Discrete & Computational Geometry (2020) 64:985–994
https://doi.org/10.1007/s00454-019-00143-5

RICKY POLLACK MEMORIAL ISSUE

Rational Points of Some Elliptic Curves Related to the Tilings of the Equilateral Triangle

Miklós Laczkovich[1]

Received: 3 February 2019 / Revised: 7 October 2019 / Accepted: 9 October 2019 /
Published online: 22 October 2019

Abstract
Let n be a positive and squarefree integer. We show that the equilateral triangle can be dissected into $n \cdot k^2$ congruent triangles for some k if and only if $n \leq 3$, or at least one of the curves $C_n : y^2 = x(x-n)(x+3n)$ and $C_{-n} : y^2 = x(x+n)(x-3n)$ has a rational point with $y \neq 0$. We prove that if p is a positive prime such that $p \equiv 7 \pmod{24}$, then C_p and C_{-p} do not have such points. Consequently, for these primes the equilateral triangle cannot be dissected into $p \cdot k^2$ congruent triangles for any k.

Keywords Tilings of the equilateral triangle · Rank of some elliptic curves over the rationals

1 Introduction and Main Results

Let C_n denote the elliptic curve $y^2 = x(x-n)(x+3n)$, where n is an integer. The group of rational points of C_n will be denoted by Γ_n. We say that $(x, y) \in C_n$ is a nontrivial rational point of C_n if x, y are nonzero rational numbers; that is, if the order of (x, y) as an element of the group Γ_n is greater than two. Our first result shows that the existence of nontrivial rational points of C_n is closely related to the number of pieces in certain tilings of the equilateral triangle.

Theorem 1.1 *For every positive and squarefree integer n the following are equivalent.*

(i) *There is a positive integer k such that the equilateral triangle can be dissected into $n \cdot k^2$ congruent triangles.*
(ii) *Either $n \leq 3$, or at least one of the curves C_n and C_{-n} has a nontrivial rational point.*

Dedicated to the memory of Ricky Pollack.

Miklós Laczkovich
miklos.laczkovich@gmail.com

1 Eötvös Loránd University, Budapest, Hungary

The proof of Theorem 1.1 is based on the fact that the congruent copies of a triangle with sides a, b, c and corresponding angles α, β, γ tile an equilateral triangle if and only if either α, β, γ are multiples of $\pi/6$, or $\gamma \in \{\pi/3, 2\pi/3\}$ and a, b, c are pairwise commensurable (see [4, Thm. 3.3]). By the law of cosines, we have $\gamma = \pi/3$ or $2\pi/3$ if and only if $c^2 = a^2 + b^2 \pm ab$. Such triples are, e.g., $(a, b, c) = (7, 8, 13)$ or $(a, b, c) = (3, 5, 7)$.

Suppose that a, b, c are positive integers with $c^2 = a^2 + b^2 \pm ab$. Then the triangle with sides a, b, c tiles an equilateral triangle T. If the side length of T is m and the tiling has N pieces, then, comparing the areas we get $m^2 = N \cdot ab$, and thus the square free part of N is the same as that of ab. For example, if $(a, b, c) = (7, 8, 13)$, then the construction described in [3, Thm. 3.1] produces a tiling with $2,469,600 = 14 \cdot 420^2$ pieces. For the triangle with sides 3, 5, 7, a tiling with $10,935 = 15 \cdot 27^2$ pieces was found by Michael Beeson (see [2, Fig. 22, p. 28]).

As we shall see, a simple transformation maps these triples into nontrivial rational points of one of the corresponding curves C_n or C_{-n}. Thus the triple (7, 8, 13) gives the point $(-6, 48)$ of C_{-14}, and (3, 5, 7) gives the point $(-5, 50)$ of C_{-15}.

In the other direction, every nontrivial rational point of C_n or C_{-n} determines a triple (a, b, c) as above. For example, from the point $(-1, 8)$ of C_{-5} we obtain the triple (5, 16, 19), and the from the point $(-1, 30)$ of C_{17} we get (17, 225, 217). The proof of Theorem 1.1 will be given in the next section.

Remarks 1.2 1. Since every triangle Δ can be dissected into m^2 congruent triangles similar to Δ for every m, it is clear that (i) of Theorem 1.1 is equivalent to the following statement.
(i′) *There are infinitely many positive integers k such that the equilateral triangle can be dissected into $n \cdot k^2$ congruent triangles.*

2. We shall prove in Lemma 3.1 that if p is a positive prime, then the only torsion points of Γ_p and Γ_{-p} are the points having zero y-coordinates. Therefore, if n is a positive prime, then (ii) of Theorem 1.1 is equivalent to the following statement.
(ii′) *Either $n \le 3$, or at least one of the groups Γ_n and Γ_{-n} has positive rank.*

It is easy to see that if n, k are nonzero integers then C_n has a nontrivial rational point if and only if C_{nk^2} has one. Therefore, we have the following corollary of Theorem 1.1.

Corollary 1.3 *If the equilateral triangle can be dissected into N congruent triangles, then either $N = k^2$, $N = 2k^2$ or $N = 3k^2$ for some k, or at least one of the curves C_N and C_{-N} has a nontrivial rational point.*

We remark that the converse is not true. For example, $(-1, 8)$ is a nontrivial rational point of C_{-5}, but the equilateral triangle cannot be dissected into 5 congruent triangles. This follows from a result of Beeson stating that the equilateral triangle cannot be dissected into p congruent triangles for any prime $p > 3$ (see [1]). On the other hand, the equilateral triangle can be dissected into $5k^2$ congruent triangles for infinitely many positive integer k by Theorem 1.1.

In Sect. 3 we shall prove that if p is a positive prime and $p \equiv 7 \pmod{24}$, then the curves C_p and C_{-p} have no nontrivial rational points (see Corollary 3.6). Comparing with Theorem 1.1 we obtain the following.

Corollary 1.4 *If p is a positive prime such that $p \equiv 7 \pmod{24}$, then the equilateral triangle cannot be dissected into $p \cdot k^2$ congruent triangles for any k.*

2 Proof of Theorem 1.1

(i) ⇒ (ii): Suppose that the equilateral triangle T can be tiled with $n \cdot k^2$ congruent triangles having angles α, β, γ and corresponding sides a, b, c. We may assume that the sides of T equal 1.

By [4, Thm. 3.3], one of the following cases holds: $\alpha = \beta = \pi/6$ and $\gamma = 2\pi/3$; $\alpha = \pi/6$, $\beta = \pi/2$, $\gamma = \pi/3$; $\gamma \in \{\pi/3, 2\pi/3\}$ and a, b, c are pairwise commensurable.

Comparing the areas of T and the tiles we obtain $nk^2 \cdot ab \cdot \frac{\sqrt{3}}{4} = \frac{\sqrt{3}}{4}$; that is,

$$nk^2 \cdot ab = 1. \tag{1}$$

If $\alpha = \beta = \pi/6$, then $a = b$ and thus, by (1), $a = b = 1/(k \cdot \sqrt{n})$. By $c/a = \sqrt{3}$ we have $c = \sqrt{3}/(k \cdot \sqrt{n})$. Since the side of the equilateral triangle is tiled with segments of length a and c, we obtain $1 = ra + sc$ with suitable nonnegative integers r, s. Thus $r + s\sqrt{3} = k \cdot \sqrt{n}$. Since n is squarefree, this implies $n = 1$ or $n = 3$.

If $\alpha = \pi/6$, $\beta = \pi/2$ and $\gamma = \pi/3$, then $b = 2a$ and thus, by (1), $a = 1/(k \cdot \sqrt{2n})$. By $c/a = \sqrt{3}$ we have $c = \sqrt{3}/(k \cdot \sqrt{2n})$. The side of the equilateral triangle is tiled with segments of length $a, 2a$ and c, hence $1 = ra + sc$ with suitable nonnegative integers r, s. Thus $r + s\sqrt{3} = k \cdot \sqrt{2n}$. Since n is squarefree, this implies $n = 2$ or $n = 6$. Now $(9, 27)$ is a point of $C_6 : y^2 = x(x-6)(x+18)$, and thus the statement of (ii) is true in these cases.

In the remaining cases a, b, c are pairwise commensurable, and $\gamma = \pi/3$ or $\gamma = 2\pi/3$. Then we have $c^2 = a^2 + b^2 \pm ab$ by the law of cosines. Since $qa + rb + sc = 1$ with nonnegative integers q, r, s, it follows that a, b, c are rational. Replacing a by $-a$ if necessary, we may assume $c^2 = a^2 + b^2 + ab$. Under this change (1) becomes $\pm nk^2 \cdot ab = 1$. We put $t = (c - b)/a$; then t is rational, and $b = c - ta$. We have

$$\begin{aligned} c^2 &= a^2 + b^2 + ab = a^2 + (c - ta)^2 + ac - ta^2 \\ &= a^2(t^2 - t + 1) - 2act + ac + c^2, \end{aligned}$$

$a^2(t^2 - t + 1) = ac(2t - 1)$, and $a/c = (2t - 1)/d$, where $d = t^2 - t + 1$. Note that $d \neq 0$, as the polynomial $X^2 - X + 1$ has no rational roots. Then we have $b/c = 1 - (ta/c) = (1 - t^2)/d$. From (1) we get

$$1 = \pm nk^2 ab = \pm n \cdot (2t - 1)(1 - t^2) \cdot (ck/d)^2$$

and $(2t - 1)(t^2 - 1) = \mp n v^2$, where $v = d/(nkc)$ is a nonzero rational number.

Putting $x = n(2t - 1)$ we get $t = (x + n)/(2n)$, $t - 1 = (x - n)/(2n)$, $t + 1 = (x + 3n)/(2n)$, and

$$x(x - n)(x + 3n) = (2t - 1)(t^2 - 1) \cdot 4n^3 = \mp n v^2 \cdot 4n^3 = \mp y^2,$$

where $y = 2n^2 v$. Therefore, either (x, y) is a point of C_n or $(-x, y)$ is a point of C_{-n}.
(ii) ⇒ (i): It is clear that if $n \le 3$ then the equilateral triangle can be dissected into n congruent triangles.

Suppose that x, y are rational numbers, $y \neq 0$, and (x, y) is a rational point of either C_n or C_{-n}. Then one of $t = x/n$ and $t = -x/n$ satisfies $t(t+1)(t-3) = \pm y^2/n^3$. Fix such a t. Note that $t \neq 0, -1, 3$. Putting $a = 4t$, $b = t^2 - 2t - 3$ and $c = t^2 + 3$ we have $ab \neq 0$ and $a^2 + b^2 + ab = c^2$. Then $|a|, |b|, c$ are the sides of a rational triangle Δ such that $a^2 + b^2 \pm |a| \cdot |b| = c^2$, and thus, by the law of cosines, the angle between the sides of length $|a|$ and $|b|$ equals $\pi/3$ or $2\pi/3$. By [3, Thm. 3.1], there is an equilateral triangle T that can be dissected into triangles congruent to Δ. Let m be the length of the side of T, and let N be the number of pieces of the decomposition. Then $N|ab| = m^2$, hence

$$m^2/N = |ab| = 4|t(t^2 - 2t - 3)| = 4|t(t+1)(t-3)| = 4y^2/n^3$$

and $N = n^3 m^2/(4y^2) = nk^2$, where $k = nm/(2y)$. Now k is rational and n is squarefree by assumption, so $N = nk^2$ implies that k must be an integer. We have found a dissection of T into $n \cdot k^2$ congruent triangles, proving (i). □

3 Rational Points of $C_{\pm p}$

In this section we show that if p is a positive prime and $p \equiv 7 \pmod{24}$, then C_p and C_{-p} have no nontrivial rational points (see Corollary 3.6). Recall that the group of rational points of C_n is denoted by Γ_n.

Lemma 3.1 *Let p be a positive prime. Then the torsion points of the group Γ_p are the points $(0, 0)$, $(p, 0)$, $(-3p, 0)$ and $\mathcal{O}$ (the point at infinity). The torsion points of Γ_{-p} are the points $(0, 0)$, $(-p, 0)$, $(3p, 0)$ and $\mathcal{O}$.*

Proof The points listed above, being of order two and one, are torsion points. Suppose there exists another torsion point (x, y). Since the discriminant of the curves equals $p^2 \cdot (3p)^2 \cdot (4p)^2 = 3^2 \cdot 2^4 \cdot p^6$, it follows from the Nagell–Lutz theorem that $x, y \in \mathbb{Z}$, $y \neq 0$ and $y \mid 3 \cdot 2^2 \cdot p^3$. We distinguish between two cases.
Case I: $p \mid y$. Then $p \mid x$, $x = pz$, $p^2 \mid y$, $y = p^2 u$, $u \neq 0$, and

$$pu^2 = z(z \mp 1)(z \pm 3). \tag{2}$$

Clearly, $z \ge -2$. It is easy to check that if $-2 \le z \le 13$ then $z(z \mp 1)(z \pm 3)$ is not of the form qu^2, where q is prime and $u \neq 0$, except when $z = 4$ and $z(z+1)(z-3) = 5 \cdot 2^2$. This gives the point $P_1 = (20, 50)$ of Γ_{-5}. One can easily check that the x-coordinate of $2P_1$ is not an integer, hence P_1 is not a torsion point. (Thus Γ_{-5} has positive rank.) Therefore, we may assume $z \ge 14$.

If $p = 2$ or $p = 3$ then $y = p^2 u \mid 3 \cdot 2^2 \cdot p^3$ implies that all prime factors of z and $z \pm 1$ are 2 and 3. Thus $z = 2^\alpha$, $z \pm 1 = 3^\beta$ or the other way around. Then $z \le 10$ which is impossible.

Therefore, we may assume $p > 3$. Then at most one of the terms $z, z \mp 1, z \pm 3$ is divisible by p. Since $u \mid 3 \cdot 2^2 \cdot p^3$, it follows from (2) that the product of two of the terms $z, z \mp 1$ $z \pm 3$ is a divisor of $3^2 \cdot 2^4 = 144$. By $z \geq 4$ this implies $z(z-3) \leq 144$, hence $z \leq 13$ which is impossible.
Case II: $p \nmid y$. Then $y \mid 12$. Replacing x by $-x$ if necessary, we have $x(x+p)(x-3p) = \pm y^2$, and thus

$$|x(x+p)(x-3p)| = y^2 \mid 144. \tag{3}$$

It is easy to see that if a is a positive integer and x is an integer different from 0 and a, then $|x(a-x)| \geq a-1$. Therefore, $|x(x+p)| \geq p-1$, $|x(x-3p)| \geq 3p-1$, $|(x+p)(x-3p)| \geq 4p-1$,

$$(p-1)(3p-1)(4p-1) \leq |x(x+p)(x-3p)|^2 \leq 144^2,$$

and thus $p \leq 11$.

It follows from (3) that there are (positive or negative) divisors d_1, d_2 of 144 such that $d_2 - d_1 = 4p$, $|x \cdot d_1 \cdot d_2|$ is a square and is a divisor of 144, where $x = d_2 - p$. Checking the cases $p = 2, 3, 5, 7, 11$, we find that the only possibility is $p = 5$, $(d_1, d_2) = (-16, 4)$ and $x = -1$. This gives the point $P_2 = (-1, 8)$ of Γ_{-5}. One can easily check that $P_2 = P_1 + P_0$, where $P_0 = (-5, 0)$ and $P_1 = (20, 50)$. Since P_0 is a torsion point of Γ_{-5} and P_1 is not, it follows that P_2 is not a torsion point either.

□

Theorem 3.2

(i) *The rank of* Γ_p *is at most two for every positive prime* p.
(ii) *If* $p \not\equiv 1 \pmod{24}$, *then the rank of* Γ_p *is at most one.*
(iii) *If* $p = 2$, $p = 3$ *or* $p \equiv 5, 7$ *or* $19 \pmod{24}$, *then the rank of* Γ_p *is zero.*

In the proof of Theorem 3.2 we apply the method described in [5, §5, Chap. III, pp. 92–94]. Consider the curves

$$C_p : y^2 = x^3 + 2px^2 - 3p^2x \quad \text{and} \quad \overline{C}_p : y^2 = x^3 - 4px^2 + 16p^2x$$

with groups of rational points $\Gamma_p = C_p(\mathbb{Q})$ and $\overline{\Gamma}_p = \overline{C}_p(\mathbb{Q})$. We define $\alpha\colon \Gamma_p \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ by $\alpha(\mathcal{O}) = 1$, $\alpha(0,0) = -3p^2 \equiv -3$ and, for $x \neq 0$, $\alpha(x,y) = x \pmod{\mathbb{Q}^{*2}}$. Then α is a homomorphism from Γ_p into $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

We also define $\overline{\alpha}\colon \overline{\Gamma}_p \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ by $\overline{\alpha}(\mathcal{O}) = 1$, $\overline{\alpha}(0,0) = 16p^2 \equiv 1$ and, for $x \neq 0$, $\alpha(x,y) = x \pmod{\mathbb{Q}^{*2}}$. Then $\overline{\alpha}$ is a homomorphism from $\overline{\Gamma}_p$ into $\mathbb{Q}^*/\mathbb{Q}^{*2}$. The rank r of Γ_p satisfies

$$2^r = \frac{\#\alpha(\Gamma_p) \cdot \#\overline{\alpha}(\overline{\Gamma}_p)}{4} \tag{4}$$

(see [5, p. 91]). Here $\alpha(\Gamma_p)$ equals the set of divisors b_1 of $b = -3p^2 \pmod{\mathbb{Q}^{*2}}$ such that the equation

$$N^2 = b_1 M^4 + 2pM^2e^2 + (-3p^2/b_1)\, e^4 \tag{5}$$

is solvable in pairwise coprime integers N, M, e satisfying $M \neq 0$ and $\gcd(e, b_1) = \gcd(M, -3p^2/b_1) = 1$ (see [5, pp. 92–93]). Similarly, $\alpha(\overline{\Gamma}_p)$ equals the set of divisors b_1 of $\overline{b} = 16p^2 \pmod{\mathbb{Q}^{*2}}$ such that the equation

$$N^2 = b_1 M^4 - 4pM^2e^2 + (16p^2/b_1)\, e^4 \tag{6}$$

is solvable in pairwise coprime integers N, M, e satisfying $M \neq 0$ and $\gcd(e, b_1) = \gcd(M, 16p^2/b_1) = 1$.

The statement of Theorem 3.2 is an immediate consequence of (4) and of the following lemma.

Lemma 3.3

(i) $\#\alpha(\Gamma_p) \leq 8$ *for every positive prime* p.
(ii) *If* $p = 2$, $p = 3$ *or* $p \equiv 5, 7, 13$ *or* $19 \pmod{24}$, *then* $\#\alpha(\Gamma_p) \leq 4$.
(iii) $\#\alpha(\overline{\Gamma}_p) \leq 2$ *for every positive prime* p.
(iv) *If* $p \not\equiv 1 \pmod{12}$, *then* $\#\alpha(\overline{\Gamma}_p) = 1$.

Proof

(i) is obvious from $b_1 \in \{\pm 1, \pm 3, \pm p, \pm 3p\} \pmod{\mathbb{Q}^{*2}}$.
(ii) If $p = 3$ then $b_1 \in \{\pm 1, \pm 3\} \pmod{\mathbb{Q}^{*2}}$, and $\#\alpha(\Gamma_p) \leq 4$. Therefore, we may assume $p \neq 3$. We have $(p, 0), (-3p, 0) \in \Gamma_p$ and $\alpha(0, 0) = -3p^2 \equiv -3$, and thus $1, p, -3, -3p \in \alpha(\Gamma_p)$. Since $\alpha(\Gamma_p)$ is a subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$, it follows that $\#\alpha(\Gamma_p)$ equals 4 or 8, and it equals 8 if and only if $-1 \in \alpha(\Gamma_p)$.

Suppose that $\#\alpha(\Gamma_p) = 8$. Then $-1 \in \alpha(\Gamma_p)$ and thus, by $b_1 \mid 3p^2$, (5) is solvable for at least one of $b_1 = -1$ and $b_1 = -p^2$.

Suppose that $N^2 = -M^4 + 2pM^2e^2 + 3p^2e^4$ is solvable. If $p = 2$, then M is odd by $\gcd(M, 3p^2) = 1$, and $N^2 \equiv -M^4 \pmod 4$, which is impossible. If $p > 3$, then $p \nmid M$ by $\gcd(M, 3p^2) = 1$, and thus we have $\left(\frac{-1}{p}\right) = 1$ and $p \equiv 1 \pmod 4$.

We have $N^2 = (3pe^2 - M^2)(pe^2 + M^2) = A \cdot B$. Since $p \nmid M$ and $\gcd(M, e) = 1$, it follows that $\gcd(A, B) \mid 4$. If $\gcd(A, B) = 1$ or 4, then A and B are squares. Thus $3pe^2 - M^2 = n^2$, hence $-M^2 \equiv n^2 \pmod 3$, which is impossible, as $3 \nmid M$.

If $\gcd(A, B) = 2$, then $A/2$ and $B/2$ are squares. Thus $3pe^2 - M^2 = 2n^2$, hence $-M^2 \equiv 2n^2 \pmod p$. Since $p \nmid M$ and $p \equiv 1 \pmod 4$, we get $\left(\frac{2}{p}\right) = 1$ and $p \equiv 1 \pmod 8$.

Next suppose that $N^2 = -p^2M^4 + 2pM^2e^2 + 3e^4$ is solvable. Then we have $\gcd(M, 3) = 1$. If $p = 2$, then e is odd (since otherwise both N and e would be even), and $N^2 \equiv 3e^4 \pmod 4$, which is impossible. Suppose $p > 3$. Then $p \nmid e$ (since otherwise both e and N would be divisible by p), and thus $\left(\frac{3}{p}\right) = 1$ and $p \equiv \pm 1 \pmod{12}$.

We have $N^2 = (3e^2 - pM^2)(e^2 + pM^2) = C \cdot D$. Since $p \nmid e$ and $\gcd(M, e) = 1$, it follows that $\gcd(C, D) \mid 4$. If $\gcd(C, D) = 1$ or 4, then C and D are squares. Thus $3e^2 - pM^2 = n^2$, $-pM^2 \equiv n^2 \pmod 3$, $p \equiv -1 \pmod 3$ and $p \equiv -1 \pmod{12}$.

If $\gcd(C, D) = 2$, then $C/2$ and $D/2$ are squares. Thus $e^2 + pM^2 = 2n^2$, hence $e^2 \equiv 2n^2 \pmod p$, $\left(\frac{2}{p}\right) = 1$, $p \equiv \pm 1 \pmod 8$.

We proved that if $\#\,\alpha(\Gamma_p) = 8$, then $p > 3$ and either $p \equiv 1 \pmod 8$, or $p \equiv -1 \pmod{12}$. This proves (ii).

(iii) We have to estimate $\#\,\alpha(\overline{\Gamma}_p)$. It is clear that if $b_1 < 0$ then (6) has no solutions, and thus, by $b_1 \mid 16p^2$, we have $b_1 \in \{2^\alpha p^\beta : 0 \le \alpha \le 4, 0 \le \beta \le 2\}$. If $p = 2$, then we obtain $\alpha(\overline{\Gamma}_p) \subset \{1, 2\} \pmod{\mathbb{Q}^{*2}}$. Therefore, we may assume $p > 2$.

Let $b_1 = 2p^\beta$, and suppose that (6) is solvable. Then M is odd by $\gcd(M, 16p^2/b_1) = 1$, and thus the left hand side of (6) is divisible by 4, while the right hand side is not, which is impossible.

Next let $b_1 = 8p^\beta$, and suppose that (6) is solvable. Then N is even and, consequently, e is odd. Thus the left hand side of (6) is divisible by 4, while the right hand side is not, which is impossible. We obtain that $b_1 \in \{1, p, p^2, 4, 4p, 4p^2, 16, 16p, 16p^2\}$ and $b_1 \in \{1, p\} \pmod{\mathbb{Q}^{*2}}$. This proves (iii).

(iv) Suppose that $\#\,\alpha(\overline{\Gamma}_p) = 2$. Then $p \in \alpha(\overline{\Gamma}_p)$, and (6) is solvable for at least one of $b_1 = p$, $b_1 = 4p$ and $b_1 = 16p$.

Let $b_1 = p$, and suppose that $N^2 = pM^4 - 4pM^2e^2 + 16pe^4$ is solvable. Then M is odd by $\gcd(M, 16p) = 1$, and $N^2 \equiv pM^4 \pmod 4$. Hence $p > 2$ and $p \equiv 1 \pmod 4$. We have $N = pN_1$ and

$$pN_1^2 = M^4 - 4M^2e^2 + 16e^4 = (M^2 - 2e^2)^2 + 12e^4.$$

Now $p \nmid e$ by $\gcd(e, b_1) = 1$, and we get $\left(\frac{-12}{p}\right) = 1$. Since $p \equiv 1 \pmod 4$, we obtain $\left(\frac{3}{p}\right) = 1$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv 1 \pmod{12}$.

The case $b_1 = 16p$ is similar with the roles of M and e exchanged. Therefore, if (6) is solvable for $b_1 = 16p$, then $p \equiv 1 \pmod{12}$.

Finally, let $b_1 = 4p$, and suppose that $N^2 = 4pM^4 - 4pM^2e^2 + 4pe^4$ is solvable. Then $2 \nmid M$ by $\gcd(M, 4p) = 1$, and $2p \mid N$. Let $N = 2pN_1$, then $pN_1^2 = M^4 - M^2e^2 + e^4$. Since M is odd, we have $M^4 - M^2e^2 + e^4 \equiv 1 \pmod 4$, and thus $p \equiv 1 \pmod 4$. We have

$$4pN_1^2 = 4M^4 - 4M^2e^2 + 4e^4 = (2M^2 - e^2)^2 + 3e^4.$$

Now $p \nmid e$ by $\gcd(e, b_1) = 1$, and we get $\left(\frac{-3}{p}\right) = 1$. Since $p \equiv 1 \pmod 4$, we obtain $\left(\frac{3}{p}\right) = 1$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv 1 \pmod{12}$.

We proved that if $\#\,\alpha(\Gamma_p) = 2$, then $p \equiv 1 \pmod{12}$. This proves (iv). □

Our next aim is to prove

Theorem 3.4

(i) *The rank of* Γ_{-p} *is at most two for every positive prime* p.
(ii) *If* $p \not\equiv 1 \pmod{12}$*, then the rank of* Γ_{-p} *is at most one.*
(iii) *If* $p = 2$*,* $p = 3$ *or* $p \equiv 7 \pmod{24}$*, then the rank of* Γ_{-p} *is zero.*

We consider the curves

$$C_{-p} : y^2 = x^3 - 2px^2 - 3p^2x \quad \text{and} \quad \overline{C}_{-p} : y^2 = x^3 + 4px^2 + 16p^2x.$$

First we prove the following lemma.

Lemma 3.5

(i) $\#\,\alpha(\Gamma_{-p}) \le 8$ *for every prime* p.
(ii) *If* $p = 2$, $p = 3$ *or* $p \equiv 7 \pmod{12}$*, then* $\#\,\alpha(\Gamma_{-p}) \le 4$.
(iii) $\#\,\alpha(\overline{\Gamma}_{-p}) \le 2$ *for every prime* p.
(iv) *If* $p \ne 3$ *and* $p \not\equiv 1,\ 13$ *or* $19 \pmod{24}$*, then* $\#\,\alpha(\overline{\Gamma}_{-p}) = 1$.

Proof The proof of the statement (i) is the same as in the case of Lemma 3.3.
(ii) Suppose $\#\,\alpha(\Gamma_{-p}) = 8$. As in the proof of (ii) of Lemma 3.3, this implies $p \ne 3$ and $-1 \in \alpha(\Gamma_{-p})$. Therefore, by $b_1 \mid -3p^2$, $N^2 = b_1M^4 - 2pM^2e^2 + (-3p^2/b_1)e^4$ is solvable for at least one of $b_1 = -1$ and $b_1 = -p^2$.

Suppose that $N^2 = -M^4 - 2pM^2e^2 + 3p^2e^4$ is solvable. If $p = 2$, then M is odd by $\gcd(M, 3p^2) = 1$, and $N^2 \equiv -M^4 \pmod 4$, which is impossible. If $p > 3$, then $p \nmid M$ by $\gcd(M, 3p^2) = 1$, and thus we have $\left(\frac{-1}{p}\right) = 1$ and $p \equiv 1 \pmod 4$.

Next suppose that $N^2 = -p^2M^4 - 2pM^2e^2 + 3e^4$ is solvable; then $\gcd(M, 3) = 1$. If $p = 2$, then e is odd (since otherwise both N and e would be even), and $N^2 \equiv 3e^4 \pmod 4$, which is impossible. Suppose $p > 3$. Then $p \nmid e$ by $\gcd(e, b_1) = 1$, and thus $\left(\frac{3}{p}\right) = 1$ and $p \equiv \pm 1 \pmod{12}$.

We have $N^2 = (3e^2 + pM^2)(e^2 - pM^2) = C \cdot D$. Since $p \nmid e$ and $\gcd(M, e) = 1$, it follows that $\gcd(C, D) \mid 4$. If $\gcd(C, D) = 1$ or 4, then C and D are squares. Thus $3e^2 + pM^2 = n^2$, $pM^2 \equiv n^2 \pmod 3$, $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod{12}$.

If $\gcd(C, D) = 2$, then $C/2$ and $D/2$ are squares. Thus $3e^2 + pM^2 = 2n^2$, hence $p \equiv pM^2 \equiv 2n^2 \equiv 2 \pmod 3$. Since $p \equiv \pm 1 \pmod{12}$, we get $p \equiv -1 \pmod{12}$.

We proved that if $\#\,\alpha(\Gamma_{-p}) = 8$, then $p \equiv 1 \pmod 4$ or $p \equiv -1 \pmod{12}$. This proves (ii).
(iii) The argument proving (iii) of Lemma 3.3 shows that $\alpha(\overline{\Gamma}_{-p}) \subset \{1, p\} \pmod{\mathbb{Q}^{*2}}$.
(iv) Suppose $\#\,\alpha(\overline{\Gamma}_{-p}) = 2$. Then $p \in \alpha(\overline{\Gamma}_{-p})$, and

$$N^2 = b_1M^4 + 4pM^2e^2 + (16p^2/b_1)\,e^4$$

is solvable for at least one of $b_1 = p$, $b_1 = 4p$ and $b_1 = 16p$.

Let $b_1 = p$, and suppose that $N^2 = pM^4 + 4pM^2e^2 + 16pe^4$ is solvable. Then M is odd by $\gcd(M, 16p) = 1$, and $N^2 \equiv pM^4 \pmod 4$. Hence $p > 2$ and $p \equiv 1 \pmod 4$. We have $N = pN_1$ and

$$pN_1^2 = M^4 + 4M^2e^2 + 16e^4 = (M^2 + 2e^2)^2 + 12e^4.$$

Now $p \nmid e$ by $\gcd(e, b_1) = 1$, and we get $\left(\frac{-12}{p}\right) = 1$. Since $p \equiv 1 \pmod 4$, we obtain $\left(\frac{3}{p}\right) = 1$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv 1 \pmod{12}$.

The case $b_1 = 16p$ is similar with the roles of M and e exchanged. Therefore, if (6) is solvable for $b_1 = 16p$, then $p \equiv 1 \pmod{12}$.

Finally, let $b_1 = 4p$, and suppose that $N^2 = 4pM^4 + 4pM^2e^2 + 4pe^4$ is solvable. Then M is odd by $\gcd(M, 4p) = 1$. Also, $2p \mid N$, and thus e is odd. Let $N = 2pN_1$, then $pN_1^2 = M^4 + M^2e^2 + e^4$. Thus $pN_1^2 \equiv 3 \pmod 8$, hence $p \equiv 3 \pmod 8$. We have

$$4pN_1^2 = 4M^4 + 4M^2e^2 + 4e^4 = (2M^2 + e^2)^2 + 3e^4.$$

Now $p \nmid e$ by $\gcd(e, b_1) = 1$, and we get $p = 3$ or $\left(\frac{-3}{p}\right) = 1$. Suppose $p \neq 3$. Since $p \equiv 3 \pmod 4$, we obtain $\left(\frac{3}{p}\right) = -1$, $p \equiv 5$ or $7 \pmod{12}$. Since $p \equiv 3 \pmod 8$, we get $p \equiv 19 \pmod{24}$.

We proved that if $\#\alpha(\overline{\Gamma}_{-p}) = 2$, then $p = 3$ or $p \equiv 1 \pmod{12}$ or $p \equiv 19$ (mod 24), This proves (iv). □

Proof of Theorem 3.4 Statements (i) and (ii) of the theorem follow from Lemma 3.5 and from (4). If $p = 2$ or $p \equiv 7 \pmod{24}$, then the rank of Γ_{-p} is zero by Lemma 3.5 and (4).

What remains to prove is that the rank of Γ_{-3} is zero. Since $\#\alpha(\overline{\Gamma}_{-3}) \leq 2$ by Lemma 3.5, it is enough to show that $\#\alpha(\Gamma_{-3}) \leq 2$.

Consider the curve $C_{-3} : y^2 = x^3 - 6x^2 - 27x$. Then $b_1 \in \{\pm 1, \pm 3, \pm 9, \pm 27\}$, and thus $\alpha(\Gamma_{-3}) \subset \{\pm 1, \pm 3\} \pmod{\mathbb{Q}^{*2}}$. We show that $3 \notin \alpha(\Gamma_{-3})$. Suppose $3 \in \alpha(\Gamma_{-3})$. Then the equation $N^2 = b_1M^4 - 6M^2e^2 - (27/b_1)e^4$ is solvable for at least one of $b_1 = 3$ and $b_1 = 27$.

Suppose that $N^2 = 3M^4 - 6M^2e^2 - 9e^4$ is solvable. Then $3 \nmid M$ by $\gcd(M, 9) = 1$, and $3 \nmid e$ since $3 \mid N$. Let $N = 3N_1$. Then $3N_1^2 = M^4 - 2M^2e^2 - 3e^4$, hence $M^4 \equiv 2M^2e^2 \pmod 3$, which is impossible.

Finally, suppose that $N^2 = 27M^4 - 6M^2e^2 - e^4$ is solvable. Then $3 \nmid e$ by $\gcd(e, b_1) = 1$. Thus $N^2 \equiv -e^2 \pmod 3$, which is impossible. □

Corollary 3.6 *If $p = 2$, $p = 3$ or $p \equiv 7 \pmod{24}$, then the curves C_p and C_{-p} have no nontrivial rational points.* □

4 Numerical Examples

As the following table shows, for all primes $3 < p < 100$, if $p \not\equiv 7 \pmod{24}$, then at least one of the curves C_p and C_{-p} has nontrivial rational points and, consequently, Γ_p or Γ_{-p} has positive rank. Note that the point $(75, 210)$ belongs to both C_{-23} and C_{73}.

The points below were found by searching for integer solutions of $N^2 = b_1M^4 \pm 2pM^2e^2 + b_2e^4$ with $b_1b_2 = -3p^2$, and putting $x = b_1M^2/e^2$, $y = b_1MN/e^3$. The solutions for $p \neq 83$ were found by using GNU Octave (https://www.gnu.org/software/octave/). I am grateful to Peter Salvi for finding a solution for $p = 83$; he used Julia 1.0 (https://julialang.org/blog/2018/08/one-point-zero).

$$p = 5 : (-1, 8) \in \Gamma_{-5},$$
$$p = 11 : (75, 720) \in \Gamma_{11},$$
$$p = 13 : (-12, 90) \in \Gamma_{13},$$
$$p = 17 : (-1, 30) \in \Gamma_{17},$$

$$
\begin{aligned}
p &= 19 : \left(\frac{17689}{225}, \frac{1374688}{3375}\right) \in \Gamma_{-19},\\
p &= 23 : (75, 210) \in \Gamma_{-23},\\
p &= 29 : \left(-\frac{529}{25}, \frac{16744}{125}\right) \in \Gamma_{-29},\\
p &= 37 : \left(\frac{231361}{324}, \frac{116481365}{5832}\right) \in \Gamma_{37},\\
p &= 41 : (-121, 198) \in \Gamma_{41},\\
p &= 43 : \left(\frac{4165798849}{21538881}, \frac{171543655606240}{99961946721}\right) \in \Gamma_{-43},\\
p &= 47 : (1875, 79050) \in \Gamma_{-47},\\
p &= 53 : \left(-\frac{167281}{4225}, \frac{89165272}{274625}\right) \in \Gamma_{-53},\\
p &= 59 : \left(-\frac{930433009}{6076225}, \frac{13189530387264}{14977894625}\right) \in \Gamma_{59},\\
p &= 61 : (-108, 1170) \in \Gamma_{61},\\
p &= 67 : \left(\frac{909373939321}{51279921}, \frac{863887766632341760}{367215514281}\right) \in \Gamma_{-67},\\
p &= 71 : (507, 9282) \in \Gamma_{-71},\\
p &= 73 : (75, 210) \in \Gamma_{73},\\
p &= 83 : \left(-\frac{2140232721200}{59682001401}, \frac{1389711692322846998O}{14580253260262899}\right) \in \Gamma_{83},\\
p &= 89 : \left(-\frac{121}{289}, \frac{489280}{4913}\right) \in \Gamma_{-89},\\
p &= 97 : \left(-\frac{121}{25}, \frac{45408}{125}\right) \in \Gamma_{-97}.
\end{aligned}
$$

Acknowledgements Open access funding provided by Eötvös Loránd University (ELTE). The author was supported by the Hungarian National Foundation for Scientific Research, Grant No. K124749.

References

1. Beeson, M.: Tiling an equilateral triangle. arXiv:1812.07014 (2018)
2. Beeson, M.: No triangle can be cut into seven congruent triangles. arXiv:1811.09723 (2018)
3. Laczkovich, M.: Tilings of triangles. Discrete Math. **140**(1–3), 79–94 (1995)
4. Laczkovich, M.: Tilings of convex polygons with congruent triangles. Discrete Comput. Geom. **48**(2), 330–372 (2012)
5. Silverman, J.H., Tate, J.: Rational Points on Elliptic Curves. Undergraduate Texts in Mathematics. Springer, New York (1992)