M. A. Kenku and F. Momose
Nagoya Math. J.
Vol. 109 (1988), 125-149

TORSION POINTS ON ELLIPTIC CURVES DEFINED OVER QUADRATIC FIELDS

M. A. KENKU AND F. MOMOSE

Let k be a quadratic field and E an elliptic curve defined over k. The authors [8, 12, 13] [23] discussed the k-rational points on E of prime power order. For a prime number p, let $n = n(k, p)$ be the least non negative integer such that

$$E_{p^\infty}(k) = \bigcup_{m \geqq 0} \ker(p^m\colon E \longrightarrow E)(k) \subset E_{p^n}$$

for all elliptic curves E defined over a quadratic field k ([15]). For prime numbers $p < 300$, $p \neq 151$, 199, 227 nor 277, we know that $n(k, 2) = 3$ or 4, $n(k, 3) = 2$, $n(k, 5) = n(k, 7) = 1$, $n(k, 11) = 0$ or 1, $n(k, 13) = 0$ or 1, and $n(k, p) = 0$ for all the prime numbers $p \geqq 17$ as above (see loc. cit.). It seems that $n(k, p) = 0$ for all prime numbers $p \geqq 17$ and for all quadratic fields k. In this paper, we discuss the N-torsion points on E for integers N of products of powers of 2, 3, 5, 7, 11 and 13. Let $N \geqq 1$ be an integer and m a positive divisor of N. Let $X_1(m, N)$ be the modular curve which corresponds to the finite adèlic modular group

$$\Gamma_1(m, N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\hat{\boldsymbol{Z}}) \middle| a - 1 \equiv c \equiv 0 \bmod N,\ b \equiv d - 1 \equiv 0 \bmod m\right\},$$

where $\hat{\boldsymbol{Z}} = \varprojlim_n \boldsymbol{Z}/n\boldsymbol{Z}$. Then $X_1(m, N)$ is defined over $\boldsymbol{Q}(\zeta_m)$, where ζ_m is a primitive m-th root of 1. Put $Y_1(m, N) = X_1(m, N)\backslash\{\text{cusps}\}$, which is the coarse moduli space $(/\boldsymbol{Q}(\zeta_m))$ of the isomorphism classes of elliptic curves E with a pair (P_m, P_N) of points P_m and P_N which generate a subgroup $\simeq \boldsymbol{Z}/m\boldsymbol{Z} \times \boldsymbol{Z}/N\boldsymbol{Z}$, up to the isomorphism $(-1)_E\colon E \simeq E$. For $m = 1$, let $X_1(N) = X_1(1, N)$, $\Gamma_1(N) = \Gamma_1(1, N)$ and $Y_1(N) = Y_1(1, N)$. For the integers $N = 2^4$, 11 and 13, $X_1(N)$ are hyperelliptic and $n(k, 2)$, $n(k, 11)$ and $n(k, 13)$ depend on k [23] (3.3). Our result is the following.

THEOREM (0.1). *Let N be an integer of a product of powers of* 2, 3, 5,

Received September 29, 1986.