TOKYO J. MATH.
VOL. 22, NO. 1, 1999

The Equation for the Modular Curve $X_1(N)$ Derived from the Equation for the Modular Curve $X(N)$

Nobuhiko ISHIDA and Noburo ISHII

Osaka Prefecture University

(Communicated by K. Shinoda)

Dedicated to Professor Toyokazu Hiramatsu on his 60th birthday

Introduction.

Let N be a positive integer greater than 6. Let $\Gamma(N)$ denote the principal congruence subgroup of level N and $\Gamma_1(N)$ a subgroup of $SL_2(\mathbf{Z})$ defined by

$$\Gamma_1(N)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(\mathbf{Z}) \;\middle|\; a\equiv d\equiv 1 \bmod N,\ c\equiv 0 \bmod N\right\}.$$

Let $X(N)$ and $X_1(N)$ be the modular curves associated with the groups $\Gamma(N)$ and $\Gamma_1(N)$ respectively. Further let $A(N)$ and $A_1(N)$ be the modular function fields associated with the groups $\Gamma(N)$ and $\Gamma_1(N)$ respectively. Then the field $A(N)$ (resp. $A_1(N)$) is identified with the function field of $X(N)$ (resp. $X_1(N)$) rational over $\mathbf{C}$ and $A(N)$ is a Galois extension over $A_1(N)$ of degree N. In [3], the second author defined a family of modular functions $X_r(\tau)$ of level $2N^2$, for N and $r\in\mathbf{Z}$, $r\not\equiv 0 \bmod N$, by

$$X_r(\tau)=\exp\left(-\frac{\pi i(r-1)(N-1)}{2N}\right)\prod_{s=0}^{N-1}\frac{K_{r,s}(\tau)}{K_{1,s}(\tau)}, \tag{0.1}$$

where $K_{u,v}(\tau)$ are the Klein forms of level N. For the Klein forms we refer to Kubert and Lang [5]. Define an integer ε_N by

$$\varepsilon_N=\begin{cases} 1 & \text{if } N \text{ is odd}, \\ 2 & \text{if } N \text{ is even}. \end{cases}$$

Then we showed that $X_2(\tau)^{\varepsilon_N}$, $X_3(\tau)$ generate $A(N)$ over $\mathbf{C}$. This result was firstly proved by the second author [3] for the cases N are primes and was extended to arbitrary N greater than 6 by the first author [1]. Furthermore if N is a prime, then the authors [2] showed $X_3(\tau)$ is integral over the ring $\mathbf{Z}[X_2(\tau)]$. In general, in [1], it was shown

Received July 31, 1997