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

Hyperelliptic Quotients of Modular Curves $X_0(N)$

Masahiro FURUMOTO and Yuji HASEGAWA

Waseda University

(Communicated by T. Suzuki)

Introduction.

Let N be a positive integer, and let

$$\Gamma_0(N)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; c\equiv 0 \,(\mathrm{mod}\, N)\right\}.$$

Let $X_0(N)$ be the modular curve which corresponds to $\Gamma_0(N)$. For each positive divisor N' of N with $(N', N/N')=1$ (in which case we write $N'\|N$), $W_{N'}=W_{N'}^{(N)}$ denotes the corresponding Atkin–Lehner involution on $X_0(N)$. (W_1 is the identity.) It is known that the $W_{N'}$ generate an elementary 2-abelian group, which we denote by $W(N)$. The group $W(N)$ is of order $2^{\omega(N)}$, where $\omega(N)$ is the number of distinct prime divisors of N. Furthermore, these involutions are all defined over $\mathbf{Q}$: $W(N)\subseteq \mathrm{Aut}_{\mathbf{Q}}(X_0(N))$.

Let W' be a subgroup of $W(N)$. Then the hyperellipticity of the quotient curve $X_0(N)/W'$ has been determined for two extreme cases (i.e., for $W'=\{1\}$ or $W(N)$).

THEOREM 1 ([12]). *There are nineteen values of N for which $X_0(N)$ is hyperelliptic, i.e., $X_0(N)$ is hyperelliptic if and only if*

$$N=22, 23, 26, 28\text{–}31, 33, 35, 37, 39\text{–}41, 46\text{–}48, 50, 59, 71.$$

THEOREM 2 ([8] [6]). *Put $X_0^*(N)=X_0(N)/W(N)$. There are 64 values of N for which $X_0^*(N)$ is hyperelliptic.*

(i) *$X_0^*(N)$ is of genus two if and only if N is in the following list (57 values in total):*

67, 73, 85, 88, 93, 103, 104, 106, 107, 112,
115, 116, 117, 121, 122, 125, 129, 133, 134, 135,
146, 147, 153, 154, 158, 161, 165, 166, 167, 168,
170, 177, 180, 184, 186, 191, 198, 204, 205, 206,
209, 213, 215, 221, 230, 255, 266, 276, 284, 285,
286, 287, 299, 330, 357, 380, 390.

Received June 28, 1997
Revised November 20, 1997

The second author is partially supported by Waseda University Grant for Special Research Projects 97A-166.