Prime twists of elliptic curves

Daniel Kriz and Chao Li

For certain elliptic curves $E/\mathbb{Q}$ with $E(\mathbb{Q})[2] = \mathbb{Z}/2\mathbb{Z}$, we prove a criterion for prime twists of $E$ to have analytic rank 0 or 1, based on a mod 4 congruence of 2-adic logarithms of Heegner points. As an application, we prove new cases of Silverman’s conjecture that there exists a positive proportion of prime twists of $E$ of rank zero (resp. positive rank).

1. Introduction

1.1. Silverman’s conjecture

Let $E/\mathbb{Q}$ be an elliptic curve. For a square-free integer $d$, we denote by $E^{(d)}/\mathbb{Q}$ its quadratic twist by $\mathbb{Q}(\sqrt{d})$. Silverman made the following conjecture concerning the prime twists of $E$ (see [10, p.653], [9, p.350]).

**Conjecture 1.1 (Silverman).** Let $E/\mathbb{Q}$ be an elliptic curve. Then there exists a positive proportion of primes $\ell$ such that $E^{(\ell)}$ or $E^{(-\ell)}$ has rank $r = 0$ (resp. $r > 0$).

**Remark 1.2.** Conjecture 1.1 is known for the congruent number curve $E : y^2 = x^3 - x$. In fact, $E^{(\ell)}$ has rank $r = 0$ if $\ell \equiv 3 \pmod{8}$ and $r = 1$ if $\ell \equiv 5, 7 \pmod{8}$. This follows from classical 2-descent for $r = 0$ and Birch [1] and Monsky [8] for $r = 1$ (see also [12]).

**Remark 1.3.** Although Conjecture 1.1 is still open in general, many special cases have been proved. For $r = 0$, see Ono [9] and Ono–Skinner [10, Cor. 2] (including all elliptic curves with conductor $\leq 100$). For $r = 1$, see Coates–Y. Li–Tian–Zhai [2, Thm. 1.1].

In our recent work [7, Thm. 4.3], we have proved Conjecture 1.1 (for both $r = 0$ and $r = 1$) for a wide class of elliptic curves with $E(\mathbb{Q})[2] = 0$. The goal of this short note is to extend our method to certain elliptic curves with $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. 
1.2. Main results

Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N$. We will use $K$ to denote an imaginary quadratic field satisfying the Heegner hypothesis for $N$:

each prime factor $\ell$ of $N$ is split in $K$.

We denote by $P \in E(K)$ the corresponding Heegner point, defined up to sign and torsion with respect to a fixed modular parametrization $\pi_E : X_0(N) \to E$. Let

$$f(q) = \sum_{n=1}^{\infty} a_n(E)q^n \in \mathcal{S}_2^{\text{new}}(\Gamma_0(N))$$

be the normalized newform associated to $E$. Let $\omega_E \in \Omega^1_{E/\mathbb{Q}} := H^0(E/\mathbb{Q}, \Omega^1)$ such that

$$\pi_{E}^*(\omega_E) = f(q) \cdot dq/q.$$

We denote by $\log_{\omega_E}$ the formal logarithm associated to $\omega_E$.

Our main result is the following criterion for prime twists of $E$ of analytic (and hence algebraic) rank 0 or 1.

**Theorem 1.4.** Let $E/\mathbb{Q}$ be an elliptic curve. Assume $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ and $E$ has no rational cyclic 4-isogeny. Assume there exists an imaginary quadratic field $K$ satisfying the Heegner hypothesis for $N$ such that

$$(\star) \quad 2 \text{ splits in } K \text{ and } \frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_2)| \cdot \log_{\omega_E}(P)}{2} \not\equiv 0 \pmod{2}.$$

Let $S$ be the set of primes

$$S := \{ \ell \mid 2N : \ell \text{ splits in } K, |E(\mathbb{F}_\ell)| \not\equiv 0 \pmod{4} \}.$$

Let $N$ be the set of signed primes

$$N = \{ d = \pm \ell : \ell \in S, \text{any odd prime } q || N \text{ splits in } \mathbb{Q}(\sqrt{d}) \}.$$

Then for any $d \in N$, we have the analytic rank $r_{\text{an}}(E^{(d)}/K) = 1$. In particular,

$$r_{\text{an}}(E^{(d)}/\mathbb{Q}) = \begin{cases} 0, & \text{if } w(E^{(d)}/\mathbb{Q}) = +1, \\ 1, & \text{if } w(E^{(d)}/\mathbb{Q}) = -1. \end{cases}$$

where $w(E^{(d)}/\mathbb{Q})$ denotes the global root number of $E^{(d)}/\mathbb{Q}$. 
Remark 1.5. Recall that $|\tilde{E}_{ns}(\mathbb{F}_\ell)|$ denotes the number of $\mathbb{F}_\ell$-points of the nonsingular part of the mod $\ell$ reduction of $E$, which is $|E(\mathbb{F}_\ell)| = \ell + 1 - a_\ell(E)$ if $\ell \nmid N$, $\ell \pm 1$ if $\ell || N$ and $\ell$ if $\ell^2 | N$.

Remark 1.6. The assumption on Heegner points in Theorem 1.4 forces $r_{an}(E/\mathbb{Q}) \leq 1$.

As a consequence, we deduce the following cases of Silverman’s conjecture.

Theorem 1.7. Let $E/\mathbb{Q}$ as in Theorem 1.4. Let $\phi : E \to E_0 := E/E(\mathbb{Q})[2]$ be the natural 2-isogeny. Assume the fields $\mathbb{Q}(E[2], E_0[2]), \mathbb{Q}(\sqrt{-N}), \mathbb{Q}(\sqrt{q})$ (where $q$ runs over odd primes $q || N$) are linearly disjoint. Then Conjecture 1.1 holds for $E/\mathbb{Q}$.

1.3. Novelty of the proof

The proof of [4, Thm. 4.3] mentioned above uses the mod 2 congruence between 2-adic logarithms of Heegner points on $E$ and $E^{(d)}$ (recalled in §3.1 below), arising from the isomorphism of Galois representations $E[2] \cong E^{(d)}[2]$. For the congruence to be nontrivial on both sides, one needs the extra factor $|E(\mathbb{F}_\ell)|$ appearing in the formula to be odd for $\ell | d$. This is only possible when $E(\mathbb{Q})[2] = 0$.

When $E(\mathbb{Q})[2] \neq 0$, we instead take advantage of the exceptional isomorphism between the mod 4 semisimplified Galois representations $E[4]^{ss} \cong E^{(d)}[4]^{ss}$, and consequently a mod 4 congruence between 2-adic logarithm of Heegner points. When $E(\mathbb{Q})[2] = \mathbb{Z}/2\mathbb{Z}$ and $E$ has no rational cyclic 4-isogeny, it is possible that the extra factor $|E(\mathbb{F}_\ell)|$ is even but nonzero mod 4. This is the key observation to prove Theorem 1.4. The application Theorem 1.7 then follows by Chebotarev’s density after translating the condition $|E(\mathbb{F}_\ell)| \not\equiv 0 \pmod{4}$ into an inert condition for $\ell$ in $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E_0[2])$ (Lemma 4.1).

2. Examples

Let us illustrate the main results by two explicit examples.

Example 2.1. Consider the elliptic curve (in Cremona’s labeling) $E = 256b1 : y^2 = x^3 - 2x$
with $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. It has $j$-invariant 1728 and CM by $\mathbb{Q}(i)$. The imaginary quadratic field $K = \mathbb{Q}(\sqrt{-7})$ satisfies the Heegner hypothesis. The associated Heegner point $y_K = (-1, -1)$ satisfies Assumption \[\star\]. The set $S$ consists of primes $\ell$ such that $\ell \equiv 1, 2, 4 \pmod{7}$ and $\ell \equiv 5 \pmod{8}$:

$$S = \{29, 37, 53, 109, 149, 197, 277, 317, 373, 389, \ldots\}.$$

By Theorem 1.4, we have

$$\text{rank}(E^{(\pm \ell)}/K) = 1,$$

for any $\ell \in S$.

We compute the global root number $w(E^{(\pm \ell)}/\mathbb{Q}) = -1$ and conclude that

$$\text{rank}(E^{(\pm \ell)}/\mathbb{Q}) = 1, \quad \text{rank}(E^{(\pm 7\ell)}/\mathbb{Q}) = 0,$$

for any $\ell \in S$.

**Remark 2.2.** Notice the two congruence conditions for $\ell \in S$ are both necessary for the conclusion: for example, we have $\text{rank}(E^{(\ell)}) = 2$ for $\ell = 31$ and $\text{rank}(E^{(7\ell)}) = 2$ for $\ell = 5$.

**Example 2.3.** Consider the elliptic curve

$$E = 256a1 : y^2 = x^3 + x^2 - 3x + 1$$

with $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. It has $j$-invariant 8000 and CM by $\mathbb{Q}(\sqrt{-2})$. The imaginary quadratic field $K = \mathbb{Q}(\sqrt{-7})$ satisfies the Heegner hypothesis. The associated Heegner point $y_K = (0, 1)$ satisfies Assumption \[\star\]. The 2-isogenous curve is

$$E_0 = 256a2 : y^2 = x^3 + x^2 - 13x - 21.$$

We have $\mathbb{Q}(E[2]) = \mathbb{Q}(E_0[2]) = \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-N}) = \mathbb{Q}(i)$. Hence $\mathbb{Q}(E[2], E_0[2])$ and $\mathbb{Q}(\sqrt{-N})$ are linearly disjoint. Since there is no odd prime $q || N$, Theorem 1.7 implies that Silverman’s conjecture holds for $E$.

In fact, the set $S$ in this case consists of primes $\ell$ such that $\ell \equiv 1, 2, 4 \pmod{7}$ and $\ell \equiv 3, 5 \pmod{8}$:

$$S = \{11, 29, 37, 43, 53, 67, 107, 109, 149, 163, 179, 197, 211, 277, 317, 331, \ldots\}.$$

Computing the global root number gives

$$\text{rank}(E^{(\ell)}/\mathbb{Q}) = 1, \quad \text{rank}(E^{(-\ell)}/\mathbb{Q}) = 0,$$

for any $\ell \in S$. 
3. Proof of Theorem 1.4

3.1. Congruences between Heegner points

We first recall Theorem 1.16 of [7].

**Theorem 3.1.** Let $E$ and $E'$ be two elliptic curves over $\mathbb{Q}$ of conductors $N$ and $N'$ respectively. Suppose $p$ is a prime such that there is an isomorphism of semisimplified $G_\mathbb{Q} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representations $E[p^m]_{\text{ss}} \cong E'[p^m]_{\text{ss}}$ for some $m \geq 1$. Let $K$ be an imaginary quadratic field satisfying the Heegner hypothesis for both $N$ and $N'$. Let $P \in E(K)$ and $P' \in E'(K)$ be the Heegner points. Assume $p$ is split in $K$. Then we have

$$\prod_{\ell \mid pNN'/M} \left( \frac{|\tilde{E}_{\text{ns}}(\mathbb{F}_\ell)|}{\ell} \right) \cdot \log_{\omega_{E}} P \equiv \pm \prod_{\ell \mid pNN'/M} \left( \frac{|\tilde{E}'_{\text{ns}}(\mathbb{F}_\ell)|}{\ell} \right) \cdot \log_{\omega_{E'}} P' \pmod{p^m}.$$ 

Here

$$M = \prod_{\ell \mid \gcd(N,N')} \ell^\text{ord}_{\ell}(NN').$$

3.2. Proof of Theorem 1.4

For a prime $\ell \nmid Nd$, we have $a_\ell(E) = \pm a_\ell(E^{(d)})$ since $E^{(d)}$ is a quadratic twist of $E$. Since $E(\mathbb{Q})[2] \neq 0$, we know that $|E(\mathbb{F}_\ell)|$ and $|E^{(d)}(\mathbb{F}_\ell)|$ are even since the reduction mod $\ell$ map is injective on prime-to-$\ell$ torsion. Hence if $\ell \neq 2$, then $a_\ell(E)$, $a_\ell(E^{(d)})$ are also even. Since $a_\ell(E) = \pm a_\ell(E^{(d)})$, we obtain the following mod 4 congruence

$$a_\ell(E) \equiv a_\ell(E^{(d)}) \pmod{4}, \quad \text{for any } \ell \nmid 2Nd.$$ 

It follows that we have an isomorphism of $G_\mathbb{Q}$-representations

$$E[4]_{\text{ss}} \cong E^{(d)}[4]_{\text{ss}}.$$
Now we can apply Theorem 3.1 to $E' = E^{(d)}$, $p = 2$ and $m = 2$. By assumption, any prime $\ell | 2N$ splits in $K$. By the definition of $\mathcal{S}$, the prime $\ell = |d|$ splits in $K$. Notice the odd prime factors of $N' = N(E^{(d)})$ are exactly the odd prime factors of $N d$, thus $K$ also satisfies the Heegner hypothesis for $N'$.

Let $\ell | \gcd(N, N')$ be an odd prime. We have:

1) if $\ell | |N|$, then $a_{\ell}(E), a_{\ell}(E^{(d)}) \in \{\pm 1\}$ is determined by their local root numbers at $\ell$. By the definition of $\mathcal{N}$, we know that $\ell$ splits in $\mathbb{Q}(\sqrt{d})$, and hence $E/\mathbb{Q}_{\ell}$ and $E^{(d)}/\mathbb{Q}_{\ell}$ are isomorphic. It follows that $a_{\ell}(E) = a_{\ell}(E^{(d)})$.

2) if $\ell^2 | N$, then $a_{\ell}(E) = a_{\ell}(E^{(d)}) = 0$.

Therefore $M$ is divisible by all the prime factors of $\gcd(N, N')$. Notice the odd part of $\gcd(N, N')$ equals to the odd part of $N^d$, so the congruence formula in Theorem 3.1 implies

$$\prod_{\ell | |2d|} \frac{|\overline{E}^{\text{ns}}(\mathbb{F}_{\ell})|}{\ell} \cdot \log_{\omega_{\ell}} P \equiv \pm \prod_{\ell | |2d|} \frac{|\overline{E}^{(d), \text{ns}}(\mathbb{F}_{\ell})|}{\ell} \cdot \log_{\omega_{\ell}(d)} P^{(d)} \pmod{4}.$$ 

For $\ell = |d|$, we have

$$|E(\mathbb{F}_{\ell})| \not\equiv 0 \pmod{4}$$

by the definition of $\mathcal{S}$. Now Assumption $\star$ implies that the left-hand-side of (1) is nonzero mod 4. Hence the right-hand-side of (1) is also nonzero. In particular, the Heegner point $P^{(d)} \in E^{(d)}(K)$ is non-torsion, and hence $r_{\text{an}}(E^{(d)}/K) = 1$ by the theorem of Gross–Zagier [3] and Kolyvagin [6], [5], as desired.

4. Proof of Theorem 1.7

4.1. Elliptic curves with partial 2-torsion and no rational cyclic 4-isogeny

Let $E$ be an elliptic curve of conductor $N$. Assume $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. Then $\mathbb{Q}(E[2])/\mathbb{Q}$ is the quadratic extension $\mathbb{Q}(\sqrt{\Delta_{E}})$, where $\Delta_{E}$ is the discriminant of a Weierstrass equation of $E$.

Let $\phi : E \to E_{0} := E/E(\mathbb{Q})[2]$ be the natural 2-isogeny. By [4], Lem. 4.2 (i), $E$ has no rational cyclic 4-isogeny if and only if $\mathbb{Q}(E_{0}[2])/\mathbb{Q}$ is a quadratic extension. Assume we are in this case, then $\mathbb{Q}(E_{0}[2]) = \mathbb{Q}(\sqrt{\Delta_{E_{0}}})$. 
Lemma 4.1. Let \( \ell \nmid N \) be a prime. Then the following are equivalent:

1) \(|E(\mathbb{F}_\ell)| \not\equiv 0 \pmod{4}\),

2) \(E(\mathbb{F}_\ell)[2] \cong E_0(\mathbb{F}_\ell)[2] \cong \mathbb{Z}/2\mathbb{Z}\),

3) \(\ell\) is inert in both \(\mathbb{Q}(E[2])\) and \(\mathbb{Q}(E_0[2])\).

Proof. Since \(E\) and \(E_0\) are isogenous and \(\ell\) is a prime of good reduction, we know that \(|E(\mathbb{F}_\ell)| = |E_0(\mathbb{F}_\ell)|\). So \(|E(\mathbb{F}_\ell)| \not\equiv 0 \pmod{4}\) if and only if \(|E_0(\mathbb{F}_\ell)| \not\equiv 0 \pmod{4}\). In this case, certainly (2) holds. Conversely, if (2) holds, then \(E(\mathbb{F}_\ell)[4] \cong \mathbb{Z}/2\mathbb{Z}\) (otherwise \(E(\mathbb{F}_\ell)[4] \cong \mathbb{Z}/4\mathbb{Z}\), and thus \(E_0(\mathbb{F}_\ell)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\) generated by \(\phi(E(\mathbb{F}_\ell)[4])\) and the kernel of the dual isogeny \(\hat{\phi} : E_0 \to E\), hence \(|E(\mathbb{F}_\ell)| \not\equiv 0 \pmod{4}\). We have shown that (1) is equivalent to (2).

Moreover, \(E(\mathbb{F}_\ell)[2] \cong \mathbb{Z}/2\mathbb{Z}\) (resp. \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\)) if and only if \(\mathbb{Q}(\sqrt{\ell})/\mathbb{Q}\ell\) is a quadratic extension (resp. the trivial extension), if and only if \(\ell\) is inert (resp. split) in \(\mathbb{Q}(E[2])\). Similarly we know that \(E_0(\mathbb{F}_\ell)[2] \cong \mathbb{Z}/2\mathbb{Z}\) if and only if \(\ell\) is inert in \(\mathbb{Q}(E_0[2])\). It follows that (2) is equivalent to (3). \(\square\)

4.2. Proof of Theorem 1.7

By assumption, the fields \(\mathbb{Q}(E[2], E_0[2]), \mathbb{Q}(\sqrt{q})\) \((q\) runs all odd prime \(q \mid N)\) are linearly disjoint. Since \(K\) satisfies the Heegner hypothesis for \(N\) and 2 splits in \(K\), we know the discriminant \(d_K\) of \(K\) is coprime to \(2\), hence \(K\) is also linearly disjoint from the fields \(\mathbb{Q}(E[2], E_0[2])\) and \(\mathbb{Q}(\sqrt{q})\)'s. It follows from Chebotarev’s density that there is a positive density set \(\mathcal{T}\) of primes \(\ell \nmid 2N\) such that

1) \(\ell\) is split in \(K\),

2) \(\ell\) is inert in both \(\mathbb{Q}(E[2])\) and \(\mathbb{Q}(E_0[2])\),

3) \(\ell\) is split in \(\mathbb{Q}(\sqrt{q})\) for any odd prime \(q \mid N\).

By Lemma 4.1 we know \(\mathcal{T} \subseteq \mathcal{S}\). For \(\ell \in \mathcal{T}\), we consider \(d = \ell^* := (-1)^{(\ell-1)/2}\ell\). By the quadratic reciprocity law, we know that odd \(q \mid N\) is split in \(\mathbb{Q}(\sqrt{\ell})\) if and only if \(\ell\) is split in \(\mathbb{Q}(\sqrt{q})\). In particular, for any \(\ell \in \mathcal{T}\), we have \(\ell^* \in \mathcal{N}\). Now Theorem 1.4 implies that \(r_{an}(E^{(\ell^*)}/K) = 1\). Moreover,

\[
r_{an}(E^{(\ell^*)}/\mathbb{Q}) = \begin{cases} 0, & w(E^{(\ell^*)}/\mathbb{Q}) = +1, \\ 1, & w(E^{(\ell^*)}/\mathbb{Q}) = -1. \end{cases}
\]
Since $\mathbb{Q}(\sqrt{\ell^*})$ has discriminant coprime to $2N$, we have the well known formula

$$w(E^{(\ell^*)}/\mathbb{Q}) = w(E/\mathbb{Q}) \cdot \left(\frac{\ell^*}{-N}\right).$$

By the quadratic reciprocity law, we obtain

$$w(E^{(\ell^*)}/\mathbb{Q}) = w(E/\mathbb{Q}) \cdot \left(\frac{-N}{\ell}\right).$$

By assumption, $\mathbb{Q}(\sqrt{-N})$ is also linearly disjoint from the fields considered above, hence the global root number $w(E^{(\ell^*)}/\mathbb{Q})$ takes both signs for a positive proportion of $\ell \in \mathcal{T}$ by Chebotarev’s density. Therefore $r_{an}(E^{(\ell^*)}/\mathbb{Q})$ takes both values 0 and 1 for a positive proportion of $\ell \in \mathcal{T}$, as desired.

Acknowledgements

The examples in this note are computed using Sage ([11]).

References


Prime twists of elliptic curves


Department of Mathematics, Massachusetts Institute of Technology
77 Massachusetts Avenue, Cambridge, MA 02139-4307, USA
E-mail address: dkriz@mit.edu

Department of Mathematics, Columbia University
2990 Broadway, New York, NY 10027, USA
E-mail address: chaoli@math.columbia.edu

Received November 27, 2017