On the Rank of Elliptic Curves with Three Rational Points of Order 2

By Shoichi KIHARA

Department of Neuropsychiatry School of Medicine, Tokushima University

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1997)

The purpose of this note is to prove.

Theorem. There are infinitely many elliptic curves with rank ≥ 4 over $\boldsymbol{Q}$, which have 3 distinct non-trivial rational points of order 2.

1. We begin by proving.

Proposition 1. Let K be any field of characteristic $\neq 2$, $A, B, C \in K^* = K - \{0\}$, $B^2 \neq 4AC$ and $A^{-1}C \in (K^*)^2$. Suppose, moreover, that the elliptic curve

$$\varepsilon : y^2 = Ax^4 + Bx^2 + C$$

has a K-point $P = (d, e)$, $d, e \in K$. Then ε has 3 distinct non-trivial K-points of order 2.

Proof. As $A, B, C \in K^*$, $B^2 \neq 4AC$ and $A^{-1}C \in (K^*)^2$, we can find $a, b, c \in K^*$ such that $A = a$, $B = 2ab + c$, $C = ab^2$ so that ε can be represented by

$$y^2 = x^2\left(a\left(x + \frac{b}{x}\right)^2 + c\right).$$

Define the birational transformations

$$\chi_P(x, y) = \left(\frac{1}{x - d}, \frac{y}{(x - d)^2}\right)$$

$$\varphi_P(u, v) = (2e^2u^2 + (4abd + 2cd + 4ad^3)u - 2ev + 2ad^2 - 2ab, 4e^3u^3 + 3e(4abd + 2cd + 4ad^3)u^2 + 2e(2ab + c + 6ad^2)u + 4ade - (4abd + 2cd + 4ad^3)v - 4e^2uv)$$

and put $\phi_P = \varphi_P \circ \chi_P$. Then the computation shows that ε is transformed by $\phi_P(x, y) = (X, Y)$ into the Weierstrass model

$$\mathscr{F} : Y^2 = X(X + 4ab)(X + 4ab + c)$$

which has 3 distinct non-trivial K-points of order 2 : (0,0) $(-4ab, 0)$, $(-4ab - c, 0)$.

Q.E.D.

2. Now let $K = \boldsymbol{Q}(t)$, t being a variable.

We shall construct an elliptic curve ε_0 over K with 5 K-points $P_0, \ldots, P_4$.

Let $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (2t + 90, 6t + 150, 10t + 234, 18t + 410)$ and consider the polynomial $f(z) = \prod_{i=1}^{4} (z - \alpha_i^2) \in K[z]$ of 4th degree. There exist uniquely $g(z)$, $r(z) \in K[z]$ of degrees 2,1, respectively, such that $f(z) = (g(z))^2 - r(z)$. As $r(z)$ is a linear polynomial, $x^2 r\left(\left(x + \frac{\beta}{x}\right)^2\right)$ with $\beta \in K^*$ is a polynomial of 4th degree over K which has only terms of degrees 4, 2, 0. For $\beta = 45(2t + 45)$, this polynomial becomes $A_0x^4 + B_0x^2 + C_0$ where

$A_0 = (t^2 + 45t + 499)(3t^2 + 135t + 1502)(3t^2 + 135t + 1546)$,

$B_0 = -(13374t^6 + 1805490t^5 + 101365376t^4 + 3029355090t^3 + 50827314206t^2 + 453946682520t + 1686020339144)$,

$C_0 = 2025(2t + 45)^2(t^2 + 45t + 499)(3t^2 + 135t + 1502)(3t^2 + 135t + 1546)$.

Observe that $A_0, B_0, C_0 \in K^*$, $B_0^2 \neq 4A_0C_0$, $A_0^{-1}C_0 \in (K^*)^2$. Using the relation $r(z) = (g(z))^2 - \prod_{i=1}^{4} (z - \alpha_i^2)$, we see that the elliptic curve

$$\varepsilon_0 : y^2 = A_0x^4 + B_0x^2 + C_0$$

has the following 5 K-points:

$P_0 = (5, 10(27t^4 + 2430t^3 + 81901t^2 + 1225170t + 6862992))$,

$P_1 = (-5, -10(27t^4 + 2430t^3 + 81901t^2 + 1225170t + 6862992))$,

$P_2 = (9, 18(15t^4 + 1350t^3 + 45429t^2 + 677430t + 3777176))$,

$P_3 = (15, 30(9t^4 + 810t^3 + 27163t^2 + 402210t + 2218808))$,

$P_4 = (45, 90(3t^4 + 270t^3 + 9309t^2 + 145530t + 867008))$.

As A_0, B_0, and C_0 satisfy the conditions for A, B, and C in Proposition 1 and $P_0 \in \varepsilon_0$, ε_0 has 3 distinct, non-trivial K-points of order 2.

Now we prove.

Proposition 2. K-rank of ε_0 is at least 4.

Proof. Let $\mathscr{F}_0$ be the Weierstrass model of ε_0 obtained by ϕ_{P_0} and $Q_i = \phi_{P_0}(P_i)$, $i = 1, \ldots, 4$. $\mathscr{F}_0$ and ε_0 have of course the same rank. Let σ be the specialization $t = 1$. $\sigma(\mathscr{F}_0)$ is a $\boldsymbol{Q}$-curve with 4 $\boldsymbol{Q}$-points $\sigma(Q_i) = R_i$, $i = 1, \ldots, 4$, and it suffices to show that $R_1, \ldots, R_4$ are independent on $\sigma(\mathscr{F}_0)$. By using the calculation system PARI, we see that the determinant of the matrix $(< R_i, R_j >)$ $(1 \leq i, j \leq 4)$ associated to the cannonical height is 531.50. That it does not vanish assures the independency of $R_1, \ldots, R_4$. Q.E.D.

As the modular invariant of ε_0 is not constant, this Proposition establishes our Theorem (cf. [1]).

Reference

[1] J. H. Silverman: The arithmetic of elliptic curves. Graduate Texts in Math., vol. 106, Springer-Verlag, New York (1986).