1 \pmod{p}$.*

Proof. If $a_p(E) = 0$, then E is supersingular and never has p -torsion over any extension of \mathbf{F}_p , so we may assume that $a_p(E) \neq 0$. In this case, the p -torsion of E decomposes as

$$E[p] = \mathbf{Z}/p(\chi) \oplus \mu_p(\chi^{-1})$$

where χ is the character of $\text{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ sending a Frobenius to $a_p(E)$. (See [5], for example.) Now $E(\mathbf{F}_{p^d})[p] \neq 0$ if and only if χ is trivial on $\text{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_{p^d})$; since this Galois group is generated by the d^{th} power of Frobenius, the lemma follows. \square

Recall that for an elliptic curve E , $\pi_E^d(x)$ denotes the number of primes $p \leq x$ such that E possesses a point of order p over an extension of \mathbf{Q}_p of degree at most d . Let $\pi_E^{d,\text{ur}}(x)$ denote the number of primes $p \leq x$ such that E possesses a point of order p over an unramified extension of \mathbf{Q}_p of degree at most d .

Lemma 4.4. *Let E be an elliptic curve. Then*

$$\pi_E^d(x) - \pi_E^{d,\text{ur}}(x)$$

is bounded by the number of primes $p \leq d$.

Proof. Fix a prime $p > d$ and a ramified extension K/\mathbf{Q}_p of degree at most d . To prove the lemma it suffices to show that if $E(K)[p] \neq 0$, then already $E(K^{\text{ur}})[p] \neq 0$ with K^{ur} the maximal unramified subfield of K . For this, recall that the restriction of the p -torsion Galois representation of E to a decomposition group at p has the form

$$\begin{pmatrix} \varepsilon\chi & * \\ 0 & \chi^{-1} \end{pmatrix}$$

with ε the cyclotomic character, χ an unramified character and $*$ either trivial or wildly ramified. K is not wildly ramified (since $d < p$) and does not contain μ_p , so that the only way that $E(K)[p]$ can be non-zero is if $*$ is trivial and χ factors through $\text{Gal}(K/\mathbf{Q}_p)$. Since χ is unramified, it must thus factor through $\text{Gal}(K^{\text{ur}}/\mathbf{Q}_p)$ as well, as desired. \square

Recall that $\mathcal{S}_{A,B}$ denotes the set of elliptic curves $E_{a,b}$ with $a, b \in \mathbf{Z}$ and $|a| \leq A$, $|b| \leq B$.

Proposition 4.5. *Fix $A, B > 0$. Then*

$$\frac{1}{\#\mathcal{S}_{A,B}} \sum_{E \in \mathcal{S}_{A,B}} \pi_E^d(x) = O(d^2) + d \cdot O\left(\left(\frac{1}{A} + \frac{1}{B}\right)x^{3/2} \log x + \frac{1}{AB}x^{7/2} \log x\right).$$

Proof. By Lemma 4.4 we have

$$\frac{1}{\#\mathcal{S}_{A,B}} \sum_{E \in \mathcal{S}_{A,B}} \pi_E^d(x) = \frac{1}{\#\mathcal{S}_{A,B}} \sum_{E \in \mathcal{S}_{A,B}} \pi_E^{d,\text{ur}}(x) + d \cdot O(1).$$

It thus suffices to consider the latter sum.

Let K_p^d denote the unramified extension of \mathbf{Q}_p of degree d and let $\tilde{\pi}_E^d(x)$ denote the number of $p \leq x$ such that $E(K_p^d)[p] \neq 0$. By Lemma 3.1, $E(K_p^d)[p] \neq 0$ can be detected by looking at E over \mathbf{Z}/p^2 . Since there are

$$\left(\frac{2A}{p^2} + O(1)\right) \cdot \left(\frac{2B}{p^2} + O(1)\right)$$

elliptic curves in $\mathcal{S}_{A,B}$ reducing to any fixed elliptic curve over \mathbf{Z}/p^2 , applying Lemma 3.1 and reversing the order of summation we find that

$$\begin{aligned} \frac{1}{\#\mathcal{S}_{A,B}} \sum_{E \in \mathcal{S}_{A,B}} \tilde{\pi}_E^d(x) &= \frac{1}{\#\mathcal{S}_{A,B}} \sum_{p \leq x} \#\{E \in \mathcal{S}_{A,B}; E(K_p^d)[p] \neq 0\} \\ &= \frac{1}{\#\mathcal{S}_{A,B}} \sum_{p \leq x} \left(\frac{2A}{p^2} + O(1)\right) \cdot \left(\frac{2B}{p^2} + O(1)\right) \nu_d(p) \\ &= \sum_{p \leq x} \frac{\nu_d(p)}{p^4} + O\left(\left(\frac{1}{A} + \frac{1}{B}\right) \sum_{p \leq x} \frac{\nu_d(p)}{p^2} + \frac{1}{AB} \sum_{p \leq x} \nu_d(p)\right) \end{aligned}$$

since

$$\#\mathcal{S}_{A,B} = 4AB(1 + o(1)).$$

Applying the estimates of Lemma 4.2 and summing over d now yields the result. \square

Corollary 4.6. *If $A, B \gg x^{7/4+\varepsilon}$, then*

$$\frac{1}{\#\mathcal{S}_{A,B}} \sum_{E \in \mathcal{S}_{A,B}} \pi_E^d(x) \ll d^2$$

as $x \rightarrow \infty$.

5. DEFORMATION THEORY

Fix an elliptic curve E over \mathbf{Q} without complex multiplication. Let S denote the set of primes at which E has bad reduction. For a prime p consider the Galois representation

$$\bar{\rho}_{E,p} : \text{Gal}(\mathbf{Q}_{S \cup \{p\}}/\mathbf{Q}) \rightarrow \text{GL}_2(\mathbf{F}_p)$$

giving the Galois action on the p -torsion points $E[p]$. A *deformation* of $\bar{\rho}_{E,p}$ to a local ring R with residue field \mathbf{F}_p is a strict equivalence class of Galois representations

$$\text{Gal}(\mathbf{Q}_{S \cup \{p\}}/\mathbf{Q}) \rightarrow \text{GL}_2(R)$$

which yield $\bar{\rho}_{E,p}$ on composition with the reduction map

$$\text{GL}_2(R) \rightarrow \text{GL}_2(\mathbf{F}_p);$$

here two Galois representations are considered to be strictly equivalent if they are conjugate by a matrix which reduces to the identity in $\text{GL}_2(\mathbf{F}_p)$.

When $\bar{\rho}_{E,p}$ is absolutely irreducible (which is true for sufficiently large p) it is known [9, Section 1.2] that there exists a *universal deformation*

$$\rho_{E,p}^{\text{univ}} : \text{Gal}(\mathbf{Q}_{S \cup \{p\}}/\mathbf{Q}) \rightarrow \text{GL}_2(R_{E,p}^{\text{univ}})$$

in the category of inverse limits of artinian local rings with residue field \mathbf{F}_p ; the ring $R_{E,p}^{\text{univ}}$ is called the *universal deformation ring* of $\bar{\rho}_{E,p}$. Thus any deformation of $\bar{\rho}_{E,p}$ to such a ring R is obtained from ρ^{univ} by composition with a unique map $R_{E,p}^{\text{univ}} \rightarrow R$.

It is of fundamental interest to understand the structure of $R_{E,p}^{\text{univ}}$. Let $\text{ad } \bar{\rho}_{E,p}$ denote the adjoint representation of $\bar{\rho}_{E,p}$ and set

$$d_i := \dim_{\mathbf{F}_p} H^i(\mathbf{Q}_{S \cup \{p\}}/\mathbf{Q}, \text{ad } \bar{\rho}_{E,p}).$$

We have the following result of Mazur [9, Section 1.6 and Section 1.10].

Proposition 5.1. *With notation as above, $R_{E,p}^{\text{univ}}$ is a quotient of a power series ring in d_1 variables over \mathbf{Z}_p by an ideal generated by at most d_2 elements. Furthermore, one has $d_1 - d_2 = 3$. In particular, if $d_2 = 0$ (in which case one says that the deformation theory of $\bar{\rho}_{E,p}$ is unobstructed), then $R_{E,p}^{\text{univ}}$ is (non-canonically) isomorphic to a power series ring in three variables over \mathbf{Z}_p .*

In [10], Mazur further asks if the deformation theory of $\bar{\rho}_{E,p}$ is unobstructed for all but finitely many primes p . (We remark that the analogous question for modular forms of weight at least 3 was answered affirmatively in [13].) Using Poitou–Tate duality and work of Flach [4] on symmetric square Selmer groups, he proved the following result.

Proposition 5.2. *Let p be a prime of good reduction for E such that $\bar{\rho}_{E,p}$ is absolutely irreducible. If the deformation theory of $\bar{\rho}_{E,p}$ is obstructed, then one of the following holds:*

- (1) $p \leq 3$;
- (2) $p \in S$;
- (3) $\ell \equiv 1 \pmod{p}$ for some $\ell \in S$;
- (4) The Galois representation $\bar{\rho}_{E,p}$ is not surjective;
- (5) p divides the (appropriately normalized) special value $L(\text{Sym}^2 E, 2)/\Omega$ of the symmetric square L -function of E ;

(6) $H^0(\mathbf{Q}_\ell, \text{Sym}^2 E[p]) \neq 0$ for some $\ell \in S \cup \{p\}$.

Furthermore each of these conditions holds for all but finitely many primes p , with the possible exception of the vanishing of $H^0(\mathbf{Q}_p, \text{Sym}^2 E[p])$ in (6).

To answer Mazur's question it thus suffices to show that $H^0(\mathbf{Q}_p, \text{Sym}^2 E[p]) = 0$ for all but finitely many p . The next proposition gives some reformulations of this condition.

Proposition 5.3. *Let p be an odd prime of good reduction for E . Then the following are equivalent:*

- (1) $H^0(\mathbf{Q}_p, \text{Sym}^2 E[p]) \neq 0$;
- (2) $a_p(E) = \pm 1$ and the restriction of $\bar{\rho}_{E,p}$ to a decomposition group at p is semi-simple;
- (3) $a_p(E) = \pm 1$ and f_E possesses a companion form modulo p .

If $p \geq 7$, then these conditions are further equivalent to:

- (4) $E(K)[p] \neq 0$ with K some quadratic extension of \mathbf{Q}_p .

Proof. The equivalence of (1) and (2) is [10, Lemma of p. 172]. The equivalence of (2) and (3) is the main result of [5]. Finally, for the equivalence of (1) and (4) we modify the argument of [1, Lemma 2.3(i)]. It is clear that if $x \in E(K)[p]$ is non-trivial, then $x \otimes x$ gives a non-zero element of $H^0(\mathbf{Q}_p, \text{Sym}^2 E[p])$. For the converse, suppose that $t \in H^0(\mathbf{Q}_p, \text{Sym}^2 E[p])$ is non-trivial. Let ε denote the mod p cyclotomic character. Since $p \geq 7$ we may choose $\sigma \in \text{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ such that $\varepsilon(\sigma)^4 \neq 1$. Let $\lambda, \mu \in \mathbf{F}_p$ be the eigenvalues of σ acting on $E[p]$. Then the eigenvalues of σ acting on $\text{Sym}^2 E[p]$ are λ^2 , $\lambda\mu = \varepsilon(\sigma)$, and μ^2 . Since t is fixed by σ , one of these must equal 1; as $\varepsilon(\sigma) \neq 1$ we may assume without loss of generality that $\lambda^2 = 1$.

Now consider σ^2 , which has $E[p]$ eigenvalues $\lambda^2 = 1$ and $\varepsilon(\sigma)^2$. These eigenvalues are distinct, so we may choose a basis x, y of $E[p]$ with σ^2 -eigenvalues 1 and $\varepsilon(\sigma)^2$, respectively. Since $\varepsilon(\sigma)^4 \neq 1$, one computes easily that the σ^2 -invariant subspace of $\text{Sym}^2 E[p]$ is spanned by $x \otimes x$. Since t must lie in this subspace, it follows that $x \otimes x$ is fixed by all of $\text{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$. Thus $\text{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ acts on x by a quadratic character, so that x is defined over a quadratic extension of \mathbf{Q}_p . \square

Combined with Proposition 5.3, Theorem 1.2 immediately yields Theorem 1.3. Furthermore, it shows that the exceptional case in Proposition 5.2 occurs on average finitely often. Unfortunately, already the condition (2) of Proposition 5.2 fails to satisfy such a strong bound, so that we can not state such a result for the deformation theory of E .

Nevertheless, for certain elliptic curves one has $a_p(E) = \pm 1$ for finitely many p , so that one can verify Conjecture 1.1 for $d = 2$ for these curves and thus settle these questions. More precisely, we have the following. (For an alternate proof of the 15-isogeny case, see [3, Theorem 1.4].)

Proposition 5.4. *Let E be an elliptic curve over \mathbf{Q} without complex multiplication. Assume that E admits either a rational 2-isogeny or a rational 15-isogeny. Then Conjecture 1.1 holds for E with $d = 2$. In particular, the deformation theory of $\bar{\rho}_{E,p}$ is unobstructed for all but finitely many primes p .*

Proof. We in fact show that E does not have a point of order p over \mathbf{F}_{p^2} for all but finitely many p . Since for $p \geq 7$ this occurs if and only if $a_p(E) = \pm 1$, it suffices to show that occurs for only finitely many primes p .

If E possesses a rational 2-isogeny, then it has rational 2-torsion. Thus in particular $E(\mathbf{F}_p)[2] \neq 0$ for all but finitely many primes p . Fix such a $p > 2$. Then

$$a_p(E) = p + 1 - \#E(\mathbf{F}_p) \equiv 0 \pmod{2},$$

so that certainly $a_p(E) \neq \pm 1$, as desired.

Now let E be an elliptic curve admitting a 15-isogeny. The modular curve $X_0(15)$ has four non-cuspidal rational points; as the four elliptic curves in the isogeny class 50A of [2] admit rational 15-isogenies and are distinct over \mathbf{Q} , it follows that every elliptic curve admitting a rational 15-isogeny is isogenous to a twist of the curve 50A1. Since isogeny does not change Fourier coefficients and twisting changes them only up to sign (and introducing some zeroes), it suffices to prove the proposition for the elliptic curve 50A1.

Let E denote the elliptic curve 50A1; it has Weierstrass equation

$$y^2 + xy + y = x^3 - x - 2.$$

Then E has the rational 3-torsion points

$$\{(2, 1), (2, -4)\} \in E[3]$$

and admits a rational 5-isogeny. Thus

$$\bar{\rho}_{E,3} \cong \begin{pmatrix} 1 & * \\ 0 & \varepsilon \end{pmatrix} \quad \bar{\rho}_{E,5} \cong \begin{pmatrix} \chi & * \\ 0 & \varepsilon\chi^{-1} \end{pmatrix}$$

with ε cyclotomic and χ some Dirichlet character. One finds that E has a 5-torsion point

$$P = (-\zeta_5^3 - \zeta_5^2 - 1, -\zeta_5^3 - 2\zeta_5 - 1)$$

with ζ_5 a primitive 5th root of unity. Using this one explicitly computes χ as a Dirichlet character of conductor 5; combined with the knowledge of $\bar{\rho}_{E,3}$, we conclude that

$$\bar{\rho}_{E,15} \cong \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

with χ_1, χ_2 Dirichlet characters of conductor 15 given by

n	1	2	4	7	8	11	13	14
$\chi_1(n)$	1	13	4	13	7	1	7	4
$\chi_2(n)$	1	14	1	4	14	11	4	11

In particular, we have

$$a_p(E) \equiv \chi_1(p) + \chi_2(p) \pmod{15}$$

for all $p \geq 7$. Thus

$$a_p(E) \in \{0, 2, 5, 6, 11, 12\}$$

modulo 15, so that $a_p(E) \neq \pm 1$ for all $p \geq 7$, as desired. \square

REFERENCES

- [1] J. Coates and A. Sydenham, *On the symmetric square of a modular elliptic curve*, in *Elliptic curves, modular forms and Fermat's last theorem*, International Press, 1997.
- [2] J.E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1997.
- [3] C. David, H. Kisilevsky and F. Pappalardi, *Galois representations with non-surjective traces*, *Canad. J. Math.* **51** (1999), 936–951.
- [4] M. Flach, *A finiteness theorem for the symmetric square of an elliptic curve*, *Invent. Math.* **109** (1992), 307–327.
- [5] B. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, *Duke Math. J.* **61** (1990), 445–517.
- [6] N. Katz, *Serre–Tate local moduli*, in: *Surfaces algébriques (Orsay, 1976–78)*, Lecture Notes in Math. **868**, Springer–Verlag, Berlin–New York, 1981.
- [7] S. Lang and H. Trotter, *Frobenius distributions in GL_2 -extensions of the rational numbers*, *Lectures Notes in Math.* **504**, Springer–Verlag, Berlin–New York, 1976.
- [8] H. Lenstra, *Factoring integers with elliptic curves*, *Annals of Math.* **126** (1987), 649–673.
- [9] B. Mazur, *Deforming Galois representations*, in: *Galois groups over \mathbf{Q} (Berkeley, 1987)*, MSRI Publ. **16**, Springer, New York, 1989.
- [10] ———, *An “infinite fern” in the universal deformation space of Galois representations*, *Collect. Math.* **48** (1997), 155–193.
- [11] J. Silverman, *Arithmetic of elliptic curves*, Springer–Verlag, New York, 1986.
- [12] T. Weston, *An overview of a theorem of Flach*, appendix to *Deformations of Galois representations* by F.Q. Gouvea in *Arithmetic algebraic geometry*, American Mathematical Society, 2001.
- [13] ———, *Unobstructed modular deformation problems*, *American J. Math* **126** (2004), 1237–1252.

(Chantal David) DEPARTMENT OF MATHEMATICS AND STATISTICS, CONCORDIA UNIVERSITY, MONTREAL, QC

(Tom Weston) DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF MASSACHUSETTS AMHERST, MA

E-mail address, Chantal David: cdavid@mathstat.concordia.ca

E-mail address, Tom Weston: weston@math.umass.edu