Journal of Number Theory 148 (2015) 137–152

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Injectivity of the specialization homomorphism of elliptic curves

Ivica Gusić [a], Petra Tadić [b,*,1]

[a] *Faculty of Chemical Engineering and Technology, University of Zagreb, Marulićev trg 19, 10000 Zagreb, Croatia*
[b] *Department of Economics and Tourism, Juraj Dobrila University of Pula, Preradovićeva 1, 52100 Pula, Croatia*

A R T I C L E I N F O

Article history:
Received 19 January 2013
Received in revised form 24 September 2014
Accepted 27 September 2014
Available online 31 October 2014
Communicated by David Goss

MSC:
11G05
14H52

Keywords:
Elliptic curve
Specialization homomorphism
Number field
Class number
Quadratic field
Cubic field
Rank
Pari
Magma

A B S T R A C T

Let $E : y^2 = x^3 + Ax^2 + Bx + C$ be a nonconstant elliptic curve over $\mathbb{Q}(t)$ with at least one nontrivial $\mathbb{Q}(t)$-rational 2-torsion point. We describe a method for finding $t_0 \in \mathbb{Q}$ for which the corresponding specialization homomorphism $t \mapsto t_0 \in \mathbb{Q}$ is injective. The method can be directly extended to elliptic curves over $K(t)$ for a number field K of class number 1, and in principal for arbitrary number field K. One can use this method to calculate the rank of elliptic curves over $\mathbb{Q}(t)$ of the form as above, and to prove that given points are free generators. In this paper we illustrate it on some elliptic curves over $\mathbb{Q}(t)$ from an article by Mestre.

* Corresponding author.
E-mail addresses: igusic@fkit.hr (I. Gusić), petra.tadic.zg@gmail.com (P. Tadić).

[1] The second author was supported by the Austrian Science Fund (FWF): P 24574-N26 and both authors were supported by the Croatian Science Foundation under the project No. 6422.

http://dx.doi.org/10.1016/j.jnt.2014.09.023

1. Introduction

Let

$$E = E(t) : y^2 = x^3 + Ax^2 + Bx + C \tag{1.1}$$

be a nonconstant (non-isotrivial) elliptic curve over $\mathbb{Q}(t)$, i.e., E is not isomorphic over $\mathbb{Q}(t)$ to an elliptic curve over $\mathbb{Q}$. For the sake of simplicity we will assume that $A, B, C \in \mathbb{Z}[t]$. It is known that the set $E(\mathbb{Q}(t))$ of $\mathbb{Q}(t)$-rational points of E is finitely generated. Let D denote the discriminant of the polynomial $f(x) := x^3 + Ax^2 + Bx + C$. We note that $D \in \mathbb{Z}[t]$. Let $t_0 \in \mathbb{Q}$ be such that $D(t_0) \neq 0$. Then by specializing t to t_0 the specialization $E(t_0)$ of $E(t)$ is an elliptic curve over $\mathbb{Q}$ and we have a specialization homomorphism $\sigma = \sigma_{t_0} : E(\mathbb{Q}(t)) \to E(t_0)(\mathbb{Q})$ (note that it is well defined). For more on this topic see [Sil4, Appendix C §20]. The specialization homomorphism can be defined for general non-split elliptic surfaces and in a more general situation. In 1952 A. Néron [Né] showed that the specialization fails to be injective for $t_0 \in \mathbb{Q}$ on a small subset (of density 0) (see [Se, Section 11.1]). J.H. Silverman [Sil1,Sil2] in 1983 using heights and J. Top in 1985 in his master's thesis (see [To]) by extending Néron's techniques proved the so called Silverman specialization theorem, which says that the specialization homomorphism is in fact injective for all but finitely many rational t_0. As far as we know, there is no practical algorithm for determining such a t_0 (for general non-split elliptic surfaces). As we learned from J.H. Silverman, all constants in [Sil2], Section 4, Theorem B, and Section 5, Theorem C can, in principal, be effectively computed. Therefore, one can find a computable constant C, such that for all algebraic t_0 with height greater than C, the specialization homomorphism at t_0 is injective. However, the constants are too large to be practical. Similarly for methods from [Sil3]. In this paper we use the ideas from Néron and Top (which also appear in [Ha]). We obtain a method for finding a specialization $t \mapsto t_0 \in \mathbb{Q}$ such that the specialization homomorphism is injective, in the case of elliptic curves of shape (1.1) having at least one non-trivial $\mathbb{Q}(t)$-rational 2-torsion point. This improves and extends the method from [GT1]. Let us state the main results (see Section 2 and Section 3 for the proofs):

Theorem 1.1. *Let E be a nonconstant elliptic curve over $\mathbb{Q}(t)$, given by the equation*

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

Assume that $t_0 \in \mathbb{Q}$ satisfies the following condition.

(A) For every nonconstant square-free divisor h in $\mathbb{Z}[t]$ of

$$(e_1 - e_2) \cdot (e_1 - e_3) \quad or \quad (e_2 - e_1) \cdot (e_2 - e_3) \quad or \quad (e_3 - e_1) \cdot (e_3 - e_2),$$

the rational number $h(t_0)$ is not a square in $\mathbb{Q}$.

Then the specialization homomorphism $\sigma : E(\mathbb{Q}(t)) \to E(t_0)(\mathbb{Q})$ is injective.