Journal of Pure and Applied Algebra 58 (1989) 261-265
North-Holland

ON THE MORDELL–WEIL RANK OF AN ABELIAN VARIETY OVER A NUMBER FIELD

Takeshi OOE
Department of Mathematics, Faculty of Science, University of Tokyo, Hongo, Tokyo, 113 Japan

Jaap TOP*
Rijksuniversiteit Utrecht, Mathematisch Instituut, Postbus 80.010, 3508 TA Utrecht, The Netherlands

Communicated by F. Oort
Received 22 March 1988
Revised 20 May 1988

Let K be a number field and A an abelian variety over K. The K-rational points of A are known to constitute a finitely generated abelian group (Mordell–Weil theorem). The problem studied in this paper is to find an explicit upper bound for the rank r of its free part in terms of other invariants of A/K. This is achieved by a close inspection of the classical proof of the so-called 'weak Mordell–Weil theorem'.

1. Introduction

Let K be a number field and A an abelian variety over K. The K-rational points of A are known to constitute a finitely generated abelian group (Mordell-Weil theorem) and it is an interesting question to give an explicit upper bound for the rank r of its free part in terms of other invariants of A/K.

In case A is an elliptic curve and $K=\mathbb{Q}$ there are already some theorems in this direction. For example, Tate proved the following (cf. [2, Chapter 6]):

"Let E be an elliptic curve over $\mathbb{Q}$ given by an equation $y^2=x^3+ax^2+bx$ with $a,b\in\mathbb{Z}$. Then $r\leq s+t+1$ where s and t are the numbers of prime divisors of b and a^2-4b respectively. (Note that the discriminant of this model of E is $2^4b^2(a^2-4b)$.)"

A somewhat sharper bound for elliptic curves over $\mathbb{Q}$ having $\mathbb{Q}$-rational (not necessarily 2-) torsion points can be found in [5], and for elliptic curves over $\mathbb{Q}$ having no rational 2-torsion points a similar bound is obtained in [1].

Under the assumption of very powerful conjectures (Birch and Swinnerton–Dyer, Taniyama–Weil and the generalized Riemann hypothesis), Mestre proves in [6] and

* Supported by the Dutch Organization for the Advancement of Pure Research (Z.W.O.).

[7] that for elliptic curves E over $\mathbb{Q}$, the asymptotic equality $r = O(\log N/\log\log N)$ (with N the conductor of $E/\mathbb{Q}$) holds. It seems to be beyond our present knowledge to obtain such a result without using these hypotheses. Mestre also mentions in the introduction of [6], that for elliptic curves $E/\mathbb{Q}$ one can prove $r = O(\log N)$ without using any conjectures. This type of bound is true for abelian varieties over number fields in general; our aim in this paper is to prove this fact.

More precisely our theorem is the following:

Theorem 1. *Let K be a number field and A an abelian variety over K. Write $d = [K:\mathbb{Q}]$, $g = \dim(A)$ and $r = \operatorname{rank}(A(K))$. Denote by $\mathcal{N}_{A/K}$ the conductor of A/K and by $N_{K/\mathbb{Q}}$ the norm with respect to $K/\mathbb{Q}$. Then one has*

$$r \le C_1 \log |N_{K/\mathbb{Q}} \mathcal{N}_{A/K}| + C_2 \tag{1}$$

where C_1 is a constant depending only on $[K:\mathbb{Q}]$ and on $\dim A$, and C_2 is another constant depending not only on $\dim A$ and on $[K:\mathbb{Q}]$ but also on the discriminant of $K/\mathbb{Q}$. In particular, one can take for C_1 and C_2 the values

$$C_1 = 2g \prod_{i=0}^{2g-1} (2^{2g} - 2^i)\left(1 + \frac{d}{\log 2}\left(d - 1 + \frac{\prod_{i=0}^{2g-1} (2^{2g} - 2^i) d \log d}{\log 2}\right)\right)$$

and

$$C_2 = 2g\left(2d - 1 + d \prod_{i=0}^{2g-1} (2^{2g} - 2^i) + \frac{d \log |\Delta_{K/\mathbb{Q}}| \prod_{i=0}^{2g-1} (2^{2g} - 2^i)^2}{\log 2}\right).$$

The proof will be a refinement of that of the (weak) Mordell–Weil theorem, as is already remarked in [6] for the case $K = \mathbb{Q}$, $\dim A = 1$.

2. A result from algebraic number theory

In this section we will prove the following:

Proposition 1. *Let K be a number field and L a finite extension of K. Denote by $\Delta_{L/K}$ the discriminant of this extension. Then for every prime ideal $\mathfrak{p}$ of K one has*

$$v_{\mathfrak{p}}(\Delta_{L/K}) \le [L:K] - 1 + [L:\mathbb{Q}] \log([L:K])/\log p. \tag{2}$$

where $v_{\mathfrak{p}}$ is the valuation at $\mathfrak{p}$ and p is the characteristic of the residue class field at $\mathfrak{p}$.

This is [10, Corollaire on p. 128]; see also [9, Chapter III, the end of §6]. The proof of it follows immediately from the corresponding local result:

Proposition 2. *Let $L_1 \subseteq L_2$ be a finite extension of local fields. Write, as usual, f for the degree of the corresponding extension of the residue class fields and e for the ramification index. Suppose that these residue class fields have characteristic $p > 0$. Denote by v_1 the discrete valuation on L_1. Then*

$$v_1(\Delta_{L_2/L_1}) \le f(e-1+ev_1(e)).$$

To prove this, write the extension as $L_1 \subseteq L_3 \subseteq L_2$, with L_3/L_1 unramified of degree f and L_2/L_3 totally ramified of degree e. One has $\Delta_{L_2/L_1} = \Delta^f_{L_2/L_3}$. Let v_i be the extention of v_1 to L_i for $i=2,3$ and $\mathscr{D}$ the different of L_2/L_3. Then

$$v_1(\Delta_{L_2/L_1}) = fv_3(\Delta_{L_2/L_3}) = fv_2(\mathscr{D}).$$

To compute $v_2(\mathscr{D})$, take a uniformizing element π of L_2. This element π satisfies an Eisenstein equation $f(\pi)=0$ for a polynomial f of degree e with coefficients in L_3. The ideal $\mathscr{D}$ is generated by $f'(\pi)$ and it is not hard to check that

$$v_2(f'(\pi)) \le e-1+v_3(e).$$

From this the proposition easily follows.

3. The main theorem

We will first give a corollary of Proposition 1.

Proposition 3. *For an abelian variety A defined over a number field K, let L be the field obtained by adjoining the coordinates of all m-torsion points of A to K. Denote by $\Delta_{L/K}$ the discriminant of L/K and by $\mathscr{N}_{A/K}$ the conductor of A/K. Then*

$$\Delta_{L/K} \mid (m\mathscr{N}_{A/K})^c \tag{3}$$

for a constant c depending only on m, $[K:\mathbb{Q}]$ and $\dim A$.

Proof. By [11], a prime dividing $\Delta_{L/K}$ divides either m or $\mathscr{N}_{A/K}$. Since $[L:K] \le \#\mathrm{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})$ (where $g=\dim A$), the proposition immediately follows from Proposition 1.

The following is essentially [12, Exercise 8.1].

Theorem 2. *K and A being as in Proposition* 1, *suppose that all m-torsion points of A are rational over K. Denote by $A(K)$ the group of K-rational points of A. For a finite abelian group G we let $\varrho(G)$ be the minimal number of generators of G. Then the following inequality holds*:

$$\varrho(A(K)/mA(K)) \le 2g\#S + 2g\varrho(\mathscr{H}_K[m]). \tag{4}$$

Here $g=\dim A$, S is the set consisting of archimedian primes, primes where A has bad reduction, and primes dividing m, $\mathscr{H}_K$ is the ideal class group of K, $\mathscr{H}_K[m]$ is its m-primary part.

Proof. Let $\bar{K}$ be an algebraic closure of K and G the Galois group of $\bar{K}/K$.

Multiplication by m yields an exact sequence of G-modules

$$0 \to A[m] \to A(\bar{K}) \to A(\bar{K}) \to 0$$

($A[m]$ is the group of m-torsion points of A). Using Galois cohomology we get an injective map

$$A(K)/mA(K) \to H^1(G, A[m]).$$

By the assumption it follows that $H^1(G, A[m]) = \mathrm{Hom}(G, A[m])$. Now denote by L the Galois extension of K obtained by adjoining to K the coordinates of all points $P \in A(\bar{K})$ such that $mP \in A(K)$. In fact from its definition it follows that the image of the map above consists of homomorphisms which are trivial on $\mathrm{Gal}(\bar{K}/L)$, hence we obtain an induced map

$$A(K)/mA(K) \to \mathrm{Hom}(G_{L/K}, A[m]),$$

where $G_{L/K}$ denotes the Galois group of L/K.

It is known that L has the following properties [8, Appendix II]:

(1) L/K is abelian and of exponent m.

(2) L/K is unramified outside S.

Such L/K is finite by Kummer theory and this fact is proven for example in [12, VIII, Proposition 1.6]. Close examination of this proof enables one to give an effective upper bound for $[L:K]$ as follows:

From each m-primary cyclic component of $\mathscr{H}_K$, take a generating ideal class and add a prime ideal representing it to S. We thus get a set of primes S' such that $\# S' = \# S + \varrho(\mathscr{H}_K[m])$ and that the ring of S'-integers $\mathcal{O}_{S'}$ has no m-torsion in its ideal class group. Let L' be the maximal abelian extension of K which is of exponent m and which is unramified outside S'. Then $L' = K(\sqrt[m]{a}; a \in \mathcal{O}_{S'}^* / \mathcal{O}_{S'}^{*m})$ and by Dirichlet's unit theorem (suitably modified version, see e.g. [4, V, § 1]), we find $\# S'$ cyclic components in $\mathcal{O}_{S'}^* / \mathcal{O}_{S'}^{*m}$.

So $G_{L/K}$ is a quotient of a subgroup of $(\mathbb{Z}/m\mathbb{Z})^{\# S'}$, thereby proving Theorem 2.

We are now ready to prove our main theorem.

Proof of Theorem 1. Let L be the extension of K generated by the 2-torsion points of A. We apply Theorem 2 to A/L and $m = 2$. Clearly $\mathrm{rank}\, A(K) \leq \mathrm{rank}\, A(L)$. For $S = S(A/L)$ as in Theorem 2 one has

$$\# S \leq [L:K] \log |N_{K/\mathbb{Q}} \mathcal{N}_{A/K}| + 2[L:\mathbb{Q}] \leq C(\log |N_{K/\mathbb{Q}} \mathcal{N}_{A/K}| + 2[K:\mathbb{Q}])$$

with $C = [L:K] \leq \# \mathrm{GL}_{2g}(\mathbb{Z}/2\mathbb{Z})$ bounded solely in terms of $g = \dim A$.

On the other hand, every ideal class of L contains an ideal $\mathscr{I}$ with $N_{L/\mathbb{Q}} \mathscr{I} \leq C' \sqrt{|\Delta_{L/\mathbb{Q}}|}$ for a constant C' depending only on $[K:\mathbb{Q}]$ and $\dim A$ (for an exact form of C', compare [3, V, Theorem 4]). Starting with a rational integer $a \leq C' \sqrt{|\Delta_{L/\mathbb{Q}}|}$, one finds there are at most $[L:\mathbb{Q}]^2 \log a$ prime ideals, so at most $a^{[L:\mathbb{Q}]}$ ideals which divide a. We thus get an inequality

$$\varrho(\mathscr{H}_L[2]) \leq [L:\mathbb{Q}]\log|\Delta_{L/\mathbb{Q}}|/\log 2 + 2^2\log C'.$$

But $|\Delta_{L/\mathbb{Q}}| = N_{K/\mathbb{Q}}(\Delta_{L/K})|\Delta_{K/\mathbb{Q}}|^{[L:K]}$ and by Proposition 3 it follows that $\Delta_{L/K} \mid (2\mathscr{N}_{A/K})^{\text{some constant}}$. Taking the logarithm, we obtain the desired inequality. It is a routine computation to arrive at the explicit constants mentioned in the statement of Theorem 1.

Acknowledgment

We would like to thank F. Beukers, B. Edixhoven and F. Oort for their interest in this work and for their useful advice. The first-named author would also like to express his gratitude to Japan Association for Mathematical Sciences and The Educational Project for Japanese Mathematicians. Without their support this collaboration would not have taken place. Finally it is a pleasure for us to thank the referee who suggested some useful improvements to an earlier version of this paper.

References

[1] A. Brumer and K. Kramer, The rank of elliptic curves, Duke Math. J. 44 (1977) 715–743.
[2] D. Husemöller, Elliptic Curves, Graduate Texts in Mathematics 111 (Springer, Berlin, 1987).
[3] S. Lang, Algebraic Number Theory (Addison–Wesley, Reading, MA, 1970).
[4] S. Lang, Fundamentals of Diophantine Geometry (Springer, Berlin, 1983).
[5] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Invent. Math. 25 (1974) 1–61.
[6] J.F. Mestre, Courbes elliptiques et formules explicites, in: Sém. de Théorie des Nombres, Paris, 1981/82, Progress in Mathematics 38 (Birkhäuser, Basel) 179–188.
[7] J.F. Mestre, Formules explicites et minorations de conducteurs de variétés algébriques, Compositio Math. 58 (1986) 209–232.
[8] D. Mumford, Abelian Varieties, (Oxford University Press, Oxford, 2nd ed., 1974).
[9] J.P. Serre, Corps Locaux (Hermann, Paris, 1968).
[10] J.P. Serre, Quelques applications du théorème de densité de Chebotarev, Publ. Math. I.H.E.S. 54 (1981) 123–201.
[11] J.P. Serre and J. Tate, Good reduction of abelian varieties, Ann. of Math. 88 (1968) 492–517.
[12] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 106 (Springer, Berlin, 1986).