89. A Note on the Arithmetic of an Elliptic Curve over Z_p-extensions

By François RAMAROSON
Department of Mathematics, Howard University

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1987)

1. Introduction. Let $X_0(19)$ be the modular curve which is a smooth model for the function field $\boldsymbol{Q}(j(z), j(19z))$. It has genus one and its jacobian, denoted E, is an elliptic curve defined over $\boldsymbol{Q}$. Let K be an imaginary quadratic field with discriminant less than -4 and $p>3$, a rational prime, not equal to 19. In this note we are interested in the arithmetic of E over K_∞, the anticyclotomic $\boldsymbol{Z}_p$-extension of K. Let Λ be the Iwasawa ring and $\mathcal{C}(K_\infty)$ the Heegner module as in [2]. It is a conjecture of Mazur, that $\mathcal{C}(K_\infty)$ is a Λ-module of rank 1. We have the following:

Theorem 1. *Let $\varepsilon(p)$ be 0, 1 or -1 according as p ramifies, splits or stays prime in K. Assume that:*

(i) *19 splits in K*

(ii) *$h(p-\varepsilon(p))$ is not divisible by 3, where h is the class number of K.*

Then, $\mathcal{C}(K_\infty)$ is a Λ-module of rank one.

Corollary. *Under the conditions of Theorem 1, and if K_n denotes the n-th layer of K_∞, then:*

$$\operatorname{rank} E(K_n) \longrightarrow \infty \quad \text{as} \quad n \longrightarrow \infty.$$

We will now outline briefly the main steps in the proofs. The details will appear elsewhere.

2. Notations (Gross [1], Mazur [2]). Write $(19)=\mathfrak{N}\cdot\mathfrak{N}^r$ in K and for $n\geq 0$, let $\mathcal{O}_n$ denote the order of conductor p^n. In $\mathcal{O}_n$, $(19)=\mathfrak{N}_n\cdot\mathfrak{N}_n^r$ where $\mathfrak{N}_n=\mathfrak{N}\cap\mathcal{O}_n$. Let $(\mathcal{O}_n, \mathfrak{N}_n, [\mathcal{O}_n])$ denote a Heegner point of level p^n. If ∞ denotes the cusp at infinity, then the divisor $((\mathcal{O}_n, \mathfrak{N}_n, [\mathcal{O}_n]))-(\infty)$ defines a point $x_n\in E(H_n)$, where H_n is the ring class field $K(j(\mathcal{O}_n))$. Let $e_n=N_{H_n/k_n}(x_n)$ and $\mathcal{C}(K_n)$, the submodule of $(E(K_n)\otimes\boldsymbol{Z}_p)/\text{torsion}$, generated by $\{e_n^\sigma : \sigma\in \operatorname{Gal}(K_n/K)\}$.

3. Using the action of T_p, the p-th Hecke operator, one can show the following:

Lemma 1 (Mazur [2]). *Let $a_p=1+p-\sharp(E(F_p))$, where F_p is the field with p elements. Suppose that a_p is congruent to neither 0 nor $1+\varepsilon(p) \bmod p$. Then:*

$$N_{K_m/K_n}\mathcal{C}(K_m)=\mathcal{C}(K_n)\,; \quad m\geq n\geq 0.$$

Lemma 1 allows us to consider $\mathcal{C}(K_\infty)=\varprojlim \mathcal{C}(K_n)$ where the projection maps are the norm maps. $\mathcal{C}(\bar{K}_\infty)$ is the Heegner module. It is easy to see that $\mathcal{C}(K_\infty)$ is a cyclic Λ-module. Furthermore, its rank is 0 or 1 (see [2]). In order to prove Theorem 1, it is enough to show that $e_n\neq 0$ for some n. In