London Mathematical Society ISSN 1461–1570

COMPUTATION OF SETS OF RATIONAL POINTS OF GENUS-3 CURVES VIA THE DEM'JANENKO–MANIN METHOD

MARTINE GIRARD AND LEOPOLDO KULESZ

Abstract

The authors construct two families of genus-3 curves defined over $\mathbb{Q}(t)$ with three independent morphisms to an elliptic curve of rank at most two. They give explicit examples of an application of the Dem'janenko–Manin method that completely determines both the set of the $\mathbb{Q}(t)$-rational points of the curves under consideration, and the set of $\mathbb{Q}$-rational points of some specialisations.

Introduction

In 1922, Mordell conjectured the finiteness of the set of K-rational points of a curve $\mathcal{C}$ of genus at least 2, defined on a number field K. The analogue for function fields was proved by Manin in 1966 [25], provided that the curve $\mathcal{C}$ is not isotrivial. In 1983, Faltings [13] proved Mordell's conjecture. While Manin's proof is theoretically effective, neither Faltings' proof, nor the subsequent proofs of Vojta [38], Faltings [14] and Bombieri [2] are effective. (For results regarding effectiveness, see de Diego [11] and Rémond [27].) Thus, even if the set of rational points of a given curve is theoretically known to be finite, the proof does not provide a means of achieving the effective determination of the finite set. Indeed, it is one of the major problems of the subject to find an effective proof of Faltings' theorem. Hence the explicit determination, even in special cases, remains an interesting and difficult problem.

Examples of the difficulty of proving the completeness of a known set can be found in Wetherell's successful solution to a problem of Diophantus [40], or in Flynn and Wetherell's solution [18] to a challenge of Serre [28, p. 67]. In both cases, Chabauty-like techniques are developed to obtain the results. These techniques take their name from one of the two methods available to compute these sets explicitly in the number field case: the method of Chabauty [7] (made 'effective' by Coleman [8]) applies to genus-g curves whose Jacobian has rank less than g over K; the other method, due to Dem'janenko [12] and generalised by Manin [26], applies to curves having m independent morphisms to an elliptic curve of rank less than m over K. This last method also works in the function field case, provided that the sets of points of bounded height are finite. While Chabauty's method has been successfully applied, and has given rise to new techniques of investigation (see, for instance, [4, 5, 8, 15, 16, 17] among others), there are only a few examples of computations using the Dem'janenko–Manin method [6, 23, 33]. One reason could be that the conditions for the application of this method are rather restrictive geometrically, and some particular curves of interest thus fail to satisfy the criterion.

In this paper, we address the geometric restrictions of the Dem'janenko–Manin method by explicitly constructing families of curves of genus 3, to which the method apply: we start

Received 7 November 2003, revised 22 August 2005; *published* 5 December 2005.
2000 Mathematics Subject Classification 11G30, 14Q05, 14G05

from a given elliptic curve and construct a genus-3 curve $\mathcal{C}_a$ whose Jacobian is isogenous to the product of three copies of this elliptic curve. Then we impose conditions on this curve so that the elliptic curve has rank 1 or 2, which give us two subfamilies of genus-3 curves:

$$\mathcal{C}_{f(t)} : (X^4 + Y^4 + Z^4) - \frac{(2t^4+1)}{t^2(t^2+2)}(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0$$

and

$$\mathcal{C}_{g(t)} : (X^4 + Y^4 + Z^4) - \frac{(t^4-t^2+1)}{t^2}(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0.$$

More precisely, we determine explicitly — using the Dem'janenko-Manin method — the sets of $\mathbb{Q}(t)$-rational points of the generic curves in the following families.

THEOREM 4.10. *Let $\mathcal{C}_{f(t)}$ be the curve given by the projective equation*

$$(X^4 + Y^4 + Z^4) - \frac{(2t^4+1)}{t^2(t^2+2)}(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0.$$

The set of rational points of this curve is

$$\mathcal{C}_{f(t)}(\mathbb{Q}(t)) = \{(\pm t, t, 1), (\pm t, -t, 1), (\pm t, 1, t), (\pm t, 1, -t), (1, \pm t, t), (1, \pm t, -t)\}.$$

THEOREM 5.9 *Let $\mathcal{C}_{g(t)}$ be the curve given by the projective equation*

$$(X^4 + Y^4 + Z^4) - \frac{(t^4-t^2+1)}{t^2}(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0.$$

The set of rational points of this curve is

$$\begin{aligned}\mathcal{C}_{g(t)}(\mathbb{Q}(t)) = \{&(t : \pm t^2 : 1), (t^2 : \pm t : 1), (t : \pm 1 : t^2), (t^2 : \pm 1 : t),\\ &(1 : \pm t : t^2), (1 : \pm t^2 : t), (-t : \pm t^2 : 1), (-t^2 : \pm t : 1),\\ &(-t : \pm 1 : t^2), (-t^2 : \pm 1 : t), (-1 : \pm t : t^2), (-1 : \pm t^2 : t)\}.\end{aligned}$$

We apply the method to special curves in these families, and we obtain the following theorems.

THEOREM 4.5 *The set of rational points of the curve $\mathcal{C}_{f(7)} = \mathcal{C}_{-1601/833}$ given by the projective equation*

$$833(X^4 + Y^4 + Z^4) - 1601(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0$$

is

$$\begin{aligned}\mathcal{C}_{-1601/833}(\mathbb{Q}) = \{&(\pm 1 : 7 : 7), (\pm 1 : -7 : 7), (\pm 7 : -7 : 1),\\ &(\pm 7 : 7 : 1), (\pm 7 : 1 : 7), (\pm 7 : -1 : 7)\}.\end{aligned}$$

THEOREM 5.4 *The set of rational points of the curve $\mathcal{C}_{g(2)} = \mathcal{C}_{-13/4}$ given by the projective equation*

$$4(X^4 + Y^4 + Z^4) - 13(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0$$

is

$$\begin{aligned}\mathcal{C}_{-13/4}(\mathbb{Q}) = \{&(2 : \pm 4 : 1), (4 : \pm 2 : 1), (2 : \pm 1 : 4), (4 : \pm 1 : 2),\\ &(1 : \pm 2 : 4), (1 : \pm 4 : 2), (-2 : \pm 4 : 1), (-4 : \pm 2 : 1),\\ &(-2 : \pm 1 : 4), (-4 : \pm 1 : 2), (-1 : \pm 2 : 4), (-1 : \pm 4 : 2)\}.\end{aligned}$$

REMARK 1. The only points that we obtain in the special cases are the specialisations of the rational points in the generic cases.

NOTATION. In what follows, K will be either $\mathbb{Q}$ or $\mathbb{Q}(t)$, and $\mathcal{O}_K$ will be its ring of integers ($\mathbb{Z}$ or $\mathbb{Z}[t]$). For ϕ a finite morphism, $d(\phi)$ will be its degree. We will denote a projective point by $(X : Y : Z)$, and the corresponding affine point by (x, y), where $x = X/Z$ and $y = Y/Z$. Finally, we will omit the indices of curves whenever there is no ambiguity.

1. *Heights on curves*

Since naïve heights, as well as canonical heights, play a fundamental role in what follows, we recall in this section some properties of these heights. We also fix our notation.

DEFINITION 1. We define the height of an element $x \in K$ as follows.

- For $x = x_1/x_2 \in \mathbb{Q}$ with $(x_1, x_2) \in \mathbb{Z} \times \mathbb{Z}_{>0}$ and $\gcd(x_1, x_2) = 1$, define the height of x to be $h(x) = \log(\max(|x_1|, |x_2|))$.
- For $x = x_1/x_2 \in \mathbb{Q}(t)$ with $(x_1, x_2) \in \mathbb{Z}[t] \times (\mathbb{Z}[t] \setminus 0)$ and $\gcd(x_1, x_2) = 1$, define the height of x to be $h(x) = \max(\deg(x_1), \deg(x_2))$.

DEFINITION 2. Let $\mathcal{E}$ be an elliptic curve defined over K by an equation of the form $ZY^2 = F(X, Z)$ (or $y^2 = f(x)$), and let $P \in \mathcal{E}(K)$.

We define $h(P) = h(x(P))$ (where $x(P)$ is the x-coordinate of the point P in affine coordinates), and we define $\hat{h}(P)$, the canonical height of $P \in \mathcal{E}(K)$, by the formula $\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h([2^n]P)$.

The canonical height (or Néron–Tate height) has the following properties (see, for instance, [32, p. 229], [35, pp. 217–218] or [28, Chapter 2]).

THEOREM 1.1. *Let P and Q be two points in $\mathcal{E}(K)$.*

(i) $\hat{h}(P) = h(P) + O(1)$.
(ii) $\hat{h}(mP) = m^2\hat{h}(P)$ *for all* $m \in \mathbb{Z}$.
(iii) $\hat{h}(P) = 0$ *if and only if* $P \in \mathcal{E}_{\text{tors}}$ *(if $\mathcal{E}$ does not split over K in the function field case).*
(iv) *The pairing* $\langle P, Q\rangle = \frac{1}{2}(\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q))$ *is bilinear positive definite.*
(v) *The points $P_1, \ldots, P_n \in \mathcal{E}(K)$ are independent if and only if the $n \times n$ matrix with coefficients $\langle P_i, P_j\rangle$ has non-zero determinant.*

REMARK 2. Note that our normalisation of the height is twice Silverman's.

The first property of the canonical height says that the difference between $\hat{h}$ and h is bounded by a constant depending only on $\mathcal{E}$. Silverman gave the following estimates (see [34] and [35, p. 280]).

PROPOSITION 1.2. *When $\mathcal{E}$ has an equation of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathcal{O}_K$, then, for any point P in $\mathcal{E}(K)$, the following statements hold.*

- *If $K = \mathbb{Q}$, then*

$$-\tfrac{1}{12}h(j) - \mu(E) - 1.946 \leqslant \hat{h}(P) - h(P) \leqslant \mu(E) + 2.14, \tag{1}$$

where $6\mu(E) = h(\Delta) + \log(\max(|j|, 1))$.

- *If $K = \mathbb{Q}(t)$, then*

$$|\hat{h}(P) - h(P)| \leqslant h(A^3) + h(B^2). \tag{1'}$$

REMARK 3. There exist other bounds on the difference between the canonical and naïve heights on a number field (see, for instance, Siksek [31] or Cremona–Prickett–Siksek [10]).

2. *The method of Dem'janenko and Manin*

In this section, we give a description of the method, as well as a sketch of the proof. We then demonstrate how we can obtain effective results.

2.1. *General method*

Let $\mathcal{C}/K$ be a smooth projective curve of $\mathbb{P}^k$, let $\mathcal{E}/K$ be an elliptic curve, and let $\phi_1, \ldots, \phi_l$ be morphisms from $\mathcal{C}$ to $\mathcal{E}$ defined over K.

Definition 3. For a point $P = (a_0 : \ldots : a_k) \in \mathcal{C}(K)$ (we assume that $a_0, \ldots, a_k \in \mathcal{O}_K$ and that $\gcd(a_0, \ldots, a_k) = 1$), we define the *naïve height* of this point as

$$h(P) = \max(h(a_0), \ldots, h(a_k)).$$

We have (see [32, p. 229], [35, pp. 217–218], [28, Chapter 2], and [21, p. 179]):

$$\left.\begin{aligned} \hat{h}_{\mathcal{E}}(\phi_i(P)) &= h_{\mathcal{E}}(\phi_i(P)) + O(1), \\ h_{\mathcal{E}}(\phi_i(P)) &= cd(\phi_i)h_{\mathcal{C}}(P) + O(1), \end{aligned}\right\} \qquad \text{for } i \in \{1, \ldots, l\}, \tag{2}$$

where $\hat{h}$ is the canonical height on $\mathcal{E}$ and c is a constant depending on our normalisation of the various heights involved.

Definition 4. Fix $P_0 \in \mathcal{C}(K)$. For $i = 1, \ldots, l$, define $\bar{\phi}_i = \phi_i - \phi_i(P_0)$. We will say that $\phi_1, \ldots, \phi_l$ are *independent on* K, if

$$\sum_{1 \leqslant i \leqslant l} n_i \bar{\phi}_i = 0 \Longrightarrow n_1 = \ldots = n_i = \ldots = n_l = 0.$$

We can test the independence of morphisms using the following criterion of Cassels.

Lemma 2.1 (see [6]). *Let $\alpha_1, \ldots, \alpha_l$ be l morphisms from a curve $\mathcal{C}$ to an elliptic curve $\mathcal{E}$. Let D be the matrix whose coefficients are*

$$\langle \alpha_i, \alpha_j \rangle = \tfrac{1}{2}(d(\alpha_i + \alpha_j) - d(\alpha_i) - d(\alpha_j)), \qquad 1 \leqslant i, j \leqslant l.$$

The l morphisms $\alpha_1, \ldots, \alpha_l$ are independent if and only if $\det(D) \neq 0$.

We have the following result [6, 12, 28].

Theorem 2.2. *If $\phi_1, \ldots, \phi_l$ are independent over K and $l > r_K(\mathcal{E})$, then $\mathcal{C}(K)$ is finite and can be effectively determined.*

Let us give a brief outline of the proof.

Sketch of proof. Let $P \in \mathcal{C}(K)$. Combining the equations (2) with the definition of the height pairing, we obtain

$$\langle \phi_i(P), \phi_j(P) \rangle = c \langle \phi_i, \phi_j \rangle h_{\mathcal{C}}(P) + O\big(\sqrt{h(P)}\big),$$

and thus

$$\lim_{h_{\mathcal{C}}(P) \mapsto \infty} \frac{\det\big(\langle \phi_i(P), \phi_j(P) \rangle\big)}{c^l \, h_{\mathcal{C}}(P)^l} = \det\big(\langle \phi_i, \phi_j \rangle\big) \neq 0.$$

By hypothesis, the number of independent morphisms is strictly larger than the rank of the elliptic curve, and hence the regulator $\det(\langle \phi_i(P), \phi_j(P) \rangle)$ is zero. Moreover, the number of rational points of bounded height is finite (provided that the elliptic surface is non-split in the function field case; see [35, Chapter III-5]), and thus

$$\#\mathcal{C}(K) < \infty. \qquad \square$$

In a more practical way, for $1 \leqslant i, j \leqslant l$, we obtain the following inequalities:

$$\left|\frac{1}{2}(\hat{h}(\phi_i(P) + \phi_j(P)) - \hat{h}(\phi_i(P)) - \hat{h}(\phi_j(P))) - \frac{c}{2}(d(\phi_i + \phi_j) - d(\phi_i) - d(\phi_j))h(P)\right| < r_{i,j},$$

where the $r_{i,j}$ are independent of P. Denote by H, D and R the matrices whose respective (i, j)-entries are $\langle\phi_i(P), \phi_j(P)\rangle$, $\langle\phi_i, \phi_j\rangle$ and $r_{i,j}$; this set of inequalities leads to

$$\|H - ch(P)D\| \leqslant \|R\|,$$

where the norm $\|.\|$ is a norm of algebra, such that the set of $l \times l$ matrices with real coefficients $\mathcal{M}_l(\mathbb{R})$, equipped with this norm, is a Banach algebra. It is well known that if $\|A\| < 1$, the matrix $(I - A)$ is invertible.

Thus, if

$$\|H - ch(P)D\| < \frac{1}{\|(ch(P)D)^{-1}\|},$$

then

$$H(ch(P)D)^{-1}$$

would be invertible and thus H would be invertible, since the matrix D is invertible from Lemma 2.1. But this contradicts the hypothesis that $\mathrm{rank}_K(\mathcal{E}(K)) < l$, and hence

$$\|R\| \geqslant \frac{1}{\|(ch(P)D)^{-1}\|},$$

and finally,

$$h(P) \leqslant \|R\| \times \|c^{-1} D^{-1}\|.$$

We can thus obtain a bound on the naïve height of the rational points on the curve $\mathcal{C}$. Combining this bound with the study of the images of the possible rational points on the elliptic curves will enable us to determine these sets explicitly, as we shall see in Section 5.2.

Remark 4. In the particular case where there are two independent morphisms ϕ_1 and ϕ_2, of the same degree d, from the curve $\mathcal{C}/K$ to the elliptic curve $\mathcal{E}/K$, the difference between the canonical heights is then bounded above as follows:

$$|\hat{h}(\phi_1(P)) - \hat{h}(\phi_2(P))| \leqslant |\hat{h}(\phi_1(P)) - h(\phi_1(P))| + |\hat{h}(\phi_2(P)) - h(\phi_2(P))| + |h(\phi_1(P)) - h(\phi_2(P))|. \quad (3)$$

2.2. *Simplification in rank* 1

When, moreover, the elliptic curve has rank 1 over K, it is possible to simplify the previous method (see [23]).

Indeed, if R is a generator of the free part of $\mathcal{E}(K)$, then for any point P in $\mathcal{C}(K)$ there exist two integers n and m and two points T_1 and T_2 in $\mathcal{E}(K)_{\mathrm{tors}}$ such that:

$$\begin{cases}\phi_1(P) = [n]R + T_1,\\ \phi_2(P) = [m]R + T_2,\end{cases} \quad \text{and thus} \quad \begin{cases}\hat{h}(\phi_1(P)) = n^2\hat{h}(R),\\ \hat{h}(\phi_2(P)) = m^2\hat{h}(R).\end{cases} \quad (4)$$

We differentiate between two cases, as follows.

• If $n \neq \pm m$, the equations (1) (or (1′)), (2), (4) and (3) imply that there exists a constant k (depending on $\mathcal{E}$, ϕ_1 and ϕ_2) such that $|m^2 - n^2| < k$. We can thus bound the possible values of n and m. It remains to find all the K-rational points of $\mathcal{C}$ whose images on $\mathcal{E}$ are of the form nR with $n < k$. This can be done by direct computations.

• If $n = \pm m$, then $\phi_1(P) \pm \phi_2(P)$ is in $\mathcal{E}(K)_{\text{tors}}$. Since the morphisms ϕ_1 and ϕ_2 are independent, there exist a finite number of points P in $\mathcal{C}(K)$ such that $\phi_1(P) \pm \phi_2(P)$ is in $\mathcal{E}(K)_{\text{tors}}$; they can be found by direct computation.

Thus, we effectively obtain all the rational points on $\mathcal{C}$, as we shall see in Section 4.2.

3. *Application to some genus-3 curves*

We shall apply this method to compute the sets of rational points of curves in a given family. In order to do so, the curve needs to satisfy the conditions of the Dem'janenko–Manin method — that is, having more independent morphisms to an elliptic curve than the rank of this elliptic curve. A good candidate is thus a curve whose Jacobian is isogenous to the product of three copies of the same elliptic curve. We will then need only to force the rank of the elliptic curve to be strictly less than 3.

3.1. *Curves of genus 3 with given Jacobians*

We construct a curve whose Jacobian is isogenous to the product of three copies of the same elliptic curve. Indeed, this condition will ensure that there exist three independent morphisms to an elliptic curve. We will use a weaker version of a result of Howe, Leprévost and Poonen [22].

PROPOSITION 3.1. *Let k be a field of characteristic not equal to 2 with separable closure K. For $i = 1, 2, 3$, let $\mathcal{E}_i$ be the elliptic curve defined over k by $y^2 = x(x^2 + A_i x + B_i)$ where $B_i \neq 0$. Assume that the product of their discriminants is a square. Define $\Delta_i = A_i^2 - 4B_i$ and R as a square root of their product.*

Define

$$\tau = R\left(\frac{A_1^2}{\Delta_1} + \frac{A_2^2}{\Delta_2} + \frac{A_3^2}{\Delta_3} - 1\right) - 2A_1A_2A_3.$$

Let $\mathcal{C}$ be the plane quartic over k defined by

$$B_1X^4 + B_2Y^4 + B_3Z^4 + dX^2Y^2 + eX^2Z^2 + fY^2Z^2 = 0,$$

where

$$d = \frac{1}{2}\left(-A_1A_2 + \frac{A_3R}{\Delta_3}\right), \quad e = \frac{1}{2}\left(-A_1A_3 + \frac{A_2R}{\Delta_2}\right) \quad \text{and} \quad f = \frac{1}{2}\left(-A_3A_2 + \frac{A_1R}{\Delta_1}\right).$$

If $\tau \neq 0$, the Jacobian of $\mathcal{C}$ is isogenous to $\mathcal{E}_1 \times \mathcal{E}_2 \times \mathcal{E}_3$ over the field $k(\sqrt{\tau})$.

The stronger form of this proposition asserts the isomorphism over the quadratic extension $k' = k(\sqrt{\tau})$ of the polarised Jacobian of $\mathcal{C}$ with the polarised abelian variety $(\mathcal{E}_1 \times \mathcal{E}_2 \times \mathcal{E}_3)_{k'}/G_{k'}$, where G is a sub-groupscheme of the 2-torsion on the product of the elliptic curves (for more details, see [22]).

If we choose $\mathcal{E}_1 = \mathcal{E}_2 = \mathcal{E}_3$ the elliptic curve $y^2 = x(x^2 + Ax + B)$, we obtain a curve of the form $X^4 + Y^4 + Z^4 + a(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0$, where $a = d/B$. We will study some properties of this family of curves.

We recall some results obtained by the second author in [24], as well as those given by the first author in her thesis [19] and jointly with Pavlos Tzermias [20] in a particular case. Let $\mathcal{C}_a$ be the smooth plane curve given by the projective equation

$$X^4 + Y^4 + Z^4 + a(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0.$$

This curve has genus 3 and possesses an automorphism group G of order 24 on $\mathbb{Q}$, generated by:

$$\sigma_1 : (X : Y : Z) \longmapsto (-X : Y : Z);$$
$$\sigma_2 : (X : Y : Z) \longmapsto (Z : X : Y);$$
$$\sigma_3 : (X : Y : Z) \longmapsto (Y : X : Z).$$

Let $\mathcal{D}_a$ be the projective curve

$$X^4 + Y^2Z^2 + Z^4 + a(X^2YZ + X^2Z^2 + Y^3Z) = 0.$$

There exist three degree-2 morphisms from $\mathcal{C}_a$ to $\mathcal{D}_a$, namely

$$\begin{cases} \psi_1 : (X : Y : Z) \longmapsto (XZ : Y^2 : Z^2); \\ \psi_2 : (X : Y : Z) \longmapsto (YX : Z^2 : X^2); \\ \psi_3 : (X : Y : Z) \longmapsto (ZY : X^2 : Y^2). \end{cases}$$

Proposition 3.2. *The Jacobian of $\mathcal{D}_a$ is the elliptic curve $\mathcal{E}_a$ whose equation is: $v^2 = u^3 + \alpha(a)u + \beta(a)$, with*

$$\begin{cases} \alpha(a) = -(a^2 + 3a + 3)(a - 2)^2/3; \\ \beta(a) = -(2a + 3)(a - 2)^3(a + 3)a/27. \end{cases}$$

Proof. There exists a degree-4 morphism ρ from $\mathcal{D}_a$ to $\mathcal{E}_a$, given explicitly by [39]:

$$\begin{array}{rccc} \rho : & \mathcal{D}_a & \longrightarrow & \mathcal{E}_a \\ & (X : Y : Z) & \longmapsto & (u, v), \end{array}$$

where

$$\begin{cases} u = \dfrac{(2 - a)((a^2 + 2a)(X^4 + Z^4) + (2a^2 + 12a + 12)X^2Z^2)}{3((a + 2)(X^4 + Z^4) + 2aX^2Z^2)}, \\ v = \dfrac{2(a - 2)^2(a + 2)(a + 1)XZ(X^2 - Z^2)(X^2 + Z^2)}{((a + 2)(X^4 + Z^4) + 2aX^2Z^2)(2YZ + a(X^2 + Z^2))}, \end{cases} \tag{5}$$

and hence the result holds. □

Proposition 3.3. *The Jacobian $\mathcal{C}_a$ is $\mathbb{Q}(a)$-isogenous to $\mathcal{E}_a \times \mathcal{E}_a \times \mathcal{E}_a$.*

Proof. Let ω be a differential form on $\mathcal{D}_a$. Then we can easily check that $\omega_1 = \psi_1^*(\omega)$, $\omega_2 = \psi_2^*(\omega)$ and $\omega_3 = \psi_3^*(\omega)$ are independent differential forms on $\mathcal{C}_a$. Indeed, let us use the affine coordinates $x = X/Z$ and $y = Y/Z$ on $\mathcal{C}_a$ and $\mathcal{D}_a$. If we choose

$$\omega = \frac{dx}{y + \frac{a}{2}x^2 + \frac{a}{2}},$$

we will have:

$$\omega_1 = \frac{dx}{y^2 + \frac{a}{2}x^2 + \frac{a}{2}}, \qquad \omega_2 = \frac{1}{y}\omega_1 \qquad \text{and} \qquad \omega_3 = \frac{x}{y}\omega_1,$$

and thus the differential forms are independent.

Alternatively, we can apply Proposition 3.1 to three copies of $\mathcal{E}_a$. The elliptic curve $\mathcal{E}_a$ is $\mathbb{Q}(a)$-isomorphic to the elliptic curve $y^2 = x(x^2 + Ax + B)$, where $A = a(2-a)$ and $B = -(a+1)(a-2)^2$. Since $\Delta = A^2 - 4B^2 = (a-4)^2$, Δ^3 is a square and we can apply the proposition. Moreover, we find that $T = 4(a-2)^4(a+1)^2$, and $d/B = a$; hence the Jacobian of $\mathcal{C}$ is $\mathbb{Q}(a)$-isogenous to the product of three copies of $\mathcal{E}_a$. □

REMARK 5. Whenever the elliptic curve $\mathcal{E}_a$ has nonzero rank, we cannot use Chabauty's method but, as we shall see, we can (for certain curves) apply the Dem'janenko–Manin method.

REMARK 6. In his thesis [36] (see also, for instance, [1]) Jaap Top showed the same result, using a different parametrisation for the curve.

PROPOSITION 3.4. *The three morphisms $\rho \circ \psi_1$, $\rho \circ \psi_2$ and $\rho \circ \psi_3$ are independent.*

Proof. We use Cassels' criterion (Lemma 2.1), and we follow the same reasoning as in the worked-out example in his paper [6].

Using the symmetry, we see that for a point (x, y) of $\mathcal{C}$, we have

$$\rho \circ \psi_1(x, y) = \rho \circ \psi_1(x, -y) \qquad \text{and} \qquad \rho \circ \psi_2(x, y) + \rho \circ \psi_2(x, -y) = \mathcal{O}.$$

We deduce that

$$(\rho \circ \psi_1 + \rho \circ \psi_2)(x, y) = (\rho \circ \psi_1 - \rho \circ \psi_2)(x, -y).$$

Let ν be the morphism of $\mathcal{C}$ given by $(x, y) \longmapsto (x, -y)$. It obviously has degree 1, and thus

$$\deg(\rho \circ \psi_1 + \rho \circ \psi_2) = \deg(\rho \circ \psi_1 - \rho \circ \psi_2) = \deg(\rho \circ \psi_1) + \deg(\rho \circ \psi_2). \qquad \square$$

We deduce that the following corollary holds.

COROLLARY 3.5. *Let $a \in K$ be such that $\mathcal{E}_a(K)$ has rank at most 2 on K; then $\mathcal{C}_a(K)$ can be effectively determined.*

It remains to construct subfamilies for which the rank of $\mathcal{E}_a(K)$ is 1 or 2. This is the object of the next section.

3.2. *Construction of particular curves*

It is obvious that the set $\mathcal{C}_a(K)$ contains the orbit (for the action of G) of a point $P_0 = (x_0 : y_0 : z_0) \in \mathbb{P}^2(K)$ if and only if

$$a = -\frac{x_0^4 + y_0^4 + z_0^4}{x_0^2 y_0^2 + x_0^2 z_0^2 + y_0^2 z_0^2}.$$

A priori, there is nothing in the construction of the three points $\rho \circ \psi_1(P_0)$, $\rho \circ \psi_2(P_0)$ and $\rho \circ \psi_3(P_0)$ to guarantee (or exclude) dependence relations on $\mathcal{E}_a(\mathbb{Q}(a))$. In order to be able to apply the Dem'janenko–Manin method, we are going to force some relations of dependence between these three points. More precisely, we obtain the following assertions.

PROPOSITION 3.6.

- *Let $f(t) = -(2t^4+1)/t^2(t^2+2)$; then the elliptic curve $\mathcal{E}_{f(t)}$ has rank 1 over $\mathbb{Q}(t)$. Furthermore, the point $P_0 = (t : t : 1)$ and the eleven other points in its orbit are in $\mathcal{C}_{f(t)}(\mathbb{Q}(t))$.*
- *Let $g(t) = -(t^4 - t^2 + 1)/t^2$; then the elliptic curve $\mathcal{E}_{g(t)}$ has rank 2 over $\mathbb{Q}(t)$. The point $P_0 = (t^2 : t : 1)$ and the twenty-three other points in its orbit are in $\mathcal{C}_{g(t)}(\mathbb{Q}(t))$.*

Proof. These assertions on the rank are proved in Sections 4.1 and 5.1 respectively. □

REMARK 7. For $P_0 = (t : t : 1)$, we see that $\rho \circ \psi_2(P_0)$ is a 2-torsion point, and that $\rho \circ \psi_3(P_0) = -\rho \circ \psi_1(P_0)$. Also, for $P_0 = (t^2 : t : 1)$, we have $\rho \circ \psi_3(P_0) = -\rho \circ \psi_2(P_0)$.

We shall show in the next two sections that the only rational points on these curves are the points that we have already obtained by construction: that is, the points in the orbit of P_0 for the action of the automorphism group of the curve.

4. *The case $f(t)$*

Let $a = f(t) = -(2t^4+1)/t^2(t^2+2)$. Consider the elliptic curve $\mathcal{E}'_t$:

$$y^2 = x^3 - \frac{t^8 + 13\,t^4 - 6\,t^2 + 1}{3}\,x + \frac{(2\,t^4+1)(t^4+6\,t^2-1)(t^4-6\,t^2+2)}{27};$$

it is isomorphic to $\mathcal{E}_{f(t)}$ by the change of coordinates

$$\tau : (x, y) \longmapsto \left(\frac{t^4(t^2+2)^2}{(2t^2+1)^2}x,\ \frac{t^6(t^2+2)^3}{(2t^2+1)^3}y\right). \tag{6}$$

The three points of order 2 of $\mathcal{E}'_t$ are $A_t = (\alpha_1, 0)$, $B_t = (\alpha_2, 0)$ and $C_t = (\alpha_3, 0)$, where

$$\alpha_1 = \frac{-2t^4-1}{3}, \qquad \alpha_2 = \frac{t^4+6t^2-1}{3} \qquad \text{and} \qquad \alpha_3 = \frac{t^4-6t^2+2}{3}.$$

There exist three independent morphisms $\phi_i = \tau \circ \rho \circ \psi_i$ from $\mathcal{C}_{f(t)}$ to $\mathcal{E}'_t$. The image by ϕ_1 of $(t : t : 1)$ is the point P_t whose coordinates are

$$\left(\frac{12\,t^6 + 22\,t^4 - 1}{3},\ 2\,(t^2+1)(2\,t-1)(2\,t+1)(t^2+2)t^3\right).$$

We will actually consider the point Q_t such that $B_t + P_t = 2Q_t$. It has coordinates

$$\left(\frac{t^4 - 6\,t^3 + 9\,t^2 - 12\,t + 5}{3},\ -2\,t^5 + 5\,t^4 - 8\,t^3 + 11\,t^2 - 8\,t + 2\right).$$

In Section 4.1, we show that the point Q_t is a point of infinite order of $\mathcal{E}'_t(\mathbb{Q}(t))$. We know that the set of rational points of $\mathcal{C}_{f(t)}(\mathbb{Q}(t))$ contains $(t : t : 1)$ and the other eleven points in its orbit. (Likewise, the set of rational points of $\mathcal{C}_{f(7)}(\mathbb{Q})$ contains $(7 : 7 : 1)$ and the other eleven points in its orbit.) We will show in Sections 4.2.1 and 4.2.2, respectively, that in both cases this is the entire set.

4.1. *The generic rank is 1*

We show that $\mathcal{E}'_t$ is an elliptic K3 surface, and we use the Shioda–Tate formula to compute the rank.

THEOREM 4.1 (Shioda [29, 30]). *Let $\pi : S \longrightarrow \mathbb{P}^1$ be an elliptic K3 surface defined over K, and let E be the generic fibre.*

The Mordell–Weil rank is given by the formula

$$\operatorname{rank} E(K) \leqslant \operatorname{rank} E(\bar{K}) \leqslant 18 - \sum_{v \in R} (m_v - 1),$$

where R is the set of points v such that $\pi^{-1}(v)$ is singular and m_v is the number of components in the fibre $\pi^{-1}(v)$.

If, moreover, the K3 surface is defined over $\mathbb{Q}$, the first inequality is strict.

PROPOSITION 4.2. *The elliptic curve $\mathcal{E}'_t$ has rank 1 over $\mathbb{Q}(t)$. Moreover, the point Q_t is a generator of the free part of $\mathcal{E}'_t(\mathbb{Q}(t))$.*

Proof. Let us consider the minimal elliptic surface $\pi : S \longrightarrow \mathbb{P}^1$ of $\mathcal{E}'_t/\mathbb{Q}(t)$. To prove that the surface S is K3, we just need to prove the existence of a differential form without zeroes or poles on S. The differential form $\omega = dy \wedge dt/(27x^2 - t^8 + 13t^4 - 6t^2 - 1) = dx \wedge dt/2y$ satisfies this condition.

We compute the Kodaira type of the singular fibres, as follows.

t	0	1	-1	∞	$1/2$	$-1/2$	$\sqrt{2}$	$-\sqrt{2}$
fibre type	I_4	I_4	I_4	I_4	I_2	I_2	I_2	I_2

Since a fibre of Kodaira type I_n has n components, we deduce that $\operatorname{rank} \mathcal{E}'_t(\mathbb{Q}(t)) < 2$. On the other hand, the point Q_t has non-zero height (as will be proved in Lemma 4.15), so the rank over $\mathbb{Q}(t)$ is exactly 1.

We still need to show that Q_t is a generator. Since the rank of $\mathcal{E}'_t(\mathbb{Q}(t))$ is 1, Q_t could be a multiple of the generator. But then the same would apply for a specialisation such that the rank remains 1. Specialising at $t_0 = 7$ (see below, Proposition 4.3) shows that this is not the case. □

PROPOSITION 4.3. *The elliptic curve $\mathcal{E}'_7$ has rank 1 over $\mathbb{Q}$. The point Q_7 generates the Mordell–Weil group modulo torsion.*

Proof. The elliptic curve $\mathcal{E}'_7$ has equation $y^2 = x^3 - 1\,931\,907x + 1\,010\,701\,694$ and Q_7 has coordinates $(163, 26\,460)$. The program '`mwrank`' [9] gives the results. □

COROLLARY 4.4. *The set $\mathcal{C}_{f(t)}(\mathbb{Q}(t))$ can be effectively determined, as we shall see in the next section.*

4.2. *Effective computations*

We determine the set of rational points in the generic case, and also for a specialisation for which the rank of the elliptic curve is 1. Since the morphisms to the elliptic curve have the same degree, we can use the simplified version of Section 2.2.

4.2.1. *Special case*

Consider the elliptic curve corresponding to $t = 7$. We saw in the preceding section (see Proposition 4.3) that it has rank 1 over $\mathbb{Q}$, and that Q_7 generates the free part of $\mathcal{E}'_7(\mathbb{Q})$. We will determine the set of rational points on the associated genus-3 curve $\mathcal{C}_{-1601/833}$.

THEOREM 4.5. *The set of rational points of the curve $\mathcal{C}_{f(7)}$ given by the projective equation*

$$833(X^4 + Y^4 + Z^4) - 1601(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0$$

is

$$\mathcal{C}_{-1601/833}(\mathbb{Q}) = \{(\pm 1 : 7 : 7), (\pm 1 : -7 : 7), (\pm 7 : -7 : 1), (\pm 7 : 7 : 1), (\pm 7 : 1 : 7), (\pm 7 : -1 : 7)\}.$$

Indeed, we can bound the difference between four times the naïve height of a point on the curve $\mathcal{C}_{f(7)}$ and the naïve height of the image of this point on the elliptic curve as follows.

LEMMA 4.6. *For $i = 1, 2$ and $P \in \mathcal{C}(\mathbb{Q})$, we have*

$$4h_{\mathcal{C}}(P) + 5.99 \leqslant h_{\mathcal{E}'}(\phi_i(P)) \leqslant 4h_{\mathcal{C}}(P) + 17.03.$$

Proof. The images by ϕ_1 and ϕ_2 of the point $P = (X : Y : Z)$ have x-coordinates respectively equal to

$$x_1 = \frac{936\,585(X^4 + Z^4) + 22\,952\,382X^2Z^2}{-585(X^4 + Z^4) + 28\,818X^2Z^2} = \frac{U(X, Z)}{V(X, Z)} \quad \text{and} \quad x_2 = \frac{U(X, Y)}{V(X, Y)}.$$

Without loss of generality, we can assume that $i = 1$. By definition,

$$H(x_1) = \max(|U|, |V|) \leqslant \max(2 \cdot 936\,585 + 22\,952\,382, 2 \cdot 585 + 28\,818)H(P)^4$$

and thus in logarithmic heights

$$h_{\mathcal{E}'}(\phi_1(P)) \leqslant 4h_{\mathcal{C}}(P) + 17.03.$$

For the lower bound, we have

$$\begin{cases} (28\,818Z^2 - 585X^2)U(X, Z) + (936\,585X^2 + 22\,952\,382Z^2)V(X, Z) \\ \qquad = 40\,417\,650\,000Z^6, \\ (28\,818X^2 - 585Z^2)U(Z, X) + (936\,585Z^2 + 22\,952\,382X^2)V(Z, X) \\ \qquad = 40\,417\,650\,000X^6, \end{cases}$$

and thus

$$\begin{aligned} &40\,417\,650\,000(\max(|X|, |Z|))^6 \\ &\quad \leqslant (936\,585 + 22\,952\,382 + 585 + 28\,818)H(P)^2 \max(|U|, |V|) \\ &\quad \leqslant 23\,918\,370H(P)^2 H(\phi_1(P)). \end{aligned}$$

Moreover,

$$\begin{aligned} &(-36\,854\,791\,220\,709Y^2 + 33\,010\,709\,672\,391(X^2 + Z^2))V(X, Z) \\ &+ (57\,648\,953\,691Y^2 - 36\,933\,163\,209(X^2 + Z^2))U(X, Z) \\ &\quad = 28\,045\,362\,740\,850\,000Y^6, \end{aligned}$$

and thus

$$\begin{aligned} 28\,045\,362\,740\,850\,000|Y|^6 &\leqslant \max(|U|, |V|)(36\,854\,791\,220\,709 + 2 \cdot 33\,010\,709\,672\,391 \\ &\qquad + 57\,648\,953\,691 + 2 \cdot 36\,933\,163\,209)H(P)^2 \\ &\leqslant 103\,007\,725\,845\,600H(P)^2 \max(|U|, |V|). \end{aligned}$$

As $103\,007\,725\,845\,600/28\,045\,362\,740\,850\,000$ is larger than $23\,918\,370/40\,417\,650\,000$, we have, in logarithmic heights,

$$4h_{\mathcal{C}}(P) + 5.60 \leqslant h_{\mathcal{E}'}(\phi_1(P)). \qquad \square$$

Moreover, we know from Proposition 1.2 that the following statement holds.

LEMMA 4.7. *The difference between the canonical and naïve heights of a point Q on the elliptic curve $\mathcal{E}'_7$ is bounded as follows:* $|\hat{h}_{\mathcal{E}'}(Q) - h_{\mathcal{E}'}(Q)| \leqslant 14.47$.

We deduce that therefore the next lemma holds.

LEMMA 4.8. *The difference between the canonical heights of the images of a rational point P of $\mathcal{C}$ by ϕ_1 and ϕ_2 is bounded by* $|\hat{h}_{\mathcal{E}'}(\phi_1(P)) - \hat{h}_{\mathcal{E}'}(\phi_2(P))| \leqslant 40.37$.

We are now in a position to prove Theorem 4.5.

Proof of Theorem 4.5. Let $P \in \mathcal{C}(\mathbb{Q})$. Since Q_7 generates the free part of $\mathcal{E}'_7(\mathbb{Q})$, there exist some integers n and m, and some points T_1 and $T_2 \in \mathcal{E}'(\mathbb{Q})_{\text{tors}}$, such that

$$\begin{cases} \phi_1(P) = [n]Q_7 + T_1, \\ \phi_2(P) = [m]Q_7 + T_2, \end{cases} \quad \text{and hence } \hat{h}_{\mathcal{E}'}(\phi_1(P)) - \hat{h}_{\mathcal{E}'}(\phi_2(P)) = (n^2 - m^2)\hat{h}_{\mathcal{E}'}(Q_7). \tag{7}$$

- If $m = n$, then the point $\phi_1(P) - \phi_2(P)$ is a torsion point. Similarly, if $m = -n$, then the point $\phi_1(P) + \phi_2(P)$ is a torsion point. Since we know that $\mathcal{E}'_7(\mathbb{Q})_{\text{tors}} = \mathcal{E}'_7(\mathbb{Q})[2]$, we find (using `magma` [37, 3]) that the only torsion point that can be written in such a way is ∞. We obtain the two points $\phi_1(P) = \phi_2(P)$ (which comes from $(\pm 1 : -7 : 7)$) and $\phi_1(P) = -\phi_2(P)$ (which comes from the points $(\pm 1 : 7 : 7)$).
- If $m^2 \neq n^2$, we obtain an upper bound on the difference between these squares, and thus on the maximum of $|n|$ and $|m|$, as we show in Lemma 4.9.

It remains to find the points $P \in \mathcal{C}_{f(7)}(\mathbb{Q})$ such that either $\phi_1(P) = [n]Q_7 + T$ or $\phi_2(P) = [n]Q_7 + T$ with $T \in \mathcal{E}'_7(\mathbb{Q})_{\text{tors}}$ and $n \in \mathbb{Z}$ such that $|n| \leqslant 16$.

For $|n| \leqslant 16$, we compute, using `magma` [37, 3], the preimage of $[\pm n]Q_7 + T$, where T is a torsion point. We find that the only points arising from a rational point are $2Q_7 + B_7$, $-2Q_7 + B_7$ and B_7 (corresponding, respectively, to the points $\{(-1 : 7 : 7), (-1 : -7 : 7), (7 : -7 : 1), (7 : 7 : 1)\}$, $\{(-7 : 7 : 1), (1 : -7 : 7), (1 : 7 : 7), (-7 : -7 : 1)\}$ and $\{(7 : -1 : 7), (-7 : -1 : 7), (-7 : 1 : 7), (7 : 1 : 7)\}$ on the curve $\mathcal{C}$). □

LEMMA 4.9. *If $m^2 \neq n^2$, one has* $\max(|n|, |m|) \leqslant 16$.

Proof. It follows from equation (7) and Lemma 4.8 that $|n^2 - m^2|\hat{h}_{\mathcal{E}'}(Q_7) \leqslant 40.37$. Since the point Q_7 has height 1.29, we find that $|n^2 - m^2| \leqslant 31.30$, and thus

$$\max(|n|, |m|) \leqslant \tfrac{1}{2}(31.30 + 1) < 17.$$ □

REMARK 8. Using sharper bounds of Cremona, Prickett and Siksek [10], we compute that the difference between the canonical and naïve heights of a point on the elliptic curve $\mathcal{E}'_7$ is bounded in absolute value by 9.66. The bound in Lemma 4.8 becomes 30.73, and then $\max(|n|, |m|) \leqslant 12$.

4.2.2. *Generic case*

Let $P = (X : Y : Z) \in \mathcal{C}_{f(t)}(\mathbb{Q}(t))$ with $X, Y, Z \in \mathbb{Z}[t]$, and $\gcd(X, Y, Z) = 1$. We define its height to be $h_{\mathcal{C}}(P) = \max(\deg(X), \deg(Y), \deg(Z))$. Looking at the equation of $\mathcal{C}_{f(t)}$ and comparing the degrees of X, Y and Z, we see that the three quantities $\max(\deg X, \deg Z)$, $\max(\deg X, \deg Y)$ and $\max(\deg Z, \deg Y)$ are equal. We define the height $h_{\mathcal{C}}(P)$ to be the most convenient of these three equivalent values. Finally, we recall that for any point $Q \in \mathcal{E}'_t(\mathbb{Q}(t))$, we have $h_{\mathcal{E}'}(Q) = h(x(Q))$, where $x(Q)$ is the x-coordinate of the point Q.

We obtain the following result.

THEOREM 4.10. *Let $\mathcal{C}_{f(t)}$ be the curve given by the projective equation*

$$X^4 + Y^4 + Z^4 + f(t)(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0,$$

where $f(t) = -(2t^4 + 1)/t^2(t^2 + 2)$. The set of rational points of this curve is

$$\mathcal{C}_{f(t)}(\mathbb{Q}(t)) = \{(\pm t, t, 1), (\pm t, -t, 1), (\pm t, 1, t), (\pm t, 1, -t), (1, \pm t, t), (1, \pm t, -t)\}.$$

We showed in Section 4.1 that the elliptic curve $\mathcal{E}'_t$ has rank 1 over $\mathbb{Q}(t)$ (see Proposition 4.2). Since the three morphisms ϕ_i have same degree, we can apply the simplified version of the Dem'janenko–Manin method (see Section 2.2). Recall that there exist three independent morphisms $\phi_i = \tau \circ \rho \circ \psi_i$ from $\mathcal{C}_{f(t)}$ to $\mathcal{E}'_t$.

Define $(x_1, y_1) = \phi_1(X : Y : Z)$ and $(x_2, y_2) = \phi_2(X : Y : Z)$; using (5) and (6) we obtain the following equations (we give just the x-coordinates, since the other coordinates do not appear in what follows):

$$\begin{cases} x_1 = \dfrac{((X^4 + Z^4)(4t^2 - 1)(2t^4 + 1) + X^2Z^2(4t^8 - 44t^4 - 24t^2 - 2))}{3((X^4 + Z^4)(1 - 4t^2) + X^2Z^2(2 + 4t^4))} = \dfrac{U(X, Z)}{V(X, Z)}; \\ x_2 = \dfrac{U(X, Y)}{V(X, Y)} = \dfrac{u_1(X^4 + Y^4) + u_2X^2Y^2}{v_1(X^4 + Y^4) + v_2X^2Y^2}. \end{cases}$$

We can bound the difference between the height of the image of a point and four times its naïve height on the curve.

LEMMA 4.11. *For $i = 1, 2$, and $P \in \mathcal{C}(\mathbb{Q}(t))$, we have*

$$4h_{\mathcal{C}}(P) + 4 \leqslant h_{\mathcal{E}'}(\phi_i(P)) \leqslant 4h_{\mathcal{C}}(P) + 8.$$

Proof. Without loss of generality, we can assume that $i = 1$. Let U, V, u_1, u_2, v_2 and v_2 be as above. The height of $\phi_1(P)$ is equal to $h(x_1) = \max(\deg U, \deg V)$.

For the upper bound, we have

$$\begin{aligned} h_{\mathcal{E}'}(\phi_1(P)) &\leqslant 4\max(\deg X, \deg Z) + \max(\deg(v_1), \deg(v_2), \deg(u_1), \deg(u_2)) \\ &\leqslant 4h_{\mathcal{C}}(P) + 8. \end{aligned}$$

For the lower bound, we have

$$\begin{cases} (v_1X^2 + v_2Z^2)U(X, Z) - (u_1X^2 + u_2Z^2)V(X, Z) = WZ^6, \\ (v_1Z^2 + v_2X^2)U(X, Z) - (u_1Z^2 + u_2X^2)V(X, Z) = WX^6, \end{cases}$$

where $W = -36t^2(4t^2 - 1)(t^2 + 2)^2(t^2 - 1)^2$. This implies that

$$\begin{aligned} &6h_{\mathcal{C}}(P) + \deg W \\ &\quad\leqslant \max(\deg U, \deg V) + 2h_{\mathcal{C}}(P) + \max(\deg(u_1), \deg(u_2), \deg(v_1), \deg(v_2)), \end{aligned}$$

and hence

$$4h_{\mathcal{C}}(P) + 12 \leqslant \max(\deg U, \deg V) + 8. \qquad \square$$

Moreover, we know from Proposition 1.2 that the following assertion holds.

LEMMA 4.12. *The difference between the canonical and naïve heights of a point Q on the elliptic curve $\mathcal{E}'_t$ is bounded as follows: $|\hat{h}_{\mathcal{E}'}(Q) - h_{\mathcal{E}'}(Q)| \leqslant 48$.*

Hence the next lemma follows.

LEMMA 4.13. *The difference between the canonical heights of the images of a $\mathbb{Q}(t)$-rational point P of $\mathcal{C}$ satisfies*

$$|\hat{h}_{\mathcal{E}'}(\phi_1(P)) - \hat{h}_{\mathcal{E}'}(\phi_2(P))| \leqslant 100 = k_1. \tag{8}$$

Proof. The difference between the naïve heights of the images of a $\mathbb{Q}(t)$-rational point of $\mathcal{C}$ satisfies

$$|h_{\mathcal{E}'}(\phi_1(P)) - h_{\mathcal{E}'}(\phi_2(P))| \leqslant 4.$$ □

We can now prove Theorem 4.10.

Proof of Theorem 4.10. We use the results that we obtained in the special case, and the fact that the specialisation is injective on the torsion part.

Let $P \in \mathcal{C}_{f(t)}(\mathbb{Q}(t))$. Since Q_t generates $\mathcal{E}'_t(\mathbb{Q}(t))$, there exist two integers n and m, and two points $T_1, T_2 \in \mathcal{E}'(\mathbb{Q}(t))_{\text{tors}}$ such that

$$\begin{cases} \phi_1(P) = [n]Q_t + T_1, \\ \phi_2(P) = [m]Q_t + T_2, \end{cases} \quad \text{and thus } \hat{h}_{\mathcal{E}'}(\phi_1(P)) - \hat{h}_{\mathcal{E}'}(\phi_2(P)) = (n^2 - m^2)\hat{h}_{\mathcal{E}'}(Q_7). \tag{9}$$

Two cases arise, depending on the respective values of n and m.

- If $m = \pm n$, then the point $\phi_1(P) \pm \phi_2(P)$ is an element of $\mathcal{E}'_t(\mathbb{Q}(t))_{\text{tors}}$, say T. The specialisation is injective on the torsion part, and thus a point of the form $\phi_1(P)+\phi_2(P) = T$ will specialise to $\phi_1(P) + \phi_2(P) = T_0$, where T_0 is the specialisation of T. We saw in the proof of Theorem 4.5 that T_0 is necessarily ∞. The only points of $\mathcal{C}(\mathbb{Q}(t))$ such that $\phi_1(P) = \pm\phi_2(P)$ are $(\pm 1 : t : t)$ (for which $\phi_1(P) = -\phi_2(P)$) and $(\pm 1 : -t : t)$ (for which $\phi_1(P) = \phi_2(P)$).
- If $m \neq \pm n$, then according to Lemma 4.14 we can bound the maximum of $|n|$ and $|m|$ above by a constant k_3. The image by ϕ_1 of a $\mathbb{Q}(t)$-rational point P satisfies $\phi_1(P) = mQ_t + T$, where $T \in \mathcal{E}'_t(\mathbb{Q}(t))_{\text{tors}}$ and $|m| \leqslant k_3$. This point specialises to $\phi_1(P) = mQ_7 + T_0$ with $T_0 \in \mathcal{E}'_7(\mathbb{Q})_{\text{tors}}$, the specialisation of T and $|m| \leqslant k_3$. On the other hand, we know that the rational points of the elliptic curve $\mathcal{E}'_7$ arising from rational points on $\mathcal{C}_{f(7)}$ satisfy $\phi_1(P) - mQ_7 \in \mathcal{E}'_7(\mathbb{Q})_{\text{tors}}$ with $|m| \leqslant 16$, according to Lemma 4.9. We saw in the preceding section that these points are $2Q_7 + B_7$, $-2Q_7 + B_7$ and B_7, and thus the only points of $\mathcal{E}'_t(\mathbb{Q}(t))$ coming from the $\mathbb{Q}(t)$-rational point on $\mathcal{C}_{f(t)}$ are $2Q_t + B_t$, $-2Q_t + B_t$ and B_t. The computation of their preimages gives the set $\{(1 : \pm t : t), (-1 : \pm t : t), (t : \pm 1 : t), (-t : \pm 1 : t), (t : t : \pm 1), (-t : t : \pm 1)\}$. □

LEMMA 4.14. *If $n^2 \neq m^2$, we have* $\max(|n|, |m|) \leqslant 68 = k_3$.

Proof. The equations (4) and (8) and the following lemma yield

$$|n^2 - m^2| \leqslant \frac{k_1}{\hat{h}(Q_t)} \leqslant \frac{400}{3} = k_2.$$

It follows that

$$n^2 \neq m^2 \Longrightarrow \max(|n|, |m|) \leqslant \tfrac{1}{2}(k_2 + 1) \leqslant 68 = k_3.$$ □

LEMMA 4.15. *The canonical height of the point Q_t is $\hat{h}_{\mathcal{E}'}(Q_t) = 3/4$.*

Proof. Recall that our definition of the naïve height is the height on $\mathbb{P}^1$, and hence twice Silverman's.

Let us sketch quickly how to compute the local height $\lambda_v(P)$ of a point P (see [35, p. 478]) when E is of the form $y^2 = x^3 + Ax + B$.

- *Non-singular reduction*: $P \in E^0(K)$ if and only if $v(2y(P)) \leqslant 0$ or $v(3x^2 + A) \leqslant 0$, in which case $\lambda_v(P) = \max\{0, v(x(P)^{-1})\} + v(\Delta)/6$.
- *Singular reduction*: if $P \notin E^0(K)$, two cases arise:
    - *Multiplicative reduction*: if $v(\Delta) > 0$ and $v(c_4) = 0$,
    $$\lambda_v(P) = B_2\left(\min\left\{\frac{v(2y(P))}{v(\Delta)}, \frac{1}{2}\right\}\right) v(\Delta) \qquad \text{where } B_2(X) = X^2 - X + \frac{1}{6};$$
    - *Additive reduction*: if $v(\Delta) > 0$ and $v(c_4) > 0$,
    $$\lambda_v(P) = \begin{cases} -\frac{2}{3}v(2y) + \frac{v(\Delta)}{6} & \text{if } v(3x^4 + 6Ax^2 + 12Bx - A^2) \geqslant 3v(2y), \\ -\frac{1}{4}v(3x^4 + 6Ax^2 + 12Bx - A^2) + \frac{v(\Delta)}{6} & \text{otherwise.} \end{cases}$$

The discriminant of the elliptic curve is
$$\Delta = t^4(2t+1)^2(2t-1)^2(t^2+2)^2(t-1)^4(t+1)^4,$$
and the point Q_t has coordinates $((t^4 - 6t^3 + 9t^2 - 12t + 5)/3, -(2t-1)(t^2+2)(t-1)^2)$; thus $3x(Q_t)^2 + \alpha(t) = 2(t-1)^2(2t-1)(t^2-2t+2)(t^2+2)$.

We compute the local heights as shown in Table 1. Thus $\hat{h}_{\mathcal{E}'}(Q_t) = 3/4$. □

Table 1: Local heights of Q_t.

v	reduction	$\lambda_v(Q_t)$
t	non-singular	$2/3$
$2t+1$	non-singular	$1/3$
$2t-1$	multiplicative	$1/6$
t^2+2	multiplicative	$-1/6$
$t-1$	multiplicative	$-1/3$
$t+1$	non-singular	$2/3$
'$1/t$'	multiplicative	$-1/12$

5. *The case $g(t)$*

Let $a = g(t) = -(t^4 - t^2 + 1)/t^2$. The elliptic curve $\mathcal{E}_{g(t)}$ is isomorphic to the curve $\mathcal{E}_t^*$:
$$y^2 = x^3 + a_4(t)x + a_6(t)$$
where
$$a_4(t) = -(t^8 - 5t^6 + 9t^4 - 5t^2 + 1)(t^2 + t + 1)^2(t^2 - t + 1)^2/3$$

and

$$a_6(t) = -(t^4 - t^2 + 1)(t^4 - 4t^2 + 1)(t^2 - 2)(2t^2 - 1)(t^2+t+1)^3(t^2-t+1)^3/27$$

via the change of coordinates

$$\tau = (x, y) \longmapsto (t^4 x, t^6 y). \tag{10}$$

The three points of order 2 of $\mathcal{E}_t^*$ are $A_t = (\alpha_1, 0)$, $B_t = (\alpha_2, 0)$ and $C_t = (\alpha_3, 0)$, where

$$\alpha_1 = -\frac{(t^2+t+1)(t^2-t+1)(t^4-4t^2+1)}{3};$$
$$\alpha_2 = \frac{(t^2-2)(2t^2-1)(t^2+t+1)(t^2-t+1)}{3};$$
$$\alpha_3 = -\frac{(t^2+t+1)(t^2-t+1)(t^4-t^2+1)}{3}.$$

We have the three independent morphisms $\phi_i = \tau \circ \rho \circ \psi_i$ from $\mathcal{C}_{g(t)}$ to $\mathcal{E}_t^*$. The images of the point $(t^2 : t : 1)$ by the morphisms ϕ_1 and ϕ_2 are the points P_t and Q_t, of coordinates, respectively,

$$\left(\frac{-(t^{12}-2t^{10}+2t^8-14t^6+2t^4-2t^2+1)}{3(t-1)^2(t+1)^2}, \frac{2(t^2-t-1)(t^2+t-1)(t^4+1)(1+t^2)t^4}{(t-1)^3(t+1)^3}\right)$$

and

$$\left(\frac{-(t^4+3t^2-1)(t^4-3t^2-1)}{3}, -2(1+t^2)(t^2-t-1)(t^2+t-1)t^3\right).$$

In Section 5.1, we shall see that P_t and Q_t are points of infinite order in $\mathcal{E}_t^*(\mathbb{Q}(t))$. More precisely, we show that if R_t is a point such that $2R_t = P_t + Q_t$, then the two points R_t and P_t generate the free part of $\mathcal{E}_t^*(\mathbb{Q}(t))$. We know that the set of rational points $\mathcal{C}_{g(t)}(\mathbb{Q}(t))$ contains $(t^2 : t : 1)$ and the twenty-three other points in its orbit under the automorphism group. Likewise, the set of rational points $\mathcal{C}_{g(2)}(\mathbb{Q})$ contains $(4 : 2 : 1)$ and the twenty-three other points in its orbit under the automorphism group. We will show in Sections 5.2.1 and 5.2.2, respectively, that there is no other point in $\mathcal{C}_{g(t)}(\mathbb{Q}(t))$ or $\mathcal{C}_{g(2)}(\mathbb{Q})$).

5.1. *The generic rank is* 2

We carry out a descent on the elliptic curve $\mathcal{E}_t^*$. For details and a proof of Proposition 5.1, see Appendix A.

The point $P_t + Q_t$ is equal to $2R_t$ where R_t is the point

$$\left((t^2+t+1)(2t^6-2t^5-4t^3+3t^2+t-1)/3, -(t^2-t-1)(t^2+t+1)^2(t-1)^2t^3\right).$$

Proposition 5.1. *The elliptic curve $\mathcal{E}_t^*$ has rank* 2 *over $\mathbb{Q}(t)$. Moreover, the points P_t and R_t generate $\mathcal{E}_t^*(\mathbb{Q}(t))$.*

Lemma 5.2. *The elliptic curve $\mathcal{E}_2^*$ has rank* 2 *over $\mathbb{Q}$, and the two points P_2 and R_2 generate the free part of $\mathcal{E}_2^*(\mathbb{Q})$.*

Proof. Indeed, the elliptic curve $\mathcal{E}_2^*$ has the Weierstrass equation

$$y^2 = x^3 - 8967x - 62\,426.$$

Using the `mwrank` program [9], we find that it has rank 2 over $\mathbb{Q}$, and that a set of generators of the free part of $\mathcal{E}_2^*(\mathbb{Q})$ is $G_1 = (-1519/25, -63\,504/125)$ and $G_2 = (245, 3528)$. Since $G_2 = R_2 - P_2 + A_2$ and $G_1 = P_2 - 2R_2 + B_2$, the result follows. □

COROLLARY 5.3. *The set $\mathcal{C}_{g(t)}(\mathbb{Q}(t))$ can be effectively determined, as we shall see in the next section.*

5.2. *Effective computations*

We determine the group of rational points in the generic case, as well as for a specialisation for which the rank is 2. Contrary to the preceding case, we cannot simplify the method and use the general method described in Section 2.1.

5.2.1. *Special case*

Let us consider the curve $\mathcal{C}_{g(2)} = \mathcal{C}_{-13/4}$. The associated elliptic curve $\mathcal{E}_2^*$ has rank 2, as we saw in Lemma 5.2. We show that the following theorem holds.

THEOREM 5.4. *Let $\mathcal{C}_{g(2)} = \mathcal{C}_{-13/4}$ be the curve given by the projective equation*

$$4(X^4 + Y^4 + Z^4) - 13(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0.$$

The set of rational points of this curve is

$$\begin{aligned}\mathcal{C}_{-13/4}(\mathbb{Q}) = \{&(2 : \pm 4 : 1), (4 : \pm 2 : 1), (2 : \pm 1 : 4), (4 : \pm 1 : 2),\\ &(1 : \pm 2 : 4), (1 : \pm 4 : 2), (-2 : \pm 4 : 1), (-4 : \pm 2 : 1),\\ &(-2 : \pm 1 : 4), (-4 : \pm 1 : 2), (-1 : \pm 2 : 4), (-1 : \pm 4 : 2)\}.\end{aligned}$$

Recall that there exist three independent morphisms $\phi_i = \tau \circ \rho \circ \psi_i$ from $\mathcal{C}$ to $\mathcal{E}_2^*$. Define $P_i = (x_i, y_i) = \phi_i(X : Y : Z)$. It follows from (5) and (10) that:

$$\begin{cases} x_1 = -\dfrac{455X^4 - 658X^2Z^2 + 455Z^4}{5X^4 + 26X^2Z^2 + 5Z^4} = \dfrac{U(X,Z)}{V(X,Z)};\\[2mm] y_1 = -\dfrac{158\,760(X^4 - Z^4)XZ}{(8Y^2 - 13X^2 - 13Z^2)(5X^4 + 26X^2Z^2 + 5Z^4)} = \dfrac{W(X,Z)}{V(X,Z)T(X,Y,Z)};\\[2mm] x_2 = \dfrac{U(Y,X)}{V(Y,X)};\\[2mm] y_2 = \dfrac{W(Y,X)}{V(Y,X)T(Y,Z,X)};\\[2mm] x_3 = \dfrac{U(Z,Y)}{V(Z,Y)};\\[2mm] y_3 = \dfrac{W(Z,Y)}{V(Z,Y)T(Z,X,Y)}. \end{cases}$$

We need to obtain bounds on the naïve heights of the P_i as well as those of the $P_i + P_j$. Since X, Y and Z play similar roles, we just need to compute such bounds for the naïve heights of P_1 and of $P_1 + P_2$.

NOTATION. Let $f = \sum_{i+j\leqslant d} a_{i,j} X^i Y^j Z^{d-i-j}$ be a homogeneous polynomial of degree d. We will denote by $\|f\|$ the quantity $\sum_{i+j\leqslant d} |a_{i,j}|$.

LEMMA 5.5. *For $i = 1, 2, 3$, and $P \in \mathcal{C}(\mathbb{Q})$, we have*

$$4h_{\mathcal{C}}(P) - 0.30 \leqslant h_{\mathcal{E}^*}(\phi_i(P)) \leqslant 4h_{\mathcal{C}}(P) + 7.36.$$

Proof. We show this result for $i = 1$.

The height of the point $\phi_1(P)$ is equal to $h(x_1) = \log\max(|U_1|, |V_1|)$.

For the upper bound, we have

$$H(\phi_1(P)) = H(x_1) \leqslant \max(2 \cdot 455 + 658,\ 2 \cdot 5 + 26)H(P)^4,$$

and hence in logarithmic heights

$$h_{\mathcal{E}^*}(\phi_1(P)) \leqslant 4h_{\mathcal{C}}(P) + \log(1568) \leqslant 4h_{\mathcal{C}}(P) + 7.36.$$

For the lower bound, we have

$$\begin{cases} (5X^2 + 26Z^2)U(X, Z) + (455X^2 - 658Z^2)V(X, Z) = 15\,120Z^6, \\ (5Z^2 + 26X^2)U(X, Z) + (455Z^2 - 658X^2)V(X, Z) = 15\,120X^6. \end{cases}$$

We deduce that

$$15120 \cdot (\max(|X|, |Z|))^6 \leqslant (455 + 658 + 5 + 26)H(P)^2H(\phi_1(P)).$$

Furthermore, we have

$$(3\,615\,612Y^2 + 554\,827(X^2 + Z^2))V(X, Z) + (26\,364Y^2 - 28\,561(X^2 + Z^2))U(X, Z) = 3\,144\,960Y^6$$

and hence

$$\begin{aligned} 3\,144\,960|Y|^6 &\leqslant (3\,615\,612 + 554\,827 + 26\,364 + 28\,561)H(P)^2H(\phi_1(P)) \\ &\leqslant 4\,225\,364H(P)^2H(\phi_1(P)). \end{aligned}$$

Since $4\,225\,364/3\,144\,960$ is larger than $1\,144/15\,120$, we obtain, in logarithmic heights,

$$4h_{\mathcal{C}}(P) - 0.30 \leqslant 4h_{\mathcal{C}}(P) + \log(3\,144\,960/4\,225\,364) \leqslant h_{\mathcal{E}^*}(\phi_1(P)). \qquad \square$$

LEMMA 5.6. *For $i \neq j$ and $P \in \mathcal{C}(\mathbb{Q})$, we have*

$$8h_{\mathcal{C}}(P) - 10.99 \leqslant h_{\mathcal{E}^*}(\phi_i(P) + \phi_j(P)) \leqslant 8h_{\mathcal{C}}(P) + 18.68.$$

Proof. Once again, without loss of generality we can assume that $i = 1$ and $j = 2$. We just need to compute the x-coordinate of the point $\phi_1(P) + \phi_2(P)$, given our definition of the naïve height on $\mathcal{E}_2^*$.

The x-coordinate of $(\phi_1 + \phi_2)(P)$ is $N(X, Y, Z)/D(X, Y, Z)$, where

$$\begin{aligned} N(X, Y, Z) = {} & 4\,803\,435X^2(Y^6 + Z^6) + 5\,669\,664X^2YZ(Y^4 + Z^4) \\ & + 26\,935\,545X^2Y^2Z^2(Y^2 + Z^2) + 20\,180\,160X^2Y^3Z^3 \\ & - 1\,632\,540(Y^8 + Z^8) - 2\,131\,584YZ(Y^6 + Z^6) - 259\,917Y^2Z^2(Y^4 + Z^4) \\ & + 22\,176Y^3Z^3(Y^2 + Z^2) + 25\,762\,170Y^4Z^4 \end{aligned}$$

and

$$\begin{aligned} D(X, Y, Z) = {} & 36\,720X^2(Y^6 + Z^6) - 20\,832X^2YZ(Y^4 + Z^4) + 53\,520X^2Y^2Z^2(Y^2 + Z^2) \\ & - 138\,816X^2Y^3Z^3 - 12\,480(Y^8 + Z^8) + 4\,992YZ(Y^6 + Z^6) \\ & + 55\,536Y^2Z^2(Y^4 + Z^4) - 11\,232Y^3Z^3(Y^2 + Z^2) - 73\,632Y^4Z^4. \end{aligned}$$

For the upper bound, we have

$$\begin{aligned} H(\phi_1(P)+\phi_2(P)) &= \max(|N(X,Y,Z)|, |D(X,Y,Z|) \\ &\leqslant \max(\|N\|, \|D\|) \max(|X|,|Y|,|Z|)^8 \\ &\leqslant \max(128\,852\,052, 603\,072)\, H(P)^8 \\ &\leqslant 128\,852\,052\, H(P)^8. \end{aligned}$$

Hence in logarithmic heights,

$$h_{\mathcal{E}^*}(\phi_1(P)+\phi_2(P)) \leqslant 8\, h_{\mathcal{C}}(P) + 18.68.$$

For the lower bound, we need to apply the Nullstellensatz. We have the following relations:

$$\begin{cases} p(X,Y,Z)N(X,Y,Z) - q(X,Y,Z)D(X,Y,Z) = 42\,201\,460\,546\,560\,000\,000 Z^{18}, \\ p(X,Z,Y)N(X,Y,Z) - q(X,Y,Z)D(X,Z,Y) = 42\,201\,460\,546\,560\,000\,000 Y^{18}, \end{cases} \tag{11}$$

where p and q are the homogeneous polynomials of degree 10 in X, Y and Z appearing in Appendix B. From these relations, we deduce that

$$\begin{aligned} &4\,689\,051\,171\,840\,000\,000\, |Z|^{18} \\ &\quad\leqslant \left|p(X,Y,Z)N(X,Y,Z) - q(X,Y,Z)D(X,Y,Z)\right| \\ &\quad\leqslant \left|p(X,Y,Z)N(X,Y,Z)\right| + \left|q(X,Y,Z)D(X,Y,Z)\right| \\ &\quad\leqslant (\|p\| + \|q\|) \max(|X|,|Y|,|Z|)^{10} \max(|N(X,Y,Z)|, |D(X,Y,Z)|) \\ &\quad\leqslant 276\,933\,645\,164\,286\,638\,003\,166\, H(P)^{10} H(\phi_1(P)+\phi_2(P)). \end{aligned} \tag{12}$$

We have a similar relation with Y and Z playing reverse roles.

Moreover,

$$r(X,Y,Z)N(X,Y,Z) + s(X,Y,Z)D(X,Y,Z) = 290\,118\,638\,109\,081\,600 X^{18}, \tag{13}$$

where r and s are the homogeneous polynomials of degree 10 in X, Y and Z appearing in Appendix B. Thus

$$\begin{aligned} &290\,118\,638\,109\,081\,600\, |X|^{16} \\ &\quad\leqslant |r(X,Y,Z)| + |s(X,Y,Z)| \max(|N(X,Y,Z)|, |D(X,Y,Z)|) \\ &\quad\leqslant \|r\| + \|s\| \max(|X|,|Y|,|Z|)^{10} \max(|N(X,Y,Z)|, |D(X,Y,Z)|) \\ &\quad\leqslant 78\,178\,083\,802\,519\,280\, H(P)^8\, H(\phi_1(P)+\phi_2(P)). \end{aligned} \tag{14}$$

Because the number $78\,178\,083\,802\,519\,280/290\,118\,638\,109\,081\,600$ is smaller than $276\,933\,645\,164\,286\,638\,003\,166/4\,689\,051\,171\,840\,000\,000$, we obtain from the two inequalities (12) and (14) that

$$\begin{aligned} &4\,689\,051\,171\,840\,000\,000\, \max(|X|,|Y|,|Z|)^{18} \\ &\quad\leqslant 276\,933\,645\,164\,286\,638\,003\,166 \max(|X|,|Y|,|Z|)^{10}\, H(\phi_1(P)+\phi_2(P)); \end{aligned}$$

hence in logarithmic heights

$$8\, h_{\mathcal{C}}(P) - 10.99 \leqslant h_{\mathcal{E}^*}(\phi_1(P)+\phi_2(P)).$$ □

From Proposition 1.2, we know that the next lemma holds.

LEMMA 5.7. *The difference between the canonical and naïve heights of a point Q on the elliptic curve is bounded as follows:* $|\hat{h}_{\mathcal{E}^*}(Q) - h_{\mathcal{E}^*}(Q)| \leqslant 9.692$.

Hence the following statement holds as well.

LEMMA 5.8. *For $P \in \mathcal{C}(\mathbb{Q})$ and $j \neq i$, we have the following inequalities:*

$$|\hat{h}_{\mathcal{E}^*}(\phi_i(P) + \phi_j(P)) - (\hat{h}_{\mathcal{E}^*}(\phi_i(P)) + \hat{h}_{\mathcal{E}^*}(\phi_j(P)))| \leqslant 3 \cdot 9.7 + 25.71 \leqslant 55 = 2r_{i,j}$$

and

$$|\hat{h}_{\mathcal{E}^*}(\phi_i(P)) - 4h_{\mathcal{C}}(P)| \leqslant 7.66 + 9.7 \leqslant 17.36 = r_{i,i}. \tag{15}$$

Proof. Indeed, we can bound the difference between the naïve heights of the various points on the elliptic curve

$$\left|h_{\mathcal{E}^*}(\phi_i(P)) - h_{\mathcal{E}^*}(\phi_j(P))\right| \leqslant 7.66$$

and

$$\left|h_{\mathcal{E}^*}(\phi_i(P) + \phi_j(P)) - (h_{\mathcal{E}^*}(\phi_i(P)) + h_{\mathcal{E}^*}(\phi_j(P)))\right| \leqslant 25.71.$$

These inequalities, combined with Lemma 5.7, give the result. □

We are now in a position to prove Theorem 5.4.

Proof of Theorem 5.4. Form, as in Section 2.1, the matrices H, D and R whose (i, j)-entries are, respectively, $\frac{1}{2}(\hat{h}_{\mathcal{E}^*}(\phi_i(P) + \phi_j(P)) - (\hat{h}_{\mathcal{E}^*}(\phi_i(P)) + \hat{h}_{\mathcal{E}^*}(\phi_j(P))))$, $\frac{1}{4}(d(\phi_i + \phi_j) - d(\phi_i) - d(\phi_j))$ and $r_{i,j}$.

The matrix R is equal to

$$\begin{pmatrix} 17.36 & 27.5 & 27.5 \\ 27.5 & 17.36 & 27.5 \\ 27.5 & 27.5 & 17.36 \end{pmatrix}$$

and D is equal to

$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Equip $\mathcal{M}_3(\mathbb{R})$ with the following norm of algebra $\|.\|$:

$$\|(a_{i,j})_{1 \leqslant i,j \leqslant l}\| = \max_{1 \leqslant i \leqslant l} \sum_{1 \leqslant j \leqslant l} (|a_{i,j}|).$$

We have $\|M\| = (2 \cdot 27.5 + 17.36)$ and $\|D^{-1}\| = 0.25$, whence $h_{\mathcal{C}}(P) \leqslant 18.09$, and thus $\max(|X|, |Y|, |Z|) \leqslant 71\,843\,449$.

From Relation (15), the canonical height of the image of a $\mathbb{Q}$-rational point of $\mathcal{C}$ by ϕ_1 satisfies

$$\hat{h}_{\mathcal{E}^*}(\phi_1(P) \leqslant 89.72. \tag{16}$$

Define $G_2 = R_2 - P_2 + A_2$ and $G_1 = P_2 - 2R_2 + B_2$. A point on the elliptic curve $\mathcal{E}_2^*$ can be written as $Q = nG_1 + mG_2 + T$, where T is a torsion point and m and n are integers. Since we have

$$\hat{h}(Q) = n^2\hat{h}(G_1) + 2mn\langle G_1, G_2\rangle + m^2\hat{h}(G_2),$$

$\hat{h}_{\mathcal{E}^*}(G_1) = 3.13$ and $\hat{h}_{\mathcal{E}^*}(G_2) = 1.93$, we can determine the set of values of m and n for which a point of the form $Q = nG_1 + mG_2 + T$ has canonical height at most 89.72. For such values, we compute the preimages of these points by ϕ_1, and we find that the only points coming from rational points on $\mathcal{C}$ are $G_1 + B_2 = Q_2$ and $G_1 + 2G_2 + B_2 = P_2$ and their opposites, which come, respectively, from

$$\begin{aligned}
&\{(-2:-4:1), (4:1:2), (1:-4:2), (4:-1:2),\\
&\ (-2:4:1), (-2:1:4), (1:4:2), (-2:-1:4)\},\\
&\{(-4:2:1), (1:-2:4), (1:2:4), (-4:-2:1)\},\\
&\{(-4:1:2), (-1:-4:2), (2:4:1), (-1:4:2),\\
&\ (2:-1:4), (2:-4:1), (-4:-1:2), (2:1:4)\},
\end{aligned}$$

and

$$\{(-1:2:4), (-1:-2:4), (4:2:1), (4:-2:1)\}. \qquad \square$$

REMARK 9. Using sharper bounds of Cremona, Prickett and Siksek [10], we compute that the difference between the canonical and naïve heights of a point on the elliptic curve $\mathcal{E}_2^*$ is bounded in absolute value by 6.07. The bounds $r_{i,j}$ and $r_{i,i}$ in Lemma 5.8 become 22 and 13.73 respectively. The height $h_{\mathcal{C}}(P)$ is then bounded above by 14.42 and in Equation (16) becomes $\hat{h}_{\mathcal{E}^*}(\phi_1(P) \leqslant 65.31$.

5.2.2. *Generic case*

We determine the set of $\mathbb{Q}(t)$-rational points of $\mathcal{C}_{g(t)}$.

THEOREM 5.9. *Let $\mathcal{C}_{g(t)}$ be the curve given by the projective equation*

$$(X^4 + Y^4 + Z^4 + g(t)(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0,$$

where $g(t) = -(t^4 - t^2 + 1)/t^2$.

The set of rational points of this curve is

$$\begin{aligned}
\mathcal{C}_{g(t)}(\mathbb{Q}(t)) = \{&(t:\pm t^2:1), (t^2:\pm t:1), (t:\pm 1:t^2), (t^2:\pm 1:t),\\
&(1:\pm t:t^2), (1:\pm t^2:t), (-t:\pm t^2:1), (-t^2:\pm t:1),\\
&(-t:\pm 1:t^2), (-t^2:\pm 1:t), (-1:\pm t:t^2), (-1:\pm t^2:t)\}.
\end{aligned}$$

As before, we first obtain bounds on the various intervening heights.

LEMMA 5.10. *For $P \in \mathcal{C}(\mathbb{Q}(t))$, and $i = 1, 2, 3$, we have*

$$4h_{\mathcal{C}}(P) + 2 \leqslant h_{\mathcal{E}^*}(\phi_i(P)) \leqslant 4h_{\mathcal{C}}(P) + 12.$$

Proof. Without loss of generality, we can assume that $i = 1$. The x-coordinate of the point $\phi_i(P)$ is

$$x_1 = \frac{U(X,Z)}{V(X,Z)} = \frac{u_1(X^4 + Z^4) + u_2X^2Z^2}{v_1(X^4 + Z^4) + v_2X^2Z^2},$$

where

$$\begin{cases}
u_1(t) = -(t^4 + t^2 + 1)(t^4 - t^2 + 1)(t^2 - t - 1)(t^2 + t - 1),\\
u_2(t) = -(t^4 + t^2 + 1)(2t^8 - 16t^6 + 30t^4 - 16t^2 + 2),\\
v_1(t) = 3(t^2 - t - 1)(t^2 + t - 1),\\
v_2(t) = 6(t^4 - t^2 + 1).
\end{cases}$$

For the upper bound, we have

$$\begin{aligned} h_{\mathcal{E}^*}(\phi_1(P)) &= h(x_1) \\ &\leqslant 4\max(\deg X, \deg Z) + \max(\deg(v_1), \deg(v_2), \deg(u_1), \deg(u_2)) \\ &\leqslant 4h_{\mathcal{C}}(P) + 12. \end{aligned}$$

For the lower bound, we have

$$\begin{cases} (v_1X^2 + v_2Z^2)U(X,Z) - (u_1X^2 + u_2Z^2)V(X,Z) = TZ^6, \\ (v_1Z^2 + v_2X^2)U(X,Z) - (u_1Z^2 + u_2X^2)V(X,Z) = TX^6, \end{cases}$$

where $T(t) = -12t^2(t^2-1)^2(t^2-t-1)(t^2-t+1)(t^2+t-1)(t^2+t+1)$, and hence

$$\begin{aligned} 6h_{\mathcal{C}}(P) + \deg T &\leqslant \max(\deg U, \deg V) + 2\max(\deg X, \deg Z) \\ &\qquad + \max(\deg(v_1), \deg(v_2), \deg(u_1), \deg(u_2)) \\ &\leqslant \max(\deg U, \deg V) + 2h_{\mathcal{C}}P) + 12. \end{aligned}$$

□

LEMMA 5.11. *For $P \in \mathcal{C}(\mathbb{Q}(t))$ and $i \neq j$, we have*

$$8h_{\mathcal{C}}(P) + 2 \leqslant h_{\mathcal{E}^*}(\phi_1(P) + \phi_2(P)) \leqslant 8h_{\mathcal{C}}(P) + 20.$$

Proof. Recall that in the generic case, the naïve height of the point $(X : Y : Z) \in \mathcal{C}(\mathbb{Q}(t))$ is defined as $\max(\deg(X), \deg(Y), \deg(Z))$, which is equal to the maximum of any two of these three degrees. Since the numerator and the denominator of the x-coordinate of the point that we are interested in is symmetric in Y and Z, we will take $\max(\deg(Y), \deg(Z))$ as our favoured definition of $h_{\mathcal{C}}(P)$.

The x-coordinate of the point $\phi_1(P) + \phi_2(P)$ is $N(X,Y,Z)/D(X,Y,Z)$, where

$$\begin{aligned} N = {} & (t^4+t^2+1) \\ & \Big(X^2(t^4-t^2+1)\Big((t^2-1)^2(t^4-3t^2+1)(3t^4-7t^2+3)(t^4+1)(Y^6+Z^6) \\ &\qquad + 8t^2\big((t^{12}+1) - 6(t^{10}+t^2) + 14(t^8+t^4) - 17t^6\big)(Y^5Z + Z^5Y) \\ &\qquad + (t^4-3t^2+1)\big(9(t^{12}+1) - 33(t^{10}+t^2) + 81(t^8+t^4) - 82t^6\big) \\ &\qquad\quad (Y^4Z^2 + Y^2Z^4) \\ &\qquad + 8t^2(2t^4-t^2+2)(t^8-5t^6+10t^4-5t^2+1)Y^3Z^3\Big) \\ & - t^2(t^4-3t^2+1)(3t^4-7t^2+3)(t^4-t^2+1)^2(Y^8+Z^8) \\ & - 8t^4(t^4-t^2+1)(t^8-5t^6+9t^4-5t^2+1)(Y^7Z+YZ^7) \\ & + \big(3(t^{20}+1) - 31(t^{18}+t^2) + 134(t^{16}+t^4) \\ &\quad - 357(t^{14}+t^6) + 641(t^{12}+t^8) - 716t^{10}\big)(Y^6Z^2+Y^2Z^6) \\ & + 8t^2\big((t^{16}+1) - 8(t^{14}+t^2) + 28(t^{12}+t^4) - 58(t^{10}+t^6) + 53t^8\big)(Y^5Z^3+Y^3Z^5) \\ & + \big(6(t^{20}+1) - 53(t^{18}+t^2) + 234(t^{16}+t^4) \\ &\quad - 615(t^{14}+t^6) + 1084(t^{12}+t^8) - 1086t^{10}\big)Y^4Z^4\Big) \end{aligned}$$

and

$$D = 4t^2\Big(X^2\big(3(t^2-1)^2(t^4-3t^2+1)(t^4+1)(Y^6+Z^6) \\ - 6(t^{12}-6t^{10}+11t^8-11t^6+11t^4-6t^2+1)(Y^5Z+YZ^5) \\ + 3(t^4-3t^2+1)(3t^8-9t^6+4t^4-9t^2+3)(Y^4Z^2+Y^2Z^4) \\ + (-12t^{12}+66t^{10}-126t^8+108t^6-126t^4+66t^2-12)Y^3Z^3\big) \\ + 3(t^4-t^2+1)\big(-t^2(t^4-3t^2+1)(Y^8+Z^8) \\ + 2t^2(t^4-4t^2+1)(Y^7Z+Z^7Y) \\ + (t^8-6t^6+15t^4-6t^2+1)(Y^6Z^2+Y^2Z^6) \\ - 2(t^2-1)^2(t^4-4t^2+1)(Y^5Z^3+Y^3Z^5) \\ + 2(t^8-7t^6+10t^4-7t^2+1)Y^4Z^4\big)\Big).$$

For the upper bound, we have

$$h_{\mathcal{E}^*}(\phi_1(P)+\phi_2(P)) = \max(\deg(N(X,Y,Z)), \deg(D(X,Y,Z))) \leqslant 8h_{\mathcal{C}}(P)+20.$$

For the lower bound, we find two polynomials p and q such that

$$\begin{cases} p(X,Y,Z)N(X,Y,Z)+q(X,Y,Z)D(X,Y,Z) = W(t)\,Z^{18}, \\ p(X,Z,Y)N(X,Y,Z)+q(X,Y,Z)D(X,Z,Y) = W(t)\,Y^{18}, \end{cases} \tag{17}$$

where $W(t) = 36t^{14}(t^2-1)^8(t^4-3t^2+1)^7(t^4+t^2+1)(3t^4-7t^2+3)(t^4+1)^2$. These polynomials are given in Appendix C. They are homogeneous of degree 10 in X, Y and Z, with coefficients in $\mathbb{Z}[t]$, the maximal degree in t of the coefficients being 72.

It follows that

$$\deg W + 18\max(\deg(Y),\deg(Z)) \leqslant 10\max(\deg(X),\deg(Y),\deg(Z) \\ + \max(\deg(N(X,Y,Z)),\deg(D(X,Y,Z))) + 72 \\ \leqslant 72 + h_{\mathcal{E}^*}(\phi_1(P)+\phi_2(P)) + 10h_{\mathcal{C}}(P). \qquad \square$$

From Proposition 1.2, we have the following lemma.

LEMMA 5.12. *Let $Q \in \mathcal{E}_t^*(\mathbb{Q}(t))$. The difference between its naïve and canonical heights is bounded above as $|\hat{h}_{\mathcal{E}^*}(Q) - h_{\mathcal{E}^*}(Q)| \leqslant 96$.*

Thus the following lemma also holds.

LEMMA 5.13. *We have, for any $P \in \mathcal{C}(\mathbb{Q}(t))$ and $i \neq j$:*

$$|\hat{h}_{\mathcal{E}^*}(\phi_i(P)) - 4h_{\mathcal{C}}(P)| \leqslant 108 = r_{i,i}$$

and

$$|\hat{h}_{\mathcal{E}^*}(\phi_i(P)+\phi_j(P)) - (\hat{h}_{\mathcal{E}^*}(\phi_i(P)) + \hat{h}_{\mathcal{E}^*}(\phi_j(P)))| \leqslant 304 = 2\,r_{i,j}.$$

Proof. This is a straightforward application of Lemmas 5.10, 5.11 and 5.12 and relation (3), since $\deg(\phi_i+\phi_j) = \deg(\phi_i)+\deg(\phi_j)$. $\square$

LEMMA 5.14. *The naïve height of $P \in \mathcal{C}(\mathbb{Q}(t))$ satisfies $h_{\mathcal{C}}(P) \leqslant 38$.*

Proof. Form the matrices H, D and R whose respective (i, j)-entries are:

$$H_{i,j} = \tfrac{1}{2}(\hat{h}_{\mathcal{E}^*}(\phi_i(P) + \phi_j(P)) - (\hat{h}_{\mathcal{E}^*}(\phi_i(P)) + \hat{h}_{\mathcal{E}^*}(\phi_j(P))));$$
$$D_{i,j} = \tfrac{1}{4}(d(\phi_i + \phi_j) - d(\phi_i) - d(\phi_j));$$
$$R_{i,j} = r_{i,j}.$$

Define, as in the proof of Theorem 4.5, the norm of algebras $\|.\|$ as follows:

$$\|(a_{i,j})_{1\leqslant i,j\leqslant l}\| = \max_{1\leqslant i\leqslant l} \sum_{1\leqslant j\leqslant l} (|a_{i,j}|).$$

The relations of Lemma 5.13 imply that

$$\|H - Dh_{\mathcal{C}}(P)\| \leqslant \|R\|.$$

Since H is not invertible, we find that

$$h_{\mathcal{C}}(P) \leqslant \|R\| \times \|D^{-1}\|,$$

whence the result holds. □

This result, combined with the second relation of Lemma 5.13, yields the next lemma.

LEMMA 5.15. *The canonical height of the image by ϕ_1 of a $\mathbb{Q}(t)$-rational point of $\mathcal{C}$ is at most* 260.

We will thus be able to determine the set of $\mathbb{Q}(t)$-rational points on $\mathcal{C}$. Indeed, we know from Proposition 5.1 that the two points P_t and R_t generate the free part of the Mordell–Weil group $\mathcal{E}_t^*(\mathbb{Q}(t))$. Let us define, as in the proof of Lemma 5.2, the two points $G_1 = P_t - 2R_t + B_t$ and $G_2 = R_t - P_t + A_t$. These two points also generate the free part of the Mordell–Weil group and, since their heights are smaller, we will favour them. A point on the curve $\mathcal{E}_t^*$ can be written as $Q = nG_1 + mG_2 + T$, where T is a torsion point. Since

$$\hat{h}_{\mathcal{E}^*}(Q) = n^2\hat{h}_{\mathcal{E}^*}(G_1) + 2mn\langle G_1, G_2\rangle + m^2\hat{h}_{\mathcal{E}^*}(G_2),$$

it follows, using the values of the heights computed in Lemma 5.16, that

$$\hat{h}_{\mathcal{E}^*}(Q) = 4n^2 + 3m^2 - 4mn \leqslant 260. \tag{18}$$

Proof of Theorem 5.9. As in the case of rank 1, we use the fact that specialising is injective on the torsion part, to show the result. We will use the specialisation at $t_0 = 2$. Let P be a $\mathbb{Q}(t)$-rational point of $\mathcal{C}_{f(t)}$. Its image by ϕ_1 is, modulo torsion, of the form $nG_1 + mG_2$, where m and n satisfy the relation (18). For such values of m and n, we check whether the corresponding point on the special curve has height less than 89.72 (which is the bound that we obtained on the special curve in the equation (16)). If so, we compute the preimages of this point. We find that images on the elliptic curve $\mathcal{E}_t^*$ of the rational points of the curve $\mathcal{C}_{f(t)}$ are the four points $G_1 + B_t = Q_t$ and $G_1 + 2G_2 + B_t = -P_t$ and their opposites (and are, respectively, $\{(-1/t : -1/t^2 : 1), (-1/t : 1/t^2 : 1), (1/t : -t : 1), (1/t : t : 1), (-t : -t^2 : 1), (-t : t^2 : 1), (t : -1/t : 1), (t : 1/t : 1)\}$, $\{(1/t^2 : -1/t : 1), (1/t^2 : 1/t : 1), (-t^2 : -t : 1), (-t^2 : t : 1)\}$, $\{(-1/t : -t : 1), (-1/t : t : 1), (1/t : -1/t^2 : 1), (1/t : 1/t^2 : 1), (-t : -1/t : 1), (-t : 1/t : 1), (t : -t^2 : 1), (t : t^2 : 1)\}$ and $\{(-1/t^2 : -1/t : 1), (-1/t^2 : 1/t : 1), (t^2 : -t : 1), (t^2 : t : 1)\}$). □

LEMMA 5.16. *The canonical heights of G_1, G_2 and G_1+G_2 are, respectively, $\hat{h}_{\mathcal{E}^*}(G_1) = 4$, $\hat{h}_{\mathcal{E}^*}(G_2) = 3$ and $\hat{h}_{\mathcal{E}^*}(G_1 + G_2) = 3$.*

Proof. The discriminant of the elliptic curve is

$$\Delta = 16(t-1)^4(t)^4(t+1)^4(t^2-t-1)^2(t^2-t+1)^6(t^2+t-1)^2(t^2+t+1)^6.$$

Since

$$y(G_1) = -2(t-1)^2t^3(t+1)^2(t^2-t+1)^2(t^2+t+1)^2(t^2+1)^{-3}$$

and

$$3x(G_1)+a_4(t) = -(t-1)^2t^2(t+1)^2(t^2-t+1)^2(t^2+t+1)^2 \\ (t^8-5t^6-5t^2+1)(t^2+1)^{-4},$$

we have

$$y(G_2) = (t-1)^2t^3(t^2-t-1)(t^2-t+1)^2(t^2+t+1)^2$$

and

$$3x(G_2)+a_4(t) = 3(t-1)^2t^2(t^2-t-1)(t^2-t+1)^2(t^2+t+1)^2 \\ (t^6-t^5+1/3t^4-2/3t^3+1/3t^2-1/3t-1/3);$$

also

$$y(G_1+G_2) = -t(t+1)^2(t^2-t-1)(t^2-t+1)^2$$

and

$$3x(G_1+G_2)+a_4(t) = -(t+1)^2(t^2-t-1)(t^2-t+1)^2 \\ (t^6+t^5-t^4+2t^3+3t^2-t+1).$$

The results follow from the local heights of G_1, G_2 and $G_3 = G_1+G_2$ in Table 2. □

Table 2: Local heights of G_1, G_2 and G_3.

v	reduction(G_1)	$\lambda_v(G_1)$	red(G_2)	$\lambda_v(G_2)$	red(G_3)	$\lambda_v(G_3)$
$(t-1)$	multiplicative	$-1/3$	mult.	$-1/3$	non-sing.	$2/3$
t	multiplicative	$-1/3$	mult.	$-1/3$	non-sing.	$2/3$
$(t+1)$	multiplicative	$-1/3$	non-sing.	$2/3$	mult.	$-1/3$
(t^2-t-1)	non-singular	$1/3$	mult.	$-1/6$	mult.	$-1/6$
(t^2-t+1)	additive	0	add.	0	add.	0
(t^2+t-1)	non-singular	$1/3$	non-sing.	$1/3$	non-sing.	$1/3$
(t^2+t+1)	additive	0	add.	0	non-sing.	1
(t^2+1)	non-singular	2	non-sing.	0	non-sing.	0
'$1/t$'	multiplicative	$-1/3$	non-sing.	$8/3$	mult.	$-1/3$

Acknowledgements. The authors are grateful to Marc Hindry for the continuing interest he took in this paper, and for all his helpful comments. The first author thanks David Kohel for useful discussions. During part of the development of this paper, she was supported by the European Research and Training Network GTEM (Universiteit Leiden and Università di Roma, Tor Vergata). Finally, the authors would like to thank the anonymous referee for suggesting using the properties of K3 surfaces.

Appendix A. *Proof of Proposition* 5.1

In this section, we prove the following proposition.

PROPOSITION 5.1. *The elliptic curve $\mathcal{E}_t^*$ has rank* 2 *over* $\mathbb{Q}(t)$. *Moreover the points P_t and R_t generate $\mathcal{E}_t^*(\mathbb{Q}(t))$.*

We carry out a descent on the elliptic curve $\mathcal{E}_t^*$. Consider the map

$$\begin{array}{rccl} (x-\alpha): & \mathcal{E}_t^*(\mathbb{Q}(t) & \longrightarrow & (\mathbb{Q}(t)^*/\mathbb{Q}(t)^{*2})^3 \\ & P & \longmapsto & (x(P)-\alpha_1, x(P)-\alpha_2, x(P)-\alpha_3) \bmod \mathbb{Q}(t)^{*2}. \end{array}$$

As usual, we first define it on $\mathcal{E}_t^*(\mathbb{Q}(t)) \setminus \mathcal{E}_t^*(\mathbb{Q}(t))[2]$, and then extend it to the whole group by defining, say, the image of A_t to be

$$(x-\alpha)(A_t) = ((\alpha_1-\alpha_2)(\alpha_1-\alpha_3), (\alpha_1-\alpha_2), (\alpha_1-\alpha_3)) \bmod \mathbb{Q}(t)^{*2}.$$

It is well known that this map has kernel $2\mathcal{E}_t^*(\mathbb{Q}(t))$. The point $P_t + Q_t$ is in the kernel: it is equal to $2R_t$ where R_t is the point

$$\big(t^2+t+1)(2t^6-2t^5-4t^3+3t^2+t-1)/3, -(t^2-t-1)(t^2+t+1)^2(t-1)^2t^3\big).$$

LEMMA A.1. *The points A_t, B_t, C_t, Q_t, P_t+R_t, A_t+P_t, B_t+P_t, C_t+P_t, A_t+R_t, B_t+R_t, C_t+R_t, $A_t+P_t+R_t$, $B_t+P_t+R_t$ and $C_t+P_t+R_t$ are not equal to twice a point in $\mathcal{E}_t^*(\mathbb{Q}(t))$.*

Proof. If one of these fifteen points were equal to twice a point, it would remain so for any specialisation. When we specialise at $t_0 = 4$, none of these fifteen points is in the kernel of $(x-\alpha)$; hence the result holds. □

Proof of Proposition 5.1. Let $(x(t), y(t))$ be a point in $\mathcal{E}_t^*(\mathbb{Q}(t))$. We can assume that

$$x(t) = \frac{p(t)}{q(t)^2},$$

where $p(t)$ and $q(t)$ are polynomials with integral coefficients.

We have the following relations:

$$\begin{cases} p(t) - \alpha_1\, q(t)^2 \equiv \mu_1(t)\mu_2(t) \bmod \mathbb{Q}(t)^{*2}, \\ p(t) - \alpha_2\, q(t)^2 \equiv \mu_1(t)\mu_3(t) \bmod \mathbb{Q}(t)^{*2}, \\ p(t) - \alpha_3\, q(t)^2 \equiv \mu_2(t)\mu_3(t) \bmod \mathbb{Q}(t)^{*2}, \end{cases}$$

where the μ_i are square-free polynomials with integral coefficients. Furthermore, we can assume that the leading coefficient of μ_1 is positive. Since $\mu_1(t)$ divides $\alpha_1-\alpha_2$, we know that $\mu_2(t)$ divides $\alpha_1-\alpha_3$ and $\mu_3(t)$ divides $\alpha_2-\alpha_3$, and since

$$\begin{cases} \alpha_1 - \alpha_2 = -(t^2+t-1)(t^2-t-1)(t^2+t+1)(t^2-t+1), \\ \alpha_2 - \alpha_3 = (t^2+t+1)(t^2-t+1)(t-1)^2(t+1)^2, \\ \alpha_1 - \alpha_3 = t^2(t^2+t+1)(t^2-t+1), \end{cases}$$

we can deduce as before the various values that the μ_i can take. Let S be the image by $(x-\alpha)$ of $(\mathcal{E}_t^*(\mathbb{Q}(t))/(2\mathcal{E}_t^*(\mathbb{Q}(t)))$; that is,

$$S = \{(\mu_1(t)\mu_2(t), \mu_1(t)\mu_3(t), \mu_2(t)\mu_3(t)) \bmod \mathbb{Q}(t)^{*2}\}.$$

Let F_t be the subgroup of $\mathcal{E}_t^*(\mathbb{Q}(t))$ generated by P_t, R_t and the points of order 2. The next two lemmas give the result. Indeed, Lemma A.3 implies that

$$F_t \longrightarrow\!\!\!\!\!\rightarrow \mathcal{E}_t^*(\mathbb{Q}(t))/(2\mathcal{E}_t^*(\mathbb{Q}(t))) \ ,$$

and thus that $(\mathcal{E}_t^*((\mathbb{Q}(t)) : F_t)$ is finite. On the other hand, since we show in Lemma 5.2 that when specialising at $t_0 = 2$, the points P_2 and R_2 generate the free part of $\mathcal{E}_2^*(\mathbb{Q})$, the same holds for P_t and R_t. □

By a direct computation, we obtain the following lemma.

LEMMA A.2. *The images of $\mathcal{O}$, A_t, B_t, C_t, P_t, R_t, $P_t + R_t$, $A_t + P_t$, $B_t + P_t$, $C_t + P_t$, $A_t + R_t$, $B_t + R_t$, $C_t + R_t$, $A_t + P_t + R_t$, $B_t + P_t + R_t$ and $C_t + P_t + R_t$ are, respectively:*

$$(1, 1, 1);$$

$$\big((t^2-t-1)(t^2+t-1), -(t^2-t+1)(t^2+t+1)(t^2-t-1)(t^2+t-1),\\ (t^2-t+1)(t^2+t+1)\big);$$

$$\big((t^2-t+1)(t^2+t+1)(t^2-t-1)(t^2+t-1),\\ (t^2-t-1)(t^2+t-1), (t^2-t+1)(t^2+t+1)\big);$$

$$\big(-(t^2-t+1)(t^2+t+1), -(t^2-t+1)(t^2+t+1), 1\big);$$

$$\big((t^2-t+1)(t^2+t+1)(t^2-t-1)(t^2+t-1),\\ (t^2-t+1)(t^2+t+1)(t^2-t-1)(t^2+t-1), 1\big);$$

$$\big(-(t^2-t-1)(t^2+t-1), -(t^2-t-1)(t^2+t-1), 1\big);$$

$$\big((t^2+t+1)(t^2-t-1), (t^2+t+1)(t^2-t-1), 1\big);$$

$$\big(-(t^2+t+1)(t^2+t-1), -(t^2+t+1)(t^2+t-1), 1\big);$$

$$\big(1, (t^2-t+1)(t^2+t+1), (t^2-t+1)(t^2+t+1)\big);$$

$$\big(-(t^2-t+1)(t^2+t+1), -1, (t^2-t+1)(t^2+t+1)\big);$$

$$\big(-(t^2+t-1)(t^2+t+1), -(t^2-t+1)(t^2+t-1), (t^2+t+1)(t^2-t+1)\big);$$

$$\big((t^2+t-1)(t^2-t+1), (t^2+t-1)(t^2+t+1), (t^2+t+1)(t^2-t+1)\big);$$

$$\big(-(t^2-t-1)(t^2-t+1), -(t^2-t-1)(t^2-t+1), 1\big);$$

$$\big((t^2+t+1)(t^2-t-1), (t^2-t-1)(t^2-t+1), (t^2-t+1)(t^2+t+1)\big);$$

$$\big(-(t^2-t-1)(t^2-t+1), -(t^2-t-1)(t^2+t+1), (t^2-t+1)(t^2+t+1)\big);$$

$$\big((t^2-t+1)(t^2+t-1), (t^2-t+1)(t^2+t-1), 1\big).$$

LEMMA A.3. *The set S consists of the sixteen 3-tuples of Lemma A.2.*

Proof. Let $t_0 \in \mathbb{Q}$:

$$\begin{array}{ccccc} \mathcal{E}_t^*(\mathbb{Q}(t))/(2\mathcal{E}_t^*(\mathbb{Q}(t))) & \hookrightarrow & S & \hookrightarrow & (\mathbb{Q}(t)^*/\mathbb{Q}(t)^{*2})^3 \\ \downarrow & & \downarrow s & & \\ \mathcal{E}_{t_0}^*(\mathbb{Q})/(2\mathcal{E}_{t_0}^*(\mathbb{Q})) & \hookrightarrow & S_{t_0} & \hookrightarrow & (\mathbb{Q}^*/\mathbb{Q}^{*2})^3 \end{array}$$

where

$$S_{t_0} = \{(\mu_1(t_0)\mu_2(t_0), \mu_1(t_0)\mu_3(t_0), \mu_2(t_0)\mu_3(t_0))\}.$$

.

To prove the lemma, we will choose a specialisation t_0 ($t_0 = 4$) such that:

- $s : S \longrightarrow S_{t_0}$ is injective,
- the elliptic curve $\mathcal{E}_{t_0}^*$ has rank 2 over $\mathbb{Q}$, and
- the points P_{t_0} and R_{t_0} are of infinite order.

The set S_4 consists of the following sixteen 3-tuples:

(1, 1, 1);
(−11.19, −3.7.11.13.19, 3.7.13);
(3.7.11.13.19, 11.19, 3.7.13);
(−3.7.13, −3.7.13, 1);
(−11.19, −11.19, 1);
(3.7.11, 3.7.11, 1);
(1, 3.7.13, 3.7.13);
(−3.7.13, −1, 3.7.13);
(3.7.11.13.19, 3.7.11.13.19, 1);
(−3.7.19, −3.7.19, 1);
(−3.7.19, −13.19, 3.7.13);
(13.19, 3.7.19, 3.7.13);
(−11.13, −11.13, 1);
(3.7.11, 11.13, 3.7.13);
(−11.13, −3.7.11, 3.7.13);
(13.19, 13.19, 1).

These correspond to the images of, respectively, $\mathcal{O}$, A_t, B_t, C_t, P_t, R_t, $P_t + R_t$, $A_t + P_t$, $B_t + P_t$, $C_t + P_t$, $A_t + R_t$, $B_t + R_t$, $C_t + R_t$, $A_t + P_t + R_t$, $B_t + P_t + R_t$ and $C_t + P_t + R_t$ by $(x - \alpha)$. Moreover, the various values taken by the μ_i at 4 are distinct modulo square, and thus two distinct elements of S map to two distinct elements of S_4. □

Appendix B. *The polynomials in Relations* (11) *and* (13)

The polynomials p and q appearing in Relation (11) are:

$$
\begin{aligned}
p(X, Y, Z) = \\
&- 787\,974\,229\,481\,472\,000X^2Y^6Z^2 + 104\,322\,667\,181\,990\,081\,056X^2Y^5Z^3 \\
&- 24\,579\,619\,375\,702\,779\,280X^2Y^4Z^4 - 114\,255\,704\,794\,743\,859\,872X^2Y^3Z^5 \\
&- 66\,298\,272\,558\,865\,530\,400X^2Y^2Z^6 + 56\,805\,199\,418\,666\,424\,256X^2YZ^7 \\
&+ 44\,791\,993\,768\,746\,288\,240X^2Z^8 - 604\,113\,575\,935\,795\,200Y^9Z \\
&+ 8\,360\,712\,811\,387\,924\,480Y^8Z^2 - 76\,640\,116\,755\,040\,422\,016Y^7Z^3 \\
&+ 93\,002\,141\,197\,188\,721\,472Y^6Z^4 + 219\,785\,659\,966\,557\,088\,416Y^5Z^5 \\
&- 396\,402\,629\,747\,767\,176\,784Y^4Z^6 + 35\,350\,842\,340\,341\,158\,976Y^3Z^7 \\
&+ 166\,296\,203\,715\,640\,277\,552Y^2Z^8 - 34\,989\,179\,906\,455\,188\,736YZ^9 \\
&- 14\,148\,081\,444\,190\,636\,160Z^{10}
\end{aligned}
$$

and

$$
\begin{aligned}
q(X, Y, Z) = \\
&- 13\,112\,320\,243\,227\,004\,674\,938X^2Y^5Z^3 - 18\,515\,439\,649\,318\,656\,665\,215X^2Y^4Z^4 \\
&- 60\,254\,678\,417\,569\,498\,905\,420X^2Y^3Z^5 - 34\,855\,150\,679\,099\,560\,966\,870X^2Y^2Z^6 \\
&- 17\,487\,643\,171\,783\,783\,673\,738X^2YZ^7 - 5\,859\,364\,361\,710\,538\,080\,395X^2Z^8 \\
&+ 79\,025\,607\,152\,101\,209\,600Y^9Z - 655\,609\,009\,339\,991\,383\,040Y^8Z^2 \\
&+ 7\,485\,118\,389\,439\,620\,188\,168Y^7Z^3 - 3\,873\,126\,685\,687\,330\,070\,356Y^6Z^4 \\
&+ 25\,428\,753\,173\,824\,584\,490\,158Y^5Z^5 - 69\,350\,056\,403\,838\,147\,652\,435Y^4Z^6 \\
&+ 6\,633\,432\,099\,054\,113\,371\,998Y^3Z^7 - 2\,841\,295\,646\,889\,638\,886\,031Y^2Z^8 \\
&+ 7\,194\,430\,628\,524\,830\,054\,728YZ^9 + 1\,850\,779\,885\,038\,536\,905\,180Z^{10}.
\end{aligned}
$$

The polynomials r and s appearing in Relation (13) are:

$$
\begin{aligned}
r(X, Y, Z) = \\
&126\,404\,444\,935\,639X^2Y^8 - 121\,673\,377\,735\,936X^2Y^7Z \\
&+ 719\,506\,165\,075\,360X^2Y^6Z^2 - 479\,114\,565\,193\,472X^2Y^5Z^3 \\
&+ 1\,237\,595\,162\,655\,618X^2Y^4Z^4 - 479\,114\,565\,193\,472X^2Y^3Z^5 \\
&+ 719\,506\,165\,075\,360X^2Y^2Z^6 - 121\,673\,377\,735\,936X^2YZ^7 \\
&+ 126\,404\,444\,935\,639X^2Z^8 - 43\,529\,213\,806\,732Y^10 \\
&+ 42\,270\,104\,167\,424Y^9Z - 33\,604\,899\,676\,861Y^8Z^2 \\
&- 43100395519232Y^7Z^3 + 350\,389\,186\,427\,933Y^6Z^4 \\
&- 221\,861\,481\,496\,064Y^5Z^5 + 350\,389\,186\,427\,933Y^4Z^6 \\
&- 43\,100\,395\,519\,232Y^3Z^7 - 33\,604\,899\,676\,861Y^2Z^8 \\
&+ 42\,270\,104\,167\,424YZ^9 - 43\,529\,213\,806\,732Z^{10}
\end{aligned}
$$

and

$$
\begin{aligned}
s(X, Y, Z) = {}& \\
& 126\,404\,444\,935\,639 X^2 Y^8 - 121\,673\,377\,735\,936 X^2 Y^7 Z \\
& + 719\,506\,165\,075\,360 X^2 Y^6 Z^2 - 479\,114\,565\,193\,472 X^2 Y^5 Z^3 \\
& + 1\,237\,595\,162\,655\,618 X^2 Y^4 Z^4 - 479\,114\,565\,193\,472 X^2 Y^3 Z^5 \\
& + 719\,506\,165\,075\,360 X^2 Y^2 Z^6 - 121\,673\,377\,735\,936 X^2 Y Z^7 \\
& + 126\,404\,444\,935\,639 X^2 Z^8 - 43\,529\,213\,806\,732 Y^1 0 \\
& + 42\,270\,104\,167\,424 Y^9 Z - 33\,604\,899\,676\,861 Y^8 Z^2 \\
& - 43\,100\,395\,519\,232 Y^7 Z^3 + 350\,389\,186\,427\,933 Y^6 Z^4 \\
& - 221\,861\,481\,496\,064 Y^5 Z^5 + 350\,389\,186\,427\,933 Y^4 Z^6 \\
& - 43\,100\,395\,519\,232 Y^3 Z^7 - 33\,604\,899\,676\,861 Y^2 Z^8 \\
& + 42\,270\,104\,167\,424 Y Z^9 - 43\,529\,213\,806\,732 Z^{10}.
\end{aligned}
$$

Appendix C. *The polynomials in Relation* (17)

We give here the polynomials appearing in Relation (17):

$p := 12t^2\cdot(12\cdot(t^4-3t^2+1)^3\cdot(t^4+1)\cdot(t^2-1)^2t^8\cdot(-167\cdot(t^{24}+1)-27\cdot(t^{22}+t^2)+593\cdot(t^{20}+t^4)-1082\cdot(t^{18}+t^6)+1267\cdot(t^{16}+t^8)-1589\cdot(t^{14}+t^{10})+1590t^{12})X^2Y^6Z^2+2\cdot(483\cdot(t^{60}+1)-6272\cdot(t^{58}+t^2)+35645\cdot(t^{56}+t^4)-112368\cdot(t^{54}+t^6)+185211\cdot(t^{52}+t^8)+40043\cdot(t^{50}+t^{10})-1285005\cdot(t^{48}+t^{12})+4858995\cdot(t^{46}+t^{14})-12652360\cdot(t^{44}+t^{16})+26469896\cdot(t^{42}+t^{18})-46829156\cdot(t^{40}+t^{20})+72249549\cdot(t^{38}+t^{22})-99296614\cdot(t^{36}+t^{24})+123293365\cdot(t^{34}+t^{26})-139725868\cdot(t^{32}+t^{28})+145555632t^{30})X^2Y^5Z^3+(t^4-3t^2+1)\cdot(-1707\cdot(t^{56}+1)+20483\cdot(t^{54}+t^2)-103567\cdot(t^{52}+t^4)+287943\cdot(t^{50}+t^6)-429482\cdot(t^{48}+t^8)-26946\cdot(t^{46}+t^{10})+2234521\cdot(t^{44}+t^{12})-8060726\cdot(t^{42}+t^{14})+19571872\cdot(t^{40}+t^{16})-37676878\cdot(t^{38}+t^{18})+61397255\cdot(t^{36}+t^{20})-87672254\cdot(t^{34}+t^{22})+111736501\cdot(t^{32}+t^{24})-128553030\cdot(t^{30}+t^{26})+134605790t^{28})X^2Y^4Z^4+2\cdot(741\cdot(t^{60}+1)-12853\cdot(t^{58}+t^2)+94467\cdot(t^{56}+t^4)-399129\cdot(t^{54}+t^6)+1084490\cdot(t^{52}+t^8)-1901878\cdot(t^{50}+t^{10})+1519413\cdot(t^{48}+t^{12})+3195813\cdot(t^{46}+t^{14})-17448499\cdot(t^{44}+t^{16})+47061116\cdot(t^{42}+t^{18})-95231905\cdot(t^{40}+t^{20})+159954791\cdot(t^{38}+t^{22})-232959354\cdot(t^{36}+t^{24})+300803871\cdot(t^{34}+t^{26})-348847545\cdot(t^{32}+t^{28})+366213242t^{30})X^2Y^3Z^5+(t^4-3t^2+1)\cdot(-1482\cdot(t^{56}+1)+18911\cdot(t^{54}+t^2)-109710\cdot(t^{52}+t^4)+379965\cdot(t^{50}+t^6)-858244\cdot(t^{48}+t^8)+1229692\cdot(t^{46}+t^{10})-553090\cdot(t^{44}+t^{12})-2985590\cdot(t^{42}+t^{14})+11682688\cdot(t^{40}+t^{16})-26943442\cdot(t^{38}+t^{18})+48345394\cdot(t^{36}+t^{20})-73174236\cdot(t^{34}+t^{22})+96641118\cdot(t^{32}+t^{24})-113380500\cdot(t^{30}+t^{26})+119470812t^{28})X^2Y^2Z^6+2\cdot(258\cdot(t^{60}+1)-4646\cdot(t^{58}+t^2)+39745\cdot(t^{56}+t^4)-207033\cdot(t^{54}+t^6)+728152\cdot(t^{52}+t^8)-1844086\cdot(t^{50}+t^{10})+3472862\cdot(t^{48}+t^{12})-4678266\cdot(t^{46}+t^{14})+3245671\cdot(t^{44}+t^{16})+3873556\cdot(t^{42}+t^{18})-19047239\cdot(t^{40}+t^{20})+42390550\cdot(t^{38}+t^{22})-70869136\cdot(t^{36}+t^{24})+98616608\cdot(t^{34}+t^{26})-118826777\cdot(t^{32}+t^{28})+126226282t^{30})X^2YZ^7+(t^2-1)^2\cdot(t^4-3t^2+1)\cdot(t^4+1)\cdot(225\cdot(t^{48}+1)-294\cdot(t^{46}+t^2)-8561\cdot(t^{44}+t^4)+52018\cdot(t^{42}+t^6)-156825\cdot(t^{40}+t^8)+322592\cdot(t^{38}+t^{10})-494112\cdot(t^{36}+t^{12})+557260\cdot(t^{34}+t^{14})-448183\cdot(t^{32}+t^{16})+206862\cdot(t^{30}+t^{18})+81089\cdot(t^{28}+t^{20})-321670\cdot(t^{26}+t^{22})+412478t^{24})X^2Z^8+2t^8\cdot(t^2-1)^2\cdot(t^4-3t^2+1)^2\cdot(3t^4-7t^2+3)\cdot(t^4+1)\cdot(-167\cdot(t^{24}+1)-27\cdot(t^{22}+t^2)+593\cdot(t^{20}+t^4)-1082\cdot(t^{18}+t^6)+1267\cdot(t^{16}+t^8)-1589\cdot(t^{14}+t^{10})+1590t^{12})Y^9Z+2t^6\cdot(t^4-3t^2+1)\cdot(1002\cdot(t^{44}+1)-5296\cdot(t^{42}+t^2)+5633\cdot(t^{40}+t^4)+20552\cdot(t^{38}+t^6)-88704\cdot(t^{36}+t^8)+203008\cdot(t^{34}+t^{10})-364324\cdot(t^{32}+t^{12})+552232\cdot(t^{30}+t^{14})-720433\cdot(t^{28}+t^{16})+848256\cdot(t^{26}+t^{18})-934950\cdot(t^{24}+t^{20})+969408t^{22})Y^8Z^2+2t^2\cdot(-483\cdot(t^{56}+1)+5288\cdot(t^{54}+t^2)-28039\cdot(t^{52}+t^4)+90108\cdot(t^{50}+t^6)-153770\cdot(t^{48}+t^8)-53680\cdot(t^{46}+t^{10})+1155465\cdot(t^{44}+t^{12})-4000714\cdot(t^{42}+t^{14})+9393644\cdot(t^{40}+t^{16})-17647930\cdot(t^{38}+t^{18})+28117047\cdot(t^{36}+t^{20})-39194680\cdot(t^{34}+t^{22})+48953117\cdot(t^{32}+t^{24})-55668848\cdot(t^{30}+t^{26})+58080390t^{28})Y^7Z^3+t^2\cdot(1707\cdot(t^{56}+1)-22121\cdot(t^{54}+t^2)+135700\cdot(t^{52}+t^4)-493973\cdot(t^{50}+t^6)+1065790\cdot(t^{48}+t^8)-888390\cdot(t^{46}+t^{10})-2664315\cdot(t^{44}+t^{12})+13835240\cdot(t^{42}+t^{14})-37364364\cdot(t^{40}+t^{16})+76022040\cdot(t^{38}+t^{18})-127866713\cdot(t^{36}+t^{20})+185508918\cdot(t^{34}+t^{22})-238339445\cdot(t^{32}+t^{24})+275593630\cdot(t^{30}+t^{26})-289081008t^{28})Y^6Z^4+2\cdot(t^2-1)^2\cdot(483\cdot(t^{56}+1)-5063\cdot(t^{54}+t^2)+27940\cdot(t^{52}+t^4)-103945\cdot(t^{50}+t^6)+246281\cdot(t^{48}+t^8)-261850\cdot(t^{46}+t^{10})-458696\cdot(t^{44}+t^{12})+2958664\cdot(t^{42}+t^{14})-8475492\cdot(t^{40}+t^{16})+17807380\cdot(t^{38}+t^{18})-30553628\cdot(t^{36}+t^{20})+44867626\cdot(t^{34}+t^{22})-58061640\cdot(t^{32}+t^{24})+67401684\cdot(t^{30}+t^{26})-70796288t^{28})Y^5Z^5+(-1707\cdot(t^{60}+1)+21599\cdot(t^{58}+t^2)-137824\cdot(t^{56}+t^4)+577902\cdot(t^{54}+t^6)-1665837\cdot(t^{52}+t^8)+3090484\cdot(t^{50}+$

$$t^{10})-2228215\cdot(t^{48}+t^{12})-7579569\cdot(t^{46}+t^{14})+37142033\cdot(t^{44}+t^{16})-98469940\cdot(t^{42}+t^{18})+198704699\cdot$$
$$(t^{40}+t^{20})-333522747\cdot(t^{38}+t^{22})+484873874\cdot(t^{36}+t^{24})-625011079\cdot(t^{34}+t^{26})+724432929\cdot(t^{32}+t^{28})-$$
$$760426324t^{30})Y^4Z^6+2\cdot(t^2-1)^2\cdot(258\cdot(t^{56}+1)-4463\cdot(t^{54}+t^2)+35943\cdot(t^{52}+t^4)-170838\cdot(t^{50}+t^6)+$$
$$519984\cdot(t^{48}+t^8)-1031866\cdot(t^{46}+t^{10})+1182130\cdot(t^{44}+t^{12})+178573\cdot(t^{42}+t^{14})-4632398\cdot(t^{40}+t^{16})+$$
$$13475611\cdot(t^{38}+t^{18})-26692738\cdot(t^{36}+t^{20})+42438714\cdot(t^{34}+t^{22})-57554922\cdot(t^{32}+t^{24})+68535965\cdot(t^{30}+$$
$$t^{26})-72569146t^{28})Y^3Z^7+(225\cdot(t^{60}+1)+390\cdot(t^{58}+t^2)-27173\cdot(t^{56}+t^4)+225321\cdot(t^{54}+t^6)-1023532\cdot$$
$$(t^{52}+t^8)+3070864\cdot(t^{50}+t^{10})-6477581\cdot(t^{48}+t^{12})+9563806\cdot(t^{46}+t^{14})-8063433\cdot(t^{44}+t^{16})-4244136\cdot$$
$$(t^{42}+t^{18})+32684669\cdot(t^{40}+t^{20})-77772366\cdot(t^{38}+t^{22})+133154204\cdot(t^{36}+t^{24})-187239110\cdot(t^{34}+t^{26})+$$
$$226859325\cdot(t^{32}+t^{28})-241456546t^{30})Y^2Z^8+2t^2\cdot(-246\cdot(t^{56}+1)+4042\cdot(t^{54}+t^2)-34063\cdot(t^{52}+t^4)+175714\cdot$$
$$(t^{50}+t^6)-594561\cdot(t^{48}+t^8)+1396716\cdot(t^{46}+t^{10})-2353043\cdot(t^{44}+t^{12})+2680150\cdot(t^{42}+t^{14})-1083348\cdot(t^{40}+$$
$$t^{16})-3672338\cdot(t^{38}+t^{18})+11878579\cdot(t^{36}+t^{20})-22367380\cdot(t^{34}+t^{22})+32845223\cdot(t^{32}+t^{24})-40636480\cdot$$
$$(t^{30}+t^{26})+43535510t^{28})YZ^9+t^2\cdot(t^4-3t^2+1)\cdot(-222\cdot(t^{52}+1)+440\cdot(t^{50}+t^2)+9017\cdot(t^{48}+t^4)-64405\cdot$$
$$(t^{46}+t^6)+221863\cdot(t^{44}+t^8)-515712\cdot(t^{42}+t^{10})+909956\cdot(t^{40}+t^{12})-1267554\cdot(t^{38}+t^{14})+1410138\cdot(t^{36}+$$
$$t^{16})-1237794\cdot(t^{34}+t^{18})+809881\cdot(t^{32}+t^{20})-285993\cdot(t^{30}+t^{22})-144409\cdot(t^{28}+t^{24})+316308t^{26})Z^{10})$$

and

$$q:=(t^4+t^2+1)\cdot(2\cdot(-1449\cdot(t^{68}+1)+23646\cdot(t^{66}+t^2)-175934\cdot(t^{64}+t^4)+781423\cdot(t^{62}+t^6)-2213821\cdot$$
$$(t^{60}+t^8)+3491489\cdot(t^{58}+t^{10})+1436003\cdot(t^{56}+t^{12})-29075153\cdot(t^{54}+t^{14})+109895174\cdot(t^{52}+t^{16})-$$
$$285753826\cdot(t^{50}+t^{18})+599390367\cdot(t^{48}+t^{20})-1077302888\cdot(t^{46}+t^{22})+1711924522\cdot(t^{44}+t^{24})-$$
$$2451882396\cdot(t^{42}+t^{26})+3206159912\cdot(t^{40}+t^{28})-3861537630\cdot(t^{38}+t^{30})+4308327962\cdot(t^{36}+t^{32})-$$
$$4466947922t^{34})X^2Y^5Z^3+(t^4-3t^2+1)\cdot(-675\cdot(t^{64}+1)-3255\cdot(t^{62}+t^2)+104186\cdot(t^{60}+t^4)-764280\cdot$$
$$(t^{58}+t^6)+3138540\cdot(t^{56}+t^8)-8433300\cdot(t^{54}+t^{10})+15177590\cdot(t^{52}+t^{12})-15558655\cdot(t^{50}+t^{14})-6714483\cdot$$
$$(t^{48}+t^{16})+75290212\cdot(t^{46}+t^{18})-213820216\cdot(t^{44}+t^{20})+433730140\cdot(t^{42}+t^{22})-723459458\cdot(t^{40}+t^{24})+$$
$$1045727606\cdot(t^{38}+t^{26})-1343288664\cdot(t^{36}+t^{28})+1554141900\cdot(t^{34}+t^{30})-1630319336t^{32})X^2Y^4Z^4+2\cdot$$
$$(-2898\cdot(t^{68}+1)+44997\cdot(t^{66}+t^2)-334324\cdot(t^{64}+t^4)+1564930\cdot(t^{62}+t^6)-5025808\cdot(t^{60}+t^8)+10800131\cdot$$
$$(t^{58}+t^{10})-10991607\cdot(t^{56}+t^{12})-22848513\cdot(t^{54}+t^{14})+151673396\cdot(t^{52}+t^{16})-469443352\cdot(t^{50}+t^{18})+$$
$$1084107489\cdot(t^{48}+t^{20})-2077648276\cdot(t^{46}+t^{22})+3457641269\cdot(t^{44}+t^{24})-5123708529\cdot(t^{42}+t^{26})+$$
$$6868388768\cdot(t^{40}+t^{28})-8414772861\cdot(t^{38}+t^{30})+9482771075\cdot(t^{36}+t^{32})-9864270494t^{34})X^2Y^3Z^5+$$
$$(t^4-3t^2+1)\cdot(-1350\cdot(t^{64}+1)+552\cdot(t^{62}+t^2)+114617\cdot(t^{60}+t^4)-993962\cdot(t^{58}+t^6)+4638155\cdot(t^{56}+$$
$$t^8)-14657269\cdot(t^{54}+t^{10})+33954704\cdot(t^{52}+t^{12})-59166432\cdot(t^{50}+t^{14})+74263851\cdot(t^{48}+t^{16})-48272593\cdot$$
$$(t^{46}+t^{18})-56742700\cdot(t^{44}+t^{20})+267715077\cdot(t^{42}+t^{22})-580999217\cdot(t^{40}+t^{24})+953888248\cdot(t^{38}+t^{26})-$$
$$1311943293\cdot(t^{36}+t^{28})+1571195883\cdot(t^{34}+t^{30})-1665773502t^{32})X^2Y^2Z^6+2\cdot(-1449\cdot(t^{68}+1)+22800\cdot$$
$$(t^{66}+t^2)-168017\cdot(t^{64}+t^4)+777372\cdot(t^{62}+t^6)-2529621\cdot(t^{60}+t^8)+5971142\cdot(t^{58}+t^{10})-9420344\cdot$$
$$(t^{56}+t^{12})+4248391\cdot(t^{54}+t^{14})+31695531\cdot(t^{52}+t^{16})-138442827\cdot(t^{50}+t^{18})+369404790\cdot(t^{48}+t^{20})-$$
$$773498804\cdot(t^{46}+t^{22})+1367936263\cdot(t^{44}+t^{24})-2114975473\cdot(t^{42}+t^{26})+2917709590\cdot(t^{40}+t^{28})-$$
$$3639994007\cdot(t^{38}+t^{30})+4142781593\cdot(t^{36}+t^{32})-4323006980t^{34})X^2YZ^7+(t^2-1)^2\cdot(t^4-3t^2+1)\cdot(3t^4-$$
$$7t^2+3)\cdot(t^4+1)\cdot(-225\cdot(t^{52}+1)+519\cdot(t^{50}+t^2)+8039\cdot(t^{48}+t^4)-60216\cdot(t^{46}+t^6)+216669\cdot(t^{44}+t^8)-$$
$$526599\cdot(t^{42}+t^{10})+951383\cdot(t^{40}+t^{12})-1298442\cdot(t^{38}+t^{14})+1298915\cdot(t^{36}+t^{16})-783107\cdot(t^{34}+t^{18})-$$
$$183853\cdot(t^{32}+t^{20})+1320306\cdot(t^{30}+t^{22})-2233904\cdot(t^{28}+t^{24})+2587750t^{26})X^2Z^8+2t^8\cdot(t^2-1)^2\cdot(t^4-$$
$$3t^2+1)^2\cdot(3t^4-7t^2+3)^2\cdot(t^4-t^2+1)\cdot(167\cdot(t^{28}+1)+27\cdot(t^{26}+t^2)-426\cdot(t^{24}+t^4)+1109\cdot(t^{22}+t^6)-$$
$$1860\cdot(t^{20}+t^8)+2671\cdot(t^{18}+t^{10})-2857\cdot(t^{16}+t^{12})+3178t^{14})Y^9Z+2t^8\cdot(t^4-3t^2+1)\cdot(3t^4-7t^2+3)\cdot$$
$$(t^4-t^2+1)\cdot(-2558\cdot(t^{40}+1)+15565\cdot(t^{38}+t^2)-31484\cdot(t^{36}+t^4)+1704\cdot(t^{34}+t^6)+141692\cdot(t^{32}+t^8)-$$
$$443936\cdot(t^{30}+t^{10})+896120\cdot(t^{28}+t^{12})-1430237\cdot(t^{26}+t^{14})+1926498\cdot(t^{24}+t^{16})-2264520\cdot(t^{22}+t^{18})+$$
$$2378952t^{20})Y^8Z^2+2t^2\cdot(t^4-t^2+1)\cdot(1449\cdot(t^{60}+1)-20748\cdot(t^{58}+t^2)+129536\cdot(t^{56}+t^4)-419764\cdot(t^{54}+$$
$$t^6)+522948\cdot(t^{52}+t^8)+1319680\cdot(t^{50}+t^{10})-8196331\cdot(t^{48}+t^{12})+22270848\cdot(t^{46}+t^{14})-42191536\cdot$$
$$(t^{44}+t^{16})+62988680\cdot(t^{42}+t^{18})-78596584\cdot(t^{40}+t^{20})+85074840\cdot(t^{38}+t^{22})-82947550\cdot(t^{36}+t^{24})+$$
$$76712372\cdot(t^{34}+t^{26})-71380460\cdot(t^{32}+t^{28})+69438360t^{30})Y^7Z^3+t^2\cdot(675\cdot(t^{64}+1)+1905\cdot(t^{62}+t^2)-$$
$$104267\cdot(t^{60}+t^4)+715026\cdot(t^{58}+t^6)-2224079\cdot(t^{56}+t^8)+3544000\cdot(t^{54}+t^{10})-2808981\cdot(t^{52}+t^{12})+$$
$$4743421\cdot(t^{50}+t^{14})-30721447\cdot(t^{48}+t^{16})+120031450\cdot(t^{46}+t^{18})-317378872\cdot(t^{44}+t^{20})+651141358\cdot$$
$$(t^{42}+t^{22})-1107843292\cdot(t^{40}+t^{24})+1622849762\cdot(t^{38}+t^{26})-2097376992\cdot(t^{36}+t^{28})+2431051782\cdot(t^{34}+$$
$$t^{30})-2550812818t^{32})Y^6Z^4+2\cdot(-1449\cdot(t^{68}+1)+25095\cdot(t^{66}+t^2)-196730\cdot(t^{64}+t^4)+935959\cdot(t^{62}+$$
$$t^6)-2832279\cdot(t^{60}+t^8)+4498770\cdot(t^{58}+t^{10})+3303023\cdot(t^{56}+t^{12})-43848719\cdot(t^{54}+t^{14})+152510330\cdot$$
$$(t^{52}+t^{16})-363417987\cdot(t^{50}+t^{18})+692175673\cdot(t^{48}+t^{20})-1123356832\cdot(t^{46}+t^{22})+1609945176\cdot(t^{44}+$$
$$t^{24})-2092506284\cdot(t^{42}+t^{26})+2518586000\cdot(t^{40}+t^{28})-2848798720\cdot(t^{38}+t^{30})+3056272480\cdot(t^{36}+t^{32})-$$
$$3127151492t^{34})Y^5Z^5+(-675\cdot(t^{68}+1)-555\cdot(t^{66}+t^2)+91649\cdot(t^{64}+t^4)-931131\cdot(t^{62}+t^6)+4976052\cdot$$
$$(t^{60}+t^8)-16865050\cdot(t^{58}+t^{10})+39156244\cdot(t^{56}+t^{12})-64567019\cdot(t^{54}+t^{14})+73358969\cdot(t^{52}+t^{16})-$$
$$39330131\cdot(t^{50}+t^{18})-62509767\cdot(t^{48}+t^{20})+244118720\cdot(t^{46}+t^{22})-490005438\cdot(t^{44}+t^{24})+769200334\cdot$$
$$(t^{42}+t^{26})-1047323610\cdot(t^{40}+t^{28})+1285081110\cdot(t^{38}+t^{30})-1443511904\cdot(t^{36}+t^{32})+1499643124t^{34})\cdot$$
$$Y^4Z^6+2\cdot(-1449\cdot(t^{68}+1)+24249\cdot(t^{66}+t^2)-191063\cdot(t^{64}+t^4)+946842\cdot(t^{62}+t^6)-3152603\cdot(t^{60}+t^8)+$$

$6577731\cdot(t^{58}+t^{10})-4527180\cdot(t^{56}+t^{12})-24201005\cdot(t^{54}+t^{14})+118646817\cdot(t^{52}+t^{16})-327375616\cdot(t^{50}+t^{18})+690710524\cdot(t^{48}+t^{20})-1219651172\cdot(t^{46}+t^{22})+1880808185\cdot(t^{44}+t^{24})-2603310909\cdot(t^{42}+t^{26})+3297185526\cdot(t^{40}+t^{28})-3870981737\cdot(t^{38}+t^{30})+4247920987\cdot(t^{36}+t^{32})-4379420734t^{34})Y^3Z^7+(-675\cdot(t^{68}+1)+7182\cdot(t^{66}+t^2)-288\cdot(t^{64}+t^4)-400445\cdot(t^{62}+t^6)+3194378\cdot(t^{60}+t^8)-14037669\cdot(t^{58}+t^{10})+42475088\cdot(t^{56}+t^{12})-96832663\cdot(t^{54}+t^{14})+173947312\cdot(t^{52}+t^{16})-248791632\cdot(t^{50}+t^{18})+270562795\cdot(t^{48}+t^{20})-174689536\cdot(t^{46}+t^{22})-86314952\cdot(t^{44}+t^{24})+512856922\cdot(t^{42}+t^{26})-1044127936\cdot(t^{40}+t^{28})+1567739932\cdot(t^{38}+t^{30})-1952629818\cdot(t^{36}+t^{32})+2094514090t^{34})Y^2Z^8+2t^2\cdot(t^4-t^2+1)\cdot(1449\cdot(t^{60}+1)-19854\cdot(t^{58}+t^2)+123859\cdot(t^{56}+t^4)-450193\cdot(t^{54}+t^6)+940345\cdot(t^{52}+t^8)-443505\cdot(t^{50}+t^{10})-4531725\cdot(t^{48}+t^{12})+19958875\cdot(t^{46}+t^{14})-52246070\cdot(t^{44}+t^{16})+105087648\cdot(t^{42}+t^{18})-176576450\cdot(t^{40}+t^{20})+257793673\cdot(t^{38}+t^{22})-335731684\cdot(t^{36}+t^{24})+398842475\cdot(t^{34}+t^{26})-439571812\cdot(t^{32}+t^{28})+453619058t^{30})YZ^9+t^2\cdot(t^4-3t^2+1)\cdot(3t^4-7t^2+3)\cdot(t^4-t^2+1)\cdot(225\cdot(t^{52}+1)-515\cdot(t^{50}+t^2)-8141\cdot(t^{48}+t^4)+58024\cdot(t^{46}+t^6)-189169\cdot(t^{44}+t^8)+389523\cdot(t^{42}+t^{10})-525719\cdot(t^{40}+t^{12})+312426\cdot(t^{38}+t^{14})+579897\cdot(t^{36}+t^{16})-2308233\cdot(t^{34}+t^{18})+4674449\cdot(t^{32}+t^{20})-7152498\cdot(t^{30}+t^{22})+9052234\cdot(t^{28}+t^{24})-9771726t^{26})Z^{10}).$

References

1. R. Auer and J. Top, 'Some genus 3 curves with many points', *Algorithmic number theory* (Sydney, 2002), Lecture Notes in Comput. Sci. 2369 (Springer, Berlin, 2002) 163–171. 274
2. E. Bombieri, 'The Mordell conjecture revisited', *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) 17 (1990) 615–640. 267
3. W. Bosma and J. Cannon (eds), 'Handbook of Magma functions', `http://magma.maths.usyd.edu.au/`. 278
4. N. Bruin, 'The diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$', *Compositio Math.* 118 (1999) 305–321. 267
5. N. Bruin and E. V. Flynn, 'n-covers of hyperelliptic curves', *Math. Proc. Cambridge Philos. Soc.* 134 (2003) 397–405. 267
6. J. W. S. Cassels, 'On a theorem of Dem'janenko', *J. London Math. Soc.* 43 (1968) 61–66. 267, 270, 274
7. C. Chabauty, 'Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension', *C. R. Acad. Sci. Paris* 212 (1941) 1022–1024. 267
8. R. F. Coleman, 'Effective Chabauty', *Duke Math. J.* 52 (1985) 765–770. 267
9. J. E. Cremona, '`mwrank`' and other programs for elliptic curves over $\mathbb{Q}$, `http://www.maths.nott.ac.uk/personal/jec/ftp/progs/`. 276, 283
10. J. E. Cremona, M. Prickett and S. Siksek, 'Height differences bounds for elliptic curves over number fields', *J. Number Theory*, to appear. 269, 278, 287
11. T. de Diego, 'Points rationnels sur les familles de courbes de genre au moins 2', *J. Number Theory* 67 (1997) 85–114. 267
12. V. A. Dem'janenko, *Rational points of a class of algebraic curves*, Amer. Math. Soc. Transl., Ser. II 66 (Amer. Math. Soc., Providence, RI, 1968) 246–272. 267, 270
13. G. Faltings, 'Endlichkeitssätze für abelsche Varietäten über Zahlkörpern', *Invent. Math.* 73 (1983) 349–366. 267
14. G. Faltings, 'Diophantine approximation on abelian varieties', *Ann. of Math.* (2) 133 (1991) 549–576. 267
15. E. V. Flynn, 'A flexible method for applying Chabauty's theorem', *Compositio Math.* 105 (1997) 79–94. 267

16. E. V. Flynn, 'Coverings of curves of genus 2', *Algorithmic number theory* (Leiden, 2000), Lecture Notes in Comput. Sci. 1838 (Springer, Berlin, 2000) 65–84. 267

17. E. V. Flynn, B. Poonen and E. F. Schaefer, 'Cycles of quadratic polynomials and rational points on a genus-2 curve', *Duke Math. J.* 90 (1997) 435–463. 267

18. E. V. Flynn and J. L. Wetherell, 'Covering collections and a challenge problem of Serre', *Acta Arith.* 98 (2001) 197–205. 267

19. M. Girard, 'Points de weierstrass et courbes algébriques de genre 3', Ph.D. thesis, Université Paris 7 (2000). 273

20. M. Girard and P. Tzermias, 'Group generated by the Weierstrass points of a plane quartic', *Proc. Amer. Math. Soc.* 130 (2002) 667–672. 273

21. M. Hindry and J. H. Silverman, *Diophantine geometry*, Grad. Texts in Math. 201 (Springer, New York, 2000). 270

22. E. W. Howe, F. Leprévost and B. Poonen, 'Large torsion subgroups of split Jacobians of curves of genus two or three', *Forum Math.* 12 (2000) 315–364. 272

23. L. Kulesz, 'Application de la méthode de Dem'janenko–Manin à certaines familles de courbes de genre 2 et 3', *J. Number Theory* 76 (1999) 130–146. 267, 271

24. L. Kulesz, 'Courbes elliptiques de rang $\geqslant 5$ sur $\mathbb{Q}(t)$ avec un groupe de torsion isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$', *C. R. Acad. Sci. Paris Sér. I Math.* 329 (1999) 503–506. 273

25. Ju. I. Manin, 'Rational points on algebraic curves over function fields', *Izv. Akad. Nauk SSSR Ser. Mat.* 27 (1963) 1395–1440. 267

26. Ju. I. Manin, 'The p-torsion of elliptic curves is uniformly bounded', *Izv. Akad. Nauk SSSR Ser. Mat.* 33 (1969) 459–465. 267

27. G. Rémond, 'Inégalité de Vojta en dimension supérieure', *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) 29 (2000) 101–151. 267

28. J.-P. Serre, *Lectures on the Mordell–Weil theorem,* Aspects of Math. E 15 (Vieweg, 1989). 267, 269, 270

29. T. Shioda, 'On the Mordell–Weil lattices', *Comment. Math. Univ. St. Paul* 39 (1990) 211–240. 276

30. T. Shioda, 'On the rank of elliptic curves over $\mathbf{Q}(t)$ arising from K3 surfaces', *Comment. Math. Univ. St. Paul.* 43 (1994) 117–120. 276

31. S. Siksek, 'Infinite descent on elliptic curves', *Rocky Mountain J. Math.* 25 (1995) 1501–1538. 269

32. J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math. 106 (Springer, New York, 1986). 269, 270

33. J. H. Silverman, 'Rational points on certain families of curves of genus at least 2', *Proc. London Math. Soc.* (3) 55 (1987) 465–481. 267

34. J. H. Silverman, 'The difference between the Weil height and the canonical height on elliptic curves', *Math. Comp.* 55 (1990) 723–743. 269

35. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. 151 (Springer, New York, 1994). 269, 270, 271, 281

36. J. Top, 'Hecke l-series related with algebraic cycles or with siegel modular forms', PhD thesis, Utrecht University (1989). 274

37. University of Sydney Computational Algebra Group, 'Magma computational algebra system', http://magma.maths.usyd.edu.au/. 278

38. P. Vojta, 'Siegel's theorem in the compact case', *Ann. of Math.* (2) 133 (1991) 509–548. 267

39. A. Weil, 'Remarques sur un mémoire d'Hermite', *Arch. Math.* 5 (1954) 197–202. 273

40. J. L. Wetherell, 'Bounding the number of rational points on certain curves of high rank', Ph.D. thesis, University of California, Berkeley (1997). 267

Martine Girard girard@maths.usyd.edu.au
http://www.maths.usyd.edu.au/u/girard/

School of Mathematics and Statistics
University of Sydney NSW 2006
Australia

Leopoldo Kulesz lk@delzorzal.com.ar

Instituto de Desarollo Humano
Universidad Nacional de General Sarmiento
Roca 850 San Miguel
Pcia. de Buenos Aires, 1663
Argentina