GENERATORS AND INTEGRAL POINTS ON ELLIPTIC CURVES ASSOCIATED WITH SIMPLEST QUARTIC FIELDS

Sylvain Duquesne, Tadahisa Nara, Arman Shamsi Zargar

GENERATORS AND INTEGRAL POINTS ON ELLIPTIC CURVES ASSOCIATED WITH SIMPLEST QUARTIC FIELDS

SYLVAIN DUQUESNE, TADAHISA NARA, AND ARMAN SHAMSI ZARGAR

Abstract. We associate to some simplest quartic fields a family of elliptic curves that has rank at least three over $\mathbb{Q}(m)$. It is given by the equation

$$E_m : y^2 = x^3 - 36\left(36m^4 + 48m^2 + 25\right)\left(36m^4 - 48m^2 + 25\right)x.$$

Employing canonical heights we show the rank is in fact at least three for all m. Moreover, we get a parametrized infinite family of rank at least four. Further, the integral points on the curve E_m are discussed and we determine all the integral points on the original quartic model when the rank is three. Previous work in this setting studied the elliptic curves associated with simplest quartic fields of ranks at most two along with their integral points (see [4, 5]).

1. Introduction

Simplest quartic fields are defined by adjoining to $\mathbb{Q}$ a root of the polynomials $X^4-tX^3-6X^2+tX+1$, where t^2+16 is not divisible by an odd square. This ensures the irreducibility of the polynomial. The arithmetic properties of these fields have been vastly studied. For example, consult the works of Gras [11], Lazarus [16, 17], Louboutin [18], Kim [14], Olajos [20], and Duquesne [4, 5].

Inthis paper, we are studying elliptic curves $\mathcal{Q}_t$ (so called associated with simplest quartic fields) given by the equation

$$Y^2 = X^4 - tX^3 - 6X^2 + tX + 1 \tag{1.1}$$

where $t^2 + 16$ is not divisible by an odd square. Using suitable rational transformations ([4], see also [26]), the quartic curve (1.1) can be put into the Weierstrass form

$$\mathcal{C}_t : y^2 = x^3 - \left(t^2 + 16\right)x. \tag{1.2}$$

The curve $\mathcal{C}_t$ is elliptic for any rational values of t, and by [25, p. 347] the torsion subgroup of $\mathcal{C}_t$ (or $\mathcal{Q}_t$) is $\mathcal{T} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}$, depending on whether t^2+16 is square or not, respectively.

Remark 1.1. As stated in [4], it is easy to prove that the condition of simplest quartic fields ($t^2 + 16$ not divisible by an odd square) implies that $t^2 + 16$ is not a square (if $t \neq 0$). As a consequence, $\mathcal{T} = \mathbb{Z}/2\mathbb{Z}$ in this work and is of course generated by $T = (0, 0)$.

The works in [4, 5] studied the *rank* and *integral points* on the curves arising from simplest cubic and quartic fields. Therein, the integral points of curves with generic

2010 *Mathematics Subject Classification.* 11G05, 14H52, 11D25, 14G05.

Key words and phrases. elliptic curve, simplest quartic field, Mordell-Weil group, rank, infinite family, integral points.

This work was supported in part by French projects ANR-16-CE39-0012 "SafeTLS" and ANR-11-LABX-0020-01 "Centre Henri Lebesgue".

ranks one and two have been studied. In this work we study the same notions on a subfamily of the families in [4, 5] that has rank at least three. This subfamily, parametrized by m, is introduced in Section 2. In Section 3 we prove that the three independent points over $\mathbb{Q}(m)$ are in fact independent for each m. Using precise estimates of their canonical heights (computed in Section 4), we also prove that these three points can be extended to a Mordell-Weil basis for each m in Section 5. This allows to determine integral points of this rank-3 family in Section 6. Finally, we exhibit a subfamily of rank at least four in section 7.

In [10] Fujita and Terai studied a family of elliptic curves given by the equation

$$y^2 = x^3 - stx,$$

where s, t are non-square integers such that $t - s = \alpha^2$ and $c^4 s - t = \beta^2$ for some integers c, α, β. Then they showed that the points $(-s, s\alpha)$ and $\left(c^2 s, cs\beta\right)$ can be extended to a Mordell-Weil basis. In [7] Fujita constructed a subfamily of rank at least three together with explicit generators.

It is easy to check that the curves we are proposing form another subfamily of the family in [10]. Compared to the one given by Fujita in [7], our subfamily has many integral points and a rank-4 subfamily can be deduced. We can also compute all the integral points on the quartic model $\mathcal{Q}_t$ when the rank is exactly three which was not the case in previous works ([6], [8], [9]).

2. A family with rank at least three over $\mathbb{Q}(m)$

In this section we exhibit a rank-3 elliptic curve over $\mathbb{Q}(m)$ associated with simplest quartic fields.

Theorem 2.1. *Let $a = 36m^4 + 48m^2 + 25$ and $b = 36m^4 - 48m^2 + 25$ for some $m \in \mathbb{Z}$ and let E_m be the elliptic curve defined by the equation*

$$E_m : y^2 = x^3 - 36abx. \tag{2.1}$$

E_m is associated with simplest quartic fields and the points

$$\begin{aligned} P_1(m) &= \left(-144, 72\left(36m^4 - 7\right)\right), \\ P_2(m) &= \left(-2b, 8\left(6m^2 + 5\right)b\right), \\ P_3(m) &= (-6b, 144mb), \end{aligned}$$

are free generators of the Mordell-Weil group over $\mathbb{Q}(m)$.

Proof. According to [4], the curve $\mathcal{C}_t$ defined as in (1.2) is of generic-rank equal to two if $t = 6k^2 + 2k - 1$ and has short Weierstrass form

$$y^2 = x^3 - \left(2k^2 - 2k + 1\right)\left(18k^2 + 30k + 17\right)x. \tag{2.2}$$

To get a rank-3 family, we need a third point on this curve. An experimental approach showed that $-3\left(2k^2 - 2k + 1\right)$ often appears as the x-coordinate of a point. Indeed, assuming $k = m^2 - \frac{1}{6}$ for some rational values of m, we get the new point $\left(-3\left(2k^2 - 2k + 1\right), 12m\left(2k^2 - 2k + 1\right)\right)$.

Replacing k by $m^2 - \frac{1}{6}$ into equation (2.2) and scaling, we get the curve stated in Theorem 2.1. It is then associated with simplest quartic field for $t = 6m^4 - \frac{7}{6}$ (we have $ab = 36(t^2 + 16)$). The points $P_1(m)$ and $P_2(m)$ are corresponding to those of [4] and $P_3(m)$ is the new point we get here.

We then use specialization arguments to prove that $P_1(m), P_2(m)$ and $P_3(m)$ are free generators over $\mathbb{Q}(m)$: we can prove using Magma [3] that the curve $E_2(\mathbb{Q})$

has rank 3 and is generated by $P_1(2), P_2(2), P_3(2)$ and $(0,0)$. Hence, by the specialization theorem of Silverman ([24],[25]), the curve E_m has rank at least three and the points $P_1(m), P_2(m)$ and $P_3(m)$ are independent over $\mathbb{Q}(m)$.

To show that the exact rank of E_m over $\mathbb{Q}(m)$ is three, we use the criterion of Gusić and Tadić ([12, Theorem 1.3]). If the curve is given in Legendre form $y^2 = (x-e_1)(x-e)(x-\bar{e})$ in $\mathbb{Z}[t]$ and assuming that for every non-constant square-free divisor h of $e_1^2 - (e+\bar{e})e_1 + e\bar{e}$ or $(e-\bar{e})^2$ in $\mathbb{Z}[t]$, $h(t_0)$ is not a square in $\mathbb{Q}$, this criterion states that the specialization homomorphism at t_0 is injective. In our case, we have

$$e_1^2 - (e+\bar{e})e_1 + e\bar{e} = -6^2 \cdot \left(36m^4 + 48m^2 + 25\right) \cdot \left(36m^4 - 48m^2 + 25\right),$$
$$(e-\bar{e})^2 = 12^2 \cdot \left(36m^4 + 48m^2 + 25\right) \cdot \left(36m^4 - 48m^2 + 25\right).$$

It is readily checked that $m = 2$ satisfies the condition of the criterion. As a consequence, the rank is exactly equal to three over $\mathbb{Q}(m)$ and the points $P_i(m)$ are free generators. □

Remark 2.2. One can get other families of rank at least three arising from the rank two family of [4]. For example, by considering $k = sm^2 + tm - \frac{1}{6}$ and forcing $-3\left(18k^2 + 30k + 17\right)$ as the x-coordinate of a third point, we get that $m(sm+t)$ must be a square, which has parametric solution $m = \frac{u^2 t}{s(s-u^2)}$, giving rise to $k = -\frac{1}{6}\frac{-6t^2u^2+s^2-2u^2s+u^4}{(s-u^2)^2}$. In this way, a curve of rank at least three is found over $\mathbb{Q}(s,t,u)$.

Our aim in the next three sections is to prove that E_m has rank at least three over $\mathbb{Q}$ for all m.

3. Independence of the three points modulo torsion subgroup

Let E_m be an elliptic curve as defined in Theorem 2.1. In order to prove the independence of $P_1(m), P_2(m)$ and $P_3(m)$ for any value of m, we need the following lemma

Lemma 3.1. *Let P be a point in $E_m(\mathbb{Q})$. If $P \in 2E_m(\mathbb{Q})$, then the x-coordinate $x(P)$ of P is a square.*

Proof. For an elliptic curve $y^2 = x^3 - nx$ and $P = 2Q$ with a rational point $Q = (x_1, y_1)$, the doubling formula gives

$$x(P) = \left(\frac{3x_1^2 + n}{2y_1}\right)^2 - 2x_1 = \left(\frac{x_1^2 + n}{2y_1}\right)^2.$$

□

For reader convenience and because the points $P_i(m)+P_j(m)$ are used in several places, we give here their explicit coordinates:

$$P_1(m)+P_2(m) = \left(18b, 72\left(6m^2-5\right)\left(36m^4-48m^2+25\right)\right),$$

$$P_1(m)+P_3(m) = \left(6b\frac{\left(6m^2+6m+7\right)^2}{\left(6m^2+6m-1\right)^2}, \right.$$
$$\left. 144b\frac{\left(6m^2+6m+7\right)\left(-25-43m-36m^2+36m^4+36m^5\right)}{\left(6m^2+6m-1\right)^3}\right),$$

$$P_2(m)+P_3(m) = \left(12\left(6m^2-6m+5\right)^2, \right.$$
$$\left. 36\left(36m^4-96m^3+96m^2-80m+25\right)\left(6m^2-6m+5\right)\right).$$

Proposition 3.2. For $k_i \in \{0,1\}$ none of the points $k_0T + k_1P_1(m) + k_2P_2(m) + k_3P_3(m)$ lies in $2E_m(\mathbb{Q})$ except the neutral element O. This implies the points $P_1(m), P_2(m), P_3(m)$ are independent.

Proof. Due to Lemma 3.1, it suffices to show that the x-coordinates of the relevant points are non-squares.

Let us first assume $k_0 = 0$. It is clear that $x(P_1) = -144$, $x(P_2+P_3) = 12\left(6m^2-6m+5\right)^2$, $x(P_1+P_2+P_3) = -3\left(6m^2+6m-5\right)^2$ are non-squares. The other cases are almost clear too because, as b is odd, the 2-primary components of the x-coordinates are non-squares.

Next assume $k_0 = 1$. The addition formula trivially gives for any point $P \neq T$

$$x(P+T) = -\frac{36ab}{x(P)} \equiv -ab\,x(P) \pmod{\mathbb{Q}^{\times 2}}$$

and so it suffices to show $-ab\,x(k_1P_1 + k_2P_2 + k_3P_3)$ are non-squares. Clearly $-ab\,x(P_1) = 144ab$ is a non-square since $36ab$ is a non-square according to Remark 1.1. In the other cases it is not difficult to see the 2- or 3-primary components are non-squares since ab is neither divisible by 2 nor 3. □

4. Estimates of the canonical height of points on $E_m(\mathbb{Q})$

The *canonical height* $\hat{h}(P)$ of a point P on an elliptic curve defined over $\mathbb{Q}$ is defined by the limit

$$\lim_{n\to\infty} \frac{h\left(2^nP\right)}{4^n},$$

where $h(P) = \log\max\{|a|,|b|\}$ for $x(P) = a/b$, $\gcd(a,b) = 1$. It is a quadratic form and the associated scalar product is called the *height pairing*

$$\langle P, Q\rangle = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right). \tag{4.1}$$

The goal of this section is to estimate the canonical height of the $P_i(m)$ as well as their height pairings because it will enable us to estimate how far this set of independent points is from a Mordell-Weil basis by using Siksek's theorem (given below in the case of three points).

Theorem 4.1 ([23, Theorem 3.1])**.** *Let E be an elliptic curve over $\mathbb{Q}$ of rank $r \geq 3$. Let P_1, P_2 and P_3 be independent points in $E(\mathbb{Q})$ modulo $E(\mathbb{Q})_{tors}$. Choose a basis $\{G_1, G_2, \ldots, G_r\}$ for $E(\mathbb{Q})$ modulo $E(\mathbb{Q})_{tors}$ such that $P_1, P_2, P_3 \in \mathbb{Z}G_1 + \mathbb{Z}G_2 + \mathbb{Z}G_3$. Suppose that $E(\mathbb{Q})$ contains no point Q of infinite order with $\hat{h}(Q) \leq \lambda$ where*

λ is some positive real number. Then, the lattice index ν of $\mathbb{Z}P_1 + \mathbb{Z}P_2 + \mathbb{Z}P_3$ in $\mathbb{Z}G_1 + \mathbb{Z}G_2 + \mathbb{Z}G_3$ satisfies

$$\nu \leq \sqrt{\frac{2R(P_1, P_2, P_3)}{\lambda^3}}$$

where $R(P_1, P_2, P_3)$ is the determinant of the height pairing matrix $H(P_1, P_2, P_3)$ defined by

$$H(P_1, P_2, P_3) = \left(\langle P_i, P_j \rangle\right)_{1 \leq i,j \leq 3}.$$

Before estimating these heights, let us determine the value λ, the lower bound of infinite order points on $E_m(\mathbb{Q})$. For this, we use a known result:

Lemma 4.2 ([10, Proposition 3.3])**.** *Let n be a positive, fourth-power-free integer and E the elliptic curve given by $y^2 = x^3 - nx$. If $n \not\equiv 12 \pmod{16}$, then*

$$\hat{h}(P) > 0.125 \log n + 0.3917$$

for any non-torsion point P in $E(\mathbb{Q})$.

In our case we obtain the estimate:

Proposition 4.3. Let E_m be as in Theorem 2.1 for $m \geq 5$. For any non-torsion point P in $E_m(\mathbb{Q})$, we have

$$\hat{h}(P) > \log m + 1.735. \tag{4.2}$$

Proof. As E_m is associated with a simplest quartic field, $36ab$ is assumed to be not divisible by an odd square and so is fourth-power-free (remember a and b are odd). Moreover, $36ab \equiv 4\left(4m^4 + 9\right)^2 \equiv 4\left(8m^4 + 1\right) \equiv 4 \pmod{16}$, so Lemma 4.2 is applicable, and we have

$$\begin{aligned}\hat{h}(P) > \log m + \frac{1}{8}\log\left(36\, ab/m^8\right) + 0.3917 &> \log m + \frac{1}{8}\log\left(36 \cdot 1295\right) + 0.3917 \\ &> \log m + 1.7354\cdots\end{aligned}$$

where the second inequality is given by a bit of calculus:

$$ab/m^8 \geq ab/m^8\Big|_{m=5} = 1295.19\cdots.$$

This is because ab/m^8 is growing for $m \geq 2$ and we chose $m = 5$ to get a result close to the limit of this function which is 1296. □

Next we should estimate the canonical heights of specific points. Though estimating directly following the definition is hard, we will instead use the local decomposition of the canonical height:

$$\hat{h}(P) = \hat{h}_{\mathrm{fin}}(P) + \hat{h}_{\infty}(P).$$

The finite part of this decomposition is obtained thanks to the following lemma of [10] (Lemma 3.2)

Lemma 4.4. *Let n be a fourth-power-free integer and E the elliptic curve given by $y^2 = x^3 - nx$. For any point $P = \left(\alpha/\delta^2, \beta/\delta^3\right)$ in $E(\mathbb{Q})$ with $\alpha, \beta, \delta \in \mathbb{Z}$, $\gcd(\alpha, \delta) = \gcd(\beta, \delta) = 1$ and $\delta > 0$, we have*

$$\hat{h}_{\mathrm{fin}}(P) = 2\log\delta - \frac{1}{2}\log \prod_{2 \neq p_i \mid \alpha, \beta, n} p_i^{e_i} + \hat{h}_2(P)$$

where $p_i^{e_i} \| n$ with $e_i \in \{1, 2, 3\}$ and $\hat{h}_2(P)$ is given by the following:

(i) *if δ is even, then $\hat{h}_2(P) = 0$;*
(ii) *if δ is odd, then for v_2 denoting the valuation on $\mathbb{Z}$ normalized by $v_2(2) = 1$, $\hat{h}_2(P)$ is given by Table 1.*

TABLE 1. $\hat{h}_2(P)$ in terms of the 2-valuation of n, α and β

n	α	β	$\hat{h}_2(P)$
even	odd	odd	0
odd	even	even	0
odd	odd	even	$-\frac{1}{2}\log 2$
$v_2(n) = 1$	even	even	$-\frac{1}{2}\log 2$
$v_2(n) = 2$ and $\frac{n}{4} \equiv 1 \pmod 4$	$v_2(\alpha) = 1$	$v_2(\beta) \geq 3$	$-\frac{3}{2}\log 2$
$v_2(n) = 2$ and $\frac{n}{4} \equiv 3 \pmod 4$	$v_2(\alpha) = 1$	$v_2(\beta) = 2$	$-\frac{7}{4}\log 2$
$v_2(n) = 2$	$v_2(\alpha) \geq 2$	$v_2(\beta) \geq 2$	$-\log 2$
$v_2(n) = 3$	$v_2(\alpha) \geq 3$	$v_2(\beta) \geq 3$	$-\frac{3}{2}\log 2$

For a point $P = \left(\alpha/\delta^2, \beta/\delta^3\right)$ in $E(\mathbb{Q})$ as in Lemma 4.4, we compute $\hat{h}_\infty(P)$ using Tate's series [24]:

$$\hat{h}_\infty(P) = \log|x(P)| + \frac{1}{4}\sum_{k=0}^{\infty}\frac{c_k}{4^k} \tag{4.3}$$

where $c_k = \log|z\left(2^k P\right)|$, $z(Q) = \left(1 + n/x(Q)^2\right)^2$. Then we have

$$\begin{aligned}\hat{h}_\infty(P) &= \log\left|\frac{\alpha}{\delta^2}\right| + \frac{1}{4}\log\left(1 + \frac{n\delta^4}{\alpha^2}\right)^2 + \frac{1}{4}\sum_{k=1}^{\infty}\frac{c_k}{4^k} \\ &= \log|\alpha| - 2\log\delta + \frac{1}{2}\log\left(\alpha^2 + n\delta^4\right) - \frac{1}{2}\log\alpha^2 + \frac{1}{4}\sum_{k=1}^{\infty}\frac{c_k}{4^k} \\ &= -2\log\delta + \frac{1}{2}\log\left(\alpha^2 + n\delta^4\right) + \frac{1}{4}\sum_{k=1}^{\infty}\frac{c_k}{4^k}.\end{aligned}$$

Note that the series converges for any non-torsion point $P \in E(\mathbb{Q})$ by the fact that $2^k P$ lies in the connected component of E containing O (called the *identity component* and denoted by E^0) so that $x\left(2^k P\right) \geq \sqrt{n}$ for $k \geq 1$. As a consequence

$$0 \leq \frac{1}{4}\sum_{k=1}^{\infty}\frac{c_k}{4^k} \leq \frac{1}{4}\sum_{k=1}^{\infty}\frac{\log 2^2}{4^k} = \frac{1}{6}\log 2.$$

And finally, we have

$$\hat{h}(P) = \frac{1}{2}\log\left\{\frac{\alpha^2 + n\delta^4}{\prod_{2\neq p_i|\alpha,n} p_i^{e_i}}\right\} + \hat{h}_2(P) + S \quad \text{with} \quad 0 \leq S \leq \frac{1}{6}\log 2. \tag{4.4}$$

Before starting computation, we make a little change in choice of points we deal with. The set $\{P_1(m), P_2(m), P_3(m)\}$ can be extended to a basis if and only if $\{P_1(m) + P_2(m), P_2(m), P_3(m)\}$ can be. So we put

$$Q_1 = P_1(m) + P_2(m), \quad Q_2 = P_2(m), \quad Q_3 = P_3(m)$$

and use this set to simplify forthcoming arguments. Indeed the height pairing $\langle Q_i, Q_j\rangle_{i\neq j}$ will be bounded independently of m which is not the case for the $P_i(m)$. We also omitted the variable m for better readability.

Proposition 4.5. For $m \geq 20$, we have the following height estimates on $E_m(\mathbb{Q})$:

$$\begin{array}{lll} \hat{h}(Q_1) = 2\log m + c_1, & \hat{h}(Q_2) = 2\log m + c_2, & \hat{h}(Q_3) = 2\log m + c_3, \\ \hat{h}(Q_1+Q_2) = 4\log m + c_{12}, & \hat{h}(Q_1+Q_3) = 4\log m + c_{13}, & \hat{h}(Q_2+Q_3) = 4\log m + c_{23} \end{array}$$

with some c_i, c_{ij} dependent on m, satisfying

$$\begin{array}{lll} c_1 \in [2.595,\, 2.713], & c_2 \in [2.596,\, 2.714], & c_3 \in [1.791,\, 1.910], \\ c_{12} \in [7.128,\, 7.245], & c_{13} \in [4.388,\, 4.524], & c_{23} \in [4.311,\, 4.504]. \end{array}$$

For later use (in Proposition 5.3), we define $\underline{c_j}$ and $\overline{c_j}$ to be the lower and upper bounds of c_j, respectively. For example $\underline{c_1} = 2.595$ and $\overline{c_1} = 2.713$.

Proof. The points are explicitly

$$\begin{aligned} &Q_1 = \left(18b, 72b\left(6m^2-5\right)\right), \quad Q_2 = \left(-2b, 8b\left(6m^2+5\right)\right), \quad Q_3 = \left(-6b, -144bm\right), \\ &Q_1+Q_2 = \left(-2^6 3^4 m^4/5^2, 2^4 3^3 m^2\left(252m^4-625\right)/5^3\right), \\ &Q_1+Q_3 = \left(-3\left(6m^2+6m-5\right)^2, -9\left(36m^4-24m^3-24m^2+20m+25\right)\left(6m^2+6m-5\right)\right), \\ &Q_2+Q_3 = \left(12\left(6m^2-6m+5\right)^2, -36\left(36m^4-96m^3+96m^2-80m+25\right)\left(6m^2-6m+5\right)\right). \end{aligned}$$

We use the formula (4.4) with $n = 36ab$ to compute the heights. For this, we first need to determine $\prod_{2\neq p_i\mid \alpha, n} p_i^{e_i}$ and $\hat{h}_2$, where $e_i = v_{p_i}(36ab)$. Recall $v_2(ab) = v_3(ab) = 0$ and $\gcd(a,b) = 1$ (otherwise $36ab$ is divisible by an odd square).

Let us treat in details the case $P = Q_1$ for which $\alpha = 18b, \beta = 72b\left(6m^2-5\right)$ and $\delta = 1$ with the notations of Lemma 4.4. Of course, $\gcd(\alpha, 36ab) = 18b$ so we have $\prod_{2\neq p_i\mid \alpha, n} p_i^{e_i} = \prod_{2\neq p_i\mid \alpha} p_i^{e_i}$. Moreover, if $p_i(\neq 2)$ divides $\alpha = 18b$, then p_i does not divide a (because $\gcd(a,b) = 1$, and $v_3(a) = 0$). So for p_i dividing α we have $v_{p_i}(36ab) = v_{p_i}(36b) = v_{p_i}(9b)$. Therefore $\prod_{2\neq p_i\mid \alpha, n} p_i^{e_i} = 9b$.
On the other hand, $v_2(n) = 2$, $v_2(18b) = 1$ and $v_2\left(72b\left(6m^2-5\right)\right) = 3$ so that Table 1 gives $\hat{h}_2(Q_1) = -\frac{3}{2}\log 2$.

Similar arguments yield Table 2, where we use the Bezout identities

$$\begin{aligned} a\left(\pm 6m+1\right) + \left(6m^2 \pm 6m + 5\right)\left(\mp 36m^3 + 30m^2 \mp 48m + 15\right) &= 100, \\ b\left(\mp 6m+1\right) + \left(6m^2 \pm 6m + 5\right)\left(\pm 36m^3 - 30m^2 \mp 48m + 65\right) &= 300 \end{aligned}$$

for the cases $Q_1 + Q_3$ and $Q_2 + Q_3$.

TABLE 2. Values of $\prod_{2\neq p_i\mid \alpha, n} p_i^{e_i}$ and $\hat{h}_2$

	Q_1	Q_2	Q_3	Q_1+Q_2	Q_1+Q_3	Q_2+Q_3
$\prod_{2\neq p_i\mid \alpha, n} p_i^{e_i}$	$9b$	b	$9b$	9	9	9
$\hat{h}_2$	$-\frac{3}{2}\log 2$	$-\frac{3}{2}\log 2$	$-\frac{3}{2}\log 2$	$-\log 2$	0	$-\log 2$

Let us back to the computation of $\hat{h}(Q_1)$ using (4.4). We have

$$\frac{\alpha^2 + n\delta^4}{\prod_{2\neq p_i\mid \alpha, n} p_i^{e_i}} = 36b + 4a = m^4\left(1440 - \frac{8\left(192m^2-125\right)}{m^4}\right).$$

It can then be easily proved that $f_1(m) = 1440 - \frac{8\big(192m^2-125\big)}{m^4}$ is monotonically increasing for $m \geq 20$ and so

$$1436 < f_1(20) \leq f_1(m) \leq \lim_{m\to\infty} f_1(m) = 1440.$$

Hence by (4.4) we get

$$2\log m + \frac{1}{2}\log 1436 - \frac{3}{2}\log 2 \leq \hat{h}(Q_1) \leq 2\log m + \frac{1}{2}\log 1440 - \frac{3}{2}\log 2 + \frac{1}{6}\log 2$$

which results in the relevant estimate of c_1.

Similarly we have

$$\frac{\alpha^2 + n\delta^4}{\prod_{2\neq p_i|\alpha,n} p_i^{e_i}} = \begin{cases} m^4 f_j(m) & \text{for } Q_j \\ m^8 f_{jk}(m) & \text{for } Q_j + Q_k \end{cases}$$

where

$$\begin{aligned}
f_2(m) &= 8\big(192m^2 + 125\big)/m^4 + 1440, \quad f_3(m) = 200/m^4 + 288 \\
f_{12}(m) &= -2500\big(504m^4 - 625\big)/m^8 + 6225984 \\
f_{13}(m) &= \big(5184m^7 + 3456m^6 - 7776m^5 - 8280m^4 + 6480m^3 + 2400m^2 \\
&\quad - 3000m + 3125\big)/m^8 + 6480 \\
f_{23}(m) &= -4\big(20736m^7 - 48384m^6 + 72576m^5 - 78120m^4 + 60480m^3 \\
&\quad - 33600m^2 + 12000m - 3125\big)/m^8 + 25920.
\end{aligned}$$

Again, all of these functions are monotonic for $m \geq 20$ and so

$$\begin{array}{rcccccccc}
1440 & = & \lim\limits_{m\to\infty} f_2(m) & \leq & f_2(m) & \leq & f_2(20) & < & 1444 \\
288 & = & \lim\limits_{m\to\infty} f_3(m) & \leq & f_3(m) & \leq & f_3(20) & < & 289 \\
6225976 & < & f_{12}(20) & \leq & f_{12}(m) & \leq & \lim\limits_{m\to\infty} f_{12}(m) & = & 6225984 \\
6480 & = & \lim\limits_{m\to\infty} f_{13}(m) & \leq & f_{13}(m) & \leq & f_{13}(20) & < & 6747 \\
22222 & < & f_{23}(20) & \leq & f_{23}(m) & \leq & \lim\limits_{m\to\infty} f_{23}(m) & = & 25920
\end{array}$$

which lead to the estimates of $c_2, c_3, c_{12}, c_{23}, c_{31}$ by using (4.4) with Table 2. □

Corollary 4.6. For $m \geq 20$ we have the following estimates of the height pairings:

$$\langle Q_1, Q_2\rangle = d_{12}, \quad \langle Q_1, Q_3\rangle = d_{13}, \quad \langle Q_2, Q_3\rangle = d_{23},$$

with some d_{ij} dependent on m, satisfying

$$d_{12} \in [0.850,\, 1.027], \quad d_{13} \in [-0.118,\, 0.069], \quad d_{23} \in [-0.157,\, 0.059].$$

Proof. This is a direct application of Proposition 4.5 and formula (4.1). □

In a more general way, we can get an approximation of $\hat{h}(k_1Q_1 + k_2Q_2 + k_3Q_3)$ in terms of the k_i's that will be useful in the following. For this, we need some results on approximation of an eigenvalue of a matrix.

Lemma 4.7. *Let $A, A', R = (r_{ij})$ be $n \times n$ real symmetric matrices with the equality $A = A' + R$. Then for any eigenvalue λ' of A' there exists an eigenvalue λ of A such that*

$$|\lambda - \lambda'| \leq \sqrt{\sum_{i,j} r_{ij}^2} = \sqrt{\operatorname{tr}(R^2)}.$$

Proof. Let λ' be an eigenvalue of A' and $u' = (u_1, ..., u_n)$ a corresponding unit eigenvector. Then by [21, Corollary 3.3] we have $|\lambda - \lambda'| \leq \|Au' - \lambda' u'\|_2$ for some eigenvalue λ of A, where $\|\cdot\|_2$ denotes the 2-norm of vectors. Now we have

$$\|Au' - \lambda' u'\|_2 = \|(A' + R)u' - \lambda' u'\|_2 = \|Ru'\|_2 = \sqrt{\sum_i \left(\sum_j r_{ij} u_j\right)^2}$$
$$\leq \sqrt{\sum_i \sum_j r_{ij}^2 \sum_j u_j^2} = \sqrt{\sum_{i,j} r_{ij}^2}.$$

□

Proposition 4.8. For $m \geq 20$ and for any integers k_1, k_2, k_3 we have the estimate

$$\hat{h}(k_1 Q_1 + k_2 Q_2 + k_3 Q_3) = \left(k_1^2 + k_2^2 + k_3^2\right)(2 \log m + \gamma)$$

with some γ possibly dependent on m, k_1, k_2, k_3, satisfying $\gamma \in [1.454,\ 3.854]$.

Proof. By using the bilinearity of height pairings,

$$\begin{aligned}\hat{h}(k_1 Q_1 + k_2 Q_2 + k_3 Q_3) &= \langle k_1 Q_1 + k_2 Q_2 + k_3 Q_3,\ k_1 Q_1 + k_2 Q_2 + k_3 Q_3 \rangle \\ &= \sum_{i=1,2,3} k_i^2 \hat{h}(Q_i) + 2 \sum_{1 \leq i < j \leq 3} k_i k_j \langle Q_i, Q_j \rangle \\ &= 2\left(k_1^2 + k_1^2 + k_3^2\right) \log m + k^T B k,\end{aligned}$$

where $k = (k_1, k_2, k_3)^T$ and, using notations of Proposition 4.5 and Corollary 4.6,

$$B = \begin{bmatrix} c_1 & d_{12} & d_{13} \\ d_{12} & c_2 & d_{23} \\ d_{13} & d_{23} & c_3 \end{bmatrix}.$$

Note that B is symmetric and so all the eigenvalues are real. Further by an elementary property of the Rayleigh quotient,

$$\lambda_{\min}\left(k_1^2 + k_2^2 + k_3^2\right) \leq k^T B k \leq \lambda_{\max}\left(k_1^2 + k_2^2 + k_3^2\right)$$

where $\lambda_{\min}$ and $\lambda_{\max}$ are the minimal and maximal eigenvalues of B. In order to estimate $\lambda_{\min}$ and $\lambda_{\max}$ thanks to Lemma 4.7, we approximate B with the matrix B' whose coefficients are the middle value of each interval for the coefficients of B given in Proposition 4.5 and Corollary 4.6. For example, taking $c_1' = (\underline{c_1} + \overline{c_1})/2 = 2.654$ we have $c_1 = c_1' + r$ with $|r| \leq |\underline{c_i} - \overline{c_i}|/2 = 0.059$. Explicitly,

$$B' = \begin{bmatrix} 2.654 & 0.9385 & -0.0245 \\ 0.9385 & 2.655 & -0.049 \\ -0.0245 & -0.049 & 1.8505 \end{bmatrix}.$$

The eigenvalues of B' are $1.71378\cdots, 1.85116\cdots$ and $3.59454\cdots$ and $B = B' + R$ for some symmetric matrix $R = (r_{ij})$ such that

$$\begin{array}{lll} |r_{11}| \leq 0.059, & |r_{22}| \leq 0.059, & |r_{33}| \leq 0.0595, \\ |r_{12}| \leq 0.0885, & |r_{13}| \leq 0.0935, & |r_{23}| \leq 0.108. \end{array} \Rightarrow \sqrt{\sum_{i,j} r_{ij}^2} \leq 0.259.$$

Then by Lemma 4.7 we have

$$\lambda_{\min} \geq 1.713 - 0.259 = 1.454 \quad \text{and} \quad \lambda_{\max} \leq 3.595 + 0.259 = 3.854$$

which ends the proof. □

5. Generators of $E_m(\mathbb{Q})$

In this section we prove the following.

Theorem 5.1. *Let E_m be an elliptic curve associated with a simplest quartic field and given by the equation* (2.1)*. Let $P_1(m)$, $P_2(m)$ and $P_3(m)$ be as in Theorem 2.1. These three points can be extended to a basis for $E_m(\mathbb{Q})$. In particular, if the rank is three, then*

$$E_m(\mathbb{Q}) = \langle T, P_1(m), P_2(m), P_3(m)\rangle.$$

As mentioned in Section 4, we will work with Q_1, Q_2 and Q_3 instead of $P_1(m)$, $P_2(m)$ and $P_3(m)$. Let us first present the strategy of the proof. If $\{G_1, G_2, G_3\}$ is a subset of a basis for $E_m(\mathbb{Q})$, then $Q_1, Q_2, Q_3 \in \mathbb{Z}G_1 + \mathbb{Z}G_2 + \mathbb{Z}G_3$ modulo torsion, and there exists a matrix $M \in M_{3\times 3}(\mathbb{Z})$ and $l_1, l_2, l_3 \in \{0, 1\}$ such that

$$\begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} = M \begin{bmatrix} G_1 \\ G_2 \\ G_3 \end{bmatrix} + \begin{bmatrix} l_1T \\ l_2T \\ l_3T \end{bmatrix}.$$

The lattice index of $\{Q_1, Q_2, Q_3\}$ in $\{G_1, G_2, G_3\}$ is $\nu = |\det(M)|$ and we have to show that $\nu = 1$ to prove Theorem 5.1.

As T is a 2-torsion point, for any prime $p \neq 2$, we have

$$\begin{bmatrix} Q_1 \\ Q_2 \\ Q_3 \end{bmatrix} \equiv \overline{M} \begin{bmatrix} G_1 \\ G_2 \\ G_3 \end{bmatrix} \pmod{pE(\mathbb{Q})},$$

where $\overline{M}$ is the image of M in $M_{3\times 3}(\mathbb{Z}/p\mathbb{Z})$. Then, if $p \mid \nu$, there exists a matrix $A \in M_{3\times 3}(\mathbb{Z}/p\mathbb{Z})$ with $\det(A) \neq 0$ such that $\overline{AM}$ has a zero row, which means there exists a non-zero $(k_1, k_2, k_3) \in (\mathbb{Z}/p\mathbb{Z})^3$ such that $k_1Q_1 + k_2Q_2 + k_3Q_3 \in pE(\mathbb{Q})$. ($(k_1, k_2, k_3)$ corresponds to a row of such A.) This gives a criteria to check if $p \mid \nu$, that allows to prove that ν is not divisible by 3.

Proposition 5.2. For $k_i \in \{0, \pm 1\}$ none of the points $k_1Q_1 + k_2Q_2 + k_3Q_3$ lies in $3E_m(\mathbb{Q})$ except O.

Proof. Put $Q = k_1Q_1 + k_2Q_2 + k_3Q_3$. First assume $m \geq 20$. If $Q \in 3E(\mathbb{Q}) \setminus \mathcal{T}$, say $Q = 3R$ for some $R \in E(\mathbb{Q}) \setminus \mathcal{T}$, then by Proposition 4.3

$$\hat{h}(Q) = 3^2\hat{h}(R) \geq 9\log m + 15.6177.$$

On the other hand, since $|k_i| \leq 1$, we have by Proposition 4.8

$$\hat{h}(Q) \leq 3(2\log m + 3.854) = 6\log m + 11.562$$

which contradicts the above estimate. For $1 \leq m < 20$ the assertion is verified by the Sage function `().is_divisible_by(3)`. □

The case of $p = 2$ is slightly different because T is a 2-torsion point. So the torsion part remains and we get

$$\begin{bmatrix} Q_1 - l_1T \\ Q_2 - l_2T \\ Q_3 - l_3T \end{bmatrix} \equiv \overline{M} \begin{bmatrix} G_1 \\ G_2 \\ G_3 \end{bmatrix} \pmod{2E(\mathbb{Q})}.$$

Applying the same argument that when $p \neq 2$, we get that if $2 \mid \nu$, there exists a non-zero $(k_0, k_1, k_2, k_3) \in (\mathbb{Z}/2\mathbb{Z})^4$ such that $k_0T + k_1Q_1 + k_2Q_2 + k_3Q_3 \in 2E(\mathbb{Q})$. Therefore Proposition 3.2 implies ν is not divisible by 2. To complete the proof of Theorem 5.1, we will use Siksek's theorem which gives an upper bound for ν.

Proposition 5.3. The lattice index ν is strictly less than 4.

Proof. Let us first assume that $m \geq 20$. With the notations of Proposition 4.5 and Corollary 4.6, we have

$$H(Q_1, Q_2, Q_3) = \begin{bmatrix} 2\log m + c_1 & d_{12} & d_{13} \\ d_{12} & 2\log m + c_2 & d_{23} \\ d_{13} & d_{23} & 2\log m + c_3 \end{bmatrix}.$$

Then, we have the expression

$$R(Q_1, Q_2, Q_3) = 8\log^3 m + C_2 \log^2 m + C_1 \log m + C_0$$

with $\begin{cases} C_2 = 4\,(c_1 + c_2 + c_3), \\ C_1 = 2\,(c_1c_2 + c_1c_3 + c_2c_3 - d_{12}^2 - d_{13}^2 - d_{23}^2), \\ C_0 = c_1c_2c_3 - c_3d_{12}^2 - c_2d_{13}^2 - c_1d_{23}^2 + 2\,d_{12}d_{13}d_{23}. \end{cases}$

Recall $\underline{c_j}$ and $\overline{c_j}$ are the lower and upper bounds for c_j in Proposition 4.5. Similarly we define the bounds $\underline{d_{ij}}$, $\overline{d_{ij}}$ for d_{ij} by the values in Corollary 4.6. Then

$$\begin{aligned} C_2 &\leq 4(\overline{c_1} + \overline{c_2} + \overline{c_3}) \leq 29.35 \\ C_1 &\leq 2(\overline{c_1c_2} + \overline{c_1c_3} + \overline{c_2c_3} - \underline{d_{12}}^2 - \overline{d_{13}}^2 - \overline{d_{23}}^2) \leq 34 \\ C_0 &\leq \overline{c_1c_2c_3} - \underline{c_3}\underline{d_{12}}^2 - \underline{c_2}\overline{d_{13}}^2 - \underline{c_1}\overline{d_{23}}^2 + 2\,\overline{d_{12}}\underline{d_{13}d_{23}} \leq 12.79. \end{aligned}$$

As we can take $\lambda = \log m + 1.735$ by Proposition 4.3, Siksek's Theorem 4.1 gives

$$\begin{aligned} \nu \leq \sqrt{\frac{2R(Q_1, Q_2, Q_3)}{\lambda^3}} &\leq \sqrt{\frac{2\left(8\log^3 m + 29.35\log^2 m + 34\log m + 12.79\right)}{(\log m + 1.735)^3}} \\ &\leq 4\sqrt{\frac{8\log^3 m + 29.35\log^2 m + 34\log m + 12.79}{8\log^3 m + 41.64\log^2 m + 72.24\log m + 41.78}} < 4. \end{aligned}$$

For $1 \leq m < 20$ we can estimate $\sqrt{2R(Q_1, Q_2, Q_3)/\lambda^3}$ individually to be less than 4 (we used an algorithm of Cremona and Siksek to compute λ which is implemented in Sage as `height_function().min()`). □

6. Integral points on E_m

In the previous sections we got a parametrized family of curves of rank at least three with many integral points. Indeed, there are at least 23 integral points on $E_m(\mathbb{Q})$ according to the following theorem.

Theorem 6.1. *Let $m \in \mathbb{Z}$ such that the rank of $E_m(\mathbb{Q})$ is exactly three. Then all the integral points (up to their additive inverses) having their x-coordinate bounded by $36(t^2 + 13)$ are*

$$\{T, Q_1, Q_2, Q_3, Q_1 + T, Q_2 + T, Q_3 + T, Q_1 - Q_2, Q_1 \pm Q_3, Q_2 \pm Q_3\}.$$

Proof. Let $P = [\alpha, \beta] \in E_m(\mathbb{Z})$ with $|\alpha| \leq 36(t^2+13)$. Using wide bounds ($\hat{h}_2(P) \leq 0, \prod p_i^{e_i} \geq 1$) in (4.4), we get

$$\hat{h}(P) \leq \frac{1}{2}\log(\alpha^2 + 36ab) + \frac{1}{6}\log 2.$$

The hypothesis on α means that $|\alpha| \leq ab - 3\times 36$ (remember that $ab = 36(t^2+16)$). Then we have

$$\begin{aligned}\alpha^2 + 36ab &\leq (ab - 3\times 36)^2 + 36ab \\ &\leq (ab)^2 - 36(5ab - 9\times 36) \\ &\leq (ab)^2.\end{aligned}$$

As a consequence and using the fact that $ab < 36^2 m^8$ if $m \geq 2$, we get

$$\begin{aligned}\hat{h}(P) &\leq \log ab + \frac{1}{6}\log 2 \\ &\leq 8\log m + \log(36^2) + \frac{1}{6}\log 2 \\ &\leq 8\log m + 7.283.\end{aligned}$$

As the rank is assumed to be exactly three, the integral point P can be written as $P = k_0 T + k_1 Q_1 + k_2 Q_2 + k_3 Q_3$ with $k_i \in \mathbb{Z}$. Then, if $m \geq 20$, Proposition 4.8 gives

$$\hat{h}(P) \geq (k_1^2 + k_2^2 + k_3^2)(2\log m + 1.454)$$

which would not contradict the above upper bound only if all the k_i belong to $\{-1, 0, 1\}$ or if one of the k_i is ± 2 and the other ones are zero.
To conclude, we then have to prove that the points Q_1+Q_2, $Q_1 \pm Q_2 + T$, $Q_1 \pm Q_3 + T$, $Q_2 \pm Q_3 + T$, $\pm Q_1 \pm Q_2 \pm Q_3 + k_0 T$, $2Q_1 + k_0 T$, $2Q_2 + k_0 T$, $2Q_3 + k_0 T$ (for $k_0 = 0$ or 1) are not integral. $Q_1 + Q_2$ is the simplest to prove because its x-coordinate is $-\frac{5184}{25}m^4$ which is an integer only if $m \equiv 0 \pmod 5$. But in this case, $36ab$ is divisible by 25 which is an odd square so E_m is not associated to a simplest quartic field. For the other points, the technique is always the same and is given here only for $Q_2 \pm Q_3 + T$ as an example. We have

$$x(Q_2 \pm Q_3 + T) = -3\frac{ab}{\left(6m^2 \mp 6m + 5\right)^2}.$$

Computing Bezout's coefficients between the numerator and the denominator, we get the identities

$$\begin{aligned}a \cdot (\pm 6m + 1) + \left(6m^2 \pm 6m + 5\right)\left(\mp 36m^3 + 30m^2 \mp 48m + 15\right) &= 100, \\ b \cdot (\mp 6m + 1) + \left(6m^2 \pm 6m + 5\right)\left(\pm 36m^3 - 30m^2 \mp 48m + 65\right) &= 300.\end{aligned}$$

Then, any prime dividing both the numerator and the denominator of $x(Q_2 \pm Q_3 + T)$ is a divisor of 300. We deduce that there are no such prime because $\left(6m^2 \mp 6m + 5\right)$ is never divisible by $2, 3$ or 5 (remember $m \equiv 0 \pmod 5$ does not define a simplest quartic field). Then, the denominator of $x(Q_2 \pm Q_3 + T)$ is always $\left(6m^2 \mp 6m + 5\right)^2$ and $Q_2 \pm Q_3 + T$ is never integral.

For $m < 20$ we use the Sage function `S_integral_points`. □

Remark 6.2. For $m = 1$, the rank is three and E_m has extra integral points $Q_1 - Q_2 - Q_3$, $Q_1 - 2Q_3$, $2Q_1 - Q_2 + Q_3$ with the additive inverses. For $m = 2$, the rank is three and E_m has extra integral points $2Q_1 - Q_2, -Q_3$ with the additive inverse. However, for all those points the x-coordinates are greater than $36(t^2+13)$. On the other hand for $m = 7$, the rank is five and extra integral points exist, coming from the other generators.

Corollary 6.3. Let $m \in \mathbb{Z}$ such that the rank of $E_m(\mathbb{Q})$ is exactly three. Then all the integral points (up to their additive inverses) in the compact component of $E_m(\mathbb{R})$ are

$$\{T, Q_2, Q_3, Q_1 + T, Q_1 - Q_2, Q_1 \pm Q_3\}.$$

Proof. The x-coordinate of a point in the compact component of $E_m(\mathbb{R})$ is between $-\sqrt{36ab}$ and 0, then it is a direct consequence of Theorem 6.1. □

We conjecture that, when $m \geq 3$ and the rank is exactly three, E_m has no other integral point that the ones given in Theorem 6.1 also in the non-compact component. It can not be proven with our method because their x-coordinate is potentially not bounded. However, we can determine all the integral points on the original quartic model of the curves thanks to the following proposition which is a variant of Proposition 3.3 and Lemma 10.5 in [4].

Proposition 6.4. Let $t \in \mathbb{Q}$ defining a simplest quartic field such that $6t \in \mathbb{Z}$ and let $[X, Y]$ be an integral point on the quartic model $\mathcal{Q}_t$. Let $P = \varphi([X, Y]) + [0, 0]$ where φ is the isomorphism map from $\mathcal{Q}_t$ to $\mathcal{C}_t$. Then, the coordinates $x(P)$ and $y(P)$ of P satisfy $6x(P)$ and $6y(P) \in \mathbb{Z}$ and, if we assume that $Y < 0$, we have $|x(P)| \leq t^2 + 13$.

Proof. If $[X, Y]$ is not $[0, \pm 1]$, the map φ from $\mathcal{Q}_t$ to $\mathcal{C}_t$ is defined by

$$\begin{cases} x = \dfrac{2Y - 2X^2 + tX + 2}{X^2} \\ y = \dfrac{Y + X^2 + 1}{X} x. \end{cases}$$

Then the coordinates of P are

$$\begin{aligned} x(P) &= 2Y + 2X^2 - tX - 2, \\ y(P) &= -4XY + tY - 4X^3 + 3tX^2 + 12X - t. \end{aligned}$$

These formulas are also valid if $[X, Y] = [0, \pm 1]$. So finally, $6x(P)$ and $6y(P) \in \mathbb{Z}$.

We assume now that $Y = -\sqrt{X^4 - tX^3 - 6X^2 + tX + 1}$. So $x(P) \geq -t^2 - 13$ if and only if

$$2\sqrt{X^4 - tX^3 - 6X^2 + tX + 1} \leq t^2 + 11 + 2X^2 - tX.$$

Then it is sufficient to prove that $f(t, X) = 4(X^4 - tX^3 - 6X^2 + tX + 1) - (t^2 + 11 + 2X^2 - tX)^2 \leq 0$ to ensure that $x(P)$ is greater than or equal to $-t^2 - 13$. It is not difficult to check that $f(t, X)$ is a polynomial of degree two in X whose discriminant is always negative as well as its leading term, so $f(t, x) \leq 0$.

To prove that $x(P) \leq t^2 + 13$, we need

$$-2\sqrt{X^4 - tX^3 - 6X^2 + tX + 1} \leq t^2 + 15 - 2X^2 + tX. \tag{6.1}$$

This is always true if the right hand side is positive which is obviously verified for X in the range $\left[\frac{t-\sqrt{9t^2+120}}{4}, \frac{t+\sqrt{9t^2+120}}{4}\right]$. Outside this range, $t^2 + 15 - 2X^2 + tX < 0$ so that (6.1) is true if and only if $g(t, X) = (t^2 + 15 - 2X^2 + tX)^2 - 4(X^4 - tX^3 - 6X^2 + tX + 1) \leq 0$. Again $g(t, X)$ is a polynomial of degree 2 in X having a negative leading term. Its roots can be of course, explicitly computed and we can check that there are in the range $\left[\frac{t-\sqrt{9t^2+120}}{4}, \frac{t+\sqrt{9t^2+120}}{4}\right]$, so $g(t, x) \leq 0$ outside this range and (6.1) is always true. Finally, we have $|x(P)| \leq t^2 + 13$. □

Theorem 6.5. *Let $m \in \mathbb{Z}$ such that $t = 6m^4 - \frac{7}{6}$ defines a simplest quartic field. The rank of $\mathcal{Q}_t$ is at least three and if it is exactly three, then all the integral points on $\mathcal{Q}_t$ are $[0, \pm 1]$ and $[-3, \pm 12m^2]$.*

Proof. To get the curve E_m from t, we first put $t = 6k^2+2k-1$ and then $k = m^2-\frac{1}{6}$ so that $t = 6m^4 - \frac{7}{6}$. The curve $\mathcal{Q}_t$ is then isomorphic to E_m and has rank at least three thanks to Theorem 5.1. Let $[X, Y]$ be an integral point on $\mathcal{Q}_t$. We assume that $Y \leq 0$ without loss of generality. Proposition 6.4 associates to $[X, Y]$ a point P on $\mathcal{C}_t$ such that $6x(P)$ and $6y(P)$ are in $\mathbb{Z}$ and $|x(P)| \leq t^2 + 13$. This point is then scaled on E_m, via the map $(x, y) \mapsto (6^2x, 6^3y)$, to an integral point having its x-coordinate bounded by $36(t^2 + 13)$. Theorem 6.1 gives all such points on E_m when the rank is exactly three. Finally, we just have to send them back to $\mathcal{Q}_t$ to check if there are integral or not. □

7. An infinitude of curves of rank at least four

In this section, we deduce from the previous rank-3 family an infinite subfamily of curves of rank at least four.

Theorem 7.1. *Let (u, v) be a point on the rank-2 elliptic curve*

$$e : v^2 = u(u - 299)(u + 2701).$$

Let $\mathcal{E}_u$ be the elliptic curve defined by the equation

$$\mathcal{E}_u : Y^2 = X^3 - 36ABX$$

$$\text{with } A = u^4 + 9604\left(u^3 - 807599u\right) + 24684006u^2 + 807599^2,$$
$$\text{and } B = u^4 + 4\left(u^3 - 807599u\right) + 1624806u^2 + 807599^2.$$

$\mathcal{E}_u$ is associated with simplest quartic fields and

$$\mathcal{P}_1(u) = \left(-7200^2u^2, 43200u\left(u^4 + 4804\left(u^3 - 807599u\right) + 1634406u^2 + 807599^2\right)\right),$$
$$\mathcal{P}_2(u) = \left(-2B, 8\left(u^2 + 5402u - 807599\right)B\right),$$
$$\mathcal{P}_3(u) = (-6B, 1440vB),$$
$$\mathcal{P}_4(u) = \left(294B, 5040\left(u^2 + 807599\right)B\right),$$

are independent points of the Mordell-Weil group over $\mathbb{Q}(u)$.

Proof. As we have seen in the proof of Theorem 2.1, the numbers which are multiples of a or b have more chance to be the x-coordinate of some point on E_m. In order to get a fourth point $P_4(m) = (x_4, y_4)$ on the curve, we then assume that $x_4 = \lambda b$. It is easy to verify that it holds if and only if the quartic

$$36m^4\lambda\left(\lambda^2 - 36\right) - 48m^2\lambda\left(\lambda^2 + 36\right)m^2 + 25\lambda\left(\lambda^2 - 36\right)$$

is a square. $\lambda = \pm 6$ clearly plays a special role and in fact it gives the point $P_3(m)$. More generally, this condition means that the values of m for which such a fourth point exists are parametrized by points on an elliptic curve. In order to have an infinite subfamily of curves E_m of rank at least four, we need this elliptic curve to have infinitely many points. We found that for $\lambda = 294$, the associated elliptic curve has rank two and then will provide an infinite family of elliptic curves E_m with a fourth point. In this case, m is parametrized by the rank-2 elliptic curve

$$M^2 = 900m^4 - 1201m^2 + 625$$

where $M = \frac{y_4}{1008b}$. Its Weierstrass form is $v^2 = u(u-299)(u+2701)$ via

$$m = \frac{v}{60u} \quad \text{and} \quad M = \frac{1}{60}\left(\frac{807599}{u} - 1201 + \frac{v^2}{2u^2}\right).$$

For any point (u, v) on e (and there are infinitely many because e has rank two), the corresponding curve E_m then has a fourth point. The corresponding coefficients a and b are given by $a = \frac{A}{600^2u^2}$ and $b = \frac{B}{600^2u^2}$.

Rescaling the curve E_m via $X = 600^2u^2x, Y = 600^3u^3y$, we get the curve $\mathcal{E}_u$ with the four points $\mathcal{P}_1(u), \mathcal{P}_2(u), \mathcal{P}_3(u)$ and $\mathcal{P}_4(u)$ given in the theorem (from the points $P_i(m)$ on E_m).

The free part of $e(\mathbb{Q})$ is generated by $G_1 = (-1, 900)$ and $G_2 = (-851, 42250)$. Using the specialization at $(u, v) = G_1$, we observe that the four points

$$\begin{aligned}
\mathcal{P}_1(-1) &= (-51840000, -28343411136000000),\\
\mathcal{P}_2(-1) &= (-1304442000000, -4242045384000000000),\\
\mathcal{P}_3(-1) &= (-3913326000000, 845278416000000000),\\
\mathcal{P}_4(-1) &= (191752974000000, 2654737745184000000000)
\end{aligned}$$

have regulator 1809.9746... (according to Magma) on the rank-5 specialized curve

$$\mathcal{E}_{-1} : y^2 = x^3 - 154967005201320000000000000x.$$

□

References

1. J. Aguirre, F. Castañeda and J.C. Peral, *High rank elliptic curves of the form $y^2 = x^3 + Bx$*, Rev. Mat. Complut. **XIII** (**1**) (2000) 17–31.
2. J. Aguirre, F. Castañeda and J.C. Peral, *High rank elliptic curves with torsion group $\mathbb{Z}/(2\mathbb{Z})$*, Math. Comp. **73** (**245**) (2003) 323–331.
3. W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997) 235–265.
4. S. Duquesne, *Elliptic curves associated with simplest quartic fields*, J. Théor. Nombres Bordeaux **19** (**1**)(2007) 81–100.
5. S. Duquesne, *Integral points on elliptic curves defined by simplest cubic fields*, Exp. Math. **10** (**1**) (2001) 91–102.
6. Y. Fujita, *Generators for congruent number curves of ranks at least two and three*, J. Ramanujan Math. Soc. **29** (**3**) 307–319 (2014).
7. Y. Fujita, *Generators for the elliptic curve $y^2 = x^3 - nx$ of rank at least three*, J. Number Theory **133** (**5**) (2013) 1645–1662.
8. Y. Fujita, H. Nara, *Generators and integral points on twists of the Fermat cubic*, Acta Arith. **168** (**1**) (2015) 1–6.
9. Y. Fujita, N. Terai, *Generators and integral points on the elliptic curve $y^2 = x^3 - nx$*, Acta Arith. **160** (**4**) (2013) 333–348.
10. Y. Fujita, N. Terai, *Generators for the elliptic curve $y^2 = x^3 - nx$*, J. Théor. Nombres Bordeaux. **23** (**2**) (2011) 403–416.
11. M. N. Gras, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de $\mathbb{Q}$*, Publ. Math. Fac. Sci. Besancon, fasc **2** (1977/1978).
12. I. Gusić, P. Tadić, *Injectivity of specialization homomorphism of elliptic curves*, J. Number Theory **148** (2015) 137–152.
13. S. Kihara, *On an elliptic curves over $\mathbf{Q}(t)$ of rank ≥ 9 with a non-trivial 2-torsion point*, Proc. Japan Acad. Ser. A Math. Sci. **77** (**1**) (2001) 11–12.
14. H. K. Kim, *Evaluation of zeta functions at $s = -1$ of the simplest quartic fields*, Proceedings of the 2003 Nagoya Conference "Yokoi-Chowla Conjecture and Related Problems", Saga Univ., Saga (2004) 63-73.
15. L. Kulesz and C. Stahlke, *Elliptic curves of high rank with a non-trivial torsion group over $\mathbb{Q}$*, Exp. Math. **10** (**3**) (2001) 475–480.

16. A. J. Lazarus, *Class numbers of simplest quartic fields*, Number theory (Banff, AB, 1988), de Gruyter, Berlin (1990) 313–323.
17. A. J. Lazarus, *On the class number and unit index of simplest quartic fields*, Nagoya Math. J. **121** (1991) 1–13.
18. S. Louboutin, *The simplest quartic fields with ideal class groups of exponents less than or equal to 2*, J. Math. Soc. Japan **56** (**3**) (2004) 717–727.
19. K. Nagao, *Construction of high-rank elliptic curves with a non-trivial torsion point*, Math. Comp. **66** (**217**) (1997) 411–415.
20. P. Olajos, *Power integral bases in the family of simplest quartic fields*, Exp. Math. **14** (**2**) (2005) 129–132.
21. Y. Saad, *Numerial Methods for Large Eigenvalue Problems*, 2nd ed., SIAM, Philadelphia, 2011.
22. Sage software, available at http://sagemath.org.
23. S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain J. Math. **25** (**4**) (1995), 1501–1538.
24. J. Silverman, *Computing heights on elliptic curves*, Math. Comp. **51** (**183**) (1988) 339–358.
25. J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 2009.
26. L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, 2nd ed., CRC Press, Taylor & Francis Group, Boca Raton, FL, 2008.

Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France
Email address: sylvain.duquesne@univ-rennes1.fr

Faculty of Engineering, Tohoku-Gakuin University, 1–13–1 Chuo, Tagajo, Miyagi 985–8537, Japan
Email address: sa4m19@math.tohoku.ac.jp

Department of Mathematics and Applications, Faculty of Science, University of Mohaghegh Ardabili, Ardabil 56199–11367, Iran
Email address: shzargar.arman@gmail.com