THERE ARE INFINITELY MANY ELLIPTIC CURVES OVER THE RATIONALS OF RANK 2

DAVID ZYWINA

Abstract. We show that there are infinitely many elliptic curves $E/\mathbb{Q}$, up to isomorphism over $\overline{\mathbb{Q}}$, for which the finitely generated group $E(\mathbb{Q})$ has rank exactly 2. Our elliptic curves are given by explicit models and their rank is shown to be 2 via a 2-descent. That there are infinitely many such elliptic curves makes use of a theorem of Tao and Ziegler.

1. Introduction

For an elliptic curve E over $\mathbb{Q}$, the abelian group $E(\mathbb{Q})$ consisting of the rational points of E is finitely generated. The possible torsion subgroups of $E(\mathbb{Q})$ that can occur have been classified by Mazur [Maz77, Theorem 8]. On the other hand, the rank of E, i.e., the rank of $E(\mathbb{Q})$, is a more mysterious invariant. For each integer $0 \leq r \leq 1$, it is known that there are infinitely many elliptic curves over $\mathbb{Q}$ of rank r (for example, see [Sil09, Corollary X.6.2.1] and [Sat87]). Loosely, we expect "most" elliptic curves over $\mathbb{Q}$ to have rank 0 or 1.

There are in fact infinitely many elliptic curve over $\mathbb{Q}$ that have rank *at least* 2. Indeed, if one takes a nonisotrivial elliptic curve $\mathcal{E}$ over the function field $\mathbb{Q}(T)$ for which $\mathcal{E}(\mathbb{Q}(T))$ has rank 2, then specialization at all but finitely many $t \in \mathbb{Q}$ will produce an elliptic curve over $\mathbb{Q}$ of rank *at least* 2, cf. [Sil83]. Our main result gives what seems to be the first integer $r \geq 2$ that we can confirm is the rank of infinitely many elliptic curves over $\mathbb{Q}$.

Theorem 1.1. *There are infinitely many elliptic curves over $\mathbb{Q}$, up to isomorphism over $\overline{\mathbb{Q}}$, of rank 2.*

We will prove Theorem 1.1 by showing that a specific class of elliptic curves over $\mathbb{Q}$ has rank 2.

Theorem 1.2. *Let m and n be any natural numbers for which m, $m+16n^2$ and $m+25n^2$ are primes congruent to 11 modulo 24. Let E be the elliptic curve over $\mathbb{Q}$ defined by the equation*

$$y^2 = x^3 - 5(m+16n^2)x^2 + 4(m+16n^2)(m+25n^2)x.$$

Then $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2$.

We will make use of the *Polynomial Szemerédi theorem for primes* due to Tao and Ziegler [TZ08] to guarantee that there are infinitely many pairs (m, n) of natural numbers for which m, $m+16n^2$ and $m+25n^2$ are primes congruent to 11 modulo 24. This is the source of the infiniteness in our proof of Theorem 1.1.

With $E/\mathbb{Q}$ as in Theorem 1.2, we have the following points in $E(\mathbb{Q})$:

$$P_0 = (0,0), \quad P_1 = (m+16n^2, 6n(m+16n^2)), \quad P_2 = (36n^2, 12n(m-2n^2)).$$

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

The point P_0 has order 2 and our proof will show that P_1 and P_2 generate a free abelian group of rank 2. Moreover, we will see that the points P_0, P_1 and P_2 generate the group $E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

The bad primes of E are precisely 2, 3, m, $m + 16n^2$ and $m + 25n^2$. To determine $E(\mathbb{Q})/2E(\mathbb{Q})$ we will perform a descent using an isogeny of degree 2. Our complete knowledge of the bad primes will allow us to directly compute the relevant Selmer groups. For the elliptic curves $E/\mathbb{Q}$ we are considering, we are fortunate to always have $\text{Ш}(E/\mathbb{Q})[2] = 0$.

1.1. **Aside: remarks concerning our curves.** The proof of Theorem 1.2 is a straightforward and pleasant descent computation. The serious work in the theorem was finding these elliptic curves in the first place! Let us briefly make a few observations of the important properties that these curves have. This will hopefully serve as motivation. This material will not be used elsewhere in the paper.

Let $\mathcal{E}$ be the elliptic curve over the function field $\mathbb{Q}(T)$ defined by the Weierstrass equation

$$y^2 = x^3 - 5(T + 16)x^2 + 4(T + 16)(T + 25)x;$$

it has discriminant $2^8 3^2 T(T+16)^3(T+25)^2$. The two points $(T+16, 6(T+16))$ and $(36, 12(T-2))$ in $E(\mathbb{Q}(T))$ have infinite order and are independent. Moreover, $\mathcal{E}(\mathbb{Q}(T))$ has rank 2. The singular fibers of $\mathcal{E}$ are at 0, -16, -25 and ∞ with Kodaira symbols I_1, III, I_2 and I_0^*, respectively.

Since $\mathcal{E}$ is nonisotrivial, it produces infinitely many elliptic curves over $\mathbb{Q}$ of rank at least 2. For every $t \in \mathbb{Q} - \{0, -16, -25\}$, let $\mathcal{E}_t$ be the elliptic curve over $\mathbb{Q}$ obtained by replacing T by t. From a theorem of Silverman [Sil83], $\mathcal{E}_t$ has rank at least 2 for all but finitely many t. The challenge for us is that the ranks could be larger.

Now consider $t = m/n^2$ with m and n fixed natural numbers that are relative prime. The curve $\mathcal{E}_t$ is isomorphic to the elliptic curve $E/\mathbb{Q}$ defined by the equation in Theorem 1.2; the isomorphism is simply scaling the variables by suitable powers of n. The discriminant for the Weierstrass model of E is

$$2^8 \cdot 3^2 \cdot m \cdot (m + 16n^2)^3 \cdot (m + 25n^2)^2$$

which gives constraints on the possible bad primes of E. We chose t to have square denominator since otherwise the curve $\mathcal{E}_t$ might also have bad reduction at primes dividing the denominator of t (this was arranged by having the singular fiber of $\mathcal{E}$ at ∞ to have Kodaira symbol I_0^*).

We now assume that m and n are chosen so that m, $m+16n^2$ and $m+25n^2$ are all primes with $m > 5$. Using this, we find that $\mathcal{P} := \{2, 3, m, m + 16n^2, m + 25n^2\}$ is precisely the set of bad primes for E. Note that in order to apply the theorem of Tao and Ziegler and obtain infinitely many such pairs (m, n), it was important for the singular fibers of $\mathcal{E}$ to occur only at integers and ∞.

Let $W(E) \in \{\pm 1\}$ be the global root number of $E/\mathbb{Q}$. The *parity conjecture* predicts that the rank of E is even if and only if $W(E) = 1$. Since we are trying to find elliptic curves of rank 2, we should thus restrict to pairs (m, n) for which we know that $W(E) = 1$. We have $W(E) = -\prod_{p \in \mathcal{P}} W_p$, where W_p is the local root number of E at p. After some local root number computations, we find that

$$W(E) = W_2 \cdot W_3 \cdot (-1)^{\frac{m+1}{2}}.$$

The assumption $m \equiv 11 \pmod{24}$ in Theorem 1.2 implies that $W_2 = W_3 = 1$ and hence $W(E) = 1$. If instead we were to take $m \equiv 5 \pmod{24}$, then we would always have $W(E) = -1$. In the case $m \equiv 5 \pmod{24}$, a similar proof to that of this paper will show that there are infinitely many elliptic curves over $\mathbb{Q}$ with root number -1 and rank 2 or 3. This can be used to show that, assuming the parity conjecture, there are infinitely many elliptic curves over $\mathbb{Q}$ of rank 3. Similarly, there were earlier results showing that, under the parity conjecture, there are infinitely many elliptic curves over $\mathbb{Q}$ of rank 2, cf. [BJ16, Jeo19].

Our elliptic curve E has a rational 2-torsion point and we can thus perform a descent by using an isogeny $\phi\colon E \to E'$ of degree 2. In our proof of Theorem 1.2, we will compute the Selmer groups $\mathrm{Sel}_\phi(E/\mathbb{Q})$ and $\mathrm{Sel}_{\hat{\phi}}(E'/\mathbb{Q})$, where $\hat{\phi}\colon E' \to E$ is the dual isogeny of ϕ. The natural homomorphisms

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \hookrightarrow \mathrm{Sel}_\phi(E/\mathbb{Q}) \quad \text{and} \quad E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \hookrightarrow \mathrm{Sel}_{\hat{\phi}}(E'/\mathbb{Q}) \tag{1.1}$$

will be shown to be isomorphisms and from this we will compute $E(\mathbb{Q})/2E(\mathbb{Q})$.

The congruence conditions on m, $m+16n^2$ and $m+25n^2$ in Theorem 1.2 will be used during the Selmer group computations. Without these imposed congruences one can find examples where $E/\mathbb{Q}$ has root number 1 and the homomorphisms (1.1) are not both isomorphisms; in such cases we will have $Ш(E/\mathbb{Q})[2] \neq 0$.

This article is a sequel to [Zyw25] where we find an example of a nonisotrivial elliptic curve $\mathcal{E}$ over $\mathbb{Q}(T)$ for which $\mathcal{E}_t$ is an elliptic curve over $\mathbb{Q}$ of rank 0 for infinitely many $t \in \mathbb{Q}$. The computations here are much simpler that in [Zyw25] in part because the extra rational points give rise to elements in our Selmer groups.

2. Descent via two-isogeny

In this section, we recall basic definitions and results concerning descent via a two-isogeny. See [Sil09, §X.4], and especially [Sil09, §X.4 Example 4.8], for the relevant formulae.

We start with an elliptic curve $E/\mathbb{Q}$ defined by a Weierstrass equation $y^2 = x(x^2+ax+b)$, where a and b are integers. With $a' := -2a$ and $b' := a^2 - 4b$, we let E' be the elliptic curve over $\mathbb{Q}$ given by the model $y^2 = x(x^2 + a'x + b')$. There is an isogeny $\phi\colon E \to E'$ given by

$$\phi(x, y) = \Big(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2}\Big).$$

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'. We have

$$\hat{\phi}(x, y) = \Big(\frac{y^2}{4x^2}, \frac{y(b' - x^2)}{8x^2}\Big).$$

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

$$y^2 = dx^4 + a'x^2 + b'/d. \tag{2.1}$$

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

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

Since $E[\phi]$ and $\{\pm 1\}$ are isomorphic $\mathrm{Gal}_{\mathbb{Q}}$-modules, we have a natural isomorphism

$$H^1(\mathrm{Gal}_{\mathbb{Q}}, E[\phi]) \xrightarrow{\sim} H^1(\mathrm{Gal}_{\mathbb{Q}}, \{\pm 1\}) \xrightarrow{\sim} \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \tag{2.2}$$

where the last isomorphism is using that each extension of $\mathbb{Q}$ of degree at most 2 is obtained by adjoining the square root from a unique square class. Using the isomorphism (2.2), we may view δ as a homomorphism

$$\delta \colon E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

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 $\delta((0, 0)) = b' \cdot (\mathbb{Q}^\times)^2$.

Let $\mathrm{Sel}_\phi(E/\mathbb{Q}) \subseteq H^1(\mathrm{Gal}_{\mathbb{Q}}, E[\phi])$ be the ϕ-Selmer group of E. Using (2.2), we can identify $\mathrm{Sel}_\phi(E/\mathbb{Q})$ with a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. In fact, we have

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

which we will use as our working definition of the ϕ-Selmer group.

The importance of $\mathrm{Sel}_\phi(E/\mathbb{Q})$ is that it is a finite computable group that contains the image of δ. In particular, δ gives rise to an injective homomorphism

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \hookrightarrow \mathrm{Sel}_\phi(E/\mathbb{Q}).$$

For a prime p, we will denote by $\mathrm{ord}_p \colon \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ to be the p-adic discrete valuation normalized so that $\mathrm{ord}_p(p) = 1$.

Lemma 2.1. *Let d be a squarefree integer representing a square class in $\mathrm{Sel}_\phi(E/\mathbb{Q})$. Then d divides b'.*

Proof. Suppose that there is a prime $p|d$ that does not divide b'. By our assumptions on d, we will have $C_d(\mathbb{Q}_p) \neq \emptyset$. The integer d is not a square in $\mathbb{Q}_p$, since it is only divisible by p once, and hence (2.1) has no $\mathbb{Q}_p$-points at infinity. Fix a point $(x, y) \in \mathbb{Q}_p^2$ satisfying (2.1).

Suppose that $x \in \mathbb{Z}_p$. We have $dx^4 + a'x^2 \in \mathbb{Z}_p$ and $\mathrm{ord}_p(b'/d) = -1$, where we have used that a' and b' are integers and that $p \nmid b'$. Therefore, $\mathrm{ord}_p(y^2) = \mathrm{ord}_p(b'/d) = -1$ which contradicts that $\mathrm{ord}_p(y^2) = 2\,\mathrm{ord}_p(y)$ is an even integer. We thus have $x \notin \mathbb{Z}_p$.

Define $e := -\mathrm{ord}_p(x) \geq 1$. Comparing p-adic valuations, we find that $\mathrm{ord}_p(y^2) = \mathrm{ord}_p(dx^4) = -4e + 1$ which again contradicts that $\mathrm{ord}_p(y^2)$ is even. □

Similarly, we have a homomorphism $\delta' \colon E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ that has kernel $\hat{\phi}(E'(\mathbb{Q}))$ and the image of δ' lies in the $\hat{\phi}$-Selmer group $\mathrm{Sel}_{\hat{\phi}}(E'/\mathbb{Q}) \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

There is an exact sequence

$$0 \to E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2]) \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\hat{\phi}} E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \to 0.$$

Once we know the group $E(\mathbb{Q})/2E(\mathbb{Q})$, it will be straightforward to compute the rank of $E(\mathbb{Q})$.

3. Proof of Theorem 1.2

Let $E/\mathbb{Q}$ be an elliptic curve from Theorem 1.2; it is given by an equation

$$y^2 = x\big(x^2 - 5(m+16n^2)x + 4(m+16n^2)(m+25n^2)\big),$$

where m and n are natural numbers for which m, $m+16n^2$ and $m+25n^2$ are primes congruent to 11 modulo 24. The discriminant of this Weierstrass model is

$$\Delta = 2^8 \cdot 3^2 \cdot m \cdot (m+16n^2)^3 \cdot (m+25n^2)^2.$$

The above Weierstrass model of $E/\mathbb{Q}$ is minimal since the exponents of the primes dividing Δ are all strictly less than 12. Define the points $P_0 = (0,0)$ and $P_1 = (m+16n^2, 6n(m+16n^2))$ of $E(\mathbb{Q})$.

We follow the notation of §2; we have $a = -5(m+16n^2)$, $b = 4(m+16n^2)(m+25n^2)$, $a' = -2a = 10(m+16n^2)$ and $b' = a^2 - 4b = 9m(m+16n^2)$. Define the elliptic curve E' over $\mathbb{Q}$ by

$$y^2 = x(x^2 + a'x + b') = x\big(x^2 + 10(m+16n^2)x + 9m(m+16n^2)\big).$$

Define the points $Q_0 = (0,0)$ and $Q_1 = (-(m+16n^2), 12n(m+16n^2))$ of $E'(\mathbb{Q})$.

As in §2, we have an explicit isogeny $\phi\colon E \to E'$ of degree 2 with its dual isogeny $\hat{\phi}$. Along with P_0 and P_1, we also define a third point of $E(\mathbb{Q})$:

$$P_2 := \hat{\phi}(Q_1) = (36n^2, 12n(m-2n^2)).$$

3.1. **Selmer group computations.** We will now show that the Selmer groups $\mathrm{Sel}_\phi(E/\mathbb{Q})$ and $\mathrm{Sel}_{\hat{\phi}}(E/\mathbb{Q})$ both have cardinality at most 4. To ease notation, we will denote an element of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ by the unique squarefree integer it contains.

Lemma 3.1. *We have* $\mathrm{Sel}_\phi(E/\mathbb{Q}) \subseteq \{1, -m, -(m+16n^2), m(m+16n^2)\}$.

Proof. Take any squarefree integer d representing an element of $\mathrm{Sel}_\phi(E/\mathbb{Q})$. Let C_d be the smooth projective curve over $\mathbb{Q}$ defined by the affine equation

$$y^2 = dx^4 + 10(m+16n^2)x^2 + 9m(m+16n^2)/d. \tag{3.1}$$

Multiplying by d and completing the square gives

$$dy^2 = (dx^2 + 5(m+16n^2))^2 - 16(m+16n^2)(m+25n^2). \tag{3.2}$$

We have $C_d(\mathbb{Q}_p) \neq \emptyset$ for all primes p by our choice of d.

Suppose that $d \equiv 3 \pmod 4$. The model (3.1) has no $\mathbb{Q}_2$-point at infinity since d is not a square in $\mathbb{Q}_2$. Choose a pair $(x,y) \in \mathbb{Q}_2^2$ satisfying (3.1). If $x \in 2\mathbb{Z}_2$, then $y \in \mathbb{Z}_2$ and $y^2 \equiv 9m(m+16n^2)/d \equiv m^2/3 \equiv 3 \pmod 4$. We thus have $x \notin 2\mathbb{Z}_2$ since 3 is not a square modulo 4. Now suppose that $x \in \mathbb{Z}_2^\times$. By (3.2), we have $dy^2 = z^2 - 16(m+16n^2)(m+25n^2)$ with $z := dx^2 + 5(m+16n^2) \in \mathbb{Z}_2$ and $y \in \mathbb{Z}_2$. We have $z^2 \equiv dy^2 \equiv 3y^2 \pmod{16}$ from which we deduce that $z \equiv 0 \pmod 4$. Therefore, $dx^2 \equiv -5(m+16n^2) \equiv 1 \pmod 4$, where we have used that the prime $m+16n^2$ is 3 modulo 8. So $x^2 \equiv 3 \pmod 4$ which is a contradiction. Therefore, $x \notin \mathbb{Z}_2$. Define $e := -\mathrm{ord}_2(x) \geq 1$. We have $\mathrm{ord}_2(dx^4) = -4e$, $\mathrm{ord}_2(10(m+16n^2)x^2) = -2e+1$ and $\mathrm{ord}_2(9m(m+16n^2)/d) = 1$. From (3.1), we deduce that $\mathrm{ord}_2(y^2) = -4e$ and hence $\mathrm{ord}_2(y) = -2e$. Multiplying (3.1) by 2^{4e} gives $(2^{2e}y)^2 = d(2^e x)^4 + 2^{2e}10(m+16n^2)(2^e x)^2 + 2^{4e}9m(m+16n^2)/d$. Using that $2^{2e}y, 2^e x \in \mathbb{Z}_2^\times$ and reducing modulo 4, we find that d is a square modulo 4 which again is a contradiction. We conclude that $d \equiv 1 \pmod 4$.

By Lemma 2.1, d divides $9m(m+16n^2)$. Therefore, d lies in the subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ generated by -1, 3, m and $m+16n^2$. Since $d \equiv 1 \mod 4$ and all of the values -1, 3, m and $m+16n^2$ are congruent to 3 modulo 4, we have

$$d \in \{1, -3, -m, -(m+16n^2), 3m, 3(m+16n^2), m(m+16n^2), -3m(m+16n^2)\}. \tag{3.3}$$

Now suppose that d is not a square modulo the prime $p := m + 25n^2$. The model (3.1) has no $\mathbb{Q}_p$-point at infinity since d is not a square in $\mathbb{Q}_p$. Choose a pair $(x, y) \in \mathbb{Q}_p^2$ satisfying (3.1). First suppose that $x \in \mathbb{Z}_p$. By (3.2), we have $dy^2 = z^2 - 16(m+16n^2)p$ with $z \in \mathbb{Z}_p$. If $z \in \mathbb{Z}_p^\times$, then $dy^2 \equiv z^2 \pmod p$ with $z \not\equiv 0 \pmod p$ which contradicts that d is not a square modulo p. If $z \in p\mathbb{Z}_p$, then $dy^2 \equiv 16(m+16n^2)p \pmod{p^2}$ which implies that the even integer $2\operatorname{ord}_p(y) = \operatorname{ord}_p(y^2)$ is equal to 1. So we must have $x \notin \mathbb{Z}_p$. Define $e := -\operatorname{ord}_p(x) \geq 1$. We have $\operatorname{ord}_p(dx^4) = -4e$, $\operatorname{ord}_p(10(m+16n^2)x^2) = -2e$ and $\operatorname{ord}_p(9m(m+16n^2)/d) = 0$. From (3.1), we deduce that $\operatorname{ord}_p(y^2) = -4e$ and hence $\operatorname{ord}_p(y) = -2e$. Multiplying (3.1) by p^{4e} gives $(p^{2e}y)^2 = d(p^e x)^4 + p^{2e}10(m+16n^2)(p^e x)^2 + p^{4e}9m(m+16n^2)/d$. Using that $p^{2e}y, p^e x \in \mathbb{Z}_p^\times$ and reducing modulo p, we find that d is a square modulo p which again is a contradiction. We conclude that d is a square modulo p.

We now need to work out which of the integers in the set (3.3) are squares modulo $p = m + 25n^2$. Since $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$, we have $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{2}{3}\right) = 1$. We also have $\left(\frac{m+16n^2}{p}\right) = \left(\frac{-25n^2+16n^2}{p}\right) = \left(\frac{-9n^2}{p}\right) = \left(\frac{-1}{p}\right)$, where we have used $m \equiv -25n^2 \pmod p$ and $p \nmid n$ (since $n < p$). Applying these Legendre symbols to the integers in the set (3.3) and using that d is a square modulo p, we conclude that d lies in $\{1, -m, -(m+16n^2), m(m+16n^2)\}$. □

Lemma 3.2. *We have* $\operatorname{Sel}_{\hat\phi}(E'/\mathbb{Q}) \subseteq \{1, m+16n^2, m+25n^2, (m+16n^2)(m+25n^2)\}$.

Proof. Take any squarefree integer d representing an element of $\operatorname{Sel}_{\phi}(E'/\mathbb{Q})$. Let C'_d be the smooth projective curve over $\mathbb{Q}$ defined by the affine equation

$$y^2 = dx^4 - 5(m+16n^2)x^2 + 4(m+16n^2)(m+25n^2)/d. \tag{3.4}$$

Multiplying by d and completing the square gives

$$dy^2 = (dx^2 - \tfrac{5}{2}(m+16n^2))^2 - \tfrac{9}{4}m(m+16n^2). \tag{3.5}$$

Suppose that $d < 0$. Since d is not a square in $\mathbb{R}$, the model (3.4) does not have a real point at infinity. We have $C'_d(\mathbb{R}) \neq \emptyset$ by our choice of d, so there is a pair $(x, y) \in \mathbb{R}$ satisfying (3.4). Using that $d < 0$, we have

$$\begin{aligned}(dx^2 - \tfrac{5}{2}(m+16n^2))^2 - \tfrac{9}{4}m(m+16n^2) &\geq (\tfrac{5}{2}(m+16n^2))^2 - \tfrac{9}{4}m(m+16n^2)\\ &= 4(m+16n^2)(m+25n^2) > 0.\end{aligned}$$

From (3.5), we obtain $dy^2 > 0$ which contradicts that $d < 0$. Therefore, $d > 0$.

Now suppose that d is not a square modulo the prime $p := m$. The model (3.4) has no $\mathbb{Q}_p$-point at infinity since d is not a square in $\mathbb{Q}_p$. Choose a pair $(x, y) \in \mathbb{Q}_p^2$ satisfying (3.4). First suppose that $x \in \mathbb{Z}_p$. By (3.5), we have $dy^2 = z^2 - \frac{9}{4}(m+16n^2)p$ with $z \in \mathbb{Z}_p$. If $z \in \mathbb{Z}_p^\times$, then $dy^2 \equiv z^2 \pmod p$ with $z \not\equiv 0 \pmod p$ which contradicts that d is not a square modulo p. If $z \in p\mathbb{Z}_p$, then $dy^2 \equiv -\frac{9}{4}(m+16n^2)p \pmod{p^2}$ which implies that the even integer

$2\operatorname{ord}_p(y) = \operatorname{ord}_p(y^2)$ is equal to 1. So we must have $x \notin \mathbb{Z}_p$. Define $e := -\operatorname{ord}_p(x) \geq 1$. We have $\operatorname{ord}_p(dx^4) = -4e$, $\operatorname{ord}_p(5(m+16n^2)x^2) = -2e$ and $\operatorname{ord}_p(4(m+16n^2)(m+25n^2)/d) = 0$. From (3.4), we deduce that $\operatorname{ord}_p(y^2) = -4e$ and hence $\operatorname{ord}_p(y) = -2e$. Multiplying (3.4) by p^{4e} gives $(p^{2e}y)^2 = d(p^e x)^4 - p^{2e}5(m+16n^2)(p^e x)^2 + p^{4e}4(m+16n^2)(m+25n^2)/d$. Using that $p^{2e}y, p^e x \in \mathbb{Z}_p^\times$ and reducing modulo p, we find that d is a square modulo p which again is a contradiction. We conclude that d is a square modulo p.

By Lemma 2.1, d divides $4(m+16n^2)(m+25n^2)$. Since $d > 0$, we deduce that d lies in the subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ generated by 2, $m+16n^2$ and $m+25n^2$. Set $p := m$. We have $\left(\frac{2}{p}\right) = -1$ since $p = m \equiv 3 \pmod 8$. We have $\left(\frac{m+16n^2}{p}\right) = \left(\frac{16n^2}{p}\right) = 1$ and $\left(\frac{m+25n^2}{p}\right) = \left(\frac{25n^2}{p}\right) = 1$. Using these Legendre symbols with d being a square modulo p, we conclude that d lies in the set $\{1, m+16n^2, m+25n^2, (m+16n^2)(m+25n^2)\}$. ☐

3.2. **Computation of the weak Mordell–Weil group.**

Lemma 3.3.

(i) *The group $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ and is generated by the points Q_0 and Q_1.*
(ii) *The group $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ and is generated by the points P_0 and P_1.*

Proof. As noted in §2, we have a group homomorphism $\delta\colon E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ whose kernel equals $\phi(E(\mathbb{Q}))$. By Lemma 3.1, we have inclusions

$$\delta(E'(\mathbb{Q})) \subseteq \operatorname{Sel}_\phi(E/\mathbb{Q}) \subseteq \{1, -m, -(m+16n^2), m(m+16n^2)\}. \tag{3.6}$$

The inclusions of groups in (3.6) are in fact equalities since $\delta(Q_0) = b' \cdot (\mathbb{Q}^\times)^2 = m(m+16n^2) \cdot (\mathbb{Q}^\times)^2$ and $\delta(Q_1) = -(m+16n^2) \cdot (\mathbb{Q}^\times)^2$. In particular, $\delta(E'(\mathbb{Q}))$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ and is generated by $\delta(Q_0)$ and $\delta(Q_1)$. Part (i) is now immediate.

Similarly, we have a group homomorphism $\delta'\colon E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ whose kernel equals $\hat{\phi}(E'(\mathbb{Q}))$. By Lemma 3.2, we have inclusions

$$\delta'(E(\mathbb{Q})) \subseteq \operatorname{Sel}_{\hat{\phi}}(E'/\mathbb{Q}) \subseteq \{1, m+16n^2, m+25n^2, (m+16n^2)(m+25n^2)\}. \tag{3.7}$$

The inclusions of groups in (3.7) are in fact equalities since $\delta(P_0) = b \cdot (\mathbb{Q}^\times)^2 = (m+16n^2)(m+25n^2) \cdot (\mathbb{Q}^\times)^2$ and $\delta(P_1) = (m+16n^2) \cdot (\mathbb{Q}^\times)^2$. In particular, $\delta'(E(\mathbb{Q}))$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ and is generated by $\delta'(P_0)$ and $\delta'(P_1)$. Part (ii) is now immediate. ☐

Lemma 3.4. *The torsion subgroup of $E(\mathbb{Q})$ is the cyclic group of order 2 generated by P_0.*

Proof. The Weierstrass model defining our elliptic curve is minimal at 2 since it has coefficients in $\mathbb{Z}$ and its discriminant $\Delta \in \mathbb{Z}$ satisfies $\operatorname{ord}_2(\Delta) = 8 < 12$. Let $\tilde{E}$ be the (singular) curve over $\mathbb{F}_2$ obtained by reducing this model modulo 2. Let $\tilde{E}_{\text{ns}}$ be the open subvariety of $\tilde{E}$ consisting of nonsingular points; it is a commutative group variety by making use of group operations coming from E. Let $E_0(\mathbb{Q}_2)$ and $E_1(\mathbb{Q}_2)$ be the subgroups of $E(\mathbb{Q}_2)$ consisting of those points whose reduction modulo 2 lies in $\tilde{E}_{\text{ns}}(\mathbb{F}_2)$ or the identity subgroup of $\tilde{E}_{\text{ns}}(\mathbb{F}_2)$, respectively. By [Sil09, Propositions VII.2.1 and IV.3.2], any torsion element in $E_1(\mathbb{Q}_2)$ has order equal to a power of 2. The set $\tilde{E}_{\text{ns}}(\mathbb{F}_2)$ consist of the single point $(1,0)$, so we have $E_1(\mathbb{Q}_2) = E_0(\mathbb{Q}_2)$.

The order of the group $E(\mathbb{Q}_2)/E_0(\mathbb{Q}_2)$ can be computed using Tate's algorithm. Replacing y by $y+x$, we obtain an alternate model for E given by

$$y^2+2xy = x^3-(5(m+16n^2)-1)x^2+4(m+16n^2)(m+25n^2)x.$$

With notation as in Tate's algorithm [Sil94, Algorithm 9.4], we have the following information concerning the basic invariants: $a_1=2$, $a_2=-5(m+16n^2)-1$, $a_3=0$, $a_4=4(m+16n^2)(m+25n^2)$, $a_6=0$, $b_2\equiv 0 \pmod 4$, $b_4\equiv 0 \pmod 8$, $b_6=0$, $b_8\equiv 0 \pmod{16}$. We have $m\equiv 3 \pmod 4$ and $n\equiv 0 \pmod 2$ since m and $m+25n^2$ are both primes that are congruent to 3 modulo 4. Using this, we find that $a_2/2\equiv 0 \pmod 2$ and $a_4/4\equiv 1 \pmod 2$. With the above information one can directly check Tate's algorithm [Sil94, Algorithm 9.4] to find that E has Kodaira symbol I_r^* at 2 for some $r\geq 1$ and hence $c:=|E(\mathbb{Q}_2)/E_0(\mathbb{Q}_2)|$ is 2 or 4.

Combining the above results, we deduce that any element of finite order in $E(\mathbb{Q}_2)$ has order equal to a power of 2. This proves that the torsion group $E(\mathbb{Q})_{\mathrm{tors}}$ has cardinality a power of 2. The only element of order 2 in $E(\mathbb{Q})$ is $P_0=(0,0)$; using the Weierstrass equation of E, the other points of order 2 are defined over the quadratic field $\mathbb{Q}(\sqrt{m(m+16n^2)})$. Therefore, $E(\mathbb{Q})_{\mathrm{tors}}$ is a cyclic group of order 2^e for some $e\geq 1$.

Suppose that $e\geq 2$ and hence $P_0=2P$ for some $P\in E(\mathbb{Q})$. We have $P_0=2P=\hat{\phi}(\phi(P))\in\hat{\phi}(E'(\mathbb{Q}))$ which contradicts Lemma 3.3(ii). Therefore, $E(\mathbb{Q})_{\mathrm{tors}}$ is a cyclic group of order 2 generated by $(0,0)$. ☐

Lemma 3.5. *The group $E(\mathbb{Q})/2E(\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ and is generated by the points P_0, P_1 and P_2.*

Proof. Using that $\hat{\phi}\circ\phi=[2]$, we have a short exact sequence

$$0\to E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2]) \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\hat{\phi}} E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))\to 0.$$

Using Lemma 3.4 and $\phi(P_0)=0$, we find that the group $E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2])$ has order 2 and is generated by $Q_0=(0,0)$. Using Lemma 3.3 and considering the cardinalities of the groups in the short exact sequence, we deduce that $|E(\mathbb{Q})/2E(\mathbb{Q})|=8$ and hence $E(\mathbb{Q})/2E(\mathbb{Q})\cong(\mathbb{Z}/2\mathbb{Z})^3$.

Using Lemma 3.3 with the short exact sequence, we find that $E(\mathbb{Q})/2E(\mathbb{Q})$ is generated by P_0, P_1, $\hat{\phi}(Q_0)$ and $\hat{\phi}(Q_1)$. The lemma follows since $\hat{\phi}(Q_0)=0$ and $\hat{\phi}(Q_1)=P_2$. ☐

Since $E(\mathbb{Q})$ is a finitely generated abelian group, Lemmas 3.4 and 3.5 imply that $E(\mathbb{Q})\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}^2$. This completes the proof of Theorem 1.2.

4. Proof of Theorem 1.1

The set of primes that are congruent to 11 modulo 24 has natural density $1/\varphi(24)=1/8$. By [TZ08, Theorem 1.3], there are infinitely many pairs (m,n) of natural numbers for which m, $m+16n^2$ and $m+25n^2$ are primes congruent to 11 modulo 24.

Fix such a pair (m,n) and let $E/\mathbb{Q}$ be the elliptic curve defined by the model in Theorem 1.2. By Theorem 1.2, $E(\mathbb{Q})$ has rank 2.

Let $j_E\in\mathbb{Q}$ be the j-invariant of E. Recall that j_E uniquely determines E up to isomorphism over $\overline{\mathbb{Q}}$. So to complete the proof of the theorem, it suffices to show that each possible pair (m,n) gives rise to a different j-invariant j_E.

One can verify that

$$j_E = \frac{16(13m+100n^2)^3}{3^2 m(m+25n^2)^2}.$$

We now show that this expression for j_E is in lowest terms.

Lemma 4.1. *We have* $\gcd(16(13m+100n^2)^3, 3^2m(m+25n^2)^2) = 1$.

Proof. The primes 3, m and $m+25n^2$ are odd, so we need only verify that they do not divide $13m+100n^2$.

We have $n \equiv 0 \pmod 3$ since m and $m+16n^2$ are both congruent to 2 modulo 3. Therefore, $13m+100n^2 \equiv m \equiv 2 \pmod 3$ and hence $3 \nmid (13m+100n^2)$.

Suppose that m divides $13m+100n^2$. We have $0 \equiv 13m+100n^2 \equiv 100n^2 \pmod m$ and hence m divides n since $m > 5$. However, this is impossible since m and $m+16n^2$ are both prime. Therefore, $m \nmid (13m+100n^2)$.

Finally suppose that $p := m+25n^2$ divides $13m+100n^2$. We have $0 \equiv 13m+100n^2 \equiv 13(-25n^2)+100n^2 = -225n^2 \pmod p$ and hence p divides n since $p > 5$. However, this is impossible since $n < p$. Therefore, $p \nmid (13m+100n^2)$. ☐

By Lemma 4.1, the denominator of j_E is $3^2m(m+25n^2)^2$. Therefore, m and $m+25n^2$ are the two largest primes dividing the denominator of j_E. In particular, we can recover the pair (m,n) from the j-invariant of E.

References

[BJ16] Dongho Byeon and Keunyoung Jeong, *Infinitely many elliptic curves of rank exactly two*, Proc. Japan Acad. Ser. A Math. Sci. **92** (2016), no. 5, 64–66, DOI 10.3792/pjaa.92.64. MR3492814 ↑1.1

[Jeo19] Keunyoung Jeong, *Infinitely many elliptic curves of rank exactly two II*, Proc. Japan Acad. Ser. A Math. Sci. **95** (2019), no. 6, 53–57, DOI 10.3792/pjaa.95.53. MR3960281 ↑1.1

[Maz77] Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). With an appendix by Mazur and M. Rapoport. MR488287 ↑1

[Sat87] Philippe Satgé, *Un analogue du calcul de Heegner*, Invent. Math. **87** (1987), no. 2, 425–439, DOI 10.1007/BF01389425 (French). MR870738 ↑1

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 ↑1, 2, 3.2

[Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 ↑3.2

[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, 1.1

[TZ08] Terence Tao and Tamar Ziegler, *The primes contain arbitrarily long polynomial progressions*, Acta Math. **201** (2008), no. 2, 213–305, DOI 10.1007/s11511-008-0032-5. MR2461509 ↑1, 4

[Zyw25] David Zywina, *An elliptic surface with infinitely many fibers for which the rank does not jump* (2025). arXiv:2502.01026. ↑1.1

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

Email address: `zywina@math.cornell.edu`