J. Math. Soc. Japan
Vol. 39, No. 2, 1987

Rational points on the modular curves $X_0^+(N)$

By Fumiyuki MOMOSE

(Received Jan. 5, 1984)
(Revised Sept. 18, 1985)

Let $N\geqq 1$ be an integer and $X_0(N)$ be the modular curve defined over $\boldsymbol{Q}$ which corresponds to the modular group $\Gamma_0(N)$. The modular curve $X_0(N)$ is the coarse moduli space $/\boldsymbol{Q}$ of the isomorphism classes of the generalized elliptic curves E with a cyclic subgroup A of order N [**3**]. The fundamental involution w_N of $X_0(N)$ is defined by

$$(E, A)\longmapsto (E/A, E_N/A),$$

where $E_N=\ker(N: E\to E)$. Let $X_0^+(N)$ be the quotient $X_0(N)/\langle w_N\rangle$. The rational points on $X_0(N)$ are determined for all integers $N\geqq 1$ [**10**] [**5, 6, 7, 8**] [**12**]. We here discuss the rational points on $X_0^+(N)$. The author [**13, 14**] discussed the case when N are powers of a prime number. The similar method as in [**13, 14**] can be applied to the case for composite numbers N. There are $\boldsymbol{Q}$-rational points on $X_0^+(N)$ which are represented by elliptic curves with complex multiplication. We call these points *C.M. points*. Let $n(N)$ denote the number of the $\boldsymbol{Q}$-rational points on $X_0^+(N)$ which are neither cusps nor C.M. points. Then our result is as follows.

THEOREM (0.1). *Let N be a composite number. If N has a prime divisor p which satisfies the following conditions* (i) *and* (ii), *then* $n(N)=0$:
(i) $p\geqq 17$ *or* $p=11$.
(ii) $p\neq 37$ *and* $\#J_0^-(p)(\boldsymbol{Q})<\infty$.
Here $J_0^-(p)$ is the quotient $J_0(p)/(1+w_p)J_0(p)$ of the jacobian variety $J_0(p)$ of $X_0(p)$ and w_p is the automorphism of $J_0(p)$ induced by the fundamental involution w_p of $X_0(p)$.

For the prime numbers p, $17\leqq p<300$, the condition (ii) above is satisfied, except for $p=37$, 151, 199, 227 and 277 [**9**] [**22**] table 5 pp. 135-141. We here describe a sketch of the proof of theorem (0.1). Let $f=f_{N,p}$ be the morphism of $X_0(N)$ to $J_0(p)$ defined by

$$f : (E, A)\longmapsto \mathrm{cl}((E/A_p, E_p/A_p)-(E/A, (E_p+A)/A)),$$

where A_p is the subgroup of A of order p. Then f defines a morphism