Uniform bounds on the number of rational points of a family of curves of genus 2*

L. Kulesz, G. Matera
Instituto de Desarrollo Humano, Universidad Nacional de General Sarmiento
Campus Universitario, José M. Gutiérrez 1150 (1613) Los Polvorines
Buenos Aires, Argentina, {lkulesz,gmatera}@ungs.edu.ar
É. Schost
Laboratoire GAGE, École polytechnique,
F-91128 Palaiseau Cedex, France, Eric.Schost@polytechnique.fr

Abstract

We exhibit a genus–2 curve $\mathcal{C}$ defined over $\mathbb{Q}(T)$ which admits two independent morphisms to a rank–1 elliptic curve defined over $\mathbb{Q}(T)$. We describe completely the set of $\mathbb{Q}(T)$–rational points of the curve $\mathcal{C}$ and obtain a *uniform* bound for the number of $\mathbb{Q}$–rational points of a rational specialization $\mathcal{C}_t$ of the curve $\mathcal{C}$ for a certain (possibly infinite) set of values $t \in \mathbb{Q}$. Furthermore, for this set of values $t \in \mathbb{Q}$ we describe completely the set of $\mathbb{Q}$–rational points of the curve $\mathcal{C}_t$. Finally we show how these results can be strengthened assuming a height conjecture of S. Lang.

1 Introduction

In 1983, G. Faltings proved Mordell's Conjecture, which asserts that for any number field K, the set $\mathcal{C}(K)$ of K–rational points of a curve $\mathcal{C}$ defined over K of genus at least 2 is finite (see [Fal83]). In order to have more insight on Faltings' Theorem one may ask about the behaviour of the set of K–rational points of a given K–definable family $f : S \to \mathbb{P}^1(\mathbb{Q})$ of curves of (fixed) genus ≥ 2. This question is strongly related to the following conjecture of S. Lang [Lan86]:

Conjecture A *Let V be a variety of general type defined over a number field K. Then the set $V(K)$ of K-rational points of V is contained in a subvariety of V of codimension at least* 1.

*Research was partially supported by the following Argentinian and French grants : UBA-CyT X198, PIP CONICET 4571, ECOS A99E06, UNGS 30/3003. Some of the results presented here were first announced at the *Workshop Argentino de Informática Teórica*, WAIT'01, held in September 2001 (see [GKMS01]).

As an attempt to understand Conjecture A, L. Caporaso, J. Harris and B. Mazur showed the following consequence of this conjecture in the case of algebraic curves (see [CHM95], [CHM97]):

Theorem 1 *If Conjecture A is true, then for any number field K and any integer $g \geq 2$ there exists an integer $B(K,g)$ such that any non–singular curve defined over K of genus g has at most $B(K,g)$ K-rational points.*

Partial results in the direction of Theorem 1, namely uniform upper bounds on the number of $\mathbb{Q}$–rational points of families of curves of genus ≥ 2, were obtained in [Sil87], [Sil93], [Kul99], [Sto01]. These articles consider families of twists of certain fixed curves of genus ≥ 2 and a family of curves defined by a Thue's equation.

In this article we obtain uniform upper bounds on the number of $\mathbb{Q}$–rational points of the (non–isotrivial) family of plane curves $\{\mathcal{C}_t\}_{t\in\mathbb{Q}}$ of equation

$$y^2 = x^6 + tx^4 + tx^2 + 1.$$

By means of a direct computation of the invariants of the curve $\mathcal{C}_t$ we see that for all but finitely many pairs $(t,u) \in \mathbb{Q}^2$ with $t \neq u$ the curves $\mathcal{C}_t$ and $\mathcal{C}_u$ are isomorphic over $\mathbb{C}$ if and only if $u = \frac{15-t}{1+t}$ holds. Furthermore, this isomorphism is $\mathbb{Q}$–definable if and only if $2+2t$ is a square in $\mathbb{Q}$. This implies that the family of curves $\{\mathcal{C}_t\}_{t\in\mathbb{Q}}$ contains infinitely many non–$\mathbb{Q}$–isomorphic curves.

Let us observe that the family of curves $\{\mathcal{C}_t\}_{t\in\overline{\mathbb{Q}}}$ may be intrinsically defined in the following terms: it is (up to $\overline{\mathbb{Q}}$–isomorphism) the only family of genus–2 curves with two independent degree–2 morphisms to a family of elliptic curves with a distinguished rational 2–torsion point.

Indeed, following e.g. [CF96] we see that any $\overline{\mathbb{Q}}$–definable genus–2 curve with a degree–2 morphism to an elliptic curve is isomorphic to a curve $\mathcal{C}_{\alpha,\beta}$ of equation $y^2 = x^6 + \alpha x^4 + \beta x^2 + 1$ for suitable $\alpha, \beta \in \overline{\mathbb{Q}}$. This implies that the curve $\mathcal{C}_{\alpha,\beta}$ admits two independent degree–2 morphisms to the elliptic curves of equations $y^2 = x^3 + \alpha x^2 + \beta x + 1$ and $y^2 = x^3 + \beta x^2 + \alpha x + 1$. Let $\lambda \in \overline{\mathbb{Q}}$ be such that $\lambda^2 + \lambda + 1 = 0$. Then the above elliptic curves have the same j–invariant if and only if one of the following conditions hold: (i) $\beta = \alpha$; (ii) $\beta = -\alpha - 3$; (iii) $\beta = \lambda\alpha$ or $\beta = -(\lambda+1)\alpha$; (iv) $\beta = -\lambda\alpha + 3(\lambda+1)$ or $\beta = (\lambda+1)\alpha - 3\lambda$.

A direct computation shows that the unidimensional family of curves $\{\mathcal{C}_{\alpha,\beta}\}_{\alpha\in\overline{\mathbb{Q}}}$ corresponding to the cases (iii) and (iv) is $\overline{\mathbb{Q}}$–isomorphic to one of the families corresponding to the cases (i) and (ii). On the other hand, the family of curves corresponding to the case (ii) is mapped into the families of elliptic curves $\{\mathcal{E}_{\alpha,1}\}_{\alpha\in\overline{\mathbb{Q}}}, \{\mathcal{E}_{\alpha,2}\}_{\alpha\in\overline{\mathbb{Q}}}$ of equation $y^2 = x^3 + \alpha x^2 + \alpha x + 1$ and $y^2 = x^3 + \alpha x^2 - (\alpha+3)x + 1$ respectively. Since $\mathcal{E}_{\alpha,2}$ does not have any 2–torsion point defined over $\overline{\mathbb{Q}}(\alpha)$ we conclude that the family $\{\mathcal{C}_t\}_{t\in\overline{\mathbb{Q}}}$, which corresponds to the case (i), is characterized by the property of having two independent degree–2 morphism to one family of elliptic curves with a distinguished rational 2–torsion point.

Let T denote an indeterminate over $\mathbb{Q}$, let $\mathbb{Q}(T)$ and $\overline{\mathbb{Q}}(T)$ denote the field of rational functions in the variable T with coefficients in $\mathbb{Q}$ and $\overline{\mathbb{Q}}$ respectively and let $\overline{\mathbb{Q}(T)}$ denote the algebraic closure of $\mathbb{Q}(T)$. First we analyze the arithmetic behaviour of the plane curve $\mathcal{C}$ defined over $\mathbb{Q}(T)$ of equation $y^2 = x^6 + Tx^4 + Tx^2 + 1$. Our methods rely on the observation that the (independent) morphisms ϕ_1, ϕ_2 defined by

$$\phi_1(x,y) := (x^2, y), \quad \phi_2(x,y) := \left(\frac{1}{x^2}, \frac{y}{x^3}\right),$$

map the curve $\mathcal{C}$ into the elliptic curve $\mathcal{E}$ defined over $\mathbb{Q}(T)$ of equation $y^2 = x^3 + Tx^2 + Tx + 1$. We first characterize the structure of the group of $\mathbb{Q}(T)$–rational points of $\mathcal{E}$ applying Shioda's theory of Mordell–Weil lattices. Then, using a variant of Dem'janenko–Manin's method [Dem68, Man69] to find the set of rational points of a given plane curve, we obtain the following result:

Theorem 2 $\mathcal{C}\big(\mathbb{Q}(T)\big) = \{(0,1), (0,-1)\}$.

Then for a given value $t \in \mathbb{Q}$ we analyze the arithmetic behaviour of the curve $\mathcal{C}_t$ using Dem'janenko–Manin's method. For this purpose, we observe that the restriction $\phi_1|_{\mathcal{C}\cap\overline{\mathbb{Q}}^2}, \phi_2|_{\mathcal{C}\cap\overline{\mathbb{Q}}^2}$ of the morphisms ϕ_1, ϕ_2 defined above map the curve $\mathcal{C}_t$ into the elliptic curve $\mathcal{E}_t$ defined over $\mathbb{Q}$ of equation

$$y^2 = x^3 + tx^2 + tx + 1.$$

For any value $t \in \mathbb{Q}$ such that the abelian group $\mathcal{E}_t(\mathbb{Q})$ of $\mathbb{Q}$–rational points of the elliptic curve $\mathcal{E}_t$ has rank 1 and its free part is generated by the point $(0,1)$, we determine the set $\mathcal{C}_t(\mathbb{Q})$ of $\mathbb{Q}$–rational points of the curve $\mathcal{C}_t$. We prove the following result:

Theorem 3 *Let $\mathcal{P} \subset \mathbb{Q}$ denote the set of all $t \in \mathbb{Q}$ such that the abelian group $\mathcal{E}_t(\mathbb{Q})$ has rank 1 and its free part is generated by the point $(0,1)$. Then the following statements hold for all but finitely many $t \in \mathcal{P}$:*

(i) If there exists $v \in \mathbb{Q}$ such that $t = -(v^4 - v^2 + 1)/v^2$ holds, then

$$\mathcal{C}_t(\mathbb{Q}) = \left\{(0,1), (0,-1), (v,0), (-v,0), \Big(\frac{1}{v}, 0\Big), \Big(-\frac{1}{v}, 0\Big)\right\}.$$

(ii) Otherwise, we have

$$\mathcal{C}_t(\mathbb{Q}) = \{(0,1), (0,-1)\}.$$

Let h and $\widehat{h}$ denote the naive (logarithmic) height on $\mathbb{Q}$ and the canonical height on a given elliptic curve $\widetilde{\mathcal{E}}$ defined over $\mathbb{Q}$ respectively (see the next section for precise definitions). Then the statement of Theorem 3 can be significantly improved for values $t \in \mathbb{N}$ assuming that the following conjecture of S. Lang holds [Lan78]:

Conjecture B *There exists a universal constant $c > 0$ such that for any elliptic curve $\widetilde{\mathcal{E}}$ defined over $\mathbb{Q}$ of discriminant Δ and any nontorsion point $P \in \widetilde{\mathcal{E}}(\mathbb{Q})$, the estimate $\widehat{h}(P) > c \cdot h(\Delta)$ holds.*

Let us observe that Conjecture B has been proved for elliptic curves with integral j–invariant [Sil94]. Furthermore, [HS88] shows that the *abc*–conjecture implies Conjecture B.

Under the assumption of the validity of Conjecture B we have the following result, which shows that the condition that $(0, 1)$ is a generator of the free part of the group $\mathcal{E}_t(\mathbb{Q})$ is not essential for $t \in \mathbb{N}$:

Theorem 4 *If Conjecture B is true there exists a universal constant $C > 0$ with the following property: for any $t \in \mathbb{N}$ such that the abelian group $\mathcal{E}_t(\mathbb{Q})$ has rank 1, the cardinality of the set $\mathcal{C}_t(\mathbb{Q})$ is bounded by C.*

Finally, let us observe that the validity of the statement of Theorems 3 and 4 depends on either or both of the following conditions on the parameter $t \in \mathbb{Q}$:

1. The rank of the abelian group $\mathcal{E}_t(\mathbb{Q})$ is 1.
2. (0,1) is a generator of the free part of $\mathcal{E}_t(\mathbb{Q})$.

In Section 5 we discuss how restrictive these conditions on the parameter $t \in \mathbb{Q}$ are. Theorem 4 shows that our uniform upper bound on the cardinality of the set $\mathcal{C}_t(\mathbb{Q})$ does not depend on condition 2 if Conjecture B holds. We exhibit statistical results which seem to show that condition 1 holds with a probability of success of approximately $1/3$. Furthermore, let $\mathcal{Q}$ be the set of values $t \in \mathbb{Q}$ for which $\mathcal{E}_t(\mathbb{Q})$ has rank 1. Our experimental results seem to show that the set of values $t \in \mathcal{Q}$ for which (0,1) is a generator of the free part of $\mathcal{E}_t(\mathbb{Q})$ has density 1 in $\mathcal{Q}$.

The results of this article required an important computational effort. The experimental results presented in Section 5 were done using J. Cremona's software `mwrank` [Cre] and took about two months of CPU time on a 1Ghz PC. All the other symbolic computations were done using the `Magma` computer algebra system [Mag]. All software and hardware resources were provided by the French computation center MEDICIS [MED].

2 Basic Notions and Results

In this section we fix notations and recall some standard notions and results about elliptic curves, heights and morphisms. Details can be found in [Kna92], [Sil86] and [Sil94].

Let K denote any of the fields $\mathbb{Q}$ or $\mathbb{Q}(T)$ and let $\mathcal{O}_K$ denote its ring of integers i.e. $\mathbb{Z}$ or $\mathbb{Q}[T]$ respectively. For $x = x_1/x_2 \in K$ with $x_1 \in \mathcal{O}_K$, $x_2 \in \mathcal{O}_K^*$ and $\gcd(x_1, x_2) = 1$, we denote by $h(x)$ the (naive) height of x, namely $h(x) := \log(\max\{|x_1|, |x_2|\})$ if $K = \mathbb{Q}$ and $h(x) := \max\{\deg(x_1), \deg(x_2)\}$ if $K = \mathbb{Q}(T)$.

For a given algebraic curve $\mathcal{C}$ defined over K we denote by $\mathcal{C}(K)$ the set of points of the curve $\mathcal{C}$ whose coordinates lie in K.

Let $\mathcal{C}$ be the K–definable affine (hyperelliptic) curve of $\mathbb{A}^2(\overline{K})$ of equation $y^2 = f(x)$, where $f \in K[x]$ is a square–free polynomial of degree at least 3. For any point $P = \big(x(P), y(P)\big) \in \mathcal{C}(K)$ we define the (naive) height $h(P)$ of P as $h(P) := h\big(x(P)\big)$. Further, if $P \in \mathbb{P}^2(\overline{K})$ is the point of $\mathcal{C}$ at infinity we define $h(P) := 0$.

Let $\mathcal{E}$ be an elliptic curve defined over K and let $[n]$ denote the morphism of multiplication by n in $\mathcal{E}$ for any $n \in \mathbb{Z} \setminus \{0\}$. For any point $P \in \mathcal{E}(K)$ we denote by $\widehat{h}(P)$ the canonical height of P, namely $\widehat{h}(P) := \lim_{n\to\infty} 4^{-n} h([2^n]P)$. For $P, Q \in \mathcal{E}(\overline{K})$ let $\langle P, Q\rangle$ denote the Néron–Tate pairing, namely $\langle P, Q\rangle := \frac{1}{2}\big(\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)\big)$. Let us recall that $\langle\ ,\ \rangle$ induces a positive–definite bilinear form on $\mathcal{E}(K)/\mathcal{E}(K)_{\mathrm{tors}}$, where $\mathcal{E}(K)_{\mathrm{tors}}$ denote the set of K–rational points of torsion of $\mathcal{E}$.

It is well–known (see e.g. [Sil86, Theorem 9.3]) that the difference between the canonical and the naive height is uniformly bounded on any given elliptic curve $\mathcal{E}$ defined over K, i.e. there exists a universal constant $c_{\mathcal{E}} > 0$, depending only on the elliptic curve $\mathcal{E}$, such that the estimate

$$|\widehat{h}(P) - h(P)| < c_{\mathcal{E}} \tag{1}$$

holds for any $P \in \mathcal{E}(K)$. The following result will allow us to make the constant $c_{\mathcal{E}}$ explicit (see e.g. [Kna92]):

Lemma 1 *Let $\mathcal{E}$ be an elliptic curve defined over K and let $c_{\mathcal{E}} > 0$ be a constant satisfying the inequality $|h([2]P) - 4h(P)| \leq c_{\mathcal{E}}$ for any point $P \in \mathcal{E}(K)$. Then the inequality $|\widehat{h}(P) - h(P)| \leq c_{\mathcal{E}}/3$ holds for any point $P \in \mathcal{E}(K)$.*

3 Points over $\mathbb{Q}(T)$

This section is devoted to the proof of Theorem 2, which determines the set of $\mathbb{Q}(T)$–rational points of the genus–2 curve $\mathcal{C}$ of equation $y^2 = x^6 + Tx^4 + Tx^2 + 1$.

As expressed in the introduction, there are two $\mathbb{Q}(T)$–definable morphisms $\phi_1, \phi_2 : \mathcal{C} \to \mathcal{E}$ mapping this curve to the elliptic curve $\mathcal{E}$ defined over $\mathbb{Q}(T)$ of equation $y^2 = x^3 + Tx^2 + Tx + 1$. In order to determine the set $\mathcal{C}\big(\mathbb{Q}(T)\big)$ we first determine the structure of the group $\mathcal{E}\big(\mathbb{Q}(T)\big)$.

3.1 The structure of $\mathcal{E}$ over $\mathbb{Q}(T)$

In order to analyze the group $\mathcal{E}\big(\mathbb{Q}(T)\big)$ we need an explicit upper bound of the difference between the canonical and naive height on $\mathcal{E}$. Our next result yields such an upper bound for a short Weierstrass form of $\mathcal{E}$.

More precisely, making the change of variable $x' = x + T/3$ we transform the elliptic curve $\mathcal{E}$ into the elliptic curve $\mathcal{E}'$ defined over $\mathbb{Q}(T)$ of equation $y^2 = x'^3 + a'x' + b'$, where $a' := -1/3T(T-3)$ and $b' := 1/27(2T+3)(T-3)^2$. Then we have the following result:

Lemma 2 *Let notations and assumptions be as above. Then for any rational point $P \in \mathcal{E}'(\mathbb{Q}(T))$ the inequality $|\widehat{h}(P) - h(P)| \leq 3/4$ holds.*

Proof.– Following [ZS01], let $\mathcal{M}_{\mathbb{Q}(T)}$ denote the usual set of all non–equivalent absolute values over $\mathbb{Q}(T)$, namely the set of all the absolute values $v_\mathfrak{p} := -\log|\ |_\mathfrak{p}$, where either $\mathfrak{p} = \infty$ and $|F|_\mathfrak{p} := e^{\deg(F)}$, or $\mathfrak{p}$ runs over the set of all monic prime elements of $\mathbb{Q}[T]$, and $|F|_\mathfrak{p} := e^{-\mathrm{ord}_\mathfrak{p}(F)}$ denotes the standard $\mathfrak{p}$–adic valuation. For any such absolute value v, let

$$\mu_v := \min\{\tfrac{1}{2}v(a'), \tfrac{1}{3}v(b')\}, \qquad \mu := -\sum_{v\in\mathcal{M}_{\mathbb{Q}(T)}} \mu_v,$$
$$\mu_l := \frac{1}{2}\sum_{v\in\mathcal{M}_{\mathbb{Q}(T)}} \min\{0, \mu_v\}, \qquad \mu_u := \frac{1}{2}\sum_{v\in\mathcal{M}_{\mathbb{Q}(T)}} \max\{0, \mu_v\}.$$

Then [ZS01, Theorem and Proposition 4] shows that $-\mu - \mu_u \leq \widehat{h}(P) - h(P) \leq -\mu_l$ holds for any $P \in \mathcal{E}'(\mathbb{Q}(T))$.

In our case, the only nonzero values of μ_v are obtained at $\mathfrak{p} = \infty$ and $\mathfrak{p} = T - 3$, namely $\mu_\infty = -1$ and $\mu_{T-3} = 1/2$. This shows that $\mu = 1/2$, $\mu_l = -1/2$ and $\mu_u = 1/4$ hold, and then $-3/4 \leq \widehat{h}(P) - h(P) \leq 1/2$. This proves the lemma. ∎

Now we determine the structure of the group of $\mathbb{Q}(T)$–rational points of the elliptic curve $\mathcal{E}$. For this purpose, we are going to apply Shioda's theory of Mordell–Weil lattices of elliptic surfaces (cf. [Shi90, OS91, Shi91]), which actually allows us to describe the larger group $\mathcal{E}(\overline{\mathbb{Q}}(T))$.

Following [Shi90], associated to the elliptic curve $\mathcal{E}$ we have an elliptic surface $f : S \to \mathbb{P}^1(\overline{\mathbb{Q}})$ (the Kodaira–Néron model of $\mathcal{E}/\overline{\mathbb{Q}}(T)$) whose generic fiber is $\mathcal{E}$. For a given $v \in \mathbb{P}^1(\overline{\mathbb{Q}})$ let $F_v := f^{-1}(v)$ denote the fiber over v, and let R denote the set of reducible fibers F_v. For any $v \in R$, let

$$F_v = \Theta_{v,0} + \sum_{i=1}^{m_v-1} \mu_{v,i}\Theta_{v,i},$$

where $\Theta_{v,i}$ $(0 \leq i \leq m_v - 1)$ are the irreducible components of F_v occurring with multiplicity $\mu_{v,i}$ and $\Theta_{v,0}$ is the unique component meeting the zero section.

The global sections of S can be naturally identified with the points of $\mathcal{E}(\overline{\mathbb{Q}}(T))$, namely a given section $s : \mathbb{P}^1(\overline{\mathbb{Q}}) \to S$ is identified with its restriction to the generic fiber $\mathcal{E}$, which is a $\overline{\mathbb{Q}}(T)$–rational point of $\mathcal{E}$. For a given point $P \in \mathcal{E}(\overline{\mathbb{Q}}(T))$ let (P) denote the prime divisor which is the image of the section $P : \mathbb{P}^1(\overline{\mathbb{Q}}) \to S$. With this identification Shioda shows that $\mathcal{E}(\overline{\mathbb{Q}}(T))$ is isomorphic to $NS(S)/T$, where $NS(S)$ denotes the Néron–Severi group of S (the group of divisors of S modulo algebraic equivalence) and T denotes the subgroup of $NS(S)$ generated by the zero section (O) and all the irreducible components of fibers. In [OS91] there is a complete classification of the possible structures of the group $\mathcal{E}(\overline{\mathbb{Q}}(T))$ in terms of the root lattices associated with the reducible fibers F_v.

There exists a height pairing $\langle\ ,\ \rangle : \mathcal{E}\big(\overline{\mathbb{Q}}(T)\big) \times \mathcal{E}\big(\overline{\mathbb{Q}}(T)\big) \to \mathbb{Q}$, which is obtained by embedding $\mathcal{E}\big(\overline{\mathbb{Q}}(T)\big)$ into $NS(S) \otimes \mathbb{Q}$. Let us denote by ϕ this embedding. Then we have $\ker \phi = \mathcal{E}\big(\overline{\mathbb{Q}}(T)\big)_{\text{tors}}$, and using the intersection number as a pairing in $NS(S)$ the height pairing is defined by $\langle P, Q\rangle := -\big(\phi(P), \phi(Q)\big)$. In case that the elliptic surface is rational we have

$$\langle P, P\rangle = 2 + \big((P), O\big) - \sum_{v \in R} \mathrm{contr}_v(P), \tag{2}$$

where the possible terms $\mathrm{contr}_v(P)$ are described in [Shi90] in terms of the root lattice associated to the fiber F_v.

Proposition 1 *The rank of the abelian group $\mathcal{E}\big(\overline{\mathbb{Q}}(T)\big)$ is one and its free part is generated by the point $G := (0, 1)$.*

Proof.– Let us observe that the singular fibers of S are given at $v = -1, 3, \infty$. By applying Tate's algorithm for the determination of the reduction types of the fiber F_v (see [Tat75, Sil94]) we see that the special fibers at $v = -1, 3, \infty$ are of type I_1, III, I_2^* respectively. This implies $m_{-1} = 1$, $m_3 = 2$ and $m_\infty = 7$ respectively. Therefore, only $v = 3, \infty$ correspond to reducible fibers. Applying the classification of [OS91] we conclude that $\mathcal{E}\big(\overline{\mathbb{Q}}(T)\big) \cong A_1^* \oplus \mathbb{Z}/2\mathbb{Z}$ holds, i.e. $\mathcal{E}\big(\overline{\mathbb{Q}}(T)\big)$ has rank 1 and $\mathcal{E}\big(\overline{\mathbb{Q}}(T)\big)_{\text{tors}} = \mathbb{Z}/2\mathbb{Z}$.

Since $(-1, 0)$ is a nontrivial torsion point of $\mathcal{E}\big(\overline{\mathbb{Q}}(T)\big)$ we conclude that $\mathcal{E}\big(\overline{\mathbb{Q}}(T)\big)_{\text{tors}} = \langle(-1, 0)\rangle$ holds.

Let us observe that the elliptic surface associated to the elliptic curve $\mathcal{E}$ is rational. Therefore, [Shi90, Theorems 10.8 and 10.10] shows that the group $\mathcal{E}\big(\overline{\mathbb{Q}}(T)\big)$ is generated by the points $P = \big(x(P), y(P)\big)$ satisfying $\big((P), O\big) = 0$, and hence of the form $x(P) = gT^2 + aT + b$, $y(P) = hT^3 + cT^2 + dT + e$.

From [Shi90, Lemma 5.1] we see that A_1^* has a basis consisting of a vector P of (minimal) norm $\langle P, P\rangle = 1/2$. Taking into account that $\mathrm{contr}_\infty(P) \in \{0, 1, 3/2\}$ and $\mathrm{contr}_3(P) \in \{0, 1/2\}$ holds (see [Shi90]), from formula (2) we conclude that $\mathrm{contr}_\infty(P) \neq 0$ holds. Arguing as in [Shi91a] we see that this implies that P must intersect the singular fiber F_∞ (which is a cusp) at the singular point, namely at $(0, 0)$. We conclude that $g = h = 0$ holds.

Replacing $x(P) = aT + b$ in the right–hand term of the equation defining the elliptic curve $\mathcal{E}$ we see that the term $p_{a,b}(T) := (aT+b)^3 + T(aT+b)^2 + T(aT+b) + 1$ is not a square in $\overline{\mathbb{Q}}[T]$ for $a \neq 0$ because it has odd degree. Hence we have $a = 0$. Furthermore, for $b \neq 0, -1$ the polynomial $p_{0,b}(T) = T(b^2 + b) + b^3 + 1$ is not a square. Since $b = -1$ yields a torsion point we conclude that $a = b = 0$ is the only possible choice for $x(P)$. This shows that $G = (0, \pm 1)$ is a generator of the free part of $\mathcal{E}(\overline{\mathbb{Q}}(T))$. ∎

3.2 The structure of $\mathcal{C}$ over $\mathbb{Q}(T)$: Proof of Theorem 2

In this section we prove the following result:

Theorem 2 *Let $\mathcal{C}$ be the genus–2 plane curve $\mathcal{C}$ defined over $\mathbb{Q}(T)$ of equation $y^2 = x^6 + Tx^4 + Tx^2 + 1$. Then we have $\mathcal{C}\big(\mathbb{Q}(T)\big) = \{(0,1),(0,-1)\}$.*

For this purpose we are going to use a simplified version [Kul99] of the Dem'janenko–Manin's method [Dem68, Man69] for computing the set of rational points of a given genus–2 curve.

Proof.– Let us recall that we have two morphisms $\phi_1, \phi_2 : \mathcal{C} \to \mathcal{E}$ mapping the curve $\mathcal{C}$ into the elliptic curve $\mathcal{E}$, namely $\phi_1(x,y) := (x^2, y)$ and $\phi_2(x,y) := (1/x^2, y/x^3)$.

As in the proof of Lemma 2 we make the change of variable $x' = x + T/3$, which transforms the elliptic curve $\mathcal{E}$ into the elliptic curve $\mathcal{E}'$ of equation $y^2 = x'^3 + a'x' + b'$, where $a' := -1/3T(T-3)$ and $b' := 1/27(2T+3)(T-3)^2$. We denote by $\mathcal{C}'$ the genus–2 curve defined over $\mathbb{Q}(T)$ obtained from $\mathcal{C}$ under this change of variables and denote by $\phi_1', \phi_2' : \mathcal{C}' \to \mathcal{E}'$ the corresponding morphisms, namely

$$\begin{aligned} \phi_1'(x',y) &:= ((x'-T/3)^2 + T/3, y), \\ \phi_2'(x',y) &:= \big((x'-T/3)^{-2} + T/3, y(x'-T/3)^{-3}\big). \end{aligned}$$

We claim that for any $P \in \mathcal{C}'\big(\mathbb{Q}(T)\big)$ the following inequality holds:

$$|h(\phi_1'(P)) - h(\phi_2'(P))| \leq 1. \tag{3}$$

Indeed, let P be an arbitrary element of $\mathcal{C}'\big(\mathbb{Q}(T)\big)$ and let $x'(P) = N/D$ be a reduced representation of $x'(P)$. Then the abscissa of $\phi_1'(P)$ is $((3N-DT)^2 + 3TD^2)/(9D^2)$. Observe that $\big((3N-DT)^2+3TD^2\big)/(9D^2)$ is a reduced fraction and hence $h(\phi_1'(P)) = \max\{\deg((3N-DT)^2 + 3TD^2), \deg(9D^2)\}$ holds. Since the leading coefficients of $(3N-DT)^2$ and $3TD^2$ are positive rationals we conclude that $\deg\big((3N-DT)^2+3TD^2\big) = \max\{\deg\big((3N-DT)^2\big), \deg(3TD^2)\} > \deg(9D^2)$ holds and then $h\big(\phi_1'(P)\big) = \max\{\deg\big((3N-DT)^2\big), \deg(3TD^2)\}$. Similarly, we see that the abscissa of $\phi_2'(P)$ is $(27D^2 + T(3N-DT)^2)/(3(3N-DT)^2)$ and $h\big(\phi_2'(P)\big) = \max\{\deg(27D^2), \deg\big(T(3N-DT)^2\big)\}$ holds.

Let $a := \deg(D)$, $b := \deg(3N-DT)$. Then we have $h(\phi_1'(P)) = \max\{2a+1, 2b\}$ and $h(\phi_2'(P)) = \max\{2a, 2b+1\}$, which immediately implies estimate (3). This completes the proof of our claim.

Proposition 1 asserts that the abelian group $\mathcal{E}'\big(\mathbb{Q}(T)\big)$ has rank 1 and $G' := (T/3, 1)$ is a generator of its free part. Then for any point $P \in \mathcal{C}'\big(\mathbb{Q}(T)\big)$ there exist integers n, m and points $\mathcal{T}_1, \mathcal{T}_2 \in \mathcal{E}'\big(\mathbb{Q}(T)\big)_{\text{tors}}$ satisfying the identities $\phi_1'(P) = [n]G' + \mathcal{T}_1$ and $\phi_2'(P) = [m]G' + \mathcal{T}_2$. Then we have

$$\widehat{h}(\phi_1'(P)) = n^2\widehat{h}(G'), \quad \widehat{h}(\phi_2'(P)) = m^2\widehat{h}(G'). \tag{4}$$

Hence, combining identity (3) and Lemma 2 we obtain the following estimate:

$$\begin{aligned} |\widehat{h}\big(\phi_1'(P)\big) - \widehat{h}\big(\phi_2'(P)\big)| &\leq |\widehat{h}\big(\phi_1'(P)\big) - h\big(\phi_1'(P)\big)| + |\widehat{h}\big(\phi_2'(P)\big) - h\big(\phi_2'(P)\big)| \\ &\quad + |h\big(\phi_1'(P)\big) - h\big(\phi_2'(P)\big)| \\ &\leq 2 \cdot 3/4 + 1 = 5/2. \end{aligned} \tag{5}$$

Let us suppose first that $\phi_1'(P) \pm \phi_2'(P) \notin \mathcal{E}'\big(\mathbb{Q}(T)\big)_{\text{tors}}$ holds. Then $m^2 - n^2 \neq 0$ and equations (4) and (5) imply $\widehat{h}(G')|m^2 - n^2| < 5/2$. Taking into account that $h([5]G') = 15$ holds, from Lemma 2 we obtain the estimate $\widehat{h}(G') \geq 1/2$. Therefore, we have $\min\{|n|, |m|\} < 5/2$ and hence

$$n, m \in \{0, \pm 1, \pm 2\}. \tag{6}$$

A direct computation shows that the only $\mathbb{Q}(T)$–rational points of $\mathcal{C}'$ satisfying the condition $\phi_1'(P) \pm \phi_2'(P) \notin \mathcal{E}'\big(\mathbb{Q}(T)\big)_{\text{tors}}$ are $\{(T/3, 1), (T/3, -1)\}$. We conclude that the only $\mathbb{Q}(T)$–rational points of $\mathcal{C}$ satisfying the condition $\phi_1(P) \pm \phi_2(P) \notin \mathcal{E}\big(\mathbb{Q}(T)\big)_{\text{tors}}$ are $\{(0, 1), (0, -1)\}$.

On the other hand, suppose now that $\phi_1(P) \pm \phi_2(P) \in \mathcal{E}\big(\mathbb{Q}(T)\big)_{\text{tors}} = \{\mathcal{O}_{\mathcal{E}}, (-1, 0)\}$ is satisfied, where $\mathcal{O}_{\mathcal{E}}$ denotes the zero element of the group $\mathcal{E}\big(\mathbb{Q}(T)\big)$. We have that $(\phi_1 + \phi_2)(x, y) = \big(f_+(x), yg_+(x)\big)$ and $(\phi_1 - \phi_2)(x, y) = \big(f_-(x), yg_-(x)\big)$, where

$$f_+(x) = \frac{-2x^3 - 3x^2 - 2x + Tx^2}{(x^4 + 2x^3 + 2x^2 + 2x + 1)}, \quad f_-(x) = \frac{2x^3 - 3x^2 + 2x + Tx^2}{(x^4 - 2x^3 + 2x^2 - 2x + 1)}.$$

From the expression of f_+ and f_- we easily conclude that there do not exist points $P \in \mathcal{C}\big(\mathbb{Q}(T)\big)$ for which $\phi_1(P) \pm \phi_2(P) \in \{\mathcal{O}_{\mathcal{E}}, (-1, 0)\}$ holds. Therefore, the image of the morphisms ϕ_1, ϕ_2 is contained in the set $\{(0, 1), (0, -1)\}$. In particular we see that $x(P) = 0$ holds for any point $P \in \mathcal{C}\big(\mathbb{Q}(T)\big)$. This shows that $\mathcal{C}\big(\mathbb{Q}(T)\big) = \{(0, 1), (0, -1)\}$ and completes the proof of Theorem 2. ∎

4 Points over $\mathbb{Q}$

Let $t \in \mathbb{Q}$ and let $\mathcal{C}_t$ be the curve of equation $y^2 = x^6 + tx^4 + tx^2 + 1$. The purpose of this section is to analyze the arithmetic structure of the curve $\mathcal{C}_t$. For this purpose we first determine the arithmetic structure of the elliptic curve $\mathcal{E}_t$ of equation $y^2 = x^3 + tx^2 + tx + 1$.

4.1 Explicit bounds

In this section we obtain an explicit upper bound on the height $h(P)$ of any point $P \in \mathcal{E}_t(\mathbb{Q})$ in terms of the height of t. For this purpose, we first obtain an explicit upper bound on the difference between the naive and the canonical height on $\mathcal{E}_t$.

Let us observe that general estimates on the difference between the naive and the canonical height were already given in e.g. [Sil90] and [ZS01]. Nevertheless the following explicit estimate gives better bounds in this case, which allows us to significantly reduce the subsequent computational effort.

Lemma 3 *Let $t \in \mathbb{Q}$. Then for any $\mathbb{Q}$–rational point P of the elliptic curve $\mathcal{E}_t$ the following estimate holds:*

$$|\widehat{h}(P) - h(P)| \leq \frac{5h(t) + \log(1314)}{3}.$$

Proof.– Let $t := b/a$ and let P be a point of $\mathcal{E}_{b/a}(\mathbb{Q})$. Let us suppose first that P is not a 2–torsion point. This implies that $x(P)$ does not cancel the 2–division polynomial $x^3 + (b/a)x^2 + (b/a)x + 1$. Then the x–coordinate of the point $[2]P$ is given by the expression

$$x([2]P) = \frac{a^2x(P)^4 - 2abx(P)^2 - 8a^2x(P) - 4ab + b^2}{4a\big(ax(P)^3 + bx(P)^2 + bx(P) + a\big)}. \tag{7}$$

Let us write $x(P) := p/q$, where p and q are coprime integers. Then we have $h\big(P\big) = \max\{\log|p|, \log|q|\}$. Rewriting the identity (7) in terms of p and q we obtain

$$x([2]P) = \frac{a^2p^4 - 2abp^2q^2 - 8a^2pq^3 + (b^2 - 4ab)q^4}{4qa(ap^3 + bp^2q + bpq^2 + aq^3)}.$$

Let $N := a^2p^4 - 2abp^2q^2 - 8a^2pq^3 + (b^2 - 4ab)q^4$ and $D := 4qa(ap^3 + bp^2q + bpq^2 + aq^3)$ denote the numerator and denominator of the above expression. Then we have the estimates

$$\begin{aligned}
|N| &\leq (|a|^2 + 2|ab| + 8|a|^2 + |b^2 - 4ab|)\max\{|p|, |q|\}^4\\
&\leq 16\max\{|a|, |b|\}^2\max\{|p|, |q|\}^4,\\
|D| &\leq 4(|a|^2 + |ba| + |ba| + |a|^2)\max\{|p|, |q|\}^4\\
&\leq 16\max\{|a|, |b|\}^2\max\{|p|, |q|\}^4.
\end{aligned}$$

This yields

$$h\big(x([2]P)\big) \leq 4h\big(x(P)\big) + 2\max\{\log|a|, \log|b|\} + \log 16. \tag{8}$$

Following the proof of [Kna92, Proposition 4.12], let C_N, C_D, C'_N, C'_D be integers of minimal height satisfying the Bézout identities

$$C_NN + C_DD = Ca^3p^7, \quad C'_NN + C'_DD = Cq^7, \tag{9}$$

where $C := 108a^4 - 72a^2b^2 + 32ab^3 - 4b^4$. By a direct computation we obtain the following estimates:

$$\begin{aligned}
|C_N| &\leq 664\max\{|a|, |b|\}^5\max\{|p|, |q|\}^3,\\
|C_D| &\leq 650\max\{|a|, |b|\}^5\max\{|p|, |q|\}^3,\\
|C'_N| &\leq 40\max\{|a|, |b|\}^2\max\{|p|, |q|\}^3,\\
|C'_D| &\leq 38\max\{|a|, |b|\}^2\max\{|p|, |q|\}^3.
\end{aligned}$$

This implies

$$|p|^7 \leq \frac{1314\max\{|a|, |b|\}^5\max\{|p|, |q|\}^3\max\{|N|, |D|\}}{|C||a^3|}, \tag{10}$$

$$|q|^7 \leq \frac{78\max\{|a|, |b|\}^2\max\{|p|, |q|\}^3\max\{|N|, |D|\}}{|C|}. \tag{11}$$

Now we are going to express these estimates in terms of the height of N/D. Let g be the gcd of N and D. Then (9) shows that g divides Ca^3p^7 and Cq^7, i.e. g divides Ca^3. Let $n := N/g$ and $d := D/g$. Then we have

$$N = ng \leq nCa^3, \quad D = dg \leq dCa^3.$$

Combining these estimates with inequalities (10) and (11) we obtain

$$\begin{array}{rcl} |p|^7 & \leq & 1314 \max\{|a|,|b|\}^5 \max\{|p|,|q|\}^3 \max\{|n|,|d|\}, \\ |q|^7 & \leq & 78 \max\{|a|,|b|\}^5 \max\{|p|,|q|\}^3 \max\{|n|,|d|\}, \\ \max\{|p|^7,|q|^7\} & \leq & 1314 \max\{|a|,|b|\}^5 \max\{|p|,|q|\}^3 \max\{|n|,|d|\}. \end{array} \tag{12}$$

Since n and d are coprime, $h\big(x([2]P)\big) = h(N/D) = h(n/d) = \max\{\log|n|, \log|d|\}$. Taking logarithms in inequality (12) we obtain

$$4h\big(x(P)\big) \leq h\big(x([2]P)\big) + 5\max\{\log|a|, \log|b|\} + \log(1314).$$

Combining this estimate with inequality (8) we deduce the following estimate

$$|h([2]P) - 4h(P)| \leq 5\max\{\log|a|, \log|b|\} + \log(1314). \tag{13}$$

Let now $P \in \mathcal{E}(\mathbb{Q})$ be a 2–torsion point. Then $x(P)$ is a root of the polynomial $x^3 + (b/a)x^2 + (b/a)x + 1$. We easily conclude that $h\big(x(P)\big) \leq \max\{\log|a|, \log|b|\} + 2$. This implies that estimate (13) also holds in this case.

Finally, combining estimate (13) and Lemma 1 finishes the proof of the lemma. ∎

In order to find to set of $\mathbb{Q}$–rational points of the curve $\mathcal{C}_t$ we are going to follow Dem'janenko–Manin's method [Dem68, Man69, Cas68]. For this purpose we consider the morphisms $\phi_1, \phi_2 : \mathcal{C}_t \to \mathcal{E}_t$ defined by

$$\phi_1(x,y) := (x^2, y), \quad \phi_2(x,y) := \left(\frac{1}{x^2}, \frac{y}{x^3}\right).$$

The application of Dem'janenko –Manin's method requires an estimate on the difference $h(\phi_1(P) + \phi_2(P)) - 4h(P)$ for any $P \in \mathcal{C}_t(\mathbb{Q})$, which is the content of our next result.

Lemma 4 *With notations and assumptions as above, for any point $P \in \mathcal{C}_t(\mathbb{Q})$ the following inequality holds:*

$$|h\big(\phi_1(P) + \phi_2(P)\big) - 4h(P)| \leq 2h(t) + \log(62).$$

Proof.– Let $t := b/a$ and let $P := \big(x(P), y(P)\big)$ be a $\mathbb{Q}$–rational point of the curve $\mathcal{C}_t$. Suppose first that $x(P) = -1$. Then $\phi_1(P) = -\phi_2(P)$ and $h(P) = 0$. We conclude that the statement of Lemma 4 holds in this case.

Suppose now that $x(P) \neq -1$ holds. Then we have

$$x\big(\phi_1(P) + \phi_2(P)\big) = \frac{-2ax(P)^3 + (b-3a)x(P)^2 - 2ax(P)}{ax(P)^4 + 2ax(P)^3 + 2ax(P)^2 + 2ax(P) + a}. \tag{14}$$

Let us write $x(P) = p/q$, where p and q are coprime integers. Rewriting identity (14) in terms of p and q we obtain

$$x\big(\phi_1(P) + \phi_2(P)\big) = \frac{-2ap^3q + (b-3a)p^2q^2 - 2apq^3}{ap^4 + 2ap^3q + 2ap^2q^2 + 2apq^3 + aq^4}.$$

Let $N := -2ap^3q + (b-3a)p^2q^2 - 2apq^3$ and $D := ap^4 + 2ap^3q + 2ap^2q^2 + 2apq^3 + aq^4$. Then $x\big(\phi_1(P) + \phi_2(P)\big) = N/D$ and we have the estimates

$$\begin{aligned}
|N| &\leq (2|a| + |b-3a| + 2|a|)\max\{|p|,|q|\}^4 \\
&\leq 8\max\{|a|,|b|\}\max\{|p|,|q|\}^4, \\
|D| &\leq (|a| + 2|a| + 2|a| + 2|a| + |a|)\max\{|p|,|q|\}^4 \\
&\leq 8\max\{|a|,|b|\}\max\{|p|,|q|\}^4.
\end{aligned}$$

This implies

$$h\big(\phi_1(P) + \phi_2(P)\big) \leq 4h(P) + \max\{\log|a|, \log|b|\} + \log 8. \tag{15}$$

In order to prove the converse inequality, let C_N, C_D, C'_N, C'_D be integers of minimal height satisfying the Bézout identities:

$$C_N N + C_D D = Cp^7, \quad C'_N N + C'_D D = Cq^7,$$

where $C := 3a^3 + 2a^2b - ab^2$. By a direct computation we obtain the estimates

$$\begin{aligned}
|C_N| &\leq 28\max\{|a|,|b|\}^2\max\{|p|,|q|\}^3, \\
|C_D| &\leq 34\max\{|a|,|b|\}^2\max\{|p|,|q|\}^3, \\
|C'_N| &\leq 28\max\{|a|,|b|\}^2\max\{|p|,|q|\}^3, \\
|C'_D| &\leq 34\max\{|a|,|b|\}^2\max\{|p|,|q|\}^3.
\end{aligned}$$

Therefore we have

$$\max\{|p|^7, |q|^7\} \leq \frac{62\max\{|a|,|b|\}^2\max\{|p|,|q|\}^3\max\{|N|,|D|\}}{C}.$$

Let g be the gcd of N and D. Then g divides Cp^7 and Cq^7. Since p and q are coprime, we conclude that g divides C. Let n, d be the integers such that $N = ng$ and $D = dg$. Then we have

$$\max\{|p|^7, |q|^7\} \leq 62\max\{|a|,|b|\}^2\max\{|p|,|q|\}^3\max\{|n|,|d|\}.$$

Since n and d are coprime we see that $h\big(x\big(\phi_1(P) + \phi_2(P)\big)\big) = h(N/D) = \max\{|n|,|d|\}$ holds. Therefore, taking logarithms in the previous inequality we deduce the following estimate:

$$4h(P) \leq h\big(\phi_1(P) + \phi_2(P)\big) + 2\max\log\{|a|,|b|\} + \log(62).$$

Combining this estimate with (15) finishes the proof of the lemma. ■

Now we are ready to obtain an estimate on the height of the points of $\mathcal{C}_t(\mathbb{Q})$.

Theorem 5 *Let t be a rational number such that the elliptic curve $\mathcal{E}_t$ has rank 1 over $\mathbb{Q}$. Then for any point $P \in \mathcal{C}_t(\mathbb{Q})$ the following estimate holds:*

$$h(P) \le \frac{7h(t) + \log(81468)}{2}.$$

Proof.– Let $\phi_1, \phi_2 : \mathcal{C}_t \to \mathcal{E}_t$ be the morphisms $\phi_1(x, y) := (x^2, y)$ and $\phi_2(x, y) := (1/x^2, y/x^3)$ previously introduced. Let P be a fixed point of $\mathcal{C}_t(\mathbb{Q})$. Following the Dem'janenko–Manin's method we introduce the matrix $\widehat{H} \in \mathbb{C}^{2\times 2}$ defined in the following way:

$$\widehat{H} := \begin{pmatrix} \widehat{h}\big([2]\phi_1(P)\big) - 2\widehat{h}\big(\phi_1(P)\big) & \widehat{h}\big(\phi_1(P) + \phi_2(P)\big) - \\ & -\widehat{h}\big(\phi_1(P)\big) - \widehat{h}\big(\phi_2(P)\big) \\ \widehat{h}\big(\phi_1(P) + \phi_2(P)\big) - & \widehat{h}\big([2]\phi_2(P)\big) - 2\widehat{h}\big(\phi_2(P)\big) \\ -\widehat{h}\big(\phi_1(P)\big) - \widehat{h}\big(\phi_2(P)\big) & \end{pmatrix}.$$

Since the elliptic curve $\mathcal{E}_t$ has rank 1 we have that the points $\phi_1(P), \phi_2(P) \in \mathcal{E}_t(\mathbb{Q})$ are $\mathbb{Z}$–linear dependent. Therefore, from the positive–definiteness of the Néron–Tate pairing on $\mathcal{E}_t(\mathbb{Q})/\mathcal{E}_t(\mathbb{Q})_{\rm tors}$ we conclude that the matrix $\widehat{H}$ is singular. Let us observe that $\widehat{H}$ can be rewritten as:

$$\widehat{H} := \begin{pmatrix} 2\widehat{h}\big(\phi_1(P)\big) & \widehat{h}\big(\phi_1(P) + \phi_2(P)\big) - \\ & -\widehat{h}\big(\phi_1(P)\big) - \widehat{h}\big(\phi_2(P)\big) \\ \widehat{h}\big(\phi_1(P) + \phi_2(P)\big) - & 2\widehat{h}\big(\phi_2(P)\big) \\ -\widehat{h}\big(\phi_1(P)\big) - \widehat{h}\big(\phi_2(P)\big) & \end{pmatrix}.$$

Let $H \in \mathbb{C}^{2\times 2}$ be the following matrix:

$$H := \begin{pmatrix} 2h\big(\phi_1(P)\big) & h\big(\phi_1(P) + \phi_2(P)\big) - \\ & -h\big(\phi_1(P)\big) - h\big(\phi_2(P)\big) \\ h\big(\phi_1(P) + \phi_2(P)\big) - & 2h\big(\phi_2(P)\big) \\ -h\big(\phi_1(P)\big) - h\big(\phi_2(P)\big) & \end{pmatrix}.$$

From Lemma 3 we have the estimates:

$$\begin{aligned} |h\big(\phi_i(P)\big) - \widehat{h}\big(\phi_i(P)\big)| &< \frac{5h(t) + \log(1314)}{3}, \quad (i = 1, 2) \\ |h\big(\phi_1(P) + \phi_2(P)\big) - \widehat{h}\big(\phi_1(P) + \phi_2(P)\big)| &< \frac{5h(t) + \log(1314)}{3}. \end{aligned}$$

We conclude that the entries of the matrix $H - \widehat{H}$ are real numbers of absolute value bounded by $5h(t) + \log(1314)$.

From the definition of ϕ_1, ϕ_2 we see that $h\big(\phi_1(P)\big) = h\big(\phi_2(P)\big) = 2h(P)$ holds. We deduce that H can be expressed as $H = K + 4h(P)I$, where K is the antidiagonal matrix whose nonzero entries are $h\big(\phi_1(P)+\phi_2(P)\big)-4h(P)$ and I denotes the (2×2)–identity matrix. Applying Lemma 4 we conclude that the entries of the matrix K are real numbers of absolute value bounded by $2h(t)+\log(62)$.

Let $L := \widehat{H} - H + K$. Then the entries of L are real numbers of absolute value bounded by $7h(t)+\log(81468)$ and the matrix $\widehat{H}$ can be written as $\widehat{H} = L + 4h(P)I$.

For a given matrix $M := (m_{i,j})_{1\le i,j\le 2} \in \mathbb{C}^{2\times 2}$, let us denote by $\|M\|$ the standard ∞–matrix norm of M. We have $\|M\| \le 2\max\{|m_{i,j}| : 1\le i,j\le 2\}$. Assuming without loss of generality that $h(P)\neq 0$, we see that the matrix $(4h(P))^{-1}L + I = \big(4h(P)\big)^{-1}\widehat{H}$ is singular. This implies $\|(4h(P))^{-1}L\| \ge 1$ (see e.g. [HJ85]). Since the entries of the matrix $(4h(P))^{-1}L$ are real numbers of absolute value bounded by $(4h(P))^{-1}\big(7h(t)+\log(81468)\big)$ we deduce the estimate $h(P)\le \big(7h(t)+\log(81468)\big)/2$. ∎

From Theorem 5 we shall deduce our first uniform upper bound on the number of rational points of the family of curves $\{\mathcal{C}_t\}_{t\in\mathbb{Q}}$. For this purpose, we need the following technical result:

Lemma 5 *Let $G := (0,1)\in\mathcal{E}_t(\mathbb{Q})$. Then the following estimate holds:*

$$|h([2]G) - 2h(t)| \le \log(36).$$

Proof.– Let $t := b/a$, with $a,b\in\mathbb{Z}$ and $gcd(a,b)=1$. The x–coordinate of the point $[2]G$ is given by $x([2]G) = (-4ab+b^2)/4a^2$. Let $N := -4ab+b^2$ and $D := 4a^2$. Then we have $|N|\le 5\max\{|a|,|b|\}^2$ and $|D|\le 4\max\{|a|,|b|\}^2$, and thus

$$h([2]P) \le 2\max\{\log|a|,\log|b|\} + \log(5). \tag{16}$$

For the converse inequality, let C_N, C_D, C'_N, C'_D be integers of minimal height satisfying the Bézout identities

$$C_N N + C_D D = 4a^2, \quad C'_N N + C'_D D = b^3.$$

By a direct computation we obtain the estimates

$$4|a|^2 \le |D|, \quad |b|^3 \le (5+4)\max\{|a|,|b|\}\max\{|N|,|D|\}.$$

This implies that $\max\{|a|,|b|\}^2 \le 9\max\{|N|,|D|\}$ holds. Therefore, we have

$$2\max\{\log|a|,\log|b|\} \le \log(9) + \max\{\log|D|,\log|N|\}.$$

Let g be the gcd of N and D and let $n := N/g$, $d := D/g$. Then g divides $4a^2$ and b^3, and hence divides 4. This implies

$$2\max\{\log|a|,\log|b|\} \le \log(36) + \max\{\log|d|,\log|n|\}.$$

Since n and d are coprime, the above inequality may be rewritten as

$$2\max\{\log|a|, \log|b|\} \leq h([2]P) + \log(36).$$

Combining this estimate with estimate (16) completes the proof of the lemma. ■

Let $\mathcal{P} \subset \mathbb{Q}$ be the set of values t for which the elliptic curve $\mathcal{E}_t$ has rank 1 over $\mathbb{Q}$ and $G := (0, 1)$ is a generator of the free part of the group $\mathcal{E}_t(\mathbb{Q})$. In Section 5 we discuss in a statistical sense how many natural numbers belong to the set $\mathcal{P}$. We have the following result concerning the family of curves $\{\mathcal{C}_t\}_{t\in\mathcal{P}}$:

Corollary 1 *There exists $N \in \mathbb{N}$ such that for any $t \in \mathcal{P}$ we have*

$$\#\mathcal{C}_t(\mathbb{Q}) \leq N.$$

Proof.– Let $t \in \mathcal{P}$, let $G := (0, 1) \in \mathcal{E}_t$ and let us fix a point $P \in \mathcal{C}_t(\mathbb{Q})$. Let $\phi_1 : \mathcal{C}_t \to \mathcal{E}_t$ be the morphism defined by $\phi_1(x, y) := (x^2, y)$. Then there exists $n \in \mathbb{N}$ and $\mathcal{T} \in \mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ such that $\phi_1(P) = [n]G + \mathcal{T}$ holds. Then we have $\widehat{h}(\phi_1(P)) = n^2\widehat{h}(G)$.

First we obtain a lower bound for the quantity $\widehat{h}(G)$. From Lemma 3 we have the estimate

$$\widehat{h}([2]G) \geq h([2]G) - \frac{5}{3}h(t) - \frac{\log(1314)}{3}.$$

Lemma 5 shows that $h([2]G) \geq 2h(t) - \log(36)$ holds. Therefore, taking into account the identity $4\widehat{h}(G) = \widehat{h}([2]G)$ and the estimate $\log(61305984) < 17.94$ we obtain the lower bound

$$\widehat{h}(G) \geq \frac{h(t) - 17.94}{12}. \tag{17}$$

We now estimate the quantity $\widehat{h}\big(\phi_1(P)\big)$. On one hand, estimate (13) implies $\widehat{h}\big(\phi_1(P)\big) - h\big(\phi_1(P)\big) \leq 5h(t)/3 + \log(1314)/3$. On the other hand, Theorem 5 yields the estimate $h\big(\phi_1(P)\big) = 2h(P) \leq 7h(t) + \log(81468)$. Putting together these estimates we obtain

$$\widehat{h}(\phi_1(P)) \leq \frac{26}{3}h(t) + 13.71. \tag{18}$$

Let $t \in \mathcal{P}$ satisfy the condition $h(t) > 18.94$. Then estimate (17) implies $\widehat{h}(G)^{-1} \leq 12\big(h(t) - 17.94\big)^{-1}$, from which we deduce

$$n^2 \leq 104\,\frac{h(t) + 1.59}{h(t) - 17.94}. \tag{19}$$

Since the right–hand side of the last estimate is a bounded quantity for any $t \in \mathbb{Q}$ with $h(t) > 18.94$, we conclude that the cardinality of the set $\mathcal{C}_t(\mathbb{Q})$ is uniformly bounded in the set of values $t \in \mathcal{P}$ with $h(t) > 18.94$. On the other hand, the set of values $t \in \mathbb{Q}$ such that $h(t) \leq 18.94$ holds is finite. Hence the cardinality of the set $\mathcal{C}_t(\mathbb{Q})$ is uniformly bounded in the set of values $t \in \mathbb{Q}$ with $h(t) \leq 18.94$. This concludes the proof of the corollary. ■

Remark 1 *From (19) we easily conclude that for all but finitely many $t \in \mathcal{P}$ the estimate $n \leq 10$ holds.*

4.2 The structure of $\mathcal{C}_t(\mathbb{Q})$

In this section we prove Theorem 3, which determines the arithmetic structure of the curve $\mathcal{C}_t$ for all but finitely many values $t \in \mathcal{P}$, where $\mathcal{P}$ is the set of rational numbers t for which the elliptic curve $\mathcal{E}_t$ has rank 1 and $(0, 1)$ is a generator of the free part of the group $\mathcal{E}_t(\mathbb{Q})$.

4.2.1 The torsion subgroup of $\mathcal{E}_t(\mathbb{Q})$

In order to determine the group $\mathcal{C}_t(\mathbb{Q})$ we first describe the torsion group $\mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$. This is the subject of the following proposition.

Proposition 2 *For all but finitely many $t \in \mathbb{Q}$ the following assertions hold:*

(i) *if there exists $u \in \mathbb{Q} \setminus \{0, 1, -1\}$ such that $t = -(u^2 - u + 1)/u$ holds, then*

$$\mathcal{E}_t(\mathbb{Q})_{tors} = \left\{ \mathcal{O}_{\mathcal{E}_t}, (-1, 0), (u, 0), \left(\frac{1}{u}, 0\right) \right\},$$

all points having order 2.

(ii) *Otherwise, we have*

$$\mathcal{E}_t(\mathbb{Q})_{tors} := \{\mathcal{O}_{\mathcal{E}_t}, (-1, 0)\}.$$

Proof.– Mazur's Theorem [Maz78] asserts that the torsion subgroup of $\mathcal{E}_t(\mathbb{Q})$ is isomorphic to one of following groups:

- $\mathbb{Z}/m\mathbb{Z}$, with $1 \leq m \leq 10$ or $m = 12$;
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$, with $1 \leq m \leq 4$.

The point $P_0 := (-1, 0) \in \mathcal{E}_t(\mathbb{Q})$ is a torsion point of order 2. This restricts the choices for the torsion subgroup of $\mathcal{E}_t(\mathbb{Q})$ to $\mathbb{Z}/m\mathbb{Z}$ with $m \in \{2, 4, 6, 8, 10, 12\}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with $m \in \{1, 2, 3, 4\}$. The following lemma restricts further the possible torsion subgroups.

Lemma 6 *For all but finitely many $t \in \mathbb{Q}$ the torsion subgroup $\mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ of the group $\mathcal{E}_t(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof.– Suppose that the torsion group $\mathcal{E}_t(\mathbb{Q})_{\text{tors}}$ is not isomorphic to one of the groups $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Then, the above remarks show that $\mathcal{E}_t(\mathbb{Q})_{\text{tors}}$ has necessarily elements of order 3, 4 or 5. Let i be any of the values 3, 4 or 5. We claim that the set of values $t \in \mathbb{Q}$ such that there exists a torsion point of $\mathcal{E}_t(\mathbb{Q})$ of order i is finite.

We sketch the strategy of the proof of the general case and detail the computations in the case $i = 3$.

Let $P := \big(x(P), y(P)\big)$ be a point in $\mathcal{E}_t(\mathbb{Q})_{\text{tors}}$. Then P is an i–torsion point if and only if the i–torsion polynomial $p_i(t, x)$ of the elliptic curve $\mathcal{E}_t(\mathbb{Q})$ vanishes in $x(P)$. A direct computation shows that for any $i \in \{3, 4, 5\}$ the equation $p_i(t, x) = 0$ defines genus–0 curve $\mathcal{C}^{(i)}$. Let $x = v_1^{(i)}(u)$, $t := v_2^{(i)}(u)$ be a parametrization of the curve $\mathcal{C}^{(i)}$, where $v_1^{(i)}, v_2^{(i)}$ are suitable rational functions of $\mathbb{Q}(u)$. Replacing this parametrization in the equation $y^2 = x^3 + tx^2 + tx + 1$ of the elliptic curve $\mathcal{E}_t$ we obtain a plane curve $y^2 = v^{(i)}(u)$ which is an elliptic curve of rank 0. This implies that there exists a finite set of $\mathbb{Q}$–rational points (u, y) satisfying the equation $y^2 = v^{(i)}(u)$ and thus a finite set of $\mathbb{Q}$–rational points (t, x) satisfying the equation $p_i(t, x) = 0$. Therefore the set of points $\big(x(P), y(P), t\big) \in \mathbb{Q}^3$ such that $P := \big(x(P), y(P)\big)$ is a torsion point of order i of the curve $\mathcal{E}_t$ is finite. We conclude that set of values $t \in \mathbb{Q}$ for which the curve $\mathcal{E}_t$ has torsion points of order i is finite.

Now we detail the computations for the case $i := 3$. In this case the 3–division polynomial is $p_3(t, x) := 3x^4 + 4tx^3 + 6tx^2 + 12x - t^2 + 4t$. The equation $p_3(x, t) = 0$ defines a plane curve of genus 0 which can be parametrized as follows:

$$x = \frac{(-4 + 3u)(u + 4)}{16u}, \quad t = -\frac{(-4 + 3u)(3u^3 - 12u^2 + 144u - 64)}{64u^3}.$$

Replacing this parametrization in the equation $y^2 = x^3 + tx^2 + tx + 1$ defining the elliptic curve $\mathcal{E}_t$ we obtain the plane curve

$$y^2 = \frac{(u - 4)^2(3u^2 + 24u - 16)^3}{16384u^5}. \tag{20}$$

Making the change of variables $y = (u-4)(3u^2+24u-16)Y/128u^3$ we see that the non-zero rational solutions of (20) are in bijection with the rational solutions of the curve $Y^2 = 3u^3 + 24u^2 - 16u$. Taking into account that this is an elliptic of rank 0 over $\mathbb{Q}$ finishes the proof of our assertion in the case $i = 3$. ■

Now we can complete the proof of Proposition 2. By Lemma 6 for all but a finite set of values $t \in \mathbb{Q}$ the torsion group $\mathcal{E}_t(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the groups $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let us fix a value $t \in \mathbb{Q}$ such that the group $\mathcal{E}_t(\mathbb{Q})_{\text{tors}}$ is isomorphic to the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $\mathcal{E}_t(\mathbb{Q})_{\text{tors}}$ has three distinct elements of order 2, whose x–coordinates are three distinct rational roots of the polynomial

$$p_{2,t}(x) := x^3 + tx^2 + tx + 1 = (x + 1)(x^2 + tx - x + 1).$$

In such a case, there exists a root $u \in \mathbb{Q} \setminus \{0,-1,1\}$ of the polynomial $p_{2,t}$ and hence $t = -(u^2-u+1)/u$ holds (observe that the values $u = \pm 1$ make the curve $\mathcal{E}_t$ singular). We easily conclude that the torsion subgroup of $\mathcal{E}_t(\mathbb{Q})$ is

$$\mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}} = \Big\{\mathcal{O}_{\mathcal{E}_t}, (-1,0), (u,0), \Big(\frac{1}{u},0\Big)\Big\}.$$

On the other hand, if the group $\mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, taking into account that $(-1,0)$ is a nontrivial torsion point of $\mathcal{E}_t(\mathbb{Q})$ we conclude that $\mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}_{\mathcal{E}_t}, (-1,0)\}$ holds. This completes the proof of Proposition 2. ■

4.2.2 The set $\mathcal{C}_t(\mathbb{Q})$

Now we are able to prove Theorem 3, which determines the set of $\mathbb{Q}$–rational points of the curve $\mathcal{C}_t$ for all but finitely many values $t \in \mathcal{P}$.

Theorem 3 *For all but finitely many values $t \in \mathcal{P}$ the following assertions hold:*

(i) if there exists $v \in \mathbb{Q}$ such that $t = -(v^4 - v^2 + 1)/v^2$ holds, then

$$\mathcal{C}_t(\mathbb{Q}) = \Big\{(0,1), (0,-1), (v,0), (-v,0), \Big(\frac{1}{v},0\Big), \Big(-\frac{1}{v},0\Big)\Big\}.$$

(ii) Otherwise, we have

$$\mathcal{C}_t(\mathbb{Q}) = \{(0,1), (0,-1)\}.$$

Proof.– Let $t \in \mathbb{Q}$ and let as before $\phi_1, \phi_2 : \mathcal{C}_t \to \mathcal{E}_t$ denote the morphisms defined by $\phi_1(x,y) := (x^2, y)$ and $\phi_2(x,y) := (1/x^2, y/x^3)$. Observe that for any point $P = \big(x(P), y(P)\big)$ of $\mathcal{C}_t(\mathbb{Q})$ we have $\phi_1(P) \in \mathcal{E}_t(\mathbb{Q})$ and $\phi_2(P) \in \mathcal{E}_t(\mathbb{Q})$. Corollary 1 and Remark 1 show that for all but a finite set of values $t \in \mathcal{P}$ the points $\phi_1(P)$ and $\phi_2(P)$ can be expressed as $\phi_1(P) = [n_1](0,1) + \mathcal{T}_1$ and $\phi_2(P) = [n_2](0,1) + \mathcal{T}_2$, with $|n_1|, |n_2| \le 10$ and $\mathcal{T}_1, \mathcal{T}_2 \in \mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$.

Let us fix for the moment an integer n and a torsion point $\mathcal{T} := (t_1, t_2)$ of $\mathcal{E}_t$. Then the x–coordinate of the point $[n](0,1) + \mathcal{T} \in \mathcal{E}_t(\mathbb{Q})$ can be expressed as a rational function in the value t, which we denote by $F_{n,\mathcal{T}}(t)$. We shall see that for any point $P \in \mathcal{C}_t(\mathbb{Q})$ the definition of the morphisms ϕ_1, ϕ_2 imply that there exist $\mathcal{T}_1, \mathcal{T}_2 \in \mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ such that the condition $F_{n_1,\mathcal{T}_1}(t) F_{n_2,\mathcal{T}_2}(t) = 1$ is satisfied. The existence of this algebraic condition on the value t is a key point of the proof of Theorem 3.

Proof of Theorem 3(i). Let $t \in \mathcal{P}$ and let us suppose that there exists $v \in \mathbb{Q}$ such that $t = -(v^4 - v^2 + 1)/v^2$. Letting $u := v^2$ we see that there exists $u \in \mathbb{Q} \setminus \{0,1,-1\}$ for which $t = -(u^2 - u + 1)/u$ holds. Then Proposition 2(*i*) shows that the torsion subgroup of $\mathcal{E}_t(\mathbb{Q})$ is given by $\mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}} = \big\{\mathcal{O}_{\mathcal{E}_t}, (-1,0), (u,0), \big(\frac{1}{u},0\big)\big\} =: \{\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3, \mathcal{T}_4\}$, all points having order 2. Then any point $\mathcal{T} \in \mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ has order at most 2 and we have that for any $n \in \mathbb{Z}$ the

x–coordinates of the points $[n](0,1)+\mathcal{T}$ and $[-n](0,1)+\mathcal{T}$ agree. Therefore, in order to determine which are the possible x–coordinates of the image of a point $P \in \mathcal{C}_t(\mathbb{Q})$ we may assume without loss of generality that $n \geq 0$ holds.

For $1 \leq i \leq 4$ and $0 \leq n \leq 10$, let $F_{n,i}(u)$ denote the rational function which represents the x–coordinate of the point $[n](0,1)+\mathcal{T}_i$. Let $P := \big(x(P), y(P)\big)$ be a point of $\mathcal{C}_t(\mathbb{Q})$. Then Proposition 2$(i)$ and Remark 1 show that for all but finitely many values $t \in \mathcal{P}$ we have that $x(P)$ and u satisfy the condition:

$$x(P)^2 = F_{n_1,j_1}(u), \quad \frac{1}{x(P)^2} = F_{n_2,j_2}(u), \tag{21}$$

with $0 \leq n_1, n_2 \leq 10$ and $j_1, j_2 \in \{1,2,3,4\}$. Let us observe that the cases $n_1 = 0, j_1 = 1$ and $n_2 = 0, j_2 = 1$ cannot arise because the point $\mathcal{O}_{\mathcal{E}_t} = [0](0,1)$ does not belong to the affine part of the curve $\mathcal{E}_t$. On the other hand, the cases $n_1 = j_1 = 1$ and $n_2 = j_2 = 1$ yield the point $(0,1) = [1](0,1)$, which is the image of the points $(0, \pm 1) \in \mathcal{C}_t(\mathbb{Q})$. Finally, the cases $n_1 = 0, j_1 = 2$ and $n_2 = 0, j_2 = 2$ cannot arise because the x–coordinate of the point $[0](0,1)+(-1,0) = (-1,0)$ is not a square in $\mathbb{Q}$. In all the remaining cases (21) shows that the equation

$$F_{n_1,j_1}(u) F_{n_2,j_2}(u) = 1 \tag{22}$$

holds. A direct computation shows that this identity is satisfied for all the values $u \in \mathbb{Q}$ if and only if $n_1 = n_2 = 0$ and $j_1 = 3, j_2 = 4$ or $j_1 = 4, j_2 = 3$ hold.

In all the other cases $F_{n_1,j_1}(u) F_{n_2,j_2}(u) - 1$ is a nonzero rational function which vanishes in a finite set values $u \in \mathbb{Q}$. Since there are only a finite set of possible choices for the integers n_1, n_2, j_1, j_2, we conclude that for all but finite many values $u \in \mathbb{Q}$ the identity (22) will not be satisfied unless $n_1 = n_2 = 0$ and $j_1 = 3, j_2 = 4$ or $j_1 = 4, j_2 = 3$ hold. In this latter case the conditions $x^2 = F_{0,3}(u) = u$ or $x^2 = F_{0,4}(u) = u$ are satisfied if and only if u is a square in $\mathbb{Q}$, which holds true since by assumption $u = v^2$. Taking into account that that the fiber of the set $\{(u,0),(1/u,0)\}$ under the morphisms ϕ_1, ϕ_2 is the set $\{(\pm v, 0), (\pm 1/v, 0)\}$ we easily conclude the statement of Theorem 3(i).

Proof of Theorem 3(ii). Now we have that there does not exist $v \in \mathbb{Q}$ such that $t = -(v^4 - v^2 + 1)/v^2$. If there exists $u \in \mathbb{Q}$ for which $t = -(u^2 - u + 1)/u$ holds, the arguments of the proof of Theorem 3(i) show that $\mathcal{C}_t(\mathbb{Q}) = \{(0,1),(0,-1)\}$ holds. Therefore, we may assume without loss of generality that that there does not exist $u \in \mathbb{Q}$ such that $t = -(u^2 - u + 1)/u$ holds. Then Proposition 2(ii) shows that $\mathcal{E}_t(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}_{\mathcal{E}_t}, (-1,0)\}$ holds. Let us fix $n \in \mathbb{Z}$. Then there exist rational functions $F_{n,1}, F_{n,2} \in \mathbb{Q}(t)$ which represent the x–coordinate of the points $[n](0,1)$ and $[n](0,1)+(-1,0)$ respectively. Arguing as before we conclude that without loss of generality we may assume that $n \geq 0$ holds.

Let $P := \big(x(P), y(P)\big)$ be a point in $\mathcal{C}_t(\mathbb{Q})$. From Remark 1 we deduce that $x(P)$ and t satisfy the relation:

$$x^2(P) = F_{n_1,j_1}(t), \quad \frac{1}{x^2(P)} = F_{n_2,j_2}(t) \tag{23}$$

with $0 \leq n_1, n_2 \leq 10$ and $j_1, j_2 \in \{1, 2\}$. We observe that the cases $n_1 = 0, j_1 = 1$ and $n_2 = 0, j_2 = 1$ do not yield points of $\mathcal{C}_t(\mathbb{Q})$, because the point $[0](0,1)$ does not belong to the the affine part of the elliptic curve $\mathcal{E}_t$. On the other hand, the cases $n_1 = 0, j_1 = 2$ and $n_2 = 0, j_2 = 2$ do not yield points of $\mathcal{C}_t(\mathbb{Q})$, because the x–coordinate of the point $[0](0,1) + (-1,0) = (-1,0)$ is not a square in $\mathbb{Q}$. Finally, in the case $n_1 = j_1 = 1$ we have the point $(0,1) \in \mathcal{E}_t(\mathbb{Q})$, whose ϕ_1–fiber is the set $\{(0,1),(0,-1)\}$ for any $t \in \mathbb{Q}$.

In all the remaining cases (23) implies $F_{n_1,j_1}(t)F_{n_2,j_2}(t) = 1$. Furthermore, in all these cases $F_{n_1,j_1}(t)F_{n_2,j_2}(t) - 1$ is a nonzero element of $\mathbb{Q}(t)$, thus vanishing in a finite set of values $t \in \mathbb{Q}$. Since there are only a finite set of admissible choices for the integers n_1, n_2, j_1, j_2 we conclude that for all but a finite set of values $t \in \mathbb{Q}$ the identity $\mathcal{C}_t(\mathbb{Q}) = \{(0,1),(0,-1)\}$ holds. This concludes the proof of Theorem 3(ii). ∎

5 Experimental and conjectural results

Theorem 3 asserts that the cardinality of the set $\mathcal{C}_t(\mathbb{Q})$ is uniformly bounded in the set of values $t \in \mathbb{Q}$ satisfying the following conditions:

1. The rank of the abelian group $\mathcal{E}_t(\mathbb{Q})$ is 1.
2. (0,1) is a generator of the free part $\mathcal{E}_t(\mathbb{Q})$.

The purpose of this section is twofold. On one hand, we are going to discuss the "strength" of conditions 1 and 2 from a experimental point of view. On the other hand, we are going to show that under the assumption of the validity of Conjecture B condition 2 is not necessary.

5.1 Rank considerations

Since Theorem 2 shows that conditions 1 and 2 are satisfied by the elliptic curve $\mathcal{E}$ defined over $\mathbb{Q}(T)$, one might expect these conditions to frequently happen over $\mathbb{Q}$ i.e. for the specialized $\mathbb{Q}$–definable curves $\mathcal{E}_t$. Unfortunately, this needs not be true. Indeed, J. Cassels and A. Schinzel [CS82] exhibit a rank–0 elliptic curve $\widetilde{\mathcal{E}}$ defined over $\mathbb{Q}(T)$ with the following property: assuming Selmer's conjecture [Sel54], for any $t \in \mathbb{Q}$ the specialized curve $\widetilde{\mathcal{E}}_t$ has rank at least 1.

The general question of characterizing the behaviour of the rank of an elliptic curve defined over $\mathbb{Q}(T)$ under specializations is a difficult problem (see e.g. [Sil85]). Nevertheless there is some numerical experience, as that of S. Fermigier [Fer96] who studies 66918 elliptic curves $\widetilde{\mathcal{E}}_t$ with $t \in \mathbb{Z}$, coming from 93 $\mathbb{Q}(T)$-definable elliptic curves $\widetilde{\mathcal{E}}$ having ranks between 0 and 4 over $\mathbb{Q}(T)$. S. Fermigier shows that, with a surprising amount of uniformity, the following identity holds:

$$\operatorname{rank} \widetilde{\mathcal{E}}_t(\mathbb{Q}) = \operatorname{rank} \widetilde{\mathcal{E}}(\mathbb{Q}(T)) + N,$$

where

$N = 0$	with probability	32%,
$N = 1$	with probability	48%,
$N = 2$	with probability	18%,
$N = 3$	with probability	2%.

We computed the rank of 284051 elliptic curves $\mathcal{E}_t$ with $h(t) \leq \log(530)$. We obtain the following results:

$$\operatorname{rank} \mathcal{E}_t(\mathbb{Q}) = \operatorname{rank} \mathcal{E}(\mathbb{Q}(T)) + N,$$

where

$N = 0$	with probability	32.7%,
$N = 1$	with probability	49.9%,
$N = 2$	with probability	15.9%,
$N = 3$	with probability	1.5%.

These figures suggest that condition 1 might hold with a probability of success of approximately 1/3. We refer to [Sil98] for further discussion on the average rank of a family of elliptic curves.

5.2 Divisibility considerations

If the point $(0, 1)$ is a generator of the free part of the group $\mathcal{E}\big(\mathbb{Q}(T)\big)$, the same statement does not necessarily hold in a specialized curve $\mathcal{E}_t$: even if the elliptic curve $\mathcal{E}_t$ has rank 1 over $\mathbb{Q}$, the point $(0, 1)$ could be a multiple of a generator of the free part of $\mathcal{E}_t(\mathbb{Q})$.

This problem can be put into a general setting: let $\widetilde{\mathcal{E}}$ be a elliptic curve defined over $\mathbb{Q}(T)$; then for all but finitely many $t \in \mathbb{P}^1(\mathbb{Q})$ the specialized curve $\widetilde{\mathcal{E}}_t$ is an elliptic curve defined over $\mathbb{Q}(T)$ and we may consider the specialization homomorphism $\sigma_t : \widetilde{\mathcal{E}}\big(\mathbb{Q}(T)\big) \mapsto \widetilde{\mathcal{E}}_t(\mathbb{Q})$.

In [Sil85], J. Silverman asks whether the image of σ_t is divisible in $\widetilde{\mathcal{E}}_t(\mathbb{Q})$ for values $t \in \mathbb{N}$, i.e. whether there are points $P \in \widetilde{\mathcal{E}}_t(\mathbb{Q})$ such that $[n]P \in \sigma_t\big(\widetilde{\mathcal{E}}\big(\mathbb{Q}(T)\big)\big)$ for some integer $n \geq 2$ and $P \notin \sigma_t\big(\widetilde{\mathcal{E}}\big(\mathbb{Q}(T)\big)\big)$ for $t \in \mathbb{N}$. Theorems 2 and 3 of [Sil85] give the following result.

Theorem 6 [Sil85] *Let notations and assumptions as above. Suppose further that the elliptic curve $\widetilde{\mathcal{E}}$ has nonconstant j–invariant. Then the following assertions hold:*

- (i) *The set of values $t \in \mathbb{N}$ for which $\sigma_t\big(\widetilde{\mathcal{E}}\big(\mathbb{Q}(T)\big)\big)$ is indivisible in $\widetilde{\mathcal{E}}_t(\mathbb{Q})$ has density 1.*
- (ii) *Assuming that Conjecture B is true, there exists an absolute constant $C > 0$ with the following property : for any $t \in \mathbb{N}$ and any $P \in \mathcal{E}_t(\mathbb{Q})$ for which $P \in \sigma_t\big(\widetilde{\mathcal{E}}\big(\mathbb{Q}(T)\big)\big) \otimes \mathbb{Q}$ holds, there exists $0 \leq n < C$ such that $[n]P \in \sigma_t\big(\widetilde{\mathcal{E}}\big(\mathbb{Q}(T)\big)\big)$ holds.*

Applying Theorem 6 to the elliptic curve $\mathcal{E}$ of equation $y^2 = x^3+Tx^2+Tx+1$ we obtain the following result:

Corollary 2 *Let $\mathcal{Q}$ denote the set of values $t \in \mathbb{Q}$ such that the abelian group $\mathcal{E}_t(\mathbb{Q})$ has rank 1 and let $\mathcal{R}$ denote the (density 1) set of values $t \in \mathbb{N}$ for which $\sigma_t\big(\mathcal{E}\big(\mathbb{Q}(T)\big)\big)$ is indivisible in $\mathcal{E}_t(\mathbb{Q})$.*

(i) For any $t \in \mathcal{R} \cap \mathcal{Q}$, the point $(0,1)$ generates the free part of $\mathcal{E}_t(\mathbb{Q})$.

(ii) Assuming that Conjecture B is true, there exists $\widetilde{C} \in \mathbb{N}$ such that the following property holds: for any $t \in \mathbb{N} \cap \mathcal{Q}$, if G_t is a generator of the free part of $\mathcal{E}_t(\mathbb{Q})$ then there exists $n \leq \widetilde{C}$ such that $(0,1) - [n]G_t \in \mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ holds.

Proof.– Let $\sigma_t : \mathcal{E}\big(\mathbb{Q}(T)\big) \to \mathcal{E}_t(\mathbb{Q})$ be the specialization homomorphism of the elliptic curve $\mathcal{E}$. [Sil83] shows that for all but finitely many values $t \in \mathbb{Q}$ the homomorphism σ_t is injective. This implies that for all but finitely many values $t \in \mathbb{Q}$ the subgroup of $\mathcal{E}_t(\mathbb{Q})$ generated by the point $(0,1)$ is a torsion free subgroup of rank 1.

Let $t \in \mathcal{R} \cap \mathcal{Q}$ and let G_t be a generator of the free part of the group $\mathcal{E}_t(\mathbb{Q})$. Then there exist $m \in \mathbb{Z}$ and $\mathcal{T} \in \mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ such that $(0,1) = [m]G_t + \mathcal{T}$ holds. Therefore, multiplying this identity by $n := 3 \cdot 5 \cdot 7 \cdot 8 \cdot 11$ we conclude that $[n](0,1) = [nm]G_t$ holds. Since $[nm]G_t = [n](0,1) \in \sigma_t\big(\mathcal{E}\big(\mathbb{Q}(T)\big)\big)$, by the indivisibility of $\sigma_t\big(\mathcal{E}\big(\mathbb{Q}(T)\big)\big)$ we see that $G_t \in \sigma_t\big(\mathcal{E}\big(\mathbb{Q}(T)\big)\big)$ holds.

Let $G \in \mathcal{E}\big(\mathbb{Q}(T)\big)$ be such that $\sigma_t(G) = G_t$ holds. By Proposition 1 we have $G = [s](0,1) + [s'](-1,0)$ with $s \in \mathbb{Z}$ and $s' \in \{0,1\}$. Then we have $G_t = [s]\sigma_t(0,1) + [s']\sigma_t(-1,0) = [s](0,1) + [s'](-1,0)$. Multiplying this identity by m we have $(0,1) - \mathcal{T} = [m]G_t = [ms]\sigma_t(0,1) + [ms']\sigma_t(-1,0)$. We conclude that the point $(1-ms)(0,1)$ is a torsion point of $\mathcal{E}_t(\mathbb{Q})$, which implies $ms = 1$. From this we easily deduce that the point $(0,1)$ generates the free part of the group $\mathcal{E}_t(\mathbb{Q})$. This shows assertion (i).

For the second assertion, arguing as above we have that there exists $m \in \mathbb{Z} \setminus \{0\}$ and $\mathcal{T} \in \mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ such that $[m]G_t + \mathcal{T} = (0,1)$ holds. Then we have $[mn]G_t \in \sigma_t\big(\mathcal{E}\big(\mathbb{Q}(T)\big)\big)$, where $n := 3 \cdot 4 \cdot 5 \cdot 7 \cdot 11$. If $G_t \in \sigma_t\big(\mathcal{E}\big(\mathbb{Q}(T)\big)\big)$ and $G \in \mathcal{E}\big(\mathbb{Q}(T)\big)$ satisfies $\sigma_t(G) = G_t$, then there exists $s, s' \in \mathbb{Z}$ such that $G_t = [s](0,1) + [s'](-1,0)$ holds. Arguing as above we conclude that $ms = 1$, which implies $(0,1) - [m]G_t \in \mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ with $|m| \leq 1$.

Suppose now that $G_t \notin \sigma_t\big(\mathcal{E}\big(\mathbb{Q}(T)\big)\big)$ holds. Then Theorem 6(ii) shows that $mn \leq C'$ holds, where C' is the constant of the statement of Theorem 6(ii) for the curve $\mathcal{E}$. Thus $(0,1) - [m]G_t \in \mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ with $|m| \leq C'/n$. This concludes the proof of assertion (ii). ■

We experimentally analyzed the density of the set $\mathcal{R} \cap \mathcal{Q}$ of values $t \in \mathbb{Q}$ for which the rank of $\mathcal{E}_t(\mathbb{Q})$ is 1 and the point $(0,1)$ generates the free part of the group $\mathcal{E}_t(\mathbb{Q})$. For this purpose we tested 28469 elliptic curves $\mathcal{E}_t$ of rank 1 with $h(t) \leq \log(280)$. We found that the point $G := (0,1) \in \mathcal{E}_t(\mathbb{Q})$ is a generator of the free part of $\mathcal{E}_t(\mathbb{Q})$ in 99.4% of these curves.

From Corollary 2 we deduce the following result, which shows that if Conjecture B is true then the uniform upper bound of Corollary 1 holds for any $t \in \mathbb{N} \cap \mathcal{Q}$, even in the case that the point $(0,1) \in \mathcal{E}_t(\mathbb{Q})$ does not generate the free part of the group $\mathcal{E}_t(\mathbb{Q})$:

Theorem 4 *Assuming that Conjecture B is true, for any $t \in \mathbb{N} \cap \mathcal{Q}$ the cardinality of the set $\mathcal{C}_t(\mathbb{Q})$ is uniformly bounded.*

Proof.– Let G_t be a generator of the free part of $\mathcal{E}_t(\mathbb{Q})$. Then Corollary $2(ii)$ shows that there exists $n \leq C$ such that $(0,1) - [n]G_t \in \mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ holds, where C is the constant of Corollary $2(ii)$. Then we have $\widehat{h}(0,1) \leq C^2 \widehat{h}(G_t)$. Moreover, from the proof of Corollary 1 we see that if $h(t) > 18.94$ holds then $\widehat{h}(0,1)^{-1} \leq 12\big(h(t) - 17.94\big)^{-1}$ holds. This implies the estimate

$$\frac{1}{\widehat{h}(G_t)} \leq \frac{12C^2}{h(t) - 17.94}. \tag{24}$$

Let P be a point of $\mathcal{C}_t(\mathbb{Q})$. Then there exist $n \in \mathbb{N}$ and $\mathcal{T} \in \mathcal{E}_t(\mathbb{Q})_{\mathrm{tors}}$ such that $\phi_1(P) = [n]G_t + \mathcal{T}$ holds. Hence we have $\widehat{h}\big(\phi_1(P)\big) = n^2 \widehat{h}(G_t)$. On the other hand, from the proof of Corollary 1 we deduce the estimate

$$\widehat{h}\big(\phi_1(P)\big) \leq \frac{26}{3} h(t) + 13.71. \tag{25}$$

Let $t \in \mathbb{N}$ satisfy the condition $t > 18$. Then estimates (24) and (25) imply

$$n^2 \leq 104C^2 \, \frac{t + 1.59}{t - 17.94}.$$

Since the right–hand side of the last estimate is a bounded quantity for any $t \geq 19$, we conclude that the cardinality of the set $\mathcal{C}_t(\mathbb{Q})$ can be uniformly bounded for any $t \geq 19$ such that the rank of the group $\mathcal{E}_t(\mathbb{Q})$ is 1. On the other hand, the set of values $\{1, \ldots, 18\}$ is finite and hence the cardinality of the set $\mathcal{C}_t(\mathbb{Q})$ can be uniformly bounded for all $t \in \{1, \ldots, 18\}$. This concludes the proof of the theorem. ∎

Acknowledgments. The authors would like to thank Joseph Silverman and Noam Elkies for their corrections and suggestions that greatly improved the contents and presentation of this paper.

References

[Cas68] J.W.S. Cassels. On a theorem of Dem'janenko. *Journal of the London Mathematical Society*, 43:61–66, 1968.

[CF96] J.W.S. Cassels and E.V. Flynn. Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2, volume 230 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1996.

[CHM95] L. Caporaso, J. Harris, and B. Mazur. How many rational points can a curve have? In R.H. Dijkgraaf et al., editor, *The moduli space of curves, Proceedings of the conference held on Texel Island, Netherlands*, volume 129 of *Progress in Mathematics*, pages 13–31, Basel, 1995. Birkhäuser.

[CHM97] L. Caporaso, J. Harris, and B. Mazur. Uniformity of rational points. *Journal of the AMS*, 10(1):1–35, 1997.

[Cre] J. Cremona. `mwrank`, a program for doing 2–descent on elliptic curves over $\mathbb{Q}$. Available at `http://www.maths.nottingham.ac.uk/personal/jec`.

[CS82] J.W.S. Cassels and A. Schinzel. Selmer's conjecture and families of elliptic curves. *Bulletin of the London Mathematical Society*, 14:345–348, 1982.

[Dem68] V. Dem'janenko. Rational points of a class of algebraic curves. *Transactions of the AMS*, 66:246–272, 1968.

[Fal83] G. Faltings. Finiteness theorems for abelian varieties over number fields. *Inventiones Mathematicae*, 73(3):349–366, 1983.

[Fer96] S. Fermigier. Étude expérimentale du rang de familles de courbes elliptiques sur $\mathbb{Q}$. *Experimental Mathematics*, 5:119–130, 1996.

[GKMS01] P. Gaudry, L. Kulesz, G. Matera, and É. Schost. Uniform bounds for the number of rational points of of families of curves of genus 2. In M. Frías and J. Heintz, editors, *Proceedings of the Workshop Argentino de Informática Teórica, Buenos Aires, September 2001*, volume 30 of *Anales Jornadas Argentinas de Informática e Investigación Operativa*, pages 13–31, Buenos Aires, 2001. SADIO.

[HJ85] R.A. Horn and C.R. Johnson. *Matrix analysis.* Cambridge University Press, Cambridge, 1985.

[HS88] M. Hindry and J.H. Silverman. The canonical height and integral points on elliptic curves. *Inventiones Mathematicae*, 93(2):419–450, 1988.

[Kna92] A. Knapp. *Elliptic Curves*, volume 40 of *Mathematical Notes.* Princeton University Press, Princeton, NJ, 1992.

[Kul99] L. Kulesz. Application de la méthode de Dem'janenko–Manin à certaines familles de courbes de genre 2 et 3. *Journal of Number Theory*, 76(1):130–146, 1999.

[Lan78] S. Lang. *Elliptic curves: Diophantine Analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften*. Springer, Berlin–Heidelberg–New York, 1978.

[Lan86] S. Lang. Hyperbolic and diophantine analysis. *Bulletin of the AMS*, 14(2):159–205, 1986.

[Mag] Magma. Computational algebra system. Available at `http://www.maths.usyd.edu.au:8000/u/magma/`.

[Man69] Y. Manin. The p–torsion of elliptic curves is uniformly bounded (Russian). *Izv. Akad. Nauk SSSR*, 33:459–465, 1969.

[Maz78] B. Mazur. Rational isogenies of prime degree. *Inventiones Mathematicae*, 44:129–169, 1978.

[MED] MEDICIS. UMS CNRS/Polytechnique in computer algebra. `http://www.medicis.polytechnique.fr/`.

[OS91] K. Oguiso and T. Shioda. The Mordell–Weil lattice of a rational elliptic surface. *Commentarii Mathematici Universitatis Sancti Pauli*, 40:83–99, 1991.

[Sel54] E. Selmer. A conjecture concerning rational points on cubic curves. *Mathematica Scandinavica*, 2:49–54, 1954.

[Sil83] J.H. Silverman. Heights and the specialization map for families of abelian varieties. *Journal für die reine und angewandte Mathematik*, 342:197–211, 1983.

[Sil85] J.H. Silverman. Divisibility of specialization map for families of elliptic curves. *American Journal of Mathematics*, 107:555–565, 1985.

[Sil86] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Berlin Heidelberg New York, 1986.

[Sil87] J.H. Silverman. Rational points on certain families of curves of genus at least 2. *Proceedings of the London Mathematical Society*, 55:465–481, 1987.

[Sil90] J.H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Mathematics of Computation*, 55:723–743, 1990.

[Sil93] J.H. Silverman. A uniform bound for rational points on twists of a given curve. *Journal of the London Mathematical Society*, 47(3):385–394, 1993.

[Sil94] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, Berlin Heidelberg New York, 1994.

[Sil98] J.H. Silverman. The average rank of an algebraic family of elliptic curves. *Journal für die reine und angewandte Mathematik*, 504:227–236, 1998.

[Shi90] T. Shioda. On the Mordell–Weil lattices. *Commentarii Mathematici Universitatis Sancti Pauli*, 39(2):211–240, 1990.

[Shi91] T. Shioda. Theory of Mordell–Weil lattices. In *Proceedings of the International Congress of Mathematicians, Kyoto, 1990*, volumes I, II, *Mathematical Society of Japan*, pages 473–489, Tokyo, 1991.

[Shi91a] T. Shioda. Construction of elliptic curves with high rank via the invariants of the Weyl group. *Journal of the Mathematical Society of Japan*, 43(4):673–719, 1991.

[Sto01] M. Stoll. Uniform Chabauty bounds for twists. Preprint, 2001.

[Tat75] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic surface. In B.J. Birch and W. Kuyk, editors, *Modular functions of of one variable IV*, volume 476 of *Lect. Notes in Math.*, pages 33–52, Berlin, 1975. Springer Verlag.

[ZS01] H.G. Zimmer and S. Schmitt. Height estimates for elliptic curves in short Weierstraß form over global fields and comparison. *Archiv der Math.*, 77:22–31, 2001.