RATIONAL POINTS OF INFINITE ORDER ON ELLIPTIC CURVES

François Ramaroson

Let N be a prime number of the form $N=u^2+64$, where $u \in \mathbf{Z}$, and let l be a prime greater than 3, congruent to 3 mod 4 which is a quadratic residue mod N. Denote by K the imaginary quadratic field $Q(\sqrt{-l})$.

According to Setzer [13], there are (up to isomorphism) two elliptic curves defined over Q having a rational point of order two and with conductor N:

$$E: y^2 = x^3 + ux^2 - 16x \quad \text{and} \quad E': y^2 = x^3 - 2ux^2 + Nx$$

where u is chosen, so that $u \equiv 1 \pmod 4$. E and E' are isogenous over Q. In fact, $E' \approx E/C$, where C is the subgroup of E generated by the rational point of order two.

A global minimal model for E is:

$$y^2 + xy = x^3 + \left(\frac{u-1}{4}\right)x^2 - x.$$

Direct calculations from this model give:

(1) The minimal discriminant is N;

(2) The j-invariant is $(N-16)^3/N$.

PROPOSITION 0.1.

(1) $\operatorname{rank}(E(Q)) = \operatorname{rank}(E'(Q)) = 0$;

(2) $Ш(E, Q)_2 = Ш(E', Q)_2 = 0$.

Proof. This proposition follows directly from Mazur [9] (Corollary 9.10, p. 257), as E and E' have prime conductors. □

PROPOSITION 0.2. $E(Q) \approx \mathbf{Z}/2\mathbf{Z} \approx E'(Q)$.

Proof. We work it out for E.

By Proposition 0.1, $E(Q)$ is a torsion group. Suppose $E(Q)$ has a point M of order $p \neq 2$, with p prime. Since E has good reduction at 2, we have an injection $E(Q_2)_p \hookrightarrow \tilde{E}(\mathbf{F}_2)_p$, where $\tilde{E}$ is the reduced curve mod 2 and $\mathbf{F}_2$ the residue field with 2 elements.

After we reduce the global minimal model

$$y^2 + xy = x^3 + \left(\frac{u-1}{4}\right)x^2 - x$$

modulo 2, we get:

$$y^2 + xy = x^3 + x^2 - x \quad \text{if } u \not\equiv 1 \pmod 8,$$

$$y^2 + xy = x^3 - x \quad \text{if } u \equiv 1 \pmod 8.$$

Received September 21, 1983. Revision received March 28, 1985.
Michigan Math. J. 33 (1986).