ACTA ARITHMETICA
153.1 (2012)

Rational points on some elliptic surfaces

by

Enrico Jabara (Venezia)

1. Introduction. Let $\mathscr{E}$ be the elliptic surface given by the equation

$$(*)\qquad \mathscr{E}:\ y^2 = x^3 + A(t)x + B(t)$$

with $A, B \in \mathbb{Q}[t]$. The discriminant of $\mathscr{E}$ (which may be considered as an elliptic curve defined over $\mathbb{Q}(t)$) is defined by $\Delta(t) = -16(4A(t)^3 + 27B(t)^2)$ and its j-invariant by $j(t) = -1728(4A(t)^3)\Delta(t)^{-1}$. The surface $\mathscr{E}$ is said to be *isotrivial* if its j-invariant is constant. We say that $\mathscr{E}$ is *split* (or splits) if there is an elliptic curve $\mathcal{C}$ such that $\mathscr{E} \simeq \mathcal{C} \times \mathbb{P}$ over $\mathbb{C}$; if $\mathscr{E}$ splits then $\mathscr{E}$ is necessarily isotrivial. We shall deal only with non-split elliptic surfaces.

Let $\mathscr{E}$ be the elliptic surface $(*)$; if $k \in \mathbb{Q}$ is such that $\Delta(k) \neq 0$ one may consider the elliptic curve

$$\mathscr{E}(k):\ y^2 = x^3 + A(k)x + B(k).$$

In this paper we are interested in the following

Problem 1.1. Determine whether or not there exist $k \in \mathbb{Q}$ such that the rank $\mathrm{rk}(\mathscr{E}(k))$ of the elliptic curve $\mathscr{E}(k)$ is positive.

We observe that if $\mathscr{E}$ admits a non-torsion rational point over $\mathbb{Q}(t)$ then by Silverman's specialization theorem (see Theorem III.11.4 of [5]) $\mathrm{rk}(\mathscr{E}(k)) > 0$ for all but finitely many $k \in \mathbb{Q}$. This also proves that the set of rational points on $\mathscr{E}$ is dense in the Zariski topology (see [6]).

In [6] Ulas considered the particular cases of the (isotrivial) surfaces

$$\mathscr{E}_f:\ y^2 = x^3 + f(t)x$$

with f a polynomial of degree 4 and

$$\mathscr{E}^g:\ y^2 = x^3 + g(t)$$

with g a monic polynomial of degree 6. In particular, he proved (Theorem 2.2 of [6]) that, in the first case, if $f(t) \neq f(-t)$ then Problem 1.1

2010 *Mathematics Subject Classification*: 14G05, 11G05, 11D25, 11D41.
Key words and phrases: elliptic curves, diophantine equations.

DOI: 10.4064/aa153-1-6

always has an affirmative answer. That result led him to formulate the following conjecture:

Conjecture 1.2 (cf. Conjecture 2.5 of [6]). *Let $a, b, c \in \mathbb{Q}$ with $a \neq 0$ and let $f(t) = at^4 + bt^2 + d$ be such that $f(t) \neq at^4$. Then there exists $t_0 \in \mathbb{Q}$ such that* $\mathrm{rk}(\mathscr{E}_f(t_0)) > 0$.

As a partial confirmation of Conjecture 1.2 we shall prove

Theorem A. *Let $f(t) = at^4 + bt^2 + d$ with $a, b, d \in \mathbb{Q}$, $a \neq 0$ and $f(t) \neq at^4$. Suppose that one of the following conditions holds:*

(i) $a = -\lambda^4 + \mu^2$ *with $\lambda, \mu \in \mathbb{Q}$ and $\lambda \neq 0$,*
(ii) $a = 4\lambda^4 - \mu^2$ *with $\lambda, \mu \in \mathbb{Q}$ and $\lambda \neq 0$.*

Then there exist infinitely many $k \in \mathbb{Q}$ such that $\mathrm{rk}(\mathscr{E}_f(k)) > 0$.

The following result follows from the proof of Theorem A:

Theorem B. *Let $\mathbb{K}$ be a field of characteristic different from 2. Then every element of $\mathbb{K}$ may be written in each of the following ways:*

$$a^4 - b^4 - c^2, \qquad a^4 - b^4 + c^2, \qquad a^4 + 4b^4 - c^2, \qquad -a^4 - 4b^4 + c^2,$$

with a suitable choice of $a, b, c \in \mathbb{K}$.

While Theorem B focuses on an aspect of number theory (Waring-type problems in $\mathbb{Q}$), Theorems C and D below have a more geometric vein.

With regard to surfaces of the type $\mathscr{E}^g$ with

$$g(t) = t^6 + at^4 + bt^3 + ct^2 + dt + e \in \mathbb{Q}[t]$$

Ulas proved that if $g(t) \neq g(-t)$ then Problem 1.1 has an affirmative solution (Theorem 3.1 of [6]), and has formulated the following conjecture:

Conjecture 1.3 (cf. Conjecture 3.6 of [6]). *Let $a, c, e \in \mathbb{Q}$ and let $g(t) = t^6 + at^4 + ct^2 + e$ be such that $g(t) \neq t^6$. Then there exists a $t_0 \in \mathbb{Q}$ such that* $\mathrm{rk}(\mathscr{E}^g(t_0)) > 0$.

In this article we shall generalize the results of Ulas to surfaces that are not necessarily isotrivial by proving

Theorem C. *Let $A(t) = a_3t^3 + a_2t^2 + a_1t + a_0$, $B(t) = t^6 + b_4t^4 + b_3t^3 + b_2t^2 + b_1t + b_0 \in \mathbb{Q}[t]$ and let $\mathscr{E}$ be the elliptic surface with equation*

$$\mathscr{E}:\ y^2 = x^3 + A(t)x + B(t).$$

Suppose in addition that if $A(t) = 0$ then $B(t) \neq t^6$. Then there exist infinitely many $k \in \mathbb{Q}$ such that $\mathrm{rk}(\mathscr{E}(k)) > 0$.

In particular, one also has

Corollary 1.4. *Let $g(t) \in \mathbb{Q}[t]$ be a monic polynomial of degree six and not equal to t^6. Then there exist infinitely many $k \in \mathbb{Q}$ such that* $\mathrm{rk}(\mathscr{E}^g(k)) > 0$.

Corollary 1.4 confirms Conjecture 1.3 (and answers Question 3.7 of [6]). Moreover, the following generalization of Theorem 4.1 in [6] follows easily from the proof of Theorem C:

COROLLARY 1.5. *Let* $g(z) = z^6 + az^4 + bz^3 + cz^2 + dz + e \in \mathbb{Q}[z]$. *Then the equation*

$$y^2 - x^3 - g(z) = \varrho$$

has infinitely many solutions in $\mathbb{Q}[\varrho]$.

The following generalization of Corollary 4.6 of [6] also holds:

COROLLARY 1.6. *Let* $g(z) = z^6 + 2bz^3 + dz \in \mathbb{Z}[z]$. *If* $d = \pm 1$ *then for each* $n \in \mathbb{Z}$ *the diophantine equation* $y^2 - x^3 - g(z) = n$ *has infinitely many integer solutions.*

Theorem C has an obvious application to the study of del Pezzo surfaces of degree one. In this connection see [7], where the case of $A(t) = 0$ and $B(t)$ a monic polynomial of degree 5 is treated. Another result in this direction can be obtained as follows:

Given two polynomials in $\mathbb{Q}[t]$,

$$A(t) = a_4t^4 + a_3t^3 + a_2t^2 + a_1t + a_0, \qquad B(t) = t^6 + b_4t^4 + b_3t^3 + b_2t^2 + b_1t + b_0,$$

let $\mathscr{E}$ be the elliptic surface with equation $(*)$. Associate to $\mathscr{E}$ the curve (in general, elliptic)

$$\mathcal{H}:\ v^2 = h_4u^4 + h_3u^3 + h_2u^2 + h_1u + h_0$$

where

$$(\dagger)\qquad \begin{cases} h_4 = a_4^6 + 28a_4^3 + 144, \\ h_3 = -6(a_4^3 + 16)a_4a_3, \\ h_2 = 4(a_4^3a_2 + 3a_4^2a_3^2 - 12a_4b_4 + 24a_2), \\ h_1 = -8(a_4^2b_3 - a_4a_3b_4 - 2a_4a_1 + 4a_3a_2)a_4, \\ h_0 = 16(a_4^4b_2 - a_4a_2b_4 + a_2^2). \end{cases}$$

With this notation one can state

THEOREM D. *Let* $\mathscr{E}$ *be the elliptic surface with equation* $(*)$ *and suppose that* $\mathscr{E}$ *does not split. If the curve* $\mathcal{H}$ *associated to* $\mathscr{E}$ *contains infinitely many points with rational coordinates then there exist infinitely many* $k \in \mathbb{Q}$ *such that* $\mathrm{rk}(\mathscr{E}(k)) > 0$.

We note that if $a_4 = 0$ then the equation of the curve $\mathcal{H}$ becomes

$$v^2 = 16(3u^2 + a_2)^2$$

and so Theorem C is a special case of Theorem D.

We shall prove all our results by explicitly constructing parameterizations that furnish infinitely many points belonging to the surfaces considered.

Finally we remark that several recent works contain results of similar nature (see e.g. [8], especially Theorem 2.1, and [2]).

2. Preliminary results. We state a few well known results which may be found, for example, in [4, Chap. X, §6], but, given the elementary character of this article, we prefer to present them in a simpler form.

If $\mathbb{K}$ is a field we use $\mathbb{K}^*$ to denote the multiplicative group of $\mathbb{K}$.

LEMMA 2.1. *Let $\mathbb{K}$ be a field of characteristic different from 2 and let $\nu \in \mathbb{K}^*$. Then the solutions of $y^2 = x^4 - \nu$ are in bijective correspondence with those of $Y^2 = X^3 + 4\nu X$ satisfying $X \neq 0$ by means of the maps*

$$(x, y) \mapsto \left(\frac{2\nu}{x^2 - y}, \frac{4\nu x}{x^2 - y}\right) \quad \text{and} \quad (X, Y) \mapsto \left(\frac{Y}{2X}, \frac{Y^2 - 8\nu X}{4X^2}\right).$$

Proof. The proof is a direct verification. ∎

If $\mathcal{C}$ is an elliptic curve defined over the field $\mathbb{K}$, we use $\mathcal{C}(\mathbb{K})$ to denote the group of points of $\mathcal{C}$ with (projective) coordinates in $\mathbb{K}$ and $\mathcal{C}_{\mathrm{tors}}(\mathbb{K})$ to denote its torsion subgroup. If $\mathbb{K} = \mathbb{Q}$ we let $\mathrm{rk}(\mathcal{C})$ denote the rank of $\mathcal{C}(\mathbb{Q})$.

LEMMA 2.2. *Let $\mathbb{K}$ be a field of characteristic different from 2 and let $\nu \in \mathbb{K}^*$ with $\nu \notin \pm(\mathbb{K}^*)^2$. Consider the two elliptic curves*

$$\mathcal{C}^+ : \ Y^2 = X^3 + 4\nu X \quad \text{and} \quad \mathcal{C}^- : \ Y^2 = X^3 - 4\nu X.$$

Then

(i) *ν may be written in the form $-\xi^2 + \eta^4$ $(x, y \in \mathbb{K}^*)$ if and only if $|\mathcal{C}^+(\mathbb{K})| > 2$. In particular if $\mathbb{K} = \mathbb{Q}$ one must have* $\mathrm{rk}(\mathcal{C}^+) > 0$.

(ii) *ν may be written in the form $\xi^2 - \eta^4$ $(x, y \in \mathbb{K}^*)$ if and only if $|\mathcal{C}^-(\mathbb{K})| > 2$. In particular if $\mathbb{K} = \mathbb{Q}$ one must have* $\mathrm{rk}(\mathcal{C}^-) > 0$.

Proof. We prove only (i). The first part of the assertion follows from Lemma 2.1. Now let $\mathbb{K} = \mathbb{Q}$; by hypothesis one has $\nu \notin \pm(\mathbb{Q}^*)^2$ and so $\mathcal{C}^+_{\mathrm{tors}}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ (see Proposition X.6.1 of [4]). But since $|\mathcal{C}(\mathbb{Q})| > 2$, it follows that $\mathrm{rk}(\mathcal{C}^+) > 0$. ∎

LEMMA 2.3. *Let $\mathbb{K}$ be a field of characteristic different from 2 and let $b \in \mathbb{K}^*$. Then the two elliptic curves*

$$\mathcal{C}_b : \ Y^2 = X^3 + 4bX \quad \text{and} \quad \widehat{\mathcal{C}}_b : \ Y^2 = X^3 - bX$$

are isogenous. In particular if $\mathbb{K} = \mathbb{Q}$ then $\mathrm{rk}(\mathcal{C}_b) = \mathrm{rk}(\widehat{\mathcal{C}}_b)$.

Proof. On setting

$$\phi:\ \mathcal{C}_b \to \widehat{\mathcal{C}}_b, \quad (X,Y) \mapsto \left(\frac{Y^2}{4X^2}, \frac{Y(X^2-4b)}{8X^2}\right),$$
$$\widehat{\phi}:\ \widehat{\mathcal{C}}_b \to \mathcal{C}_b, \quad (X,Y) \mapsto \left(\frac{Y^2}{X^2}, \frac{Y(X^2+b)}{X^2}\right),$$

one verifies directly that ϕ and $\widehat{\phi}$ are (dual) isogenies. ∎

LEMMA 2.4. *Let $\mathbb{K}$ be a field of characteristic different from 2 and let $\nu \in \mathbb{K}^*$ with $\nu \notin \pm(\mathbb{K}^*)^2$. Consider the two elliptic curves*

$$\widehat{\mathcal{C}}^+ :\ Y^2 = X^3 + \nu X \quad \text{and} \quad \widehat{\mathcal{C}}^- :\ Y^2 = X^3 - \nu X.$$

Then

(i) *ν may be written as $-\xi^2+4\eta^4$ ($\xi,\eta \in \mathbb{K}^*$) if and only if $|\widehat{\mathcal{C}}^+(\mathbb{K})| > 2$. In particular if $\mathbb{K} = \mathbb{Q}$ one must have* $\mathrm{rk}(\widehat{\mathcal{C}}^+) > 0$.

(ii) *ν may be written as $\xi^2 - 4\eta^4$ ($\xi,\eta \in \mathbb{K}^*$) if and only if $|\widehat{\mathcal{C}}^-(\mathbb{K})| > 2$. In particular if $\mathbb{K} = \mathbb{Q}$ one must have* $\mathrm{rk}(\widehat{\mathcal{C}}^-) > 0$.

Proof. It suffices to write $\nu = -4\nu_0$ and apply Lemmas 2.1 and 2.3. ∎

EXAMPLE 2.5. One can verify (for example using the software MAGMA [1]) that the natural numbers n less than 100 with $n \notin (\mathbb{Q}^*)^2$ such that the elliptic curves

$$Y^2 = X^3 + 4nX \quad \text{and} \quad Y^2 = X^3 - 4nX$$

both have rank 0 are 11, 27, 43, 44, 59, 75 and 91. Since none of these numbers can be expressed as a sum of two squares, Lemma 2.2 shows immediately that none of them may be written in the form $\pm x^2 \pm y^4$ with $x, y \in \mathbb{Q}$.

From Lemmas 2.3 and 2.4 it follows that the numbers listed are also not expressible in the form $\pm x^2 \pm 4y^4$.

3. Proof of Theorems A and B. We prove the following generalization of Theorem B.

THEOREM 3.1. *Let $\Psi(T) = aT^4 + bT^2 \in \mathbb{Q}[T]$ with $a \neq 0$ and suppose that a may be written in the form $a = \lambda^4 - \mu^2$, $\lambda, \mu \in \mathbb{Q}$ and $\lambda \neq 0$. Then there exist rational functions $\beta_1(\kappa,T)$, $\beta_2(\kappa,T)$, $\sigma(\kappa,T)$, depending on a parameter κ, such that the equality*

$$\beta_1(\kappa,T)^4 - \Psi(\beta_2(\kappa,T)) - \sigma(\kappa,T)^2 = T \tag{1}$$

holds identically, that is, for all κ.

Proof. We start by considering the case $\mu \neq 0$. We show that it is possible to determine polynomials $\beta_1, \beta_2, \sigma \in \mathbb{Q}(\kappa)[T]$ which satisfy (1) identically.

First we take $p, q, r, u, v \in \mathbb{Q}$ ($p \neq 0$) such that in $\mathbb{Q}[X]$ one has

$$(\lambda X + p)^4 - (\lambda^4 - \mu^2)X^4 - bX^2 - (\mu X^2 + qX + r)^2 = uX + v.$$

Then, on setting $p = \kappa \in \mathbb{Q}^*$ easy computations show that

$$q = \frac{2\lambda^3\kappa}{\mu}, \qquad r = -\frac{2\lambda^2(2\lambda^4 - 3\mu^2)\kappa^2 + b\mu^2}{2\mu^3},$$
$$u = \frac{2\lambda(2(\lambda^8 + 3\lambda^4\mu^2 + \mu^4)\kappa^2 + b\lambda^2\mu^2)\kappa}{\mu^4},$$
$$v = \frac{4(4\lambda^{12} + 12\lambda^8\mu^2 + 9\lambda^4\mu^4 + \mu^6)\kappa^4 + 4b\lambda^2\mu^2(2\lambda^4 - 3\mu^2)\kappa^2 + b^2\mu^4}{4\mu^6}.$$

For each fixed $b \in \mathbb{Q}$ it is possible to determine (infinitely many) $\kappa \in \mathbb{Q}$ such that $u(\kappa) \neq 0$. If we put $uX + v = T$ we find that $X = (T - v)/u$ and recalling that p, q, r, u, v are determined as functions of κ we deduce that

$$\beta_2(\kappa, T) = \frac{T - v}{u}, \qquad \beta_1(\kappa, T) = \frac{\lambda(T - v)}{u} + p$$

and

$$\sigma(\kappa, T) = \frac{\mu(T - v)^2}{u^2} + \frac{q(T - v)}{u} + r$$

satisfy (1) identically in κ.

Suppose now that $\mu = 0$; on making the substitution $T \rightsquigarrow T/\lambda$ one sees that there is no loss of generality in supposing that $\lambda = 1$. In this case one cannot expect that β_1, β_2 and σ will be polynomials, and indeed to handle the general case

$$\beta_1(T)^4 - a\beta_2(T)^4 - b\beta_2(T)^2 - \sigma(T)^2 = T,$$

with a a generic element of $\mathbb{Q}$, it would probably be necessary to construct a quartic contained in the surface

$$X^4 - aY^4 - bY^2 - Z^2 = T.$$

Fortunately, in the case $\Psi(T) = T^4 + bT^2$ rather than a quartic it is sufficient to consider a conic (in this regard see [3], in particular §§27–28).

We put

$$(2) \qquad (p_2T^2 + p_1T + p_0)^4 - (q_4T^4 + q_3T^3 + q_2T^2 + q_1T + q_0)^2$$
$$= (r_1T + r_0)^4 + b(r_1T + r_0)^2(s_1T + s_0)^2 + (s_1T + s_0)^4T$$

and seek to determine the coefficients $p_i, q_j, r_k, s_\ell \in \mathbb{Q}$ in such a way that (2) is satisfied identically. Without loss of generality we may suppose that $p_2 = q_4 = 1$, $r_0 = 0$ and thus $q_0 = p_0^2$. After elementary but tedious calculations one obtains

$$p_2 = 1, \quad p_1 = \frac{\kappa^4 - b^2}{4}, \quad p_0 = \frac{(\kappa^2 + b)^4}{64},$$
$$q_4 = 1, \quad q_3 = \frac{\kappa^4 - b^2}{2}, \quad q_2 = \frac{(\kappa^2 + b)^2(3\kappa^4 - 2b\kappa^2 + 3b^2)}{32},$$
$$q_1 = -\frac{(\kappa^2 + b)^4(3\kappa^4 + b^2)}{128}, \quad q_0 = \frac{(\kappa^2 + b)^8}{4096},$$
$$r_1 = \frac{\kappa^2(\kappa^2 + b)}{2}, \quad r_0 = 0, \quad s_1 = \frac{\kappa(\kappa^2 + b)}{2}, \quad s_0 = -\frac{\kappa(\kappa^2 + b)^3}{16},$$

where $\kappa \in \mathbb{Q}$ is a parameter. Thus, if one sets $K = \kappa^2 + b$ and defines

$$\beta_1(\kappa, T) = \frac{p_2T^2 + p_1T + p_0}{s_1T + s_0} = \frac{64T^2 + 16(\kappa^2 - b)T + K^4}{4\kappa K(8T - K^2)}, \tag{3}$$

$$\beta_2(\kappa, T) = \frac{r_1T + r_0}{s_1T + s_0} = \frac{8\kappa KT}{8T - K^2}, \tag{4}$$

$$\begin{aligned} \sigma(\kappa, T) &= \frac{q_4T^4 + q_3T^3 + q_2T^2 + q_1T + q_0}{(s_1T + s_0)^2} \\ &= \frac{512T^3 + 64K(5\kappa^2 - 3b)T^2 + 4K^2(11\kappa^4 - 2b\kappa^2 + 3b^2)T - K^6}{16\kappa^2K^2(8T - K^2)}, \end{aligned} \tag{5}$$

then relation (1) does indeed hold identically in κ. ∎

Proof of Theorem B. First we prove that in a field $\mathbb{K}$ of characteristic different from 2 every element τ may be written in the forms $a^4 - b^4 - c^2$ and $a^4 - b^4 + c^2$.

With the notation from the proof of the preceding theorem, let $\Psi(T) = T^4$. Then $b = 0$ and so $K = \kappa^2$. On putting $\kappa = 2\xi$, relations (3)–(5) become

$$\beta_1(\xi, T) = \frac{(T + 2\xi^4)^2}{4\xi^3(T - 2\xi^4)}, \tag{3'}$$

$$\beta_2(\xi, T) = \frac{2\xi T}{T - 2\xi^4}, \tag{4'}$$

$$\sigma(\xi, T) = \frac{T^3 + 10\xi^4T^2 + 44\xi^8T - 8\xi^{12}}{16\xi^6(T - 2\xi^4)}. \tag{5'}$$

Rereading the second part of the proof of Theorem 3.1 one sees that

$$\beta_1(\xi, T)^4 - \beta_2(\xi, T)^4 - \sigma(\xi, T)^2 = T$$

identically in $\mathbb{K}(T)$.

If $|\mathbb{K}| \le 5$ then a direct verification shows that every element of $\mathbb{F}_3$ and of $\mathbb{F}_5$ may be written in each of the forms listed in Theorem B. If instead $|\mathbb{K}| > 5$ then, for a fixed $\tau \in \mathbb{K}$, there certainly exists $\xi \in \mathbb{K}^*$ such that $\tau - 2\xi^4 \neq 0$. (Indeed, if $|\mathbb{K}| = \infty$, then there exist infinitely many $\xi \in \mathbb{K}^*$ with this property.) Hence, on putting $a = \beta_1(\xi,\tau)$, $b = \beta_2(\xi,\tau)$ and $c = \sigma(\xi,\tau)$ one has $\tau = a^4 - b^4 - c^2$. In analogous fashion, if $\xi \in \mathbb{K}$ is such that $\tau + 2\xi^4 \neq 0$ then on putting $a = \beta_2(\xi,-\tau)$, $b = \beta_1(\xi,-\tau)$ and $c = \sigma(\xi,-\tau)$, one obtains $a^4 - b^4 + c^2 = \tau$.

To prove that τ may be written in the forms $a^4+4b^4-c^2$ and $-4a^4-b^4+c^2$ it suffices to use what has just been proved and apply Lemmas 2.2–2.4. ∎

Remark 3.2. Applying to the expressions $\beta_1(\xi,T)$, $\beta_2(\xi,T)$ and $\sigma(\xi,T)$ the isogeny exhibited in the proof of Lemma 2.3 yields

$$\left(\frac{T+\beta_2(\xi,T)^4}{\beta_1(\xi,T)^2}\right)^2 - \left(\frac{\sigma(\xi,T)}{\beta_1(\xi,T)}\right)^4 - 4\beta_2(\xi,T)^4 = 4T.$$

Hence, on explicitly carrying out the substitution $T \rightsquigarrow \frac{1}{4}T$ and setting

$$B_1(\xi,T) = \frac{T^3+40\xi^4T^2+704\xi^8T-512\xi^{12}}{16\xi^3(T+8\xi^4)^2}, \qquad B_2(\xi,T) = \frac{2\xi T}{T-8\xi^4},$$

$$S(\xi,T) = \frac{T^8+s_7T^7+s_6T^6+s_5T^5+s_4T^4+s_3T^3+s_2T^2+s_1T+s_0}{256\xi^6(T+8\xi^4)^4(T-8\xi^4)^2},$$

where

$s_7 = 2^6\cdot\xi^4$, $\quad s_6 = 2^8\cdot 7\cdot\xi^8$, $\quad s_5 = 2^{12}\cdot 11\cdot\xi^{12}$, $\quad s_4 = 2^{13}\cdot 3^2\cdot 11\cdot\xi^{16}$, $s_3 = 2^{18}\cdot 31\cdot\xi^{20}$, $\quad s_2 = -2^{20}\cdot 5^2\cdot\xi^{24}$, $\quad s_1 = 2^{24}\cdot 5\cdot\xi^{28}$, $\quad s_0 = 2^{24}\xi^{32}$,

one has

$$-B_1(\xi,T)^4 - 4\cdot B_2(\xi,T)^4 + S(\xi,T)^2 = T.$$

Remark 3.3. The expressions $\beta_1(\xi,T)$, $\beta_2(\xi,T)$ and $\sigma(\xi,T)$ are related to one another via the simple equation

$$\sigma(\xi,T) = \beta_1(\xi,T)^2 - \beta_2(\xi,T)^2 - 2\xi\beta_2(\xi,T). \tag{6}$$

In particular,

$$\xi = \frac{\sigma(\xi,T)-\beta_1(\xi,T)^2+\beta_2(\xi,T)^2}{2\beta_2(\xi,T)}. \tag{7}$$

Also

$$\beta_1(\xi,T) - \beta_2(\xi,T) = \frac{T-2\xi^4}{4\xi^3}.$$

Using (7) it is easy to show that the formulas obtained in the proof of Theorem B are far from exhausting all the possible expressions of a rational number in the form $a^4 - b^4 - c^2$.

Example 3.4. We write $6 = a^4 - b^4 - c^2$. After a brief computer search one obtains several solutions. Among these we consider the following:

- $6 = 2^4 - 1 - 3^2$. Using (7) to get ξ one obtains:
  - (i) If $a = \pm 2$, $b = \pm 1$, $c = 3$ then $\xi = (3 - 2^2 + 1)(\pm 2^{-1}) = 0$ and so formulas $(3')$–$(5')$ are not applicable.
  - (ii) If $a = \pm 2$, $b = \pm 1$, $c = -3$ then $\xi = \pm 3$ but $\beta_1(\pm 3, 6) = \mp\frac{196}{117}$, $\beta_2(\pm, 6) = \mp\frac{3}{13}$ and $\sigma(\pm 3, 6) = \frac{1441}{1053}$.
- $6 = 4^4 - 3^4 - 13^2$. One obtains:
  - (i) If $a = \pm 4$, $b = \pm 3$, $c = 13$ then $\xi = 1$ and, in this case, one rediscovers precisely $\beta_1(\pm 1, 6) = \pm 4$, $\beta_2(\pm 1, 6) = \pm 3$ and $\sigma(\pm 1, 6) = 13$.
  - (ii) If $a = \pm 4$, $b = \pm 3$, $c = -13$ then $\xi = \pm\frac{10}{3}$ but now

$$\beta_1\left(\pm\frac{10}{3}, 6\right) = \mp\frac{10243^2}{2^4 \cdot 3 \cdot 5^3 \cdot 11 \cdot 887} \quad \text{and} \quad \beta_2\left(\pm\frac{10}{3}, 6\right) = \mp\frac{2^2 \cdot 3^4 \cdot 5}{11 \cdot 887}.$$

Proof of Theorem A. Let $f(t) = at^4 + bt^2 + d \in \mathbb{Q}[t]$ with $a = -\lambda^4 + \mu^2$ and $\lambda \neq 0$. We first note that it follows from the hypothesis $f(T) \neq at^4$ that the elliptic surface $\mathscr{E}$ is not split.

If one puts $\Psi(T) = -aT^4 - bT^2$ then from Theorem 3.1 it follows that there exist rational functions $\beta_1, \beta_2, \sigma \in \mathbb{Q}(X)$ depending on a parameter κ such that

$$\beta_1(\kappa, X)^4 - \Psi(\beta_2(\kappa, X)) - \sigma(\kappa, X)^2 = X$$

holds identically.

For each $\kappa \in \mathbb{Q}$ for which $\beta_1(\kappa, d)$, $\beta_2(\kappa, d)$ and $\sigma(\kappa, d)$ are defined one finds $f(\beta_2(\kappa, -d)) = -\beta_1(\kappa, -d)^4 + \sigma(\kappa, -d)^2$ and so Lemma 2.1 shows that $\mathrm{rk}(\mathcal{C}_\kappa) > 0$ where $\mathcal{C}_\kappa$ is the elliptic curve

$$\mathcal{C}_\kappa :\ Y^2 = X^3 - 4f(\beta_2(\kappa, -d))X.$$

By Lemma 2.3 the curve $\mathcal{C}_\kappa$ is isogenous to the elliptic curve $\mathscr{E}_f(k)$, where $k = \beta_2(\kappa, d)$, and in this case the assertion is proved.

Suppose now that $a = 4\lambda^4 - \mu^2$ and let $f_0(t) = \frac{1}{4}f(t) = a_0t^4 + b_0t^2 + d_0$. Then $a_0 = \lambda^4 - (\mu/2)^2$ and one can repeat the preceding proof considering the elliptic curve

$$\mathscr{E}'_{f_0} :\ y^2 = x^3 - f_0(t)x.$$

By Lemma 2.3 this curve is isogenous to $\mathscr{E}_f$ and the assertion is thus established in this case as well. ∎

Remark 3.5. Let

$$\mathscr{E} :\ y^2 = x^3 - (t^4 + d)x.$$

Then, exploiting the proof of Theorem A and formulas $(3')$–$(5')$, one can verify that on putting

$$t(\xi)=\frac{2\xi d}{d-2\xi^4},\qquad x(\xi)=\frac{(d+2\xi^4)^2}{16\xi^6(d-2\xi^4)},$$
$$y(\xi)=\frac{(d+2\xi^4)^2(d^3+10\xi^4d^2+44\xi^8d-8\xi^{12})}{64\xi^9(d-2\xi^4)^2},$$

one obtains infinitely many rational points of $\mathscr{E}$ as ξ varies in $\mathbb{Q}$ with $2\xi^4\neq d$.

4. Proof of Theorems C and D. Although Theorem C is a consequence of Theorem D (as noted at the end of §1), it is convenient to prove it separately.

Proof of Theorem C. We will use the fact that if

$$\mathscr{D}:\ y^2=x^3+m(t)x+n(t)$$

is an elliptic curve defined over $\mathbb{Q}(t)$ and if $m(t),n(t)\in\mathbb{Z}[t]$, then the points of finite order of $\mathscr{D}$ have coordinates in $\mathbb{Q}[t]$.

Let $A(t)=a_3t^3+a_2t^2+a_1t+a_0$ and $B(t)=t^6+b_4t^4+b_3t^3+b_2t^2+b_1t+b_0$ belong to $\mathbb{Q}[t]$ and let $\mathscr{E}$ be the elliptic surface

$$\mathscr{E}:\ y^2=x^3+A(t)x+B(t).$$

Carrying out, if necessary, an affine coordinate transformation, we may, without loss of generality, suppose that $A(t),B(t)\in\mathbb{Z}[t]$.

We put $X(T)=hT+k$, $Y(T)=T^3+pT^2+qT+r$ and seek to determine h,k,p,q,r as functions of the coefficients a_i and b_j so as to have

$$X(T)^3+A(T)X(T)+B(T)-Y(T)^2=LT+M \tag{8}$$

with $L,M\in\mathbb{Q}$. Comparing the terms of degree five one sees immediately that $p=0$ and so it remains to solve the system

$$\begin{cases} b_4+a_3h-2q=0,\\ b_3+a_2h+a_3k+h^3-2r=0,\\ b_2+a_1h+a_2k+3kh^2-q^2=0.\end{cases} \tag{9}$$

On putting $h=\varrho$ one obtains the following solutions of (9), depending not only on the coefficients of $A(T)$ and $B(T)$, but also on the parameter ϱ:

$$q=\frac{a_3\varrho+b_4}{2},\qquad k=\frac{a_3\varrho^2+(2a_3b_4-4a_1)\varrho+b_4^2-4b_2}{4(3\varrho^2+a_2)},$$
$$r=\frac{12\varrho^5+16a_2\varrho^3+w_2\varrho^2+w_1\varrho+w_0}{8(3\varrho^2+a_2)},$$

where $w_2=a_3^3+12b_3$, $w_1=2a_3b_4-4a_3a_1+4a_2^2$ and $w_0=4a_2b_3-4a_3b_2+a_3b_4^2$.

Corresponding to these solutions one has

$$L(\varrho) = -\frac{\Lambda(\varrho)}{16(3\varrho^2 + a_2)^2}, \qquad M(\varrho) = -\frac{\Theta(\varrho)}{64(3\varrho^2 + a_2)^3},$$

where Λ and Θ are suitable polynomials in ϱ of degree 8 and 12 respectively. If we write $\Lambda(\varrho) = l_8\varrho^8 + l_7\varrho^7 + l_6\varrho^6 + l_5\varrho^5 + l_4\varrho^4 + l_3\varrho^3 + l_2\varrho^2 + l_1\varrho + l_0$ we can verify that

$$\begin{aligned}
l_8 &= 72a_3,\\
l_7 &= \underline{72b_4},\\
l_6 &= 120a_2a_3,\\
l_5 &= 3a_3^4 + 72a_3b_3 + 120a_2b_4 - 144a_0,\\
l_4 &= 6a_3^3b_4 - 12a_3^2a_1 + 56a_3a_2^2 + 72b_4b_3 - 144b_1,\\
l_3 &= 2a_3^4a_2 + 48a_3a_2b_3 + 56a_2^2b_4 - 96a_2a_0,\\
l_2 &= 6a_3^3a_2b_4 - 12a_3^2a_2a_1 + 8a_3a_2^3 - 6a_3b_4^3\\
&\quad + 24a_3b_4b_2 + 48a_2b_4b_3 - 96a_2b_1 + 12a_1b_4^2 - 48a_1b_2,\\
l_1 &= 6a_3^2a_2b_4^2 - 8a_3^2a_2b_2 + 8a_3a_2^2b_3 - 16a_3a_2a_1b_4\\
&\quad - \underline{3b_4^4} - \underline{48b_2^2} - 16a_0a_2^2 + \underline{24b_4b_2^2} + 16a_1^2a_2 + 8a_2^3b_4,\\
l_0 &= 2a_3a_2b_4^3 - 8a_3a_2b_4b_2 + 8a_2^2b_3b_4 - 16a_2^2b_1 - 4a_2a_1b_4^2 + 16a_2a_1b_2.
\end{aligned}$$

(For the reader's convenience we have underlined the terms which do not vanish when $A(t) = 0$; this information is quite irrelevant for the proof.)

In particular $L(\varrho)$ is constant only in the following two cases:

(i) $a_3 = 0$, $a_2 = 0$, $a_0 = 0$, $b_4 = 0$, $b_2 = 0$, $b_1 = 0$,
(ii) $a_3 = 0$, $a_1 = 0$, $a_0 = 0$, $b_4 = 0$, $b_2 = 0$, $b_1 = 0$,

namely, when $L(\varrho)$ is identically zero. We will discuss cases (i) and (ii) separately. We may therefore suppose that $L(\varrho)$ is not identically zero. Let

$$V = \{\varrho \in \mathbb{Q} \mid 3\varrho^2 + a_2 \neq 0,\ \Lambda(\varrho) \neq 0\};$$

then V is an infinite set (indeed, $\mathbb{Q} \setminus V$ contains at most 10 elements). If for each $\varrho \in V$ we set

$$T(\varrho) = -\frac{M(\varrho)}{L(\varrho)} = -\frac{\Theta(\varrho)}{4(3\varrho^2 + a_2)\Lambda(\varrho)}$$

then $L(\varrho)T(\varrho) + M(\varrho) = 0$, and so on substituting into (8) we find that the point P_ϱ with coordinates $(x(\varrho), y(\varrho)) = (\varrho T(\varrho) + k(\varrho), T(\varrho)^3 + q(\varrho)T(\varrho) + r(\varrho))$ belongs to the elliptic surface

$$\mathscr{E}_\varrho:\ y^2 = x^3 + A(T(\varrho))x + B(T(\varrho)).$$

We now consider ϱ as an indeterminate. Via a change of coordinates of the type $X = \theta(\varrho)^2x$ and $Y = \theta(\varrho)^3y$, with a suitable $\theta \in \mathbb{Q}[\varrho]$, the equation of $\mathscr{E}_\varrho$ is transformed into an equation with coefficients in $\mathbb{Q}[\varrho]$:

$$\mathscr{E}'_\varrho :\ Y^2 = X^3 + \theta(\varrho)^4 A(T(\varrho))X + \theta(\varrho)^6 B(T(\varrho));$$

we choose $\theta \in \mathbb{Q}[\varrho]$ of minimal degree with respect to this property. The new coordinates of the point P_ϱ are $X(\varrho) = \theta(\varrho)^2 x(\varrho)$ and $Y(\varrho) = \theta(\varrho)^3 y(\varrho)$, which are elements of $\mathbb{Q}[\varrho]$. If one calculates the abscissa of the point $2 \cdot P_\varrho$ by using the well known duplication formulas one obtains

$$\begin{aligned} &X(2 \cdot P_\varrho) \\ &\quad = \frac{X(\varrho)^4 - 2\theta(\varrho)^4 A(T(\varrho))X(\varrho)^2 - 8\theta(\varrho)^6 B(T(\varrho))X(\varrho) + \theta(\varrho)^8 A(T(\varrho))^2}{4Y(\varrho)^2} \\ &\quad = \left(\frac{\theta(\varrho)}{2y(\varrho)}\right)^2 \cdot \left(x(\varrho)^4 - 2A(T(\varrho))x(\varrho)^2 - 8B(T(\varrho))x(\varrho) + A(T(\varrho))^2\right) \end{aligned}$$

and one can verify that $X(2 \cdot P_\varrho) \in \mathbb{Q}(\varrho)$ but $X(2 \cdot P_\varrho) \notin \mathbb{Q}[\varrho]$. Thus, by the observation made at the beginning of the proof (but see also Chap. III, §12 of [5]), the point P_ϱ is not a torsion point of $\mathscr{E}'_\varrho$ and so $\mathrm{rk}(\mathscr{E}_\varrho) = \mathrm{rk}(\mathscr{E}'_\varrho) > 0$ for each $\varrho \in V$.

To prove the assertion in the special cases (i) and (ii) we may deal with the slightly more general case of $A(t) = a_2 t^2 + a_1 t + a_0$ and $B(t) = t^6 + b_3 t^3 + b_0$, which includes both (i) and (ii).

We put $X(T) = -T^2 + k$, $Y(T) = pT^2 + qT + r$ and seek to determine k, p, q, r as functions of the coefficients a_i and b_j in such a way that

$$X(T)^3 + A(T)X(T) + B(T) - Y(T)^2 = LT + M.$$

On setting $p = \varrho$ one easily obtains

$$q = \frac{b_3 - a_1}{2\varrho}, \qquad r = -\frac{4\varrho^6 + 4a_2\varrho^4 + 3b_3^2 - 6b_3a_1 + 3a_1^2}{24\varrho^3}, \qquad k = \frac{\varrho^2 + a_2}{3},$$

and in correspondence with these solutions one finds

$$L(\varrho) = \frac{4(a_1 + b_3)\varrho^6 + 4a_2(a_1 + b_3)\varrho^4 + 3(b_3^3 - 3b_3^2 a_1 + 3b_3 a_1^2 - a_1^3)}{24\varrho^2}.$$

If $L(\varrho)$ is identically zero one must have $b_3 = 0$ and $a_1 = 0$; excluding this case one can proceed exactly as in the general case.

Finally, let $A(t) = at^2$ and $B(t) = t^6 + b$ with a and b not both zero. In this case we put $X(T) = 2T^2 + hT + k$, $Y(T) = 3T^3 + pT^2 + qT + r$ and, reasoning as above, one obtains

$$p = 2\varrho, \qquad q = \frac{2\varrho}{3}, \qquad r = \frac{\varrho^3 - 3a\varrho}{18}, \qquad h = \varrho, \qquad k = \frac{\varrho^2 - a}{6}$$

(there is another solution for which $L(\varrho)$ vanishes identically), from which

$$L(\varrho) = \frac{\varrho^5 + 6a\varrho^3 + 9a^2\varrho}{108}, \quad M(\varrho) = \frac{\varrho^6 + 3a\varrho^4 - 9a^2\varrho^2 - 3a^3 + 648b}{648}.$$

In this case too one reaches the desired conclusion by proceeding as in the general case. ∎

REMARK 4.1. Corollary 1.4 is a particular case of Theorem C when $A(t) = 0$. In [6] this corollary was proved for all polynomials $B(t)$ of degree six such that $B(t) \neq B(-t)$. Thus, the case $A(t) = 0$ and $B(t) = t^6 + b_4t^4 + b_2t^2 + b_0$ with $B(t) \neq t^6$ holds a particular interest. In this case, with the notation used in the proof of Theorem C, one obtains

$$x(\varrho) = -\frac{216\varrho^{12} - 36(b_4^3 - 4b_4b_2 + 24b_0)\varrho^6 + (b_4^2 - 4b_2)^3}{18(24b_4\varrho^6 - (b_4^2 - 4b_2)^2)\varrho^2}$$

provided that b_4 and b_2 are not both zero. If $b_4 = b_2 = 0$ one has

$$x(\varrho) = \frac{\varrho^{12} - 2^3 \cdot 3^4 \cdot b_0\varrho^6 + 2^6 \cdot 3^8 \cdot b_0^2}{18\varrho^{10}}.$$

REMARK 4.2. We again consider the case of the elliptic surface $\mathscr{E}^g$: $y^2 = x^3 + g(t)$ with $g(t) = b_6t^6 + b_4t^4 + b_3t^3 + b_2t^2 + b_1t + b_0$. To obtain the conclusions of Corollary 1.4 it is not necessary that $b_6 = 1$. Indeed, the result continues to hold in the following two cases:

- $b_6 \in (\mathbb{Q}^*)^2$ and b_4, b_2 and b_1 do not vanish simultaneously. If we write $b_6 = B^2$ then the expression
$$\left(\varrho T - \frac{4b_2B^2 - b_4^2}{12B\varrho}\right)^3 - \left(BT^3 + \frac{b_4}{2B}T + \frac{\varrho^3 + b_3}{2B}\right)^2 + g(T)$$
is linear in T and equals $L_1(\varrho)T + M_1(\varrho)$ where L_1 and M_1 are suitable rational functions of ϱ depending on the coefficients of $g(t)$, in particular
$$L_1(\varrho) = -\frac{24B^2b_4\varrho^6 + 24B^2B_4b_3\varrho^3 - 16B^4b_2^2 + 8B^2b_4^2b_2 - b_4^4}{48B^4\varrho^3}.$$
Under the hypothesis that b_4, b_2, b_1 do not vanish simultaneously one sees that $L_1(\varrho)$ does not vanish. Thus, proceeding as in the proof of Theorem C, one can conclude that there exist infinitely many $k \in \mathbb{Q}$ such that $\mathrm{rk}(\mathscr{E}^g(k)) > 0$.
- $b_6 \in (\mathbb{Q}^*)^3$ and b_3 and b_1 do not vanish simultaneously. If we write $b_6 = B^3$ then the expression
$$\left(-BT^2 + \frac{\varrho^2 - b_4}{3B^2}\right)^3 - \left(\varrho T^2 + \frac{b_3}{2\varrho}T - V(\varrho)\right)^2 + g(T),$$
where
$$V(\varrho) = \frac{4\varrho^6 - 8b_4\varrho^4 - 4(3B^3b_2 - b_4^2)\varrho^2 + 3B^3b_3}{24B^3\varrho^3},$$
is linear in T and is equal to $L_2(\varrho)T + M_2(\varrho)$ with L_2 and M_2 rational functions of ϱ depending on the coefficients of $g(t)$. In particular,

$L_2(\varrho) = b_3\varrho^{-1}V(\varrho)$. Under the hypothesis that b_3 and b_1 do not vanish simultaneously one finds that $L_2(\varrho)$ does not vanish. Thus, proceeding as in the proof of Theorem C, one can again conclude that there exist infinitely many $k \in \mathbb{Q}$ such that $\mathrm{rk}(\mathscr{E}^g(k)) > 0$.

EXAMPLE 4.3 (see Example 3.5 of [6]). Let

$$\mathscr{E}:\ y^2 = x^3 + t^6 + t^2 + 1.$$

If one writes $x = ht + k$ and $y = t^3 + qT + r$ one finds immediately that, on setting $h = \varrho$, $q = 0$, $r = \frac{1}{2}\varrho^3$ and $k = -(3\varrho)^2$, one has

$$t^6 + t^2 + 1 + \left(\varrho t - \frac{1}{3\varrho^2}\right)^3 - \left(t^3 + \frac{\varrho^3}{2}\right)^2 = \frac{1}{3\varrho^3}t - \frac{27\varrho^{12} - 108\varrho^6 + 4}{108\varrho^6}$$

where the right hand side vanishes for

$$t = \frac{27\varrho^{12} - 108\varrho^6 + 4}{36\varrho^3}.$$

Thus

$$P_\varrho(x(\varrho), y(\varrho)) \in \mathscr{E}\left(\frac{27\varrho^{12} - 108\varrho^6 + 4}{36\varrho^3}\right)$$

where

$$x(\varrho) = \frac{27\varrho^{12} - 108\varrho^6 - 8}{36\varrho^2},$$

$$y(\varrho) = \frac{19836\varrho^{36} - 236196\varrho^{30} + 953532\varrho^{24} - 1326780\varrho^{18} + 14126\varrho^{12} - 5184\varrho^6 + 64}{46656\varrho^9}.$$

EXAMPLE 4.4 (see the second part of Remark 4.2 in [6]). Let $g(t) = t^6 + 6t^4 + 6t^3 + 9t^2 - 150t$. Applying the method used in the proof of Theorem C and putting, for simplicity, $h = 2\sigma$, one obtains

$$(t^3 + 3t + 3 + 4\sigma^3)^2 - (2\sigma t)^3 - g(t) = 24(\sigma^3 + 7)t + (4\sigma^3 + 9)^2,$$

which yields

$$x(\sigma) = -\frac{\sigma(4\sigma^3 + 3)^2}{12(\sigma^3 + 7)} \quad \text{and} \quad y(\sigma) = \frac{8\Gamma(\sigma) - 13462119}{13824(\sigma^3 + 7)^3}$$

where

$$\Gamma(\sigma) = 512\sigma^{18} + 2304\sigma^{15} + 864\sigma^{12} - 92448\sigma^9 - 878634\sigma^6 - 2850903\sigma^3.$$

We note that in this particular case there exists another solution which is obtained by putting $h = 0$ in view of the identity

$$(t^3 + 3t + 3)^2 = t^6 + 6t^4 + 6t^3 + 9t^2 + 18t + 9$$

(this is probably the reason why this example was given in [6]).

Proof of Corollary 1.5. On setting $B(z) = g(z)$ and $A(z) = 0$ with the notation of the proof of Theorem C, the relation

$$y(\varrho)^2 - x(\varrho)^3 - g(T(\varrho)) = -LT(\varrho) - M$$

holds identically. Putting $T = -(\tau + M)/L$ one obtains

$$y(\varrho)^2 - x(\varrho)^3 - g\left(-\frac{\tau + M(\varrho)}{L(\varrho)}\right) = \tau$$

for every $\varrho \in \mathbb{Q}$, which proves the assertion. ∎

Proof of Corollary 1.6. We discuss only the case $d = 1$ since the case $d = -1$ is quite similar.

So let $g(z) = z^6 + 2bz^3 + z$; applying the method used in the proof of Theorem C and putting $h = 2\sigma$, one gets the identity

$$(T^3 + b + 4\sigma^3)^2 - (2\sigma T)^3 - g(T) = -T + (4\sigma^3 + b)^2.$$

Writing $n = -T + (4\sigma^3 + b)^2$ and varying the parameter σ in $\mathbb{Z}$ one obtains infinitely many desired solutions. ∎

Proof of Theorem D. Let $A(t) = a_4t^4 + a_3t^3 + a_2t^2 + a_1t + a_0$ and $B(t) = t^6 + b_4t^4 + b_3t^3 + b_2t^2 + b_1t + b_0$. We prove that given the elliptic surface

$$\mathscr{E} :\ y^2 = x^3 + A(t)x + B(t)$$

there exist infinitely many $k \in \mathbb{Q}$ such that $\mathrm{rk}(\mathscr{E}(k)) > 0$ provided that there exist infinitely many rational points on the curve

$$\mathcal{H} :\ v^2 = H(u)$$

where $H(u) = h_4u^4 + h_3u^3 + h_2u^2 + h_1u + h_0$ and the coefficients h_i are related to those of $A(t)$ and $B(t)$ by the relations (†).

If $a_4 = 0$ the assertion follows from Theorem C. Suppose, therefore, that $a_4 \neq 0$. We put $X(T) = hT + k$, $Y(T) = T^3 + pT^2 + qT + r$ and seek to determine h, k, p, q, r as functions of the coefficients a_i and b_j in such a manner that

$$X(T)^3 + A(T)X(T) + B(T) - Y(T)^2 = LT + M$$

with $L, M \in \mathbb{Q}$. By equating the coefficients of the terms of the same degree one obtains the system

$$\begin{cases} a_4h - 2p = 0, \\ b_4 + a_3h + a_4k - 2q - p^2 = 0, \\ b_3 + a_2h + a_3k + h^3 - 2r - 2pq = 0, \\ b_2 + a_1h + a_2k + 3kh^2 - 2rp - q^2 = 0. \end{cases} \tag{10}$$

On solving the first three equations of (10) in p, q, r one obtains

$$p = \frac{1}{2}a_4 h, \qquad q = \frac{1}{8}(4b_4 + 4a_3 h + 4a_4 k - a_4^2 h^2),$$
$$r = \frac{1}{16}(8b_3 + 8a_2 h + 8a_3 k + 8h^3 - 4a_4 b_4 h - 4a_4 a_3 h^2 - 4a_4^2 hk + a_4^3 h^3).$$

Substituting these values into the last equation of (10) gives rise to an equation of degree two in k with discriminant D satisfying

$$16D = H(h).$$

Hence under our hypotheses, system (10) admits infinitely many solutions. The rest of the argument is completely analogous to that in the proof of Theorem C. ■

References

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.

[2] R. Munshi, *Density of positive rank fibers in an elliptic fibration, II*, Int. J. Number Theory 6 (2010), 15–23.

[3] B. Segre, *On arithmetical properties of quadric and quartic surfaces*, Proc. London Math. Soc. 49 (1947), 353–395.

[4] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

[5] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.

[6] M. Ulas, *Rational points on certain elliptic surfaces*, Acta Arith. 129 (2007), 167–185.

[7] —, *Rational points on certain del Pezzo surfaces of degree one*, Glasgow Math. J. 50 (2008), 557–564.

[8] M. Ulas and A. Togbe, *On the diophantine equation $z^2 = f(x)^2 \pm f(y)^2$*, Publ. Math. Debrecen 76 (2010), 183–201.

Enrico Jabara
Dipartimento di Filosofia e Beni Culturali
Università di Ca' Foscari
Dorsoduro 3484/D
30123 Venezia, Italy
E-mail: jabara@unive.it

Received on 12.2.2011
and in revised form on 2.8.2011 (6618)