ELSEVIER

Journal of Pure and Applied Algebra 115 (1997) 321–323

JOURNAL OF PURE AND APPLIED ALGEBRA

A remark on the torsion subgroups of elliptic curves

Jasbir Singh Chahal*

Department of Mathematics, Brigham Young University, Provo, UT 84602, USA

Communicated by K. Gruenberg; received 29 August 1984; revised 28 November 1985

Abstract

A uniform bound is given for the order of the torsion subgroup of $E(K)$, the group of K-rational points on an elliptic curve E defined over a number field k, with K quadratic over k.

1. Introduction

For an extension K/k of number fields let $E(K)$ denote the group of K-rational points on an elliptic curve E defined over k. The following theorem, conjectured by Ogg, was proved by Mazur [3].

Theorem 1. *If E is defined over $\mathbb{Q}$, then the torsion subgroup $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to one of the following groups*:

$$\mathbb{Z}/m\mathbb{Z} \quad \textit{for } 1 \leqslant m \leqslant 10 \textit{ or } m = 12,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \quad \textit{for } 1 \leqslant m \leqslant 4.$$

In fact, there is [1] a broader conjecture. Given a number field K, there is a constant $C = C(K)$, depending only on K, such that the order

$$|E(K)_{\text{tor}}| \leqslant C \tag{1}$$

for all elliptic curves E defined over K.

* E-mail: jasbir@math.byu.edu.

PII S0022-4049(96)00157-0

Demjanenko [2] claims to have proved the conjecture in its full generality, but his proof is so cumbersome [1] that no one has either checked it completely, or found an error in it (cf. [4]).

In this note we consider a field L belonging to a tower of quadratic extensions of $\mathbb{Q}$ and an elliptic curve E defined over $\mathbb{Q}$. We shall give a uniform bound for $|E(L)_{\mathrm{tor}}|$.

2. The main result

First we make a convention. If the conjecture is true for a certain number field K, we choose $C(K)$ to be the smallest (positive) integer such that (1) holds. Otherwise, we put $C(K) = \infty$.

Theorem 2. *Suppose K/k is a quadratic extension. Then*

$$|E(K)_{\mathrm{tor}}| \leqslant 4C(k)^2$$

for all E defined over k.

Actually, more is true. For a prime p, we denote the p-primary part of an abelian group G by $G^{(p)}$, and for an integer $N \geqslant 1$, $G[N] = \{g \in G\colon Ng = 0\}$ is the subgroup of N-division elements of G.

Theorem 3. *Suppose $G_1, \ldots, G_r$ are all the groups that can occur as $E(k)_{\mathrm{tor}}$ as E ranges over the elliptic curves defined over k and K/k is a quadratic extension. Then there is an exact sequence*

$$0 \to E(K)[2] \to E(K)_{\mathrm{tor}} \to G_i \times G_j$$

for some i, j.

Corollary 4. *If $p > 2$, then*

$$E(K)_{\mathrm{tor}}^{(p)} \subset G_i^{(p)} \times G_j^{(p)}$$

for some i, j.

It suffices to prove Theorem 3. Let E be defined by

$$y^2 = x^3 + Ax + B \quad (A, B \in k).$$

Then the Galois group $\mathrm{Gal}(K/k)$ with generator σ acts on $E(K)$ in an obvious way. For $P \in E(K)$, let $Q = (x, y)$ be the point $P - \sigma P$. If $P \in E(k)$, then $Q = 0$, otherwise

[1] During the twelve years that took this paper to see the light of the day, a very nice proof by Merel of this conjecture has appeared in Inv. Math. 124 (1996) 437–449.

from $(\sigma x, \sigma y) = \sigma Q = -Q = (x, -y)$ it follows that $x, y/\sqrt{d}$ are in k and hence the point $(x, y/\sqrt{d})$ lies on the twist

$$E_d : dy^2 = x^3 + Ax + B$$

of E. Define a map $\alpha : E(K) \to E_d(k)$ by

$$\alpha(p) = \left(x(P - \sigma P), \frac{y(P - \sigma P)}{\sqrt{d}} \right),$$

where $x(P)$ (resp. $y(P)$) denote the x (resp. y)-coordinate of a point P. The map α is a homomorphism for the composite map

$$E(K) \xrightarrow{\alpha} E_d(k) \hookrightarrow E_d(K) \cong E(K)$$

is clearly a homomorphism.

Now define a homomorphism $\Phi : E(K) \to E(k) \times E_d(k)$ by

$$\Phi(P) = (\mathrm{Tr}_{K/k}(P), \alpha(P)),$$

where $\mathrm{Tr}_{K/k} : E(K) \to E(k)$ is the trace map defined by

$$\mathrm{Tr}_{K/k}(P) = \sum_{\sigma \in G} \sigma P.$$

Clearly, $\mathrm{Ker}(\Phi) = E(K)$ [2].

Remarks. (1) Let $\mathrm{rank}_k(E)$ denote the number of independent generators of $E(k)$ modulo the torsion $E(k)_{\mathrm{tor}}$. Then,

$$\mathrm{rank}_K(E) \leqslant \mathrm{rank}_k(E) + \mathrm{rank}_k(E_d).$$

(2) If $k = \mathbb{Q}$ and $p \neq 2, 3, 5, 7$, we have for any quadratic extension K of $\mathbb{Q}$,

$$E(k)^{(p)} = 0.$$

In particular, $E(k)$ cannot have a point of order eleven.

Acknowledgements

I would like to thank Madhav V. Nori for his helpful comment on the previous manuscript.

References

[1] J.W.S. Cassels, Diophantine equations with special reference to elliptic curves, J. London Math. Soc. 41 (1966) 193–291.
[2] V.A. Demjanenko, On uniform boundedness of the torsion of elliptic curves over algebraic number fields, Math. USSR Izvestija 6 (1972) 477–490.
[3] B. Mazur, Lecture Notes in Math., Vol. 601 (Springer, Berlin, 1977).
[4] J. Tate, The arithmetic of elliptic curves, Invent. Math. 23 (1974) 179–206.