

AN ELLIPTIC CURVE OF RANK ≥ 34 AND ROOT NUMBER -1 OVER A QUADRATIC FIELD

DYLAN T. COSTA AND ÁLVARO LOZANO-ROBLEDO

ABSTRACT. In this article, we find a quadratic twist over $\mathbb{Q}$ of rank ≥ 2 (and ≥ 3 assuming parity) of an elliptic curve $E/\mathbb{Q}$ of rank ≥ 32 , recently found by Elkies, Klagsbrun, and Li. We use a family of quadratic twists of rank ≥ 2 over $\mathbb{Q}(t)$ constructed by Mestre to search for twists E^D with root number -1 , computing all root numbers without factoring the (very large) twisting parameter D . As a result, we exhibit an explicit integer D , with 411 digits (a square times an integer with 381 digits), such that E^D has root number -1 and two independent rational points. In particular, the rank of E over $\mathbb{Q}(\sqrt{D})$ is at least 34, unconditionally, and at least 35 if we assume the Parity Conjecture.

1. INTRODUCTION

Let F be a number field and let E/F be an elliptic curve. The Mordell–Weil theorem states that the group $E(F)$ of F -rational points on E is finitely generated and, therefore, we have an isomorphism

$$E(F) \cong E(F)_{\text{tors}} \oplus \mathbb{Z}^{R_{E/F}},$$

where $E(F)_{\text{tors}}$ is the finite subgroup of points of finite order, and $R_{E/F} = \text{rank}_{\mathbb{Z}} E(F) \geq 0$ is the rank of E over F . It is not known whether the rank of elliptic curves over $\mathbb{Q}$ can be arbitrarily large. Recently, Noam Elkies, Zev Klagsbrun, and Samuel Li have found an elliptic curve $E/\mathbb{Q}$ with $R_{E/\mathbb{Q}} \geq 32$ (see [4] and Section 2 below), which has the largest known rank over $\mathbb{Q}$ as of the writing of this article.

In this article, we investigate rank growth of E when we base extend to a quadratic field $K = \mathbb{Q}(\sqrt{D})$. Let E^D denote the quadratic twist of E by D ; then it is well known that

$$(1) \quad R_{E/K} = R_{E/\mathbb{Q}} + R_{E^D/\mathbb{Q}}$$

(see [5], or [10, Ch. X]); in particular, the rank of E grows from $\mathbb{Q}$ to K if and only if E^D has positive rank. Moreover, if $W(E^D) = -1$ and E^D has two independent rational points, then the Parity Conjecture (Conjecture 2.1) implies that $R_{E^D/\mathbb{Q}} \geq 3$. Mestre has constructed a family of quadratic twists of E with two independent points over $\mathbb{Q}(t)$ (see [6], and also [9], [11], [3]), so our task is reduced to finding a specialization $t \in \mathbb{Q}$ for which the twist has root number -1 . The main difficulty is that the resulting twisting parameters have hundreds of digits that are hard to factor, so the usual computation of $W(E^D)$ via the conductor of E^D is not available. In this paper, we prove the following result:

Theorem 1.1. *Let $E/\mathbb{Q}$ be the elliptic curve of Section 2, with short Weierstrass model $y^2 = x^3 + ax + b$ as in Section 3, let*

$$g(t) = -ab(t^2 + 1)(b^2(t^4 + t^2 + 1)^3 + a^3t^4(t^2 + 1)^2) \in \mathbb{Z}[t],$$

let $D = g(3)$, and let $K = \mathbb{Q}(\sqrt{D})$. Then

- (1) $W(E/\mathbb{Q}) = 1$,
- (2) $W(E^D/\mathbb{Q}) = -1$, and $R_{E^D/\mathbb{Q}} \geq 2$.

Thus, $R_{E/K} \geq 34$. Moreover, if we assume the Parity Conjecture for elliptic curves over $\mathbb{Q}$, or $\text{III}(E^D/\mathbb{Q})[p^\infty]$ is finite for some prime p , then $R_{E^D/\mathbb{Q}} \geq 3$ and $R_{E/K} \geq 35$.

The integer D has 411 digits. After removing square factors of D , we have $K = \mathbb{Q}(\sqrt{D_0})$ where $D_0 = 5 \cdot 29 \cdot 67 \cdot 191 \cdot 269 \cdot 521 \cdot 709 \cdot 37847 \cdot C$ is an integer with 381 digits (see Example 4.3), and C is a composite number with 362 digits that we have not factored. The proof of Theorem 1.1 will avoid factoring C .

1.1. Structure of the article. The article is organized as follows. In Section 2 we describe the curve of Elkies, Klagsbrun, and Li, and we compute its global root number. In Section 3 we recall Mestre's family of quadratic twists of rank ≥ 2 . In Section 4 we explain how to compute root numbers of twists without factoring the twisting parameter, and in Section 5 we explain how to prove the independence of the two points without computing heights. In Section 6 we describe our search for twists of root number -1 in Mestre's family. Finally, Theorem 1.1 is shown in Section 7.

1.2. Acknowledgements: The authors thank Noam Elkies, Zev Klagsbrun, and Samuel Li for making their curve publicly available. We would like to thank ICARM (which is supported by NSF Grant DMS 2425401). The computations in this article were done with Magma [1], and we used Claude Opus 5.5 to help write the Magma code to carry out the searches and verify the results. The code and data are available at <https://github.com/alozanoroble/rank35>; in particular, the Magma file `g3-twist-data.m` verifies every claim about the case $t = 3$ when it is loaded.

1.3. Declaration of AI use: We have used Claude Opus 5.5 for literature review, to help us write Magma code, and to help us search for a twisting parameter D such that E^D has the properties in Theorem 1.1. Claude also helped putting together a first draft of this paper, but the authors rewrote it for readability.

2. THE CURVE OF ELKIES, KLAGSBRUN, AND LI

Let $E/\mathbb{Q}$ be the elliptic curve given by $E : y^2 + xy = x^3 + a_4x + a_6$, with

$$\begin{aligned} a_4 &= -2862392899139891916550046700194750245224 \\ &\quad 0040593445344054331428726899413, \\ a_6 &= 16366380970220279630250861194633604823688757308892533 \\ &\quad 34875693440181143871885452358966522018914326964558817. \end{aligned}$$

This curve was found by Noam Elkies, Zev Klagsbrun, and Samuel Li by specializing a rank 17 fibration of the known K3 surface of discriminant 1152, and it was submitted to the ICARM elliptic curve rank leaderboard as curve #4239 (see [4]), together with 32 rational points. We have verified with Magma that the height regulator of these points is approximately $7.166 \cdot 10^{42} \neq 0$ (with Magma's normalization of the canonical height), and that $E(\mathbb{Q})_{\text{tors}}$ is trivial. Hence, $R_{E/\mathbb{Q}} \geq 32$.

The model given above is minimal, and the conductor of E is

$$N_E = 2 \cdot 3 \cdot 5^2 \cdot 11^2 \cdot 13 \cdot 17 \cdot 23 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 89 \cdot p \cdot q,$$

where

$$\begin{aligned} p &= 2220713642109042278879558804334283, \\ q &= 3500766112881427717056865531427442780770809 \\ &\quad 0794959852326328757722465802911598967036101 \\ &\quad 6516064255191976556239262775289081591134547. \end{aligned}$$

The curve E has additive reduction at 5 (of Kodaira type I_0^*) and at 11 (of type IV), and multiplicative reduction at all other bad primes. The discriminant and the conductor agree with the values on the ICARM website.

The root number of E , denoted $W(E/\mathbb{Q})$, is not listed in [4], so we have computed it. The local root numbers $W_\ell(E/\mathbb{Q})$ are as follows:

ℓ	2	3	5	11	13	17	23	31	37	41	43	53	89	p	q
type	I_{14}	I_9	I_0^*	IV	I_2	I_2	I_2	I_2	I_3	I_5	I_2	I_2	I_2	I_1	I_1
$W_\ell(E/\mathbb{Q})$	-1	-1	1	-1	1	1	1	1	-1	-1	1	1	1	1	1

Since $W_\infty = -1$ for every elliptic curve over $\mathbb{Q}$, we compute the global root number $W(E/\mathbb{Q})$ as

$$W(E) = W_\infty(E/\mathbb{Q}) \prod_{\ell|N_E} W_\ell(E/\mathbb{Q}) = (-1) \cdot (-1)^5 = 1.$$

Thus, the Parity Conjecture below predicts that $R_{E/\mathbb{Q}}$ is even.

Conjecture 2.1 (Parity Conjecture). *Let $E/\mathbb{Q}$ be an elliptic curve. Then $W(E/\mathbb{Q}) = (-1)^{R_{E/\mathbb{Q}}}$.*

3. MESTRE'S FAMILY OF QUADRATIC TWISTS OF RANK ≥ 2

Since we are working over $\mathbb{Q}$, the curve E can be put into a short Weierstrass model. Explicitly, the change of variables $(x, y) \mapsto (36x + 3, 108(2y + x))$ takes the model of Section 2 to a short Weierstrass model, which we write again as $E : y^2 = x^3 + ax + b$, where $a = -27c_4$ and $b = -54c_6$ are given by

$$\begin{aligned} a &= -37096611972852999238488605234523963178103092609105165894413531630061639275, \\ b &= 76358987054659736642898417989682546776692102018928001307426168848663 \\ &\quad 338020996943087257548997707433748641083750. \end{aligned}$$

We define

$$(2) \quad g(t) = -ab(t^2 + 1)(b^2(t^4 + t^2 + 1)^3 + a^3t^4(t^2 + 1)^2) \in \mathbb{Z}[t],$$

a polynomial of degree 14. Mestre showed in [6] that the quadratic twist

$$E_g : y^2 = x^3 + ag(t)^2x + bg(t)^3$$

has rank at least 2 over $\mathbb{Q}(t)$, and we shall use the explicit form of the construction given in [3, Example 4.1] (see also [9, Theorem 3.7] and [11, Theorem 3]), with two independent points

$$(3) \quad \begin{aligned} P(t) &= \left(-\frac{b}{a} \cdot \frac{(t^2 + t + 1)(t^2 - t + 1)}{t^2 + 1} \cdot g(t), \frac{g(t)^2}{a^2(t^2 + 1)^2} \right), \\ Q(t) &= \left(-\frac{b}{a} \cdot \frac{(t^2 + t + 1)(t^2 - t + 1)}{t^2(t^2 + 1)} \cdot g(t), \frac{g(t)^2}{a^2t^3(t^2 + 1)^2} \right). \end{aligned}$$

For $t_0 \in \mathbb{Q}$ with $t_0 \neq 0, \pm 1$ and $g(t_0) \neq 0$, we write $D(t_0)$ for the integer $\text{num}(g(t_0)) \cdot \text{den}(g(t_0))$, which is in the same square class as $g(t_0)$. Equivalently, if $t_0 = m/n$ in lowest terms, then $D(t_0)$ is in the same square class as the integer

$$G(m, n) = n^{14}g(m/n) = -ab(m^2 + n^2)(b^2(m^4 + m^2n^2 + n^4)^3 + a^3m^4n^4(m^2 + n^2)^2).$$

We also write $D_0(t_0)$ for the integer obtained from $G(m, n)$ by removing the square factors of all primes below 10^5 . Then $E^{D(t_0)} \cong E_{g(t_0)}$ over $\mathbb{Q}$, and $P(t_0)$ and $Q(t_0)$ are rational points on $E^{D(t_0)}$. We note that $g(-t) = g(t)$ and $g(1/t) = g(t)/t^{14}$, so the parameters $\pm t_0^{\pm 1}$ produce the same twist, and for $t_0 = \pm 1$ the formulas give $Q = \pm P$.

The polynomial $g(t)$ is the product of $-ab(t^2 + 1)$ and $I(t) = b^2(t^4 + t^2 + 1)^3 + a^3t^4(t^2 + 1)^2$. Since $b^2 \approx 5.8 \cdot 10^{219}$ and $a^3 \approx -5.1 \cdot 10^{220}$, the two terms in $I(t)$ have comparable size and opposite signs, and $I(t)$ vanishes at $t \approx \pm 1.3491$ and $t \approx \pm 0.7412$. In particular, these are the regions where $|g(t)|$, and therefore $|D(t)|$, is smallest.

4. ROOT NUMBERS OF THE TWISTS

We will use the following formulas of Rohrlich for local root numbers (see [8]).

Proposition 4.1. *Let $E/\mathbb{Q}$ be an elliptic curve and S be the set of primes of bad reduction of E , together with 2 and 3. Let D be a non-zero integer, and let M be the part of $|D|$ that is relatively prime to all the primes in S . Then*

$$W(E^D/\mathbb{Q}) = W_\infty(E^D/\mathbb{Q}) \cdot \prod_{p \in S} W_p(E^D/\mathbb{Q}) \cdot \left(\frac{-1}{M}\right),$$

where $W_\infty(E^D/\mathbb{Q}) = -1$, and $\left(\frac{-1}{M}\right)$ is the Jacobi symbol. Moreover, if $p \in S$ and r_p is an integer in the same class as D in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$, then $W_p(E^D/\mathbb{Q}) = W_p(E^{r_p}/\mathbb{Q})$.

Proof. Let $p \notin S$ be a prime. If $p \nmid D$, then E^D has good reduction at p , and $W_p(E^D/\mathbb{Q}) = 1$. If $p \mid D$, then $p \geq 5$ and E has good reduction at p . If $v_p(D)$ is even, then E^D is the twist of E by a character that is unramified at p , so E^D has good reduction at p , and $W_p(E^D/\mathbb{Q}) = 1$. If $v_p(D)$ is odd, then E^D has additive reduction of type I_0^* at p , and $W_p(E^D/\mathbb{Q}) = \left(\frac{-1}{p}\right)$ by Rohrlich's formulas ([8]). Hence,

$$\prod_{p \notin S} W_p(E^D/\mathbb{Q}) = \prod_{p \mid M, v_p(M) \text{ odd}} \left(\frac{-1}{p}\right) = \left(\frac{-1}{M}\right),$$

because the Jacobi symbol is multiplicative and the primes that divide M to an even power contribute trivially. The last assertion holds because E^D and E^{r_p} are isomorphic over $\mathbb{Q}_p$. $\square$

In practice, we choose small representatives r_p : if u is the odd part of D , we let $r_2 = 2^{v_2(D) \bmod 2} \cdot (u \bmod 8)$, and for odd $p \in S$ we let $r_p = p^{v_p(D) \bmod 2}$ times 1 or the least quadratic non-residue modulo p . Then each $W_p(E^{r_p})$ is computed directly in Magma, and the Jacobi symbol $\left(\frac{-1}{M}\right)$ does not require any factorization.

Remark 4.2. *For the curve E of Section 2, the local factors in Proposition 4.1 can also be written in closed form, which gives an independent check of the Magma computations. Let χ_D be the quadratic character of $\mathbb{Q}(\sqrt{D})$. If E has multiplicative reduction at ℓ (that is, $\ell \in S \setminus \{5, 11\}$), then by [8]*

$$W_\ell(E^D) = \begin{cases} W_\ell(E) \chi_D(\ell) & \text{if } \chi_D \text{ is unramified at } \ell, \\ \chi_D(-1) & \text{if } \chi_D \text{ is ramified at } \ell. \end{cases}$$

At $\ell = 5$ and $\ell = 11$, where E has potentially good reduction, the formulas for $\ell \geq 5$ give $W_5(E^D) = \left(\frac{-1}{5}\right) = 1$ and $W_{11}(E^D) = \left(\frac{-3}{11}\right) = \left(\frac{-1}{11}\right) = -1$ for every D , because the semistability defect of E^D at 5 is 1 or 2, and at 11 it is 3 or 6. In particular, these formulas avoid any computation of local root numbers at the wild primes 2 and 3 on models with very large coefficients.

Example 4.3. *Let $t = 3$ and $D = g(3)$. Then $D > 0$ has 411 digits, and*

$$D = 2^8 \cdot 3^{12} \cdot 5^{15} \cdot 7^4 \cdot 11^8 \cdot 29 \cdot 67 \cdot 191 \cdot 269 \cdot 521 \cdot 709 \cdot 37847 \cdot C,$$

where C is a 362-digit integer with no prime factors below 10^6 , which is not a perfect power, is composite (it fails a Miller–Rabin test), and is not divisible by p or q . In particular, $D = s^2 D_0$ with $s = 2^4 \cdot 3^6 \cdot 5^7 \cdot 7^2 \cdot 11^4$ and $D_0 = 5 \cdot 29 \cdot 67 \cdot 191 \cdot 269 \cdot 521 \cdot 709 \cdot 37847 \cdot C$, which has 381 digits, and $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D_0})$. The factor $M = D/(2^8 \cdot 3^{12} \cdot 5^{15} \cdot 11^8)$ of D relatively prime to S has 384 digits and $M \equiv 1 \pmod{4}$, so $\left(\frac{-1}{M}\right) = 1$. The local root numbers are $W_p(E^D) = -1$ for $p = 11, 31, 41$, and 89, and $W_p(E^D) = 1$ for all other $p \in S$. This agrees with Remark 4.2: χ_D is unramified at every $\ell \in S \setminus \{5\}$; the odd part of D is $\equiv 5 \pmod{8}$, so $\chi_D(2) = -1$; and, writing $D_\ell = D/\ell^{v_\ell(D)}$,

the symbol $\left(\frac{D_\ell}{\ell}\right)$ equals -1 for $\ell = 3, 31, 37, 89$ and 1 for $\ell = 13, 17, 23, 41, 43, 53, p, q$. Multiplying by the values of $W_\ell(E)$ in Section 2 gives the values above. Therefore, Proposition 4.1 shows that

$$W(E^D) = (-1) \cdot (-1)^4 \cdot 1 = -1.$$

5. INDEPENDENCE WITHOUT HEIGHTS

The canonical heights of points on E^D would require the factorization of the discriminant of E^D , so instead we prove independence using the 2-descent map.

Proposition 5.1. *Let θ be a root of $x^3 + ax + b$, and let $K_3 = \mathbb{Q}(\theta)$. Let $D \in \mathbb{Q}^\times$, let $E_D: y^2 = x^3 + aD^2x + bD^3$, and let $P, Q \in E_D(\mathbb{Q})$. If $x(P) - D\theta$, $x(Q) - D\theta$, and their product are not squares in K_3 , then P and Q are independent points in $E_D(\mathbb{Q})$.*

Proof. The polynomial $x^3 + ax + b$ is irreducible, so $E_D(\mathbb{Q})[2]$ is trivial and every torsion point of $E_D(\mathbb{Q})$ has odd order. The 2-descent map

$$\delta: E_D(\mathbb{Q})/2E_D(\mathbb{Q}) \rightarrow K_3^\times/(K_3^\times)^2, \quad (x, y) \mapsto x - D\theta,$$

is an injective homomorphism (see [10, Ch. X]), and our hypotheses say that $\delta(P)$ and $\delta(Q)$ are independent in the $\mathbb{F}_2$ -vector space $K_3^\times/(K_3^\times)^2$. Suppose that $mP + nQ = T$, where T is a torsion point and $\gcd(m, n) = 1$. Since T has odd order, $T \in 2E_D(\mathbb{Q})$, so $mP + nQ \in 2E_D(\mathbb{Q})$ and $\delta(P)^m \delta(Q)^n = 1$, with m or n odd, which is a contradiction. $\square$

To show that $\alpha = x - D\theta$ is not a square in K_3 , it suffices to find an odd prime ℓ and a simple root r of $x^3 + ax + b$ modulo ℓ (which corresponds to a prime $\mathfrak{l} \mid \ell$ of degree one in K_3 , with $\theta \equiv r \pmod{\mathfrak{l}}$) such that x and D are ℓ -integral and $x - Dr$ is a quadratic non-residue modulo ℓ . Indeed, α is then a unit at $\mathfrak{l}$ whose image in the residue field $\mathbb{F}_\ell$ is not a square.

Example 5.2. *Let $t = 3$ and $D = g(3)$. Then $x(P(3)) - D\theta$ is a non-square, as witnessed by $\ell = 61$ and $r = 15$, and $x(Q(3)) - D\theta$ and the product $(x(P(3)) - D\theta)(x(Q(3)) - D\theta)$ are both non-squares, as witnessed by $\ell = 47$ and $r = 37$. In both cases r is a simple root and $\ell \nmid 90a$, so $x(P(3))$ and $x(Q(3))$, whose denominators divide $10a$ and $90a$, respectively, are ℓ -integral. Hence, Proposition 5.1 shows that $P(3)$ and $Q(3)$ are independent points of infinite order on E^D .*

6. THE SEARCH WITHIN MESTRE'S FAMILY

We have run over all $t = m/n > 1$ in lowest terms with $m \leq 60$, which, by the symmetry $t \mapsto \pm t^{\pm 1}$, covers all parameters of height at most 60, for a total of 1101 parameters. For each t , we computed $\log_{10} |D_0(t)|$, where $D_0(t)$ is defined in Section 3, and for the smallest values we computed $W(E^{D(t)}/\mathbb{Q})$ via Proposition 4.1, with the local factors at S given by Remark 4.2 (and checked against Magma), and, when $W(E^{D(t)}/\mathbb{Q}) = -1$, we verified the hypotheses of Proposition 5.1. The ten smallest values are as follows:

t	13/10	53/31	31/22	2	28/25	52/29	13/11	11/2	20/11	5
$\log_{10} D_0(t) $	371.35	373.14	373.53	374.64	375.45	375.46	376.06	376.09	376.19	376.20
$W(E^{D(t)}/\mathbb{Q})$	1	-1	-1	1	-1	-1	1	1	-1	1

The values of $|D_0(t)|$ range from $10^{371.35}$ to $10^{405.53}$, so the cancellation in $I(t)$ only saves a few digits: rational numbers of small height do not come much closer to the zeros of $I(t)$ than the parameters in the table. The parameter $t = 3$, with $\log_{10} |D_0(3)| = 380.42$, is the 28th smallest. There are 16 parameters with $W(E^{D(t)}/\mathbb{Q}) = -1$ and $|D_0(t)| < |D_0(3)|$, namely

$$t = \frac{53}{31}, \frac{31}{22}, \frac{28}{25}, \frac{52}{29}, \frac{20}{11}, \frac{43}{29}, \frac{5}{2}, \frac{53}{49}, \frac{19}{4}, \frac{29}{17}, \frac{4}{3}, \frac{55}{23}, \frac{11}{5}, \frac{8}{5}, \frac{5}{3}, \frac{42}{11},$$

and for each of them the hypotheses of Proposition 5.1 hold, so the analogue of Theorem 1.1 holds with $D = D(t)$. For instance, for $t = 53/31$ the integer $D_0(t)$ has 374 digits, and the witnesses are $(\ell, r) = (61, 15)$ for P and $(47, 37)$ for Q and for the product. Among integer parameters, the

smallest values are $t = 2, 5, 12, 11, 17$, all with root number 1, followed by $t = 3$. We have chosen to present $t = 3$ because it is the integer parameter with the smallest $|D_0(t)|$ and $W(E^{D(t)}/\mathbb{Q}) = -1$, and because $D = g(3)$ is then simply a value of g .

7. PROOF OF THEOREM 1.1

Proof. The root number of E was computed in Section 2, and $W(E^D) = -1$ by Example 4.3. By Example 5.2, we have $R_{E^D/\mathbb{Q}} \geq 2$, and therefore by Eq. (1)

$$R_{E/K} = R_{E/\mathbb{Q}} + R_{E^D/\mathbb{Q}} \geq 32 + 2 = 34.$$

If we assume the Parity Conjecture for E^D , then $R_{E^D/\mathbb{Q}}$ is odd, because $W(E^D) = -1$, and since $R_{E^D/\mathbb{Q}} \geq 2$, we conclude that $R_{E^D/\mathbb{Q}} \geq 3$, and $R_{E/K} \geq 35$.

Finally, if $\text{III}(E^D/\mathbb{Q})[p^\infty]$ is finite, then $R_{E^D/\mathbb{Q}}$ coincides with the p^∞ -Selmer corank $s_p(E^D/\mathbb{Q})$, and the p -parity theorem (Monsky [7] for $p = 2$, and Dokchitser–Dokchitser [2] for all p) shows that $(-1)^{s_p(E^D/\mathbb{Q})} = W(E^D) = -1$, so the same conclusion follows. $\square$

Under the isomorphism $E_D \cong E$ over K , which on short models is given by $(X, Y) \mapsto (X/D, Y/(D\sqrt{D}))$, the points $P(3)$ and $Q(3)$ correspond to points $P_{33}, P_{34} \in E(K)$ of the form $(x, v\sqrt{D})$ with $x, v \in \mathbb{Q}$. The non-trivial automorphism $\sqrt{D} \mapsto -\sqrt{D}$ sends P_{33} and P_{34} to $-P_{33}$ and $-P_{34}$, respectively, so they span a plane in the (-1) -eigenspace of $E(K) \otimes \mathbb{Q}$, while the 32 points $P_1, \dots, P_{32}$ in $E(\mathbb{Q})$ span a 32-dimensional subspace of the $(+1)$ -eigenspace. Hence, the points $P_1, \dots, P_{34}$ are independent in $E(K)$. The coordinates of all these points are listed in the accompanying data files.

Remark 7.1. *For every prime p , the p -parity theorem shows, unconditionally, that $s_p(E/\mathbb{Q})$ is even and $s_p(E^D/\mathbb{Q})$ is odd. Since $s_p(E/\mathbb{Q}) \geq R_{E/\mathbb{Q}} \geq 32$ and $s_p(E^D/\mathbb{Q}) \geq R_{E^D/\mathbb{Q}} \geq 2$, it follows that $s_p(E^D/\mathbb{Q}) \geq 3$, and therefore $s_p(E/K) = s_p(E/\mathbb{Q}) + s_p(E^D/\mathbb{Q}) \geq 35$. Here the last equality holds for every p , because $\text{Gal}(K/\mathbb{Q})$ acts on the p^∞ -Selmer group of E/K tensored with $\mathbb{Q}_p$, and its (± 1) -eigenspaces are identified with the corresponding spaces for $E/\mathbb{Q}$ and $E^D/\mathbb{Q}$.*

REFERENCES

- [1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.
- [2] Tim Dokchitser and Vladimir Dokchitser. On the Birch–Swinnerton-Dyer quotients modulo squares. *Ann. of Math. (2)*, 172(1):567–596, 2010.
- [3] Ivica Gusić and Petra Tadić. Injectivity of the specialization homomorphism of elliptic curves. *J. Number Theory*, 148:137–152, 2015.
- [4] ICARM. Elliptic curve rank leaderboard, curve #4239. <https://elliptic-rank.icarm.cloud/curve/4239>. Accessed October 15, 2026.
- [5] Masanari Kida. On the rank of an elliptic curve in elementary 2-extensions. *Proc. Japan Acad. Ser. A Math. Sci.*, 69(10):422–425, 1993.
- [6] Jean-François Mestre. Rang des courbes elliptiques d’invariant donné. *C. R. Acad. Sci. Paris Sér. I*, 314:919–922, 1992.
- [7] Paul Monsky. Generalizing the Birch–Stephens theorem. I. Modular curves. *Math. Z.*, 221(3):415–420, 1996.
- [8] David E. Rohrlich. Variation of the root number in families of elliptic curves. *Compositio Math.*, 87(2):119–151, 1993.
- [9] Karl Rubin and Alice Silverberg. Rank frequencies for quadratic twists of elliptic curves. *Experiment. Math.*, 10(4):559–569, 2001.
- [10] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
- [11] C. L. Stewart and J. Top. On ranks of twists of elliptic curves and power-free values of binary forms. *J. Amer. Math. Soc.*, 8:943–973, 1995.

UNIVERSITY OF CONNECTICUT, DEPARTMENT OF MATHEMATICS, STORRS, CT 06269, USA
Email address: `dylan.costa@uconn.edu`
URL: `https://dylan-costa.github.io/`

UNIVERSITY OF CONNECTICUT, DEPARTMENT OF MATHEMATICS, STORRS, CT 06269, USA
Email address: `alvaro.lozano-robledo@uconn.edu`
URL: `http://alozano.clas.uconn.edu`