GLASNIK MATEMATIČKI
Vol. 35(55)(2000), 335 – 337

ON ISOGENIES OF ELLIPTIC CURVES

Ivica Gusić
University of Zagreb, Croatia

Abstract. We give a characterization of elliptic curves which are isogenous over two different quadratic extensions of a fixed number field.

1. Main Result

Let k be a number field and let A, B be elliptic curves over k. An isogeny between A and B is a nonzero morphism $f : A \to B$ which is a homomorphism of groups. We say that A, B are isogenous if there is an isogeny $f : A \to B$. If f is defined over an extension field K/k then we say that the elliptic curves are isogenous over K (or K-isogenous). The set of isogenies from A to itself, including the zero map, form a ring $\mathrm{End}(A)$ which is called the endomorphism ring of A. An elliptic curve A is said to have complex multiplication (CM for short) if its endomorphism ring $\mathrm{End}(A)$ is strictly larger then $\mathbf{Z}$. If an elliptic curve A defined over a number field has CM, then the algebra $K_0 = \mathrm{End}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ is a quadratic imaginary field over rationals. For basic definitions and results on elliptic curves see [1] and [3].

Let A be an elliptic curve over k defined by a Weierstrass equation $y^2 = f(x)$ and let $d \in k$ be a nonsquare. By A_d we denote the elliptic curve with equation $dy^2 = f(x)$. It is easy to see that A and A_d are isomorphic over $k(\sqrt{d})$.

Let k be a number field and let A, B be elliptic curves over k without complex multiplication. Then there exists quadratic extension K/k such that every isogeny $f : A \to B$ is defined over K (see [2, Remark 5.8]). Therefore, if A, B are isogenous over two different quadratic extensions of k, than A, B are isogenous over k. The following example shows that this is not true for elliptic curves with complex multiplication.

2000 *Mathematics Subject Classification.* 14H52.
Key words and phrases. elliptic curves with complex multiplication, isogeny.

EXAMPLE 1.1. Let A be the elliptic curve with Weierstreiss equation $y^2 = x^3 + 1$ and let A_3 be the elliptic curve with equation $3y^2 = x^3 + 1$. These elliptic curves have complex multiplication with the field of complex multiplication $K_0 = \mathbf{Q}(\sqrt{-3})$.

Put $\alpha(x, y) = (x, \frac{y}{\sqrt{3}})$. Then $\alpha : A \to A_3$ is an isomorphism defined over $\mathbf{Q}(\sqrt{3})$. Similarly $\beta : A \to A$, $\beta(x, y) = (\rho x, y)$, where ρ is a nontrivial third root of unity, is an isogeny defined over $\mathbf{Q}(\sqrt{-3})$. By [3, III, sect.9] the ring $\mathrm{End}(A)$ is an order in a quadratic imaginary field. Since $\mathbf{Z}[\beta]$ is a maximal order in $\mathbf{Q}(\sqrt{-3})$, we see that $\mathrm{End}(A)$ is generated as $\mathbf{Z}$-module by 1 and β, so any endomorphism of A is defined over $\mathbf{Q}(\sqrt{-3})$. Let σ be the nontrivial automorphism of $\mathbf{Q}(\sqrt{3}, \sqrt{-3})$ over $\mathbf{Q}(\sqrt{-1})$. Then $(\alpha\circ(2\beta+1))^\sigma = -\alpha \circ (-2\beta - 1) = \alpha \circ (2\beta + 1)$, so A and A_3 are isogenous both over $\mathbf{Q}(\sqrt{3})$ and over $\mathbf{Q}(\sqrt{-1})$.

Let $\phi : A \to A_3$ be an isogeny. Then $\phi = \alpha \circ (\alpha^{-1} \circ \phi)$. Since α is defined over $\mathbf{Q}(\sqrt{3})$, and $\alpha^{-1} \circ \phi$ is defined over $\mathbf{Q}(\sqrt{-3})$, we see that ϕ is defined over $\mathbf{Q}(\sqrt{-3}, \sqrt{3})$. Let σ be the nontrivial automorphism of $\mathbf{Q}(\sqrt{3}, \sqrt{-3})$ over $\mathbf{Q}(\sqrt{-3})$. Then $\phi^\sigma = (\alpha\circ(\alpha^{-1}\circ\phi))^\sigma = -\alpha\circ(\alpha^{-1}\circ\phi) = -\phi$. Therefore, A and A_3 are not isogenous over $\mathbf{Q}$ (in fact they are not isogenous over $\mathbf{Q}(\sqrt{-3})$).

We will show that the example is typical.

THEOREM 1.2. *Let k be a number field, let $K = k(\sqrt{d})$, $M = k(\sqrt{D})$ be different quadratic extension fields of k, for $d, D \in k$. Then:*

(a) *If A, B are elliptic curves over k such that A, B are isogenous both over K and over M and such that they are not isogenous over k, then:*
   (i) *B and A_d are isogenous over k.*
   (ii) *A and B have complex multiplication.*
   (iii) *$k(\sqrt{dD}) = kK_0$, where K_0 is the corresponding field of complex multiplication.*

(b) *If $k(\sqrt{dD}) = kK_0$, where K_0 is a quadratic imaginary field over $\mathbf{Q}$, and if A is an elliptic curve over k with the field of complex multiplication K_0, then A, A_d are isogenous both over K and over M, but they are not isogenous over k.*

PROOF. a) (i) Assume A is defined by a Weierstrass equation $y^2 = f(x)$. Let $\phi : B \to A$ be an isogeny defined over K and not defined over k, and let σ be the nontrivial automorphism of K over k. Then $\phi - \phi^\sigma : B \to A$ is an isogeny. Therefore $\alpha \circ (\phi - \phi^\sigma) : B \to A_d$, where $\alpha : A \to A_d$ is defined by $\alpha(x, y) = (x, \frac{y}{\sqrt{d}})$, is an isogeny defined over k.

(ii) Follows directly from [2, Remark 5.8]

(iii) Let $\phi_d : A \to B$ be a K-isogeny and let $\phi_D : B \to A$ be an M-isogeny. Then $\psi = \phi_D \circ \phi_d : A \to A$, is defined over KM. By [1, 5.1.3] ψ is defined over kK_0. Denote by σ the nontrivial automorphism of KM/k which is trivial on M and by τ the nontrivial automorphism of KM/k which is trivial on K.

By the proof of a) (i), we see that ϕ_d,ϕ_D can be chosen such that ${\phi_d}^\sigma = -\phi_d$ and ${\phi_D}^\tau = -\phi_D$. Therefore $\psi^\sigma = -\psi$, so ψ is not defined over M. Since ψ is defined over kK_0, we see that kK_0 is quadratic over k, and since ψ is defined over KM, we see that $kK_0 \subseteq KM$ (in contrary ψ would be defined over k). Also, $\psi^\tau = -\psi$, so ψ is not defined over K nor over M. Since ψ is defined over kK_0 we see that kK_0 is different both from K and from M. Therefore $kK_0 = k(\sqrt{dD})$.

b) Let α be as above, let σ be the nontrivial automorphism of KM/k which is trivial on M and let τ be the nontrivial automorphism of KM/k which is trivial on K. Choose any $\Phi \in \mathrm{End}A \setminus \mathbf{Z}$. By [1, 5.1.3 and 5.1.1] Φ is defined over kK_0, but Φ is not defined over k. Since σ is nontrivial on kK_0, $\Psi = \alpha \circ (\Phi - \Phi^\sigma) : A \to A_d$ is an isogeny defined over KM. In fact, Ψ is defined over M, because $\Psi^\sigma = (-\alpha) \circ (\Phi^\sigma - \Phi) = \Psi$. Therefore A and A_d are isogenous both over K and over M.

Let us prove that A and A_d are not isogenous over k. Moreover, we will prove that A and A_d are not isogenous over kK_0. Let $\theta : A \to A_d$ be any isogeny. Then $\theta = \alpha \circ (\alpha^{-1} \circ \theta)$. By [1, 5.1.3] $\alpha^{-1} \circ \theta$ is defined over kK_0, so since $kK_0 \subseteq KM$ we see that θ is defined over KM. Since $\theta^{\sigma\tau} = (-\alpha) \circ (\alpha^{-1} \circ \theta) = -\theta$, θ is not defined over kK_0.

COROLLARY 1.3. *Let A,B be elliptic curves defined over a number field k. If A and B are isogenous over three different quadratic extensions over k, then they are isogenous over k.*

REMARK 1.4. In the first version of the paper, the proof of the theorem has been based on the Faltings theorem on isogenies of abelian varieties. The present proof is more elementary and is suggested by the referee.

REFERENCES

[1] G.Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami Shoten Publishers and Princeton University Press, 1971.

[2] A.Silverberg, Fields of definition for homomorphism of abelian varieties, Journal of Pure and Applied Algebra, **77**, No3 (1992)253–264.

[3] J.Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, **106**, 1986.

University of Zagreb
Faculty of Chemical Engineering and Technology
pp. 177, 10 001 Zagreb
Croatia
E-mail: igusic@pierre.fkit.hr

Received: 24.09.1998.
Revised: 22.11.1999.
Revised: 26.07.2000.