GLASNIK MATEMATIČKI
Vol. 47(67)(2012), 265 – 275

A REMARK ON THE INJECTIVITY OF THE SPECIALIZATION HOMOMORPHISM

Ivica Gusić and Petra Tadić
University of Zagreb, Croatia

Abstract. Let

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3),$$

be a nonconstant elliptic curve over $\mathbb{Q}(T)$. We give sufficient conditions for a specialization homomorphism to be injective, based on the unique factorization in $\mathbb{Z}[T]$ and $\mathbb{Z}$.

The result is applied for calculating exactly the Mordell-Weil group of several elliptic curves over $\mathbb{Q}(T)$ coming from a paper by Rubin and Silverberg.

1. Introduction

Let $E = E(T)$ be a nonconstant elliptic curve over $\mathbb{Q}(T)$, i.e. an elliptic curve that is not isomorphic over $\mathbb{Q}(T)$ to an elliptic curve over $\mathbb{Q}$. By Silverman's specialization theorem ([6, Theorem III.11.4]), for all but finitely many $t \in \mathbb{Q}$, the specialization homomorphism

$$E(\mathbb{Q}(T)) \to E(t)(\mathbb{Q})$$

is injective, where $E(t)$ is the specialization of $E(T)$. Therefore the rank of $E(\mathbb{Q}(T))$ is finite and, by Mazur's theorem, the torsion group of $E(\mathbb{Q}(T))$ is one of the following groups:

$$\mathbb{Z}/n\mathbb{Z},\ 1 \leq n \leq 10 \text{ or } n = 12, \text{ or } \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ 1 \leq n \leq 4. \tag{1.1}$$

Here we observe nonconstant elliptic curves E over $\mathbb{Q}(T)$ given by an equation of the form

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3),\ e_1, e_2, e_3 \in \mathbb{Z}[T], \tag{1.2}$$

2010 *Mathematics Subject Classification.* 11G05, 14H52.
Key words and phrases. Elliptic curve, specialization homomorphism, rank, generators.

and give sufficient conditions on the coefficients of the curve (specifically $e_1(T), e_2(T), e_3(T)$) for a specialization homomorphism to be an injection. The details are in Section 3. Basically the factorization in the unique factorization domains $\mathbb{Z}[T]$ and $\mathbb{Z}$ plays a crucial role in the question of the injectivity of the specialization homomorphism.

The proof of this result uses the idea used in the paper by Dujella ([2, Theorem 4]), which relies on the homomorphism θ (see [3, 4.4]).

The obtained result may lead to determining the rank and even proving that a certain set of points are free generators of an elliptic curve over $\mathbb{Q}(T)$ in the form (1.2), basically by looking at an elliptic curve over $\mathbb{Q}$ (one of its specialized curves which satisfies the condition of the Theorem 3.1).

In Section 4 we apply the result to a certain family of elliptic curves from the paper by Rubin and Silverberg ([5, Theorem 4.1]). For several concrete elliptic curves over $\mathbb{Q}(T)$, we calculate the rank and prove that a given set of points are free generators over $\mathbb{Q}(T)$. This is done by observing the curve's coefficients in $\mathbb{Q}(T)$ and in addition the rank and torsion and free generators of an elliptic curve over $\mathbb{Q}$ (one of its specializations). The key to this is the existence of efficient algorithms for finding free generators of a large class of elliptic curves over $\mathbb{Q}$, which is available through John Cremona's program *mwrank* ([1]).

2. The homomorphism θ

Let K be the field of rational numbers $\mathbb{Q}$ or the field of rational functions $\mathbb{Q}(T)$ in the variable T over $\mathbb{Q}$, let R be the ring of integers $\mathbb{Z}$ or the ring $\mathbb{Z}[T]$ of polynomials in the variable T over $\mathbb{Z}$, respectively. Thus, R is a unique factorization domain.

Let us define the maps

$$\theta_i^K : E(K) \to K^\times/(K^\times)^2,\ i = 1, 2, 3$$

by

$$\begin{aligned} \theta_i^K(x, y) &= x - e_i, \text{ if } x \neq e_i, \\ \theta_i^K(e_i, 0) &= (e_j - e_i)(e_k - e_i), \text{ where } i \neq j \neq k \neq i, \\ \theta_i^K(O) &= 1. \end{aligned}$$

Put $\theta^K := (\theta_1^K, \theta_2^K, \theta_3^K)$. Note that $K^\times/(K^\times)^2$ has a natural structure of a multiplicative group. Then $(K^\times/(K^\times)^2)^3$ has the corresponding group structure of the direct product.

Lemma 2.1. *The map $\theta^K : E(K) \to (K^\times/(K^\times)^2)^3$ is a homomorphism of groups with the kernel $2E(K)$. Thus, $Im(\theta^K) \cong E(K)/2E(K)$.*

Proof. The first part of the statement is in [3, Chapter 6, Proposition (4.3)]. The second part follows from [3, Chapter 1, Theorem (4.1)]. □

We restrict consideration to nonconstant elliptic curves E over K given by

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3),\ e_j \in R.$$

It is easy to see that $E(K)/2E(K)$ has $2^{\mathrm{rank}(E(K))+2}$ elements.

For each $P \in E(K)$ there exists exactly one triple

$$\mu^K := (\mu_1^K, \mu_2^K, \mu_3^K) \in (R^\times)^3,$$

where $\mu_j^K = \mu_j^K(P),\ j = 1, 2, 3$, such that the following three conditions are satisfied

(i)

$$\theta_1^K(P) \equiv \mu_1^K \mu_2^K (\mathrm{mod}\ (K^\times)^2),$$
$$\theta_2^K(P) \equiv \mu_1^K \mu_3^K (\mathrm{mod}\ (K^\times)^2),$$
$$\theta_3^K(P) \equiv \mu_2^K \mu_3^K (\mathrm{mod}\ (K^\times)^2),$$

(ii) μ_j^K are square-free and pairwise coprime in R, and

(iii) If $R = \mathbb{Z}[T]$ then the leading coefficient of $\mu_1^{\mathbb{Q}(T)} \in \mathbb{Z}[T]$ is positive, and if $R = \mathbb{Z}$ then $\mu_1^{\mathbb{Q}} \in \mathbb{Z}$ is positive.

Remark 2.2. Note that since $e_1, e_2, e_3 \in R$ we have

$$\mu_1^K | e_1 - e_2,\ \mu_2^K | e_1 - e_3,\ \mu_3^K | e_2 - e_3.$$

These relations will be crucial in the proof of Theorem 3.1.

It is easy to see that

$$\mu^K(P) = \mu^K(Q) \text{ if and and only if } \theta^K(P) = \theta^K(Q).$$

Therefore, by Lemma 2.1,

$$\mu^K(P) = \mu^K(Q) \text{ if and only if } Q - P \in 2E(K). \tag{2.2}$$

Especially,

$$\mu^K(P) = (1, 1, 1) \text{ if and only if } P \in 2E(K). \tag{2.3}$$

We will be using θ and (μ_1, μ_2, μ_3) for $R = \mathbb{Z}[T]$ and $K = \mathbb{Q}(T)$.

3. The injectivity of the specialization homomorphism

The main theorem in this section gives sufficient conditions on the coefficients of elliptic curves over $\mathbb{Q}(T)$ in the form (1.2), for a specialization homomorphism $T \mapsto t_0$ to be injective. Specifically, if the factors in the factorization of $(e_1(T) - e_2(T)) \cdot (e_1(T) - e_3(T)) \cdot (e_2(T) - e_3(T))$ in $\mathbb{Z}[T]$ evaluated at $T = t_0$ have a certain property concerning its factorizations in $\mathbb{Z}$, then the injectivity of the specialization homomorphism $T \mapsto t_0$ can be concluded.

Before the main theorem we mention the following. For a given non-zero rational number $q = \frac{a}{b}$, $(a, b \in \mathbb{Z})$, let $\mathrm{core}(q)$ denote the *integer square-free part* of q, meaning the integer that is the the square-free part of $a \cdot b$. For example, the integer square-free part of $\frac{5}{12}$ is 15. For a non-zero integer m let $\mathrm{rad}(m)$ (called the *radical* of m) denote the product of all different prime divisors of m.

THEOREM 3.1. *Let $t_0 \in \mathbb{Q}$. Let E be the nonconstant elliptic curve over $\mathbb{Q}(T)$, given by the equation*

$$E = E(T) : y^2 = (x - e_1)(x - e_2)(x - e_3), (e_1, e_2, e_3 \in \mathbb{Z}[T]).$$

Factor

$$(e_1 - e_2) \cdot (e_1 - e_3) \cdot (e_2 - e_3) = a \cdot f_1^{a_1}(T) \cdots f_k^{a_k}(T),$$

where $a \in \mathbb{Z}$ and $f_i \in \mathbb{Z}[T]$ irreducible (of positive degree) and $a_i \geq 1$. Assume that for each $i = 1, \ldots, k$ the integer square-free part of each of $f_i(t_0)$ has at least one prime factor that doesn't appear in the integer square-free part of any of the other $f_j(t_0)$ $(\forall j \neq i)$ and doesn't appear in the factorization of the radical of a. This condition includes the assumption that $f_i(t_0)$ is nonzero $(i = 1, \ldots, k)$.

With the above notations the condition can be written as:

$$\frac{|\mathrm{core}(f_i(t_0))|}{\mathrm{rad}[\gcd(\mathrm{core}(f_i(t_0)), \mathrm{rad}(a)) \cdot \prod_{j=1, j\neq i}^{k} \gcd(\mathrm{core}(f_i(t_0)), \mathrm{core}(f_j(t_0)))]} > 1,$$

for all $i = 1, \ldots, k$. Then the specialization homomorphism $E(\mathbb{Q}(T)) \to E(t_0)(\mathbb{Q})$ is injective.

PROOF. Since $(e_1(t_0) - e_2(t_0)) \cdot (e_1(t_0) - e_3(t_0)) \cdot (e_2(t_0) - e_3(t_0)) \neq 0$, the specialization $E(t_0)$ of $E(T)$ is an elliptic curve.

Let $P \in E(\mathbb{Q}(T)) \setminus \{O\}$. Then the first coordinate of P is of the form $\frac{p(T)}{q(T)^2}$ with $p(T), q(T) \in \mathbb{Z}[T]$ coprime. Therefore

$$\begin{cases} p(T) - e_1(T)q^2(T) = \mu_1^{\mathbb{Q}(T)}(P)\mu_2^{\mathbb{Q}(T)}(P)\square_{\mathbb{Z}[T]}, \\ p(T) - e_2(T)q^2(T) = \mu_1^{\mathbb{Q}(T)}(P)\mu_3^{\mathbb{Q}(T)}(P)\square_{\mathbb{Z}[T]}, \\ p(T) - e_3(T)q^2(T) = \mu_2^{\mathbb{Q}(T)}(P)\mu_3^{\mathbb{Q}(T)}(P)\square_{\mathbb{Z}[T]}, \end{cases}$$

where $\square_{\mathbb{Z}[T]}$ denotes a square of an element of $\mathbb{Z}[T]$. Let

$$\psi : E(\mathbb{Q}(T)) \to E(t_0)(\mathbb{Q})$$

be the specialization homomorphism (note that ψ is everywhere well-defined under the conditions of the theorem). Let $\bar{\mu}_j^{\mathbb{Q}(T)}(P)$, $j = 1, 2, 3$ denote the rational numbers obtained from $\mu_j^{\mathbb{Q}(T)}(P)$, by the specialization $T \mapsto t_0$.

- We first prove that $\psi(P) = O$ implies $P \in 2E(\mathbb{Q}(T))$: Let $P \in E(\mathbb{Q}(T)) \setminus \{O\}$, then $\psi(P) = O$ implies $q(t_0) = 0$ (while $p(t_0) \neq 0$). We mention that $P \neq (e_i(T), 0)$, $(i = 1, 2, 3)$, so we are in the first case in the definition of θ which we will use to prove the statement. Therefore

$$\begin{cases} p(t_0) = \bar{\mu}_1^{\mathbb{Q}(T)}(P)\bar{\mu}_2^{\mathbb{Q}(T)}(P)\square_{\mathbb{Q}}, \\ p(t_0) = \bar{\mu}_1^{\mathbb{Q}(T)}(P)\bar{\mu}_3^{\mathbb{Q}(T)}(P)\square_{\mathbb{Q}}, \\ p(t_0) = \bar{\mu}_2^{\mathbb{Q}(T)}(P)\bar{\mu}_3^{\mathbb{Q}(T)}(P)\square_{\mathbb{Q}}, \end{cases}$$

where $\square_{\mathbb{Q}}$ denotes a square of a rational number. We claim that $\mu_i^{\mathbb{Q}(T)}(P) \in \{-1, 1\}$, for each i. Assume, for example, that $\mu_2^{\mathbb{Q}(T)}(P) \notin \{-1, 1\}$. By multiplying the first two above relations, we get

$$p(t_0)^2 = \bar{\mu}_2^{\mathbb{Q}(T)}(P)\bar{\mu}_3^{\mathbb{Q}(T)}(P)\square_{\mathbb{Q}}. \tag{3.1}$$

- ► Assume that at least one of $\mu_2^{\mathbb{Q}(T)}(P), \mu_3^{\mathbb{Q}(T)}(P)$ has a positive degree. Then from Remark 2.2, the fact that $\mu_j^{\mathbb{Q}(T)}(P)$ are square-free and mutually coprime, and the condition of the Theorem, we conclude that $\bar{\mu}_2^{\mathbb{Q}(T)}(P)\bar{\mu}_3^{\mathbb{Q}(T)}(P)$ is not a square in $\mathbb{Q}$. It is in contradiction with (3.1).
- ► Assume that both $\mu_2^{\mathbb{Q}(T)}(P), \mu_3^{\mathbb{Q}(T)}(P)$ are constants. Since they are square-free and coprime, and $\mu_2^{\mathbb{Q}(T)}(P) \notin \{-1, 1\}$ we get a contradiction with (3.1).

Since we know that $\mu_i^{\mathbb{Q}(T)}(P) \in \{-1, 1\}$, for each i and using the fact that $\mu_1^{\mathbb{Q}(T)}(P) > 0$, we easily conclude that $\mu_i^{\mathbb{Q}(T)}(P) = 1$ for $i = 1, 2, 3$. Now we see that $\theta^{\mathbb{Q}(T)}(P) = (1, 1, 1)$, hence by (2.3) we have $P \in 2E(\mathbb{Q}(T))$.

Since $\psi(O) = O$ and $O \in 2E(\mathbb{Q}(T))$, we proved that $\psi(P) = O$ implies $P \in 2E(\mathbb{Q}(T))$.

- Now we prove that $\psi(P) \in 2\mathrm{Im}\psi$ if and only if $P \in 2E(\mathbb{Q}(T))$: if $\psi(P) \in 2\mathrm{Im}\psi$, then $\psi(P) = 2\psi(Q)$ for some $Q \in E(\mathbb{Q}(T))$, then $\psi(P-2Q) = O$, which implies, by the former, that $P-2Q \in 2E(\mathbb{Q}(T))$. So $P \in 2E(\mathbb{Q}(T))$. The rest is obvious.

We thus conclude that

$$E(\mathbb{Q}(T))/2E(\mathbb{Q}(T)) \cong \mathrm{Im}\psi/2\mathrm{Im}\psi. \tag{3.2}$$

Since ψ is injective on the torsion part [6, p. 272–273, proof of Theorem III.11.4], and since a possible form of the torsion part is

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ 1 \le n \le 4,$$

by (3.2) we conclude

$$2^{\mathrm{rank}(E(\mathbb{Q}(T))+2} = 2^{\mathrm{rank}(\mathrm{Im}(\psi))+2},$$

hence the rank of $E(\mathbb{Q}(T))$ is the same as the rank of $\mathrm{Im}(\psi)$.

Let $\bar{\psi} : E(\mathbb{Q}(T)) \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{Im}\psi \otimes_{\mathbb{Z}} \mathbb{Q}$ be the $\mathbb{Q}$-linear map corresponding to $\psi : E(\mathbb{Q}(T)) \to \mathrm{Im}\psi$. Since $\bar{\psi}$ is a surjective linear map among vector spaces of the same dimension, it is injective. By the fact that ψ is injective on the torsion part, we conclude that ψ is injective, too. □

This result could be applied to determining the rank (and even the free generators) of an elliptic curves over $\mathbb{Q}(T)$ in the form (1.2), by basically choosing a good candidate $t_0 \in \mathbb{Q}$ that of course satisfies the conditions of Theorem 3.1 and looking at an elliptic curve over $\mathbb{Q}$ (one of its specialized curves corresponding to $T = t_0$).

The following Corollary is used in the next section.

COROLLARY 3.2. *Let $t_0 \in \mathbb{Q}$. Let E be the nonconstant elliptic curve over $\mathbb{Q}(T)$ in the form* (1.2)*. If the condition from Theorem 3.1 is satisfied, and if*

$$|E(\mathbb{Q}(T))_{Tors}| = |E(t_0)(\mathbb{Q})_{Tors}|$$

and there exist $P_1, \dots, P_r \in E(\mathbb{Q}(T))$ such that $P_1(t_0), \dots, P_r(t_0)$ are the free generators of $E(t_0)(\mathbb{Q})$, then the specialization homomorphism

$$E(\mathbb{Q}(T)) \to E(t_0)(\mathbb{Q})$$

is an isomorphism.

Thus $E(\mathbb{Q}(T))$ and $E(t_0)(\mathbb{Q})$ have the same rank r, and $P_1, \dots, P_r$ are the free generators of $E(\mathbb{Q}(T))$.

PROOF. The specialization is obviously an epimorphism, and by Theorem 3.1 it is an isomorphism. □

REMARK 3.3. If $|E(t_0)(\mathbb{Q})_{\text{Tors}}| = 4$, then the condition $|E(\mathbb{Q}(T))_{\text{Tors}}| = |E(t_0)(\mathbb{Q})_{\text{Tors}}|$ is satisfied.

4. APPLICATION TO A FAMILY OF RUBIN AND SILVERBERG

Now we will give an example of the usage of the main Theorem 3.1 for obtaining new results concerning the paper by Rubin and Silverberg [5, Theorem 4.1]. We will determine the rank and free generators of several elliptic curves over $\mathbb{Q}(T)$ using Theorem 3.1 (moreover Corollary 3.2), by observing for each, its coefficients in $\mathbb{Z}[T]$ and one of its specialized curves over $\mathbb{Q}$. The possibility of determining the free generators of a large class of elliptic curve over $\mathbb{Q}$ is of essential importance for this, for which we use John Cremona's program *mwrank* ([1]).

The program *mwrank* uses 2-descent via 2-isogeny to determine the rank of an elliptic curve E over $\mathbb{Q}$, and obtain a set of points which generate $E(\mathbb{Q})$ modulo $2E(\mathbb{Q})$, and finally saturate it to a full basis over $\mathbb{Z}$ for $E(\mathbb{Q})$.

EXAMPLE 4.1. Let $a \in \mathbb{Q}^\times$, let $\lambda = -2a^2$, and let $g^{(a)}(T)$ be the polynomial of degree 12 in T

$$g^{(a)}(T) = 2N(\lambda, T)(N(\lambda, T) - 2D(\lambda, T)^2)(N(\lambda, T) - 2\lambda D(\lambda, T)^2),$$

where

$$\begin{aligned} D(\lambda,T) &= \lambda(2\lambda-1)T^2+2-\lambda,\\ N(\lambda,T) &= \lambda^2(\lambda+1)(2\lambda-1)^2T^4-4\lambda^2(\lambda-1)(2\lambda-1)T^3\\ &\quad +2\lambda(\lambda+1)(2\lambda^2-3\lambda+2)T^2\\ &\quad -4\lambda(\lambda-1)(\lambda-2)T+(\lambda-2)^2(\lambda+1). \end{aligned}$$

In [5, Theorem 4.1] it is proven that the elliptic curve $C^{(a)}$ over $\mathbb{Q}(T)$ with equation

$$g^{(a)}(T)y^2 = x(x-1)(x-\lambda)$$

has rank at least 3, with independent points $P^{(a)}, Q^{(a)}, R^{(a)} \in C^{(a)}(\mathbb{Q}(T))$ given by

$$\begin{aligned} P^{(a)} &= \left(\frac{N(\lambda,T)}{2D(\lambda,T)^2}, \frac{1}{4D(\lambda,T)^3}\right),\\ Q^{(a)} &= \left(\frac{\lambda^2(D(\lambda,T)^2-4\lambda T(T-1)(\lambda(2\lambda-1)T+2-\lambda))}{(\lambda(2\lambda-1)T^2-2\lambda(2\lambda-1)T+\lambda-2)^2},\right.\\ &\qquad \left.\frac{a\lambda}{(\lambda(2\lambda-1)T^2-2\lambda(2\lambda-1)T+\lambda-2)^3}\right),\\ R^{(a)} &= \left(\frac{D(\lambda,T)^2+4\lambda T(T-1)(\lambda(2\lambda-1)T+2-\lambda)}{\lambda(\lambda(2\lambda-1)T^2-(2\lambda-4)T+\lambda-2)^2},\right.\\ &\qquad \left.-\frac{a}{\lambda^2(\lambda(2\lambda-1)T^2-(2\lambda-4)T+\lambda-2)^3}\right). \end{aligned}$$

By [7, Section 4, Corollary 1] and [5, Remark 2.12], we know that the rank of $C^{(a)}$ over $\mathbb{Q}(T)$ is at most 5, for each a. Now we will show that for each integer value a, where $1 \le a \le 60$, the elliptic curve $C^{(a)}$ over $\mathbb{Q}(T)$ has rank exactly equal to 3 and torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, where free generators are the points

$$P^{(a)}, Q^{(a)}, R^{(a)} \in C^{(a)}(\mathbb{Q}(T))$$

given above. This strongly suggests that the rank in the family $C^{(a)}$ is constant and equals to 3, as well as that $P^{(a)}, Q^{(a)}, R^{(a)}$ are free generators.

The coordinate transformation

$$(x,y) \mapsto \left(g^{(a)}(T)\cdot x, g^{(a)}(T)^2\cdot y\right)$$

applied to the elliptic curve $C^{(a)}$ over $\mathbb{Q}(T)$ leads to the elliptic curve over $\mathbb{Q}(T)$ given by the equation

$$y^2 = x(x-g^{(a)}(T))(x-\lambda g^{(a)}(T)),$$

which we also denote by $C^{(a)}$. The corresponding points also remain denoted as the old ones. Then

$$e_1(T)=0,\ e_2(T)=g^{(a)}(T),\ e_3(T)=\lambda g^{(a)}(T),$$

and four torsion points are $O,\ (0,0),\ (g^{(a)}(T),0),\ (\lambda g^{(a)}(T),0)$.

PROPOSITION 4.2. *Let a be an integer such that $1 \leq a \leq 60$.*
The elliptic curve $C^{(a)}$ over $\mathbb{Q}(T)$ has rank 3, more precisely

$$C^{(a)}(\mathbb{Q}(T)) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^3,$$

and the points $P^{(a)}, Q^{(a)}, R^{(a)}$ are free generators of the group $C^{(a)}(\mathbb{Q}(T))$.

PROOF. Note that $C^{(a)}$ is a nonconstant elliptic curve over $\mathbb{Q}(T)$ for each $a \neq 0$, although its j-invariant is a rational constant. Therefore, we can apply Theorem 3.1 and Corollary 3.2. First we will give a detailed proof for $a = 1$

For $a = 1$ and $t_0 = 4$ we have

- the elliptic curve $C^{(1)}(4)$ over $\mathbb{Q}$ is given by the equation

$$y^2 = x^3 + 502511523471360x^2 - 505035662443014384369480499200x,$$

- the torsion group has four elements, *mwrank* ([1]) showed that $C^{(1)}(4)(\mathbb{Q})$ has rank 3 and free generators

$$G_1 = \left(-\frac{1689903343134720000}{1849}, -\frac{863283322778865481285632000}{79507}\right),$$
$$G_2 = (790444733644800, 20214846265347853516800),$$
$$G_3 = (13076929429218304, -1521697307273039513157632).$$

- using the commands `elladd` and `ellsub` in Pari ([4]) we obtain

$$P^{(1)}(4) = (-2g^{(1)}(4), 0) - G_2 - G_3,$$
$$Q^{(1)}(4) = (0,0) + G_1 + G_2,$$
$$R^{(1)}(4) = (-2g^{(1)}(4), 0) + G_2.$$

  Thus we conclude that $P^{(1)}(4),\ Q^{(1)}(4),\ R^{(1)}(4)$ are free generators of the group $C^{(1)}(4)(\mathbb{Q})$ which has rank 3.
- so we conclude that $\psi : C^{(1)}(\mathbb{Q}(T)) \to C^{(1)}(4)(\mathbb{Q})$ is a surjection.
- we have

$$e_1(T) = 0,\ e_2(T) = g^{(1)}(T),\ e_3(T) = -2g^{(1)}(T),$$

  so

$$(e_1(T) - e_2(T)) \cdot (e_1(T) - e_3(T)) \cdot (e_2(T) - e_2(T))$$
$$= -9172942848 \cdot (25T^4 + 60T^3 - 16T^2 - 24T + 4)^3$$
$$\cdot (25T^4 + 20T^3 + 8T^2 - 8T + 4)^3 \cdot (25T^4 - 20T^3 + 32T^2 + 8T + 4)^3,$$

thus

$$\begin{aligned} \mathrm{rad}(a) &= 6, \\ k &= 3, \\ f_1(T) &= 25T^4 + 60T^3 - 16T^2 - 24T + 4, \\ f_2(T) &= 25T^4 + 20T^3 + 8T^2 - 8T + 4, \\ f_3(T) &= 25T^4 - 20T^3 + 32T^2 + 8T + 4. \end{aligned}$$

If we take $t_0 = 4$ then we have the "prime" conditions of Theorem 3.1:

$$\begin{aligned} \mathrm{rad}(a) &= 2 \cdot 3, \\ f_1(4) &= 2^2 \cdot 2473, \\ f_2(4) &= 2^2 \cdot 5 \cdot 389, \\ f_3(4) &= 2^2 \cdot 13 \cdot 109. \end{aligned}$$

Thus the prime for $f_1(4)$ is 2473, the prime for $f_2(4)$ is 5 or 389, and the prime for $f_3(4)$ is 13 or 109.

Thus we conclude by Corollary 3.2 applied to $a = 1$ and $t_0 = 4$, that the specialization homomorphism $\psi : C^{(1)}(\mathbb{Q}(T)) \to C^{(1)}(4)(\mathbb{Q})$ is an isomorphism, so

$$C^{(1)}(\mathbb{Q}(T)) \cong C^{(1)}(4)(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^3,$$

and finally since $\psi(P^{(1)}), \psi(Q^{(1)}), \psi(R^{(1)})$ are free generators of $C^{(1)}(4)(\mathbb{Q})$ we conclude that $P^{(1)}, Q^{(1)}, R^{(1)}$ are free generators of $C^{(1)}(\mathbb{Q}(T))$ which has rank 3.

The Table 4.1. below, shows for integer values $a \in \{1, 2, \ldots, 60\}$, the corresponding t_0 for which the following conditions of the Corollary 3.2 are satisfied:

- the "prime" condition of Theorem 3.1 is satisfied for $e_1(T) = 0,\ e_2(T) = g^{(a)}(T),\ e_3(T) = \lambda g^{(a)}(T)$,
- the torsion subgroup of $C^{(a)}(t_0)(\mathbb{Q})$ has four elements,
- the rank of $C^{(a)}(t_0)(\mathbb{Q})$ is 3, and free generators G_1, G_2, G_3 are found using *mwrank* ([1])
- the combination of $P^{(a)}(t_0), Q^{(a)}(t_0), R^{(a)}(t_0)$ of the torsion point and the generators G_1, G_2, G_3 is checked, which shows that
$$P^{(a)}(t_0), Q^{(a)}(t_0), R^{(a)}(t_0)$$
are also the generators of $C^{(a)}(t_0)(\mathbb{Q})$

By Corollary 3.2 we conclude that for all integer values $a \in \{1, \ldots, 60\}$ the specialization $\psi : C^{(a)}(\mathbb{Q}(T)) \to C^{(a)}(t_0)(\mathbb{Q})$ is an isomorphism, so

$$C^{(a)}(\mathbb{Q}(T)) \cong C^{(a)}(t_0)(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^3,$$

and $P^{(a)}, Q^{(a)}, R^{(a)}$ are free generators of $C^{(a)}(\mathbb{Q}(T))$.

a	1	2	3	4	5	6	7	8	9	10
$\mathbf{t}_0$	4	$\frac{21}{2}$	-9	$-\frac{3}{20}$	5	6	$\frac{2}{7}$	$-\frac{3}{8}$	-7	$-\frac{5}{2}$
a	11	12	13	14	15	16	17	18	19	20
$\mathbf{t}_0$	-9	25	15	-10	25	$\frac{3}{16}$	-7	$-\frac{9}{2}$	-21	-8
a	21	22	23	24	25	26	27	28	29	30
$\mathbf{t}_0$	$\frac{25}{3}$	-9	-9	-8	-8	-10	-8	-7	4	-8
a	31	32	33	34	35	36	37	38	39	40
$\mathbf{t}_0$	-10	$-\frac{5}{32}$	-10	61	$\frac{7}{5}$	-6	4	$\frac{1}{2}$	4	-3
a	41	42	43	44	45	46	47	48	49	50
$\mathbf{t}_0$	$\frac{2}{41}$	$-\frac{23}{2}$	30	$\frac{6}{11}$	-6	-13	$-\frac{9}{47}$	$-\frac{11}{3}$	3	$\frac{13}{2}$
a	51	52	53	54	55	56	57	58	59	60
$\mathbf{t}_0$	$-\frac{7}{3}$	4	$\frac{55}{7}$	$\frac{11}{2}$	$\frac{47}{2}$	-6	13	$-\frac{15}{2}$	-5	$\frac{25}{3}$

Table 4.1. List of values a and corresponding t_0

For obtaining the table we observed t_0 that satisfy Corollary 3.2 such that the numerator is in absolute value ≤ 80 and the denominator minimal. We looked at t_0 for which the root number of $C^{(a)}(t_0)$ is -1 and after that we let *mwrank* try to calculate the rank (and free generators). ∎

Acknowledgements.

The authors would like to sincerely thank professor Andrej Dujella. This article would not have been possible without his kind support, help, suggestions and useful comments.

References

[1] J. E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge Univ. Press, 1997.
[2] A. Dujella, *A parametric family of elliptic curves*, Acta Arith. **94** (2000), 87–101.
[3] D. Husemöller, Elliptic Curves, Second Edition GTM **111**, Springer, New York, 2004.
[4] Pari/GP, version 2.3.3, Bordeaux, 2008, `http://pari.math.u-bordeaux.fr/`.
[5] K. Rubin and A. Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Experiment. Math. **10** (2001), 559–569.
[6] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, GTM **151**, Springer, Berlin, 1994.
[7] C. L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.

I. Gusić
Faculty of Chemical Engin. and Techn.
University of Zagreb
Marulićev trg 19, 10000 Zagreb
Croatia
E-mail: igusic@fkit.hr

P. Tadić
Geotechnical faculty
University of Zagreb
Hallerova aleja 7, 42000 Varaždin
Croatia
E-mail: petra.tadic.zg@gmail.com, ptadic@gfv.hr

Received: 14.1.2012.
Revised: 17.2.2012.