AN ELLIPTIC SURFACE WITH INFINITELY MANY FIBERS FOR WHICH THE RANK DOES NOT JUMP

DAVID ZYWINA

Abstract. Let E be a nonisotrivial elliptic curve over $\mathbb{Q}(T)$ and denote the rank of the abelian group $E(\mathbb{Q}(T))$ by r. For all but finitely many $t \in \mathbb{Q}$, specialization will give an elliptic curve E_t over $\mathbb{Q}$ for which the abelian group $E_t(\mathbb{Q})$ has rank at least r. Conjecturally, the set of $t \in \mathbb{Q}$ for which $E_t(\mathbb{Q})$ has rank exactly r has positive density. We produce the first known example for which $E_t(\mathbb{Q})$ has rank r for infinitely many $t \in \mathbb{Q}$. For our particular $E/\mathbb{Q}(T)$ which has rank 0, we will make use of a theorem of Green on 3-term arithmetic progressions in the primes to produce $t \in \mathbb{Q}$ for which E_t has only a few bad primes that we understand well enough to perform a 2-descent.

1. Introduction

Let E be an elliptic curve over the function field $\mathbb{Q}(T)$ that is nonisotrivial, i.e., its j-invariant does not lie in $\mathbb{Q}$. Fix a Weierstrass model of E with coefficients in $\mathbb{Q}[T]$ and denote its discriminant by Δ. For all $t \in \mathbb{Q}$ with $\Delta(t) \neq 0$, evaluating the coefficients of the model by t gives an elliptic curve E_t over $\mathbb{Q}$.

The group $E(\mathbb{Q}(T))$ is a finitely generated abelian group whose rank we will denote by r. A theorem of Silverman [Sil83] says that the group $E_t(\mathbb{Q})$ has rank *at least* r for all but finitely many $t \in \mathbb{Q}$. Let $\mathcal{N}(E)$ and $\mathcal{J}(E)$ be the set of $t \in \mathbb{Q}$ with $\Delta(t) \neq 0$ for which $E_t(\mathbb{Q})$ has rank equal to r and rank strictly greater than r, respectively.

Conjecturally the sets $\mathcal{N}(E)$ and $\mathcal{J}(E)$ both have positive density in $\mathbb{Q}$ with respect to the natural height, cf. [CP23, §4] for a heuristic. There has been much study on the set $\mathcal{J}(E)$ which describes the E_t for which their rank "jumps", cf. [Sal12] and the references therein. We will instead focus on the set $\mathcal{N}(E)$ and the following weaker conjecture.

Conjecture 1.1. *The set $\mathcal{N}(E)$ is infinite, i.e., there are infinitely many $t \in \mathbb{Q}$ for which $E_t(\mathbb{Q})$ has rank r.*

Our main result gives the first unconditional example for which Conjecture 1.1 holds.

Theorem 1.2. *Let $E/\mathbb{Q}(T)$ be the elliptic curve defined by the equation $y^2 = x(x^2 - x + T)$. The group $E(\mathbb{Q}(T))$ has rank 0 and $E_t(\mathbb{Q})$ has rank 0 for infinitely many $t \in \mathbb{Q}$.*

Take $E/\mathbb{Q}(T)$ as in Theorem 1.2. The goal is to find specializations $E_t/\mathbb{Q}$ for which the curve has few bad primes and for which they are all explicitly understood. In order to bound the rank of $E_t(\mathbb{Q})$, we will bound the cardinality of its 2-Selmer group and this will depend on the knowledge of these bad primes.

Let us describe the specializations we use in our proof of Theorem 1.2. Take any positive integers m and n for which m, $m+n$ and $m+2n$ are all primes that are congruent to 3

2020 *Mathematics Subject Classification.* Primary 11G18; Secondary 14J27.

modulo 8. With $t := \frac{m+n}{2m} \in \mathbb{Q}$, we shall prove that $E_t(\mathbb{Q})$ has rank 0. The elliptic curve E_t has good reduction away from the primes 2, m, $m+n$ and $m+2n$.

A theorem of Green [Gre05], later generalized by Green and Tao [GT08], will be used to show that there are infinitely many such arithmetic progressions of primes; this is the source of the infiniteness in Theorem 1.2. Alternatively, this could be proved with a minor modification of the classical circle method argument that van der Corput used in 1939 to prove that there are infinitely many 3-term arithmetic progressions of primes.

For our elliptic curve E, it is easy to show that the set $\mathcal{J}(E)$ is also infinite. Indeed, using Silverman's result one can prove that $(1, b)$ is a point of infinite order on E_{b^2} for all but finitely many $b \in \mathbb{Q}$.

In a followup paper [Zyw25], we will give another example of Conjecture 1.1 with $r = 2$.

1.1. **Some earlier conditional results.** Let $E/\mathbb{Q}(T)$ be the elliptic curve given by $y^2 = x(x+1)(x+T)$. Caro and Pasten [CP23] showed that E satisfies Conjecture 1.1 if there are infinitely many Mersenne primes. Moreover, given any Mersenne prime $p = 2^q - 1$ with $q \geq 5$, they show that $E_{2^q}(\mathbb{Q})$ has rank 0. Note that such an elliptic curve E_{2^q} has good reduction away from 2 and p. The existence of infinitely many Mersenne primes is of course a famous open problem.

Let $E/\mathbb{Q}(T)$ be the elliptic curve given by $y^2 = x^3 - (T+1)/4 \cdot x^2 - x$. If p is a prime of the form $t^2 + 64$ for an integer t, then one can show that $E_t(\mathbb{Q})$ has rank 0. These elliptic curves have been studied in [Neu71, Set75, SW04]. Note that such an elliptic curve E_t has good reduction away from p. The existence of infinitely many primes of the form $t^2 + 64$ with $t \in \mathbb{Z}$ is an open problem (a special case of the Bunyakovsky conjecture).

1.2. **Aside: the isotrivial case.** For Conjecture 1.1, it is important that E is assumed to be nonisotrivial and not just nonconstant. Consider the *isotrivial* elliptic curve $E/\mathbb{Q}(T)$ defined by $y^2 = x(x^2 - (7 + 7T^4))^2$. Cassels and Schinzel [CS82] observed that $E(\mathbb{Q}(T))$ has rank 0 and expected that $E_t(\mathbb{Q})$ has rank at least 1 for all $t \in \mathbb{Q}$. Indeed, the root number of each E_t is -1 and hence the rank of $E_t(\mathbb{Q})$ should be odd by the parity conjecture.

It is straightforward to find isotrivial and nonconstant examples for which the conclusion of Conjecture 1.1 holds. Consider the elliptic curve $E/\mathbb{Q}(T)$ defined by the equation $y^2 = x^3 + Tx$. Then $E_p(\mathbb{Q})$ has rank 0 for all primes p that are congruent to 7 or 11 modulo 16, cf. [Sil09, Proposition 6.2].

What makes the nonisotrivial case more difficult is that it is harder to produce $t \in \mathbb{Q}$ for which E_t has bad reduction at only a few primes which are easy to describe. This is clear from our example and the earlier conditional examples in §1.1.

2. Main computation

Consider any positive integers m and n for which m, $m+n$ and $m+2n$ are all primes that are congruent to 3 modulo 8. Set $a := -4m^2$ and $b := 8m^3(m+n)$, and define the elliptic curve E over $\mathbb{Q}$ by

$$y^2 = x(x^2 + ax + b) = x(x^2 - 4m^2x + 8m^3(m+n)). \tag{2.1}$$

In this section we shall prove that $E(\mathbb{Q})$ has rank 0.

Remark 2.1. Set $t := (m+n)/(2m) \in \mathbb{Q}$. In our proof of Theorem 1.2 in §3, we will see that this curve is isomorphic to the elliptic curve $E_t/\mathbb{Q}$ with notation as in Theorem 1.2.

Set $a' := -2a = 8m^2$ and $b' := a^2 - 4b = -16m^3(m+2n)$, and define the elliptic curve E' over $\mathbb{Q}$ by

$$y^2 = x(x^2 + a'x + b') = x(x^2 + 8m^2x - 16m^3(m+2n)). \tag{2.2}$$

There is an isogeny $\phi\colon E \to E'$ given by $\phi(x,y) = (y^2/x^2, y(b-x^2)/x^2)$ whose kernel $E[\phi]$ is cyclic of order 2 and generated by $(0,0)$. Let $\hat{\phi}\colon E' \to E$ be the dual isogeny of ϕ; its kernel $E'[\hat{\phi}]$ is generated by the 2-torsion point $(0,0)$ of E'.

The discriminant of the Weierstrass models (2.1) is $-2^{14}m^9(m+n)^2(m+2n)$. Therefore, E and E' both have good reduction at all primes away from the set $\{2, m, m+n, m+2n\}$.

For each prime p, we let $c_p(E)$ and $c_p(E')$ be the Tamagawa number of E and E', respectively, at p. For each prime p, we will denote by ord_p the discrete valuation on $\mathbb{Q}_p$ with valuation ring $\mathbb{Z}_p$ normalized so that $\operatorname{ord}_p(p) = 1$.

Let $W(E)$ be the global root number of $E/\mathbb{Q}$. We will now show that $W(E) = 1$; the Birch and Swinnerton–Dyer conjecture would imply that this is a necessary condition for $E(\mathbb{Q})$ to have rank 0.

Lemma 2.2.

(i) *We have* $W(E) = 1$.
(ii) *We have* $\prod_p c_p(E) = 8$.

Proof. The root number $W(E)$ is the product of the local root numbers $W_v(E)$ over the places v of $\mathbb{Q}$, see [Roh93] for descriptions of the local root numbers. The local root number at the archimedean place is -1 and $W_p(E) = 1$ for all primes p for which E has good reduction. So to determine $W(E)$, we need only compute $W_p(E)$ with $p \in \{2, m, m+n, m+2n\}$.

The elliptic curve $E/\mathbb{Q}$ is given by the Weierstrass equation

$$y^2 = x(x^2 - 4m^2x + 8m^3(m+n)) = x((x-2m^2)^2 + 4m^3(m+2n))$$

which has discriminant $\Delta = -2^{14}m^9(m+n)^2(m+2n)$. We will make use of Tate's algorithm [Sil94, Algorithm 9.4] at each bad prime. In particular, we will find that the above Weierstrass model is minimal.

First consider the prime $p := m$. Applying Tate's algorithm, we find that E has Kodaira symbol III^* at p and hence $c_p(E) = 2$. If $p > 3$, then [Roh93, Proposition 2(v)] implies that $W_p(E) = \left(\frac{-2}{p}\right) = 1$, where the last equality uses that $p \equiv 3 \pmod 8$. When $p = 3$, we also have $W_p(E) = 1$; this can be read off [Hal98, Table 2] by using only the Kodaira symbol.

Consider the prime $p := m+n$. We have $\operatorname{ord}_p(\Delta) = 2$ and $y^2 \equiv -4m^2 \cdot x^2 + x^3 \pmod p$, so E has Kodaira symbol I_2 at p and hence $c_p(E) = 2$. The curve E has nonsplit multiplicative reduction at p since $\left(\frac{-4m^2}{p}\right) = \left(\frac{-1}{p}\right) = -1$, where the last equality uses that $p \equiv 3 \pmod 4$. We have $W_p(E) = 1$ by [Roh93, Proposition 3].

Consider the prime $p := m+2n$. We have $\operatorname{ord}_p(\Delta) = 1$ and

$$y^2 \equiv x(x-2m^2)^2 \equiv 2m^2 \cdot (x-2m^2)^2 + (x-2m^2)^3 \pmod p,$$

so E has Kodaira symbol I_1 at p and hence $c_p(E) = 1$. The curve E has nonsplit multiplicative reduction at p since $\left(\frac{2m^2}{p}\right) = \left(\frac{2}{p}\right) = -1$, where the last equality uses that $p \equiv 3 \pmod 8$. We have $W_p(E) = 1$ by [Roh93, Proposition 3].

Finally consider the prime $p = 2$. Applying Tate's algorithm, we find that E has Kodaira symbol III^* at 2 and hence $c_2(E) = 2$. The root number $W_2(E)$ can be computed using

Table 1 of [Hal98] (in the notation of the table, we have $\mathrm{ord}_2(c_4) = 7$, $\mathrm{ord}_2(c_6) = 10$, $\mathrm{ord}_2(\Delta) = 14$, $c_4' = -m^4 - 3m^3n \equiv 7 \pmod 8$ and $c_6' = -5m^6 - 9m^5n \equiv 3 \pmod 8$)). We have $W_2(E) = -1$.

We have $W(E) = -\prod_p W_p(E)$ and hence $W(E) = -(-1) = 1$ by the above computations. Since $c_p(E) = 1$ for each prime p for which E has good reduction, the above computations show that $\prod_p c_p(E) = 8$. □

Lemma 2.3. *We have* $\prod_p c_p(E') = 4$.

Proof. The elliptic curve $E'/\mathbb{Q}$ is isomorphic to the curve given by the Weierstrass equation

$$y^2 = x(x^2 + 2m^2x - m^3(m+2n)) = x((x+m^2)^2 - 2m^3(m+n))$$

which has discriminant $\Delta' = 2^7m^9(m+n)(m+2n)^2$ (replacing x and y in (2.2) by $4x$ and $8y$ will produce the above model). Using that m, $m+n$ and $m+2n$ are distinct odd primes, we can apply Tate's algorithm [Sil94, Algorithm 9.4] for the primes $p \in \{2, m, m+n, m+2n\}$ to show that the above Weierstrass model is minimal and that the Kodaira symbols of E at 2, m, $m+n$ and $m+2n$ are equal to II, III*, I$_1$ and I$_2$, respectively. In these cases, the Tamagawa numbers are determined by the Kodaira symbols and we have $c_2(E') = 1$, $c_m(E') = 2$, $c_{m+n}(E') = 1$ and $c_{m+2n}(E') = 2$, cf. [Sil94, Algorithm 9.4]. The lemma follows since $c_p(E') = 1$ for all primes p for which E' has good reduction. □

We will now compute the Selmer groups associated to the isogenies ϕ and $\hat{\phi}$. For basic definitions and results see [Sil09, §X.4]. In particular, [Sil09, §X.4 Example 4.8] contains the relevant formulae for our computations. Set $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Starting with the short exact sequence $0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0$ and taking Galois cohomology yields an exact sequence

$$0 \to E(\mathbb{Q})[\phi] \to E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathrm{Gal}_{\mathbb{Q}}, E[\phi]).$$

The image of δ lies in the ϕ-Selmer group $\mathrm{Sel}_\phi(E/\mathbb{Q}) \subseteq H^1(\mathrm{Gal}_{\mathbb{Q}}, E[\phi])$. Since $E[\phi]$ and $\{\pm 1\}$ are isomorphism $\mathrm{Gal}_{\mathbb{Q}}$-modules, we have isomorphisms

$$H^1(\mathrm{Gal}_{\mathbb{Q}}, E[\phi]) \xrightarrow{\sim} H^1(\mathrm{Gal}_{\mathbb{Q}}, \{\pm 1\}) \xrightarrow{\sim} \mathbb{Q}^\times/(\mathbb{Q}^\times)^2. \tag{2.3}$$

Using (2.3) as an identification, we may view δ as a homomorphism $E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. For any point $(x, y) \in E'(\mathbb{Q}) - \{0, (0,0)\}$, we have $\delta((x,y)) = x \cdot (\mathbb{Q}^\times)^2$. We also have $\delta(0) = 1$ and $\delta((0,0)) = b' \cdot (\mathbb{Q}^\times)^2$.

For each $d \in \mathbb{Q}^\times$, let C_d be the smooth projective curve over $\mathbb{Q}$ defined by the affine equation

$$dw^2 = d^2 + a'dz^2 + b'z^4.$$

Using (2.3), we can identify $\mathrm{Sel}_\phi(E/\mathbb{Q})$ with a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. In fact, we have

$$\mathrm{Sel}_\phi(E/\mathbb{Q}) = \{d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 : C_d(\mathbb{Q}_v) \neq \emptyset \text{ for all places } v \text{ of } \mathbb{Q}\}.$$

Lemma 2.4. *We have* $|\mathrm{Sel}_\phi(E/\mathbb{Q})| = 2$.

Proof. Take any squarefree integer d that represents a square class in $\mathrm{Sel}_\phi(E/\mathbb{Q})$. We have $C_d(\mathbb{Q}_v) \neq \emptyset$ for all places v of $\mathbb{Q}$. By changing variables, we see that C_d is isomorphic to the smooth projective curve C_d' over $\mathbb{Q}$ given by the affine model

$$y^2 = dx^4 + a'/4 \cdot x^2 + b'/(16d) = dx^4 + 2m^2x^2 - m^3(m+2n)/d. \tag{2.4}$$

First suppose that d is divisible by a prime $p \nmid m(m+2n)$. Since $C'_d(\mathbb{Q}_p) \neq \emptyset$, there is a point $(x,y) \in \mathbb{Q}_p^2$ satisfying (2.4); the points at infinity are not defined over $\mathbb{Q}_p$ since d is not a square in $\mathbb{Q}_p$. If $x \in \mathbb{Z}_p$, then from (2.4) we find that $\operatorname{ord}_p(y^2)$ is equal to $\operatorname{ord}_p(-m^3(m+2n)/d) = -1$. If $x \notin \mathbb{Z}_p$, then from (2.4) we find that $\operatorname{ord}_p(y^2)$ is equal to $\operatorname{ord}_p(dx^4) = 1 + 4\operatorname{ord}_p(x)$. In either case, $\operatorname{ord}_p(y^2) = 2\operatorname{ord}_p(y)$ is an odd integer which is a contradiction. Therefore, if a prime divides d, then it must be m or $m+2n$. In particular, $d \in \{\pm 1, \pm m, \pm(m+2n), \pm m(m+2n)\}$.

Now suppose that $d \equiv \pm 3 \pmod 8$. The integer d is not a square in $\mathbb{Q}_2$, so the points at infinity of the model (2.4) are not defined over $\mathbb{Q}_2$. Since $C'_d(\mathbb{Q}_2) \neq \emptyset$, there is a point $(x,y) \in \mathbb{Q}_2^2$ satisfying (2.4). First suppose that $x \in \mathbb{Z}_2$ and hence $y \in \mathbb{Z}_2$ as well. If $x \in 2\mathbb{Z}_2$, then $y^2 \equiv -m^3(m+2n)/d \equiv \pm 3 \pmod 8$. If $x \in \mathbb{Z}_2^\times$, then $y^2 \equiv d + 2 - 1/d \equiv d + 2 - d \equiv 2 \pmod 8$. In both of these computations we have used that m and $m+2n$ are congruent to 3 modulo 8. Since 3, -3 and 2 are not squares modulo 8, we deduce that $x \notin \mathbb{Z}_2$. Define $e := -\operatorname{ord}_2(x) \geq 1$. Since m and d are odd, we find that $2\operatorname{ord}_2(y) = \operatorname{ord}_2(y^2) = \operatorname{ord}_2(dx^4) = -4e$ and hence $\operatorname{ord}_2(y) = -2e$. Multiplying (2.4) by 2^{4e} gives $(2^{2e}y)^2 = d(2^e x)^4 + 2^{2e+1}m^2(2^e x)^2 - 2^{4e}m^3(m+2n)/d$. Reducing modulo 8, we find that d is a square modulo 8 which contradicts that $d \equiv \pm 3 \pmod 8$.

We thus have $d \not\equiv \pm 3 \pmod 8$. Since m and $m+2n$ are congruent to 3 modulo 8, we must have $d \in \{\pm 1, \pm m(m+2n)\}$.

Now suppose that $d = -1$. The curve C'_d is given by the model

$$y^2 = -x^4 + 2m^2x^2 + m^3(m+2n) = -(x^2 - m^2)^2 + 2m^3(m+n). \tag{2.5}$$

Set $p := m+n$. We note that -1 is not a square modulo p since $p \equiv 3 \pmod 4$. The integer -1 is not a square in $\mathbb{Q}_p$ so the points at infinity of the model of C'_d are not defined over $\mathbb{Q}_p$. Since $C'_d(\mathbb{Q}_p) \neq \emptyset$, there is a point $(x,y) \in \mathbb{Q}_p^2$ satisfying (2.5). Define $z := x^2 - m^2 \in \mathbb{Q}_p$; we have $y^2 = -z^2 + 2m^3p$. If $z \in p\mathbb{Z}_p$, then $2\operatorname{ord}_p(y) = \operatorname{ord}_p(2m^3p) = 1$ which is impossible. If $z \in \mathbb{Z}_p^\times$, then $y^2 \equiv -z^2 \pmod p$ and hence -1 is a square modulo p which is impossible. Define $e := -\operatorname{ord}_p(z) \geq 1$. We have $2\operatorname{ord}_p(y) = \operatorname{ord}_p(y^2) = \operatorname{ord}_p(z^2) = -2e$ and hence $\operatorname{ord}_p(y) = -e$. Therefore, $(p^e y)^2 = -(p^e z)^2 + 2m^3p^{1+2e}$ and reducing modulo p shows that -1 is a square modulo p which is impossible. Therefore, $d \neq -1$.

We have now shown that every element of $\operatorname{Sel}_\phi(E/\mathbb{Q})$ is represented by the square class of an integer $d \in \{1, \pm m(m+2n)\}$. Since $\operatorname{Sel}_\phi(E/\mathbb{Q})$ is an abelian 2-group, it must be cyclic of order 1 or 2. The group $\operatorname{Sel}_\phi(E/\mathbb{Q})$ has order 2 since it contains $\delta((0,0)) = b' \cdot (\mathbb{Q}^\times)^2 = -m(m+2n) \cdot (\mathbb{Q}^\times)^2$ and $m(m+2n)$ is not a square. ∎

We now compute the cardinality of the Selmer group $\operatorname{Sel}_{\hat\phi}(E'/\mathbb{Q})$.

Lemma 2.5. *We have* $|\operatorname{Sel}_{\hat\phi}(E'/\mathbb{Q})| = 2$.

Proof. For a choice of minimal Weierstrass model $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ of $E/\mathbb{Q}$, we define the invariant differential $\omega := dx/(2y + a_1x + a_3)$ on E. We denote the integral of $|\omega|$ over $E(\mathbb{R})$ by Ω_E. We similarly define a differential ω' on E' and a period $\Omega_{E'}$.

By equation (6.2) of [SS04], which is a reformulation of a result of Cassels from [Cas65], we have

$$\frac{|\operatorname{Sel}_{\hat\phi}(E'/\mathbb{Q})|}{|\operatorname{Sel}_\phi(E/\mathbb{Q})|} = \frac{|E'(\mathbb{Q})[\hat\phi]|}{|E(\mathbb{Q})[\phi]|} \cdot \frac{\Omega_E}{\Omega_{E'}} \cdot \prod_p \frac{c_p(E)}{c_p(E')}.$$

We have $|\operatorname{Sel}_\phi(E/\mathbb{Q})| = 2$ by Lemma 2.4 and $\prod_p c_p(E)/c_p(E') = 2$ by Lemmas 2.2(ii) and 2.3. Therefore,

$$|\operatorname{Sel}_{\hat{\phi}}(E'/\mathbb{Q})| = 4 \cdot \Omega_E/\Omega_{E'}.$$

There is a unique real number c for which $c \cdot \phi^*\omega' = \omega$. From [DD15, Theorem 1.2], we have $\Omega_E/\Omega_{E'} = |c|$. As noted in the proof of [DD15, Theorem 8.2], we have $|c| \in \{1, 1/2\}$. Therefore, $\Omega_E/\Omega_{E'}$ is either 1 or 1/2.

Suppose that $\Omega_E/\Omega_{E'} = 1$. Since $\prod_p c_p(E)/c_p(E') = 2$, [DD15, Theorem 8.2] implies that the order of vanishing of the L-function $L(E, s)$ at $s = 1$ is odd. Equivalently, the global root number $W(E)$ is -1 which contradicts Lemma 2.2(i). Therefore, $\Omega_E/\Omega_{E'} = 1/2$ and we conclude that $|\operatorname{Sel}_{\hat{\phi}}(E'/\mathbb{Q})| = 2$. □

We can now bound the cardinality of the 2-Selmer group of $E/\mathbb{Q}$.

Lemma 2.6. *We have* $|\operatorname{Sel}_2(E/\mathbb{Q})| \leq 2$.

Proof. By [SS04, Lemma 6.1], we have an exact sequence

$$0 \to E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2]) \xrightarrow{\alpha} \operatorname{Sel}_\phi(E/\mathbb{Q}) \xrightarrow{\beta} \operatorname{Sel}_2(E/\mathbb{Q}) \xrightarrow{\gamma} \operatorname{Sel}_{\hat{\phi}}(E'/\mathbb{Q})$$

of groups. The discriminant of $x^2 - 4m^2x + 8m^3(m+n)$ is divisible by the prime $m+2n$ exactly once and hence is not a square. Therefore, $E(\mathbb{Q})[2] = \langle(0,0)\rangle$ and so $E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2])$ is a cyclic group of order 2. This implies that the injective homomorphism α is surjective since $|\operatorname{Sel}_\phi(E/\mathbb{Q})| = 2$ by Lemma 2.4. By the exactness, β is the zero map and hence γ is an injective homomorphism $\operatorname{Sel}_2(E/\mathbb{Q}) \hookrightarrow \operatorname{Sel}_{\hat{\phi}}(E'/\mathbb{Q})$. The lemma is now an immediate consequence of Lemma 2.5. □

Let r be the rank of $E(\mathbb{Q})$. Since $E(\mathbb{Q})$ has a point of order 2, we have $|E(\mathbb{Q})/2E(\mathbb{Q})| \geq 2^{1+r}$. There is an injective homomorphism $E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \operatorname{Sel}_2(E/\mathbb{Q})$ which implies that $E(\mathbb{Q})/2E(\mathbb{Q})$ has cardinality at most 2 by Lemma 2.6. So $2^{1+r} \leq 2$ and we conclude that $r = 0$.

3. Proof of Theorem 1.2

Let $\mathcal{A}$ be the set of primes that are congruent to 3 modulo 8; it has relative density 1/4 in the set of all primes. A theorem of Green [Gre05] implies that $\mathcal{A}$ contains infinitely many arithmetic progressions of length 3.

Now consider one of the infinitely many pairs (m, n) of positive integers for which m, $m+n$ and $m+2n$ are all primes that lie in $\mathcal{A}$. Define $t := (m+n)/(2m) \in \mathbb{Q}$. The elliptic curve $E_t/\mathbb{Q}$ is given by the equation $y^2 = x(x^2 - x + t)$. With $x' := 4m^2x$ and $y' := 8m^3y$, we find that E_t is isomorphic to the elliptic curve over $\mathbb{Q}$ given by the model

$$y'^2 = x'(x'^2 - 4m^2x' + 8m^3(m+n)).$$

By the computation of §2, we deduce that $E_t(\mathbb{Q})$ has rank 0. Note that $t = (m+n)/(2m)$ is in lowest terms, so from t we can recover the pair (m, n). We have thus proved that $E_t(\mathbb{Q})$ has rank 0 for infinitely many $t \in \mathbb{Q}$.

Finally let r be the rank of $E(\mathbb{Q}(T))$. From Silverman [Sil83], we know that r is less than or equal to the rank of $E_t(\mathbb{Q})$ for all but finitely many $t \in \mathbb{Q}$. Since we have shown that $E_t(\mathbb{Q})$ has rank 0 for infinitely many $t \in \mathbb{Q}$, we deduce that $r = 0$.

References

[CP23] Jerson Caro and Hector Pasten, *On the fibres of an elliptic surface where the rank does not jump*, Bull. Aust. Math. Soc. **108** (2023), no. 2, 276–282, DOI 10.1017/s0004972722001368. MR4640089 ↑1, 1.1

[Cas65] J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199, DOI 10.1515/crll.1965.217.180. MR179169 ↑2

[CS82] J. W. S. Cassels and A. Schinzel, *Selmer's conjecture and families of elliptic curves*, Bull. London Math. Soc. **14** (1982), no. 4, 345–348, DOI 10.1112/blms/14.4.345. MR663485 ↑1.2

[DD15] Tim Dokchitser and Vladimir Dokchitser, *Local invariants of isogenous elliptic curves*, Trans. Amer. Math. Soc. **367** (2015), no. 6, 4339–4358, DOI 10.1090/S0002-9947-2014-06271-5. MR3324930 ↑2

[Gre05] Ben Green, *Roth's theorem in the primes*, Ann. of Math. (2) **161** (2005), no. 3, 1609–1636, DOI 10.4007/annals.2005.161.1609. MR2180408 ↑1, 3

[GT08] Ben Green and Terence Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) **167** (2008), no. 2, 481–547, DOI 10.4007/annals.2008.167.481. MR2415379 ↑1

[Hal98] Emmanuel Halberstadt, *Signes locaux des courbes elliptiques en 2 et 3*, C. R. Acad. Sci. Paris Sér. I Math. **326** (1998), no. 9, 1047–1052, DOI 10.1016/S0764-4442(98)80060-8 (French, with English and French summaries). MR1647190 ↑2

[Neu71] Olaf Neumann, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. I*, Math. Nachr. **49** (1971), 107–123, DOI 10.1002/mana.19710490108 (German). MR337999 ↑1.1

[Roh93] David E. Rohrlich, *Variation of the root number in families of elliptic curves*, Compositio Math. **87** (1993), no. 2, 119–151. MR1219633 ↑2

[Sal12] Cecília Salgado, *On the rank of the fibers of rational elliptic surfaces*, Algebra Number Theory **6** (2012), no. 7, 1289–1314, DOI 10.2140/ant.2012.6.1289. MR3007150 ↑1

[SS04] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231, DOI 10.1090/S0002-9947-03-03366-X. MR2021618 ↑2, 2

[Set75] Bennett Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. (2) **10** (1975), 367–378, DOI 10.1112/jlms/s2-10.3.367. MR371904 ↑1.1

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 ↑1.2, 2

[Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 ↑2, 2

[Sil83] ———, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211, DOI 10.1515/crll.1983.342.197. MR703488 ↑1, 3

[SW04] William Stein and Mark Watkins, *Modular parametrizations of Neumann-Setzer elliptic curves*, Int. Math. Res. Not. **27** (2004), 1395–1405, DOI 10.1155/S1073792804133916. MR2052021 ↑1.1

[Zyw25] David Zywina, *There are infinitely many elliptic curves over the rationals of rank* 2 (2025). preprint. ↑1

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA

Email address: zywina@math.cornell.edu