Tôhoku Math. Journ.
39 (1987), 101-103.

THE MORDELL-WEIL RANK OF ELLIPTIC CURVES

JASBIR SINGH CHAHAL

(Received February 18, 1986)

Let E be an elliptic curve defined over a number field k (of finite degree). The Mordell-Weil Theorem states that the group $E(k)$ of k-rational points of E is finitely generated. Consequently, the group $E(k)_{\text{tor}}$ of points of finite order of $E(k)$ is finite.

Let L be the field obtained by adjoining to k all the roots of unity. It has been shown by Ribet (cf. [1]) that even for the infinite extension L/k, the group $E(L)_{\text{tor}}$ is still finite. However, as we will show here, $E(L)$ can never be finitely generated.

We will denote the Mordell-Weil rank of E over k by $r_k(E)$. It is the maximum number of free generators of $E(k)$.

THEOREM. *Suppose E is an elliptic curve defined over $\boldsymbol{Q}$ and r_0 is a positive integer. Then there is a finite extension**) *K of $\boldsymbol{Q}$, such that $r_K(E) > r_0$. Moreover, there is a constant $c = c(E)$, such that the degree of extension $[K: \boldsymbol{Q}] \leqq c2^{r_0}$.*

PROOF. Suppose E is given in the Weierstrass form

$$(1) \qquad y^2 = x^3 + Ax + B \qquad (A, B \in \boldsymbol{Q}) .$$

The polynomial $f(x) = x^3 + Ax + B$ has distinct roots e_1, e_2, e_3 and factors as

$$(2) \qquad f(x) = (x - e_1)(x - e_2)(x - e_3)$$

in its splitting field k. We may consider E to be defined over k. Let $P_j = (x_j, y_j)$, $j = 1, \cdots, m$, be all the points of finite order of $E(L) - \{O\}$.

For any $P = (x, y)$ in $E(k)$, the factors $x - e_1$, $x - e_2$, $x - e_3$ of y^2 in (2) are almost relatively prime. More precisely, there are finitely many $d_1, \cdots, d_n$ in k, such that for any $P = (x, y)$ in $E(k)$, each factor is of the form

$$(3) \qquad x - e_i = d_j z^2$$

for some j $(1 \leqq j \leqq n)$ and z in k. To prove this let S denote any finite set of primes (including all the Archemedian ones) of k. By Dirichelet's

* See the remark at the end of the paper.

theorem, the group $U_k(S)$ of S-units of k, i.e.,

$$U_k(S) = \{x \in k \mid \mathrm{ord}_{\mathfrak{p}}(x) = 0,\ \mathfrak{p} \notin S\}$$

is finitely generated, say by $\eta_1, \cdots, \eta_r$. For what follows, we may suppose that all $e_i \in \mathcal{O}_k$, the ring of integers of k. Choose a finite S containing all the prime divisors of

$$\prod_{i<j} (e_i - e_j)$$

and with the property that

$$\mathcal{O}_k(S) = \{x \in k \mid \mathrm{ord}_{\mathfrak{p}}(x) \geqq 0,\ \mathfrak{p} \notin S\}$$

is a principal ideal domain.

Now let $P = (x, y)$ be a k-rational point on E. A prime divisor $\mathfrak{p}$ of $x - e_1$ and $x - e_2$ must divide $e_1 - e_2$. Thus for any $\mathfrak{p} \notin S$, the exponent $\mathrm{ord}_{\mathfrak{p}}((x - e_2)(x - e_1)^{-1})$ in the factorization of $(x - e_2)(x - e_1)^{-1}$ is even, say $2a_{\mathfrak{p}}$. If

$$z_1 = \prod_{\mathfrak{p} \notin S} \pi_{\mathfrak{p}}^{-a_{\mathfrak{p}}} ,$$

where $\pi_{\mathfrak{p}}$ is a uniformizing parameter at $\mathfrak{p}$, then it is clear that $(x - e_2)(x - e_1)^{-1}z_1^2$ is an S-unit. So for some $m_i \in \boldsymbol{Z}$

$$x - e_2 = (x - e_1)\eta_1^{m_1} \cdots \eta_r^{m_r} z_1^{-2} . \tag{4}$$

Similarly

$$x - e_3 = (x - e_1)\eta_1^{n_1} \cdots \eta_r^{n_r} z_2^{-2} . \tag{5}$$

Substituting (4) and (5) in (2), we get

$$x - e_1 = \eta_1^{\alpha_1} \cdots \eta_r^{\alpha_r} z^2 \qquad (0 \leqq \alpha_i \leqq 1) .$$

We may suppose that no $d_i d_j^{-1}$ $(i \neq j)$ is a square in k. Now choose t in k, such that

(A) $d_i d_j^{-1} t$ is not a square in k for any pair i, j (including $i = j$) and

(B) $x_0 = e_1 + d_1 t \in \boldsymbol{Q}$ and is not a root of the polynomial $g_j(x) = f(x) - y_j^2$ for all $j = 1, \cdots, m$.

If we put $y_0 = (f(x))^{1/2}$ with x_0 as in (B), then y_0 is not in k, because otherwise (B) and (3) would contradict (A). However, for a root ζ of unity, we have $y_0 \in \boldsymbol{Q}(\zeta)$. Therefore, the point $P_0 = (x_0, y_0)$ is in $E(L)$. By (B), P_0 is not a point of finite order. If we put $K_1 = k(y_0)$, then $r_{K_1}(E) > r_k(E)$ and $[K_1 : k] = 2$. We repeat the process with k replaced by K_1 to get a quadratic extension $K_2 \subseteqq L$ of K_1, such that $r_{K_2}(E) > r_{K_1}(E)$. This process now may be continued until $r_{K_i}(E)$ exceeds r_0. To prove the last assertion, we take $c = [k : \boldsymbol{Q}]$.

COROLLARY. *For no elliptic curve E defined over $\boldsymbol{Q}$, is $E(L)$ finitely generated.*

REMARK. The finite extension K is actually the composite of the splitting field k of $x^3 + Ax + B$ and L', where L' is a composite of quadratic fields with galois group $\mathrm{Gal}(L'/\boldsymbol{Q}) \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{r_0}$. Moreover, if the discriminant

$$\Delta = -(4A^3 + 27B^2)$$

of E is a square in $\boldsymbol{Q}$, then k and hence K is abelian.

ACKNOWLEDGEMENT. The author would like to thank Professor Wolfgang M. Schmidt for inviting him to Boulder (April 15–May 15, 1985), where this work was done.

REFERENCE

[1] K. A. RIBET, Torsion points of abelian varieties in cyclotomic extensions (Appendix to N. M. Katz and S. Lang, Finiteness theorems in geometric class field theory), Enseign. Math. (2) 27 (1981), 315–319.

DEPARTMENT OF MATHEMATICS
BRIGHAM YOUNG UNIVERSITY
PROVO, UT 84602
U.S.A.