A Positive-Rank Elliptic Curve with No Dense Prime

Alper Ferudun*

September 1, 2026

Abstract

An AIM problem asks whether every positive-rank elliptic curve over $\mathbb{Q}$ has a prime p for which its rational points are dense in its p-adic points. We give a negative answer. For

$$E : y^2 = x^3 - 1516563, \qquad P = (6403/9, 511280/27),$$

an unconditional full 2-descent and saturation certify $E(\mathbb{Q}) = \mathbb{Z}P$. A rational 3-isogeny places the reduction of every rational point in a subgroup of index 3 at every good prime, while separate exact arguments exclude density at the three bad primes $2, 3, 79$. Thus the dense-prime set is empty. We also record an exact finite local criterion: density is equivalent to surjectivity on a fixed finite quotient of the Néron filtration, and at a good odd prime on $\mathcal{E}(\mathbb{Z}/p^2\mathbb{Z})$.

1 Introduction

Question 24 in the AIM list *Rational and integral points on higher dimensional varieties* asks, for a positive-rank elliptic curve $E/\mathbb{Q}$, to describe the primes p for which $E(\mathbb{Q})$ is dense in $E(\mathbb{Q}_p)$ and asks whether this set must be nonempty [1]. Jones, Pappalardi, and Stevenhagen recently exhibited rational-isogeny mechanisms forcing a rational point to be locally imprimitive at every good prime of almost every characteristic [4]. The issue for the AIM question is that the point must generate the full Mordell–Weil group and every bad prime must also be excluded.

We carry this out for one specialization of their $j = 0$ family.

Theorem 1.1. *Let*

$$E : y^2 = x^3 - 1516563 = x^3 - 3^5 79^2, \qquad P = \left(\frac{6403}{9}, \frac{511280}{27}\right).$$

Then $E(\mathbb{Q}) = \mathbb{Z}P$, and for every rational prime p the subgroup $E(\mathbb{Q})$ is not dense in $E(\mathbb{Q}_p)$. In particular,

$$\{p : E(\mathbb{Q}) \text{ is dense in } E(\mathbb{Q}_p)\} = \varnothing.$$

The Mordell–Weil assertion is certified by an unconditional eclib/mwrank full 2-descent and all-prime saturation. The accompanying source archive contains the exact input, complete transcript, software versions, an independent PARI/GP audit, and a dependency-free exact checker.

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: `https://github.com/AlperTheKing`.

2 A finite density criterion

Fix a minimal Weierstrass equation over $\mathbb{Z}_p$. Let E_0 be the subgroup reducing to the nonsingular locus of the special fibre, let E_1 be the kernel of reduction, and, with $z = -x/y$, put

$$E_n = \{Q \in E_1 : v_p(z(Q)) \geq n\} \qquad (n \geq 1).$$

Set $m_p = 1$ for odd p and $m_2 = 2$. The formal logarithm gives a topological isomorphism

$$\log_E : E_{m_p} \xrightarrow{\sim} p^{m_p}\mathbb{Z}_p;$$

see, for example, [5, Chapter IV].

Proposition 2.1. *For every subgroup $\Gamma \leq E(\mathbb{Q}_p)$,*

$$\overline{\Gamma} = E(\mathbb{Q}_p) \quad \Longleftrightarrow \quad \Gamma \longrightarrow E(\mathbb{Q}_p)/E_{m_p+1} \text{ is onto.}$$

If p is odd and E has good reduction, this finite quotient is canonically $\mathcal{E}(\mathbb{Z}/p^2\mathbb{Z})$.

Proof. The forward implication is immediate. Conversely, surjectivity supplies $Q \in \Gamma \cap E_{m_p}$ whose image generates E_{m_p}/E_{m_p+1}. Hence $v_p(\log_E Q) = m_p$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, the cyclic group $\mathbb{Z}Q$ is dense in E_{m_p}. Surjectivity also holds modulo E_{m_p}, so the closure of Γ is all of $E(\mathbb{Q}_p)$. For good odd reduction, smooth properness identifies reduction modulo p^2 with the asserted quotient. □

For Theorem 1.1 we shall only need the necessary direction: a dense subgroup must surject onto every finite local quotient.

3 The Mordell–Weil group

Direct substitution shows that $P \in E(\mathbb{Q})$. We ran eclib/mwrank release 20250627 with

```
mwrank -v 2 -S -1
[0,0,0,0,-1516563]
```

The full transcript records a full 2-descent, rank and 2-Selmer rank equal to 1, automatic saturation, and the generator

$$[19209 : 511280 : 27],$$

which has affine coordinates P. It ends with the unconditional certificate that the rank and full Mordell–Weil basis have been determined. The computation was reproduced byte-for-byte and independently cross-checked with PARI/GP 2.17.4; details are in the verification report and reproducibility directory. We cite the standard algorithms through [2, 3].

Torsion can be removed independently. Exact counts give

$$\#E(\mathbb{F}_5) = 6, \qquad \#E(\mathbb{F}_{13}) = 21,$$

so rational torsion can only have order divisible by 3. For $y^2 = x^3 + B$, with $B = -3^5 79^2$, the 3-division polynomial is

$$\psi_3(x) = 3x(x^3 + 4B).$$

The root $x = 0$ would require $y^2 = B < 0$, while another rational root would require $x^3 = 2^2 3^5 79^2$, not a rational cube. Thus the rational torsion is trivial, and the certified saturated rank-one basis proves

$$E(\mathbb{Q}) = \mathbb{Z}P. \tag{1}$$

The discriminant is

$$\Delta = -432B^2 = -2^4 3^{13} 79^4. \tag{2}$$

The equation is minimal at 2 and 79 because the displayed valuations are less than 12. It is minimal at 3 as well: otherwise a minimal integral model would have discriminant valuation 1 and multiplicative type I_1, forcing c_4 to be a unit, whereas $c_4 = 0$ for this curve and remains zero under every change of Weierstrass coordinates. Thus the bad primes are exactly $2, 3, 79$; Tate's algorithm independently returns the same data.

4 The uniform obstruction at every good prime

Put

$$q = 80^2 - 1 = 6399 = 3^4 79$$

and consider

$$E' : Y^2 = X^3 + q^2, \qquad E^* : Y^2 = X^3 - 27q^2.$$

There is a rational 3-isogeny [4, Section 6]

$$\phi(X, Y) = \left(\frac{X^3 + 4q^2}{X^2}, \frac{Y(X^3 - 8q^2)}{X^3} \right), \tag{3}$$

with kernel $\{O, (0, q), (0, -q)\}$. At

$$P' = (q, 80q) = (6399, 511920)$$

exact substitution gives

$$\phi(P') = (6403, 511280) = P^*.$$

The change of variables $(x, y) \mapsto (X, Y) = (9x, 27y)$ is an isomorphism $E \to E^*$ carrying P to P^*.

Let $p \notin \{2, 3, 79\}$. Both curves have good reduction, the scaling is integral over $\mathbb{Z}_p$, and the three kernel points remain distinct. The reduced isogeny consequently has kernel of order 3. Isogenous elliptic curves over $\mathbb{F}_p$ have equal cardinality, and hence

$$[E^*(\mathbb{F}_p) : \phi(E'(\mathbb{F}_p))] = 3. \tag{4}$$

By (1), the reduction of every rational point lies in the proper subgroup in (4). Reduction modulo p is not onto, so $E(\mathbb{Q})$ is not dense in $E(\mathbb{Q}_p)$. This proves the theorem at every good prime.

5 The three bad primes

5.1 The prime 2

Modulo 2, the affine special fibre $y^2 = x^3 + 1$ has the singular point $(0, 1)$ and the nonsingular point $(1, 0)$. Together with infinity, its nonsingular locus has order 2. The point P reduces to $(1, 0)$, so $P \in E_0 \setminus E_1$. Exact duplication gives

$$z(2P) = -\frac{5330098555443228594720}{63098649487407069202717}, \qquad v_2(z(2P)) = 5.$$

Thus $2P \in E_5 \subset E_2$. Since

$$\#(E_0/E_1) = 2, \qquad \#(E_1/E_2) = 2,$$

the quotient E_0/E_2 has order 4, while $\mathbb{Z}P$ has image of order exactly 2. Density fails at 2.

5.2 The prime 3

Here

$$z(P) = -\frac{19209}{511280}, \qquad v_3(z(P)) = 1.$$

Hence $P \in E_1(\mathbb{Q}_3)$ on the minimal equation, and (1) puts every global point in the proper open subgroup E_1. To see directly that it is proper, set $x = 1$. The equation $y^2 = -1516562$ has the simple root $y = 1$ modulo 3, so Hensel's lemma gives a $\mathbb{Q}_3$-point reducing to the nonsingular point $(1, 1)$ and lying outside E_1.

5.3 The prime 79

The point P is integral and reduces to $(18, 67)$ on $y^2 = x^3$. Because $2 \cdot 67 \not\equiv 0 \pmod{79}$, it is nonsingular; hence $E(\mathbb{Q}) \subseteq E_0(\mathbb{Q}_{79})$. This subgroup is proper. Indeed,

$$28^2 \equiv -243 \pmod{79}$$

and the root is simple. Hensel's lemma supplies $u \in \mathbb{Z}_{79}$ with $u^2 = -243$, and then

$$Q = (0, 79u) \in E(\mathbb{Q}_{79})$$

reduces to the singular point $(0, 0)$. Thus $Q \notin E_0$ and density fails at 79.

The good-prime argument and these three calculations exhaust all rational primes, proving Theorem 1.1.

6 Scope and reproducibility

The theorem disproves universal nonemptiness and determines the complete dense-prime set of the displayed curve. It does not classify dense primes for every elliptic curve by Frobenius data, establish positive density in unobstructed families, or give a modular-curve parametrization.

The arXiv source bundle includes a dependency-free exact checker for the curve, point, isogeny specialization, discriminant, finite-field counts, and bad-prime arithmetic. The complete eclib and PARI transcripts, version records, and build hashes remain in the accompanying research archive. The finite checker supports the exact arithmetic; the Mordell–Weil equality uses the recorded unconditional full descent and saturation.

Acknowledgments

The AIM problem is attributed there to Takloo-Bighash. AI-assisted tools were used to support literature search, exact computation, proof auditing, and manuscript preparation. All mathematical claims and the final text remain the author's responsibility.

References

[1] American Institute of Mathematics. Rational and integral points on higher dimensional varieties: Problems, 2006. Question 24, p. 53; attributed to Takloo-Bighash.

[2] John E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 2 edition, 1997.

[3] John E. Cremona. eclib: a library for elliptic curves over the rationals. Release 20250627, 2025.

[4] Nathan Jones, Francesco Pappalardi, and Peter Stevenhagen. Locally imprimitive points on elliptic curves. *Mathematical Proceedings of the Cambridge Philosophical Society*, 180(3):663–683, 2026.

[5] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2 edition, 2009.