ACTA ARITHMETICA
130.2 (2007)

On the arithmetic of certain modular curves

by

Daeyeol Jeon (Kongju) and Chang Heon Kim (Seoul)

0. Introduction. Let N be a positive integer and Δ a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ which contains ± 1. Let $X_\Delta(N)$ be the modular curve defined over $\mathbb{Q}$ associated to the congruence subgroup

$$\Gamma_\Delta(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; a \bmod N \in \Delta,\ N \mid c \right\}.$$

Then all the intermediate modular curves between $X_1(N)$ and $X_0(N)$ are of the form $X_\Delta(N)$. Denote the genus of $X_\Delta(N)$ by $g_\Delta(N)$. In this paper we study the arithmetic of the curves $X_\Delta(N)$.

In Section 1 we prove a genus formula for the curves $X_\Delta(N)$ which was referred to in the authors' previous works [J-K1, J-K2, J-K-S] without proof.

A smooth projective curve X defined over an algebraically closed field k is called *d-gonal* if it admits a map $\phi : X \to \mathbb{P}^1$ over k of degree d. For $d = 3$ we say that the curve is *trigonal*. Also, the smallest possible d is called the *gonality* of the curve and is denoted by $\mathrm{Gon}(X)$.

Hasegawa and Shimura [H-S1] proved that $X_0(N)$ is trigonal if and only if it is of genus $g \le 2$ or is not hyperelliptic of genus $g = 3, 4$. In fact the "if" part is well-known. The modular curves $X_0(N)$ carry the action of the Atkin–Lehner involutions W_d for any $d \,\|\, N$, i.e., for any positive integer d dividing N with $(d, N/d) = 1$. Let $X_0^{+d}(N)$ and $X_0^*(N)$ be the quotients of $X_0(N)$ by W_d and by the W_d's for all $d \,\|\, N$ respectively. In [H-S2, H-S3], Hasegawa and Shimura also determined the trigonal modular curves $X_0^{+d}(N)$ and $X_0^*(N)$, and found that there exist non-trivial trigonal modular curves, i.e., those of genus $g \ge 5$.

The authors and Schweizer [J-K-S] showed that there exist no non-trivial trigonal modular curves $X_1(N)$, which plays a central role in determining the torsion structures of elliptic curves defined over cubic number fields; such structures occur infinitely often.

2000 *Mathematics Subject Classification*: 11G18, 11G30.
Key words and phrases: genus, hyperelliptic, trigonal, modular curve.

In Section 3 we determine all the intermediate modular curves between $X_1(N)$ and $X_0(N)$ which are trigonal, and conclude that there exist no non-trivial trigonal curves. For this purpose, it is necessary to determine all the hyperelliptic intermediate modular curves, which was done by Ishii and Momose [I-M]. In fact, they claimed that there existed no such modular curves. But we find that there is a unique hyperelliptic intermediate modular curve, namely $X_{\Delta_1}(21)$ (see Theorem 2.3). As Enrique González-Jiménez pointed out, the "lost" curve $X_{\Delta_1}(21)$ is a new hyperelliptic curve in the sense of [B-G-G-P] and it is the curve labeled $C^A_{21A_{\{0,2\}}}$ with equation $y^2 = (x^2-x+1)(x^6+x^5-6x^4-3x^3+14x^2-7x+1)$.

1. A genus formula. Let $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ be the full modular group. For any integer $N \geq 1$, we have the subgroups $\Gamma_1(N)$ and $\Gamma_0(N)$ of $\Gamma(1)$ consisting of the matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ congruent modulo N to $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ respectively. We let $X_1(N)$ and $X_0(N)$ be the modular curves defined over $\mathbb{Q}$ associated to $\Gamma_1(N)$ and $\Gamma_0(N)$ respectively. The X's are compact Riemann surfaces. Let $g_0(N)$ denote the genus of $X_0(N)$. For any congruence subgroup $\Gamma \subset \Gamma(1)$, we shall denote by $\overline{\Gamma}$ the image of Γ under the natural map $\Gamma(1) \to \overline{\Gamma}(1) := \Gamma(1)/\{\pm 1\}$.

For $d \mid N$, let $\pi_d : (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/\{d, N/d\}\mathbb{Z})^*$ be the natural projection, where $\{d, N/d\}$ is the least common multiple of d and N/d. Then we have the following genus formula:

Theorem 1.1. *The genus of the modular curve $X_\Delta(N)$ is given by*

$$g_\Delta(N) = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

where

$$\mu = N \prod_{\substack{p \mid N \\ prime}} \left(1 + \frac{1}{p}\right) \frac{\varphi(N)}{|\Delta|},$$

$$\nu_2 = |\{b \bmod N \in \Delta \mid b^2 + 1 \equiv 0 \bmod N\}| \, \frac{\varphi(N)}{|\Delta|},$$

$$\nu_3 = |\{b \bmod N \in \Delta \mid b^2 - b + 1 \equiv 0 \bmod N\}| \, \frac{\varphi(N)}{|\Delta|},$$

$$\nu_\infty = \sum_{\substack{d \mid N \\ d > 0}} \frac{\varphi(d)\varphi(N/d)}{|\pi_d(\Delta)|}.$$

Proof. We follow the notations of [O1]. One has to check that the index of $\overline{\Gamma}_\Delta(N)$ in $\overline{\Gamma}(1)$ is μ, that the number of elliptic fixed points of order 2 (resp. 3) is ν_2 (resp. ν_3), and that the number of cusps is ν_∞. It is easy to show that

$$\mu=[\overline{\Gamma}(1):\overline{\Gamma}_\Delta(N)]=[\overline{\Gamma}(1):\overline{\Gamma}_0(N)][\overline{\Gamma}_0(N):\overline{\Gamma}_\Delta(N)]=N\prod_{p|N}\left(1+\frac{1}{p}\right)\frac{\varphi(N)}{|\Delta|}.$$

Put $L_0 = \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then the double coset $\Gamma(1)L_0\Gamma(1)$ has the right coset decomposition as follows:

$$\Gamma(1)L_0\Gamma(1) = \bigcup \Gamma(1)L$$

where $L = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $a > 0$, $ad = N$, b taken modulo d and $(a, b, d) = 1$.

Now we compute ν_2 and ν_3. Let A be an elliptic element in $\Gamma(1)$ and P the fixed point of A in the complex upper half-plane. Then $P = MP_0$ for some $M \in \Gamma(1)$ where $P_0 = i$ or $e^{2\pi i/3}$. Write $L_0M = BL$ for some $B \in \Gamma(1)$ and $L = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $a > 0$, $ad = N$ and $(a, b, d) = 1$. Now if $P_0 = i$, then

$$\begin{aligned} A = M\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}M^{-1} \in \Gamma_0(N) = \Gamma(1) \cap L_0^{-1}\Gamma(1)L_0 \\ \Leftrightarrow\ L\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}L^{-1} \in \Gamma(1) \\ \Leftrightarrow\ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} b/a & -(a^2+b^2)/N \\ d/a & b/a \end{pmatrix} \in \Gamma(1) \\ \Leftrightarrow\ a = 1,\ d = N \text{ and } b^2 + 1 \equiv 0 \bmod N. \end{aligned}$$

Similarly if $P_0 = e^{2\pi i/3}$, then

$$\begin{aligned} A\in\Gamma_0(N)\ \Leftrightarrow\ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} b/a & -(a^2-ab+b^2)/N \\ d/a & (a-b)/a \end{pmatrix} \in\Gamma(1) \\ \Leftrightarrow\ a = 1,\ d = N \text{ and } b^2 - b + 1 \equiv 0 \bmod N. \end{aligned}$$

Write $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} x' & y' \\ z' & w' \end{smallmatrix}\right)$. From $L_0M = BL$ it follows that

$$\begin{pmatrix} Nx & Ny \\ z & w \end{pmatrix} = \begin{pmatrix} x' & bx' + Ny' \\ z' & bz' + Nw' \end{pmatrix}. \tag{1}$$

Note that $M\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)M^{-1} = \left(\begin{smallmatrix} yw+xz & * \\ * & * \end{smallmatrix}\right)$ and $M\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)M^{-1} = \left(\begin{smallmatrix} yw+xz-yz & * \\ * & * \end{smallmatrix}\right)$. Then for the elliptic element A of order 2 (resp. 3) to lie in $\Gamma_\Delta(N)$, we need $yw + xz \bmod N \in \Delta$ (resp. $yw + xz - yz \bmod N \in \Delta$) together with the condition $b^2+1 \equiv 0 \bmod N$ (resp. $b^2-b+1 \equiv 0 \bmod N$). From (1) it is easy to see that $yw+xz \equiv -b \bmod N$ and $yw+xz-yz \equiv -b+1 \bmod N$. Thus if A is an elliptic element of order 2 (resp. 3) in $\overline{\Gamma}_\Delta$, then it determines an element $b \bmod N \in \Delta$ satisfying $b^2+1 \equiv 0 \bmod N$ (resp. $b^2-b+1 \equiv 0 \bmod N$).

Conversely, we can form an elliptic element of order 2 (resp. 3) from a solution in Δ of the congruence equation $x^2+1\equiv 0 \bmod N$ (resp. $x^2-x+1 \equiv 0 \bmod N$). We note that different solutions give $\Gamma_0(N)$-inequivalent elliptic points of order 2 (resp. 3).

Now we consider the Galois covering $p_2 : X_\Delta(N) \to X_0(N)$. If A is an elliptic element of order 2 in $\overline{\Gamma}_\Delta$ and $AP = P$, then each point in the inverse image of $\Gamma_0(N)P$ is again an elliptic point of order 2 and has ramification index 1. Thus the number of elements in $p_2^{-1}(\Gamma_0(N)P)$ would become the degree of p_2, and hence we have the following:

$$\begin{aligned}\nu_2 &= |\{b \bmod N \in \Delta \mid b^2+1\equiv 0 \bmod N\}| \cdot \text{degree of } p_2\\ &= |\{b \bmod N \in \Delta \mid b^2+1\equiv 0 \bmod N\}|\,\frac{\varphi(N)}{|\Delta|}.\end{aligned}$$

Similarly, $\nu_3 = |\{b \bmod N \in \Delta \mid b^2-b+1\equiv 0 \bmod N\}|\varphi(N)/|\Delta|$.

Finally, we compute ν_∞. We follow the notations of [O2]. Let $p_1 : X_1(N) \to X_\Delta(N)$ and $p_2 : X_\Delta(N) \to X_0(N)$ be the Galois coverings and $p = p_2 \circ p_1$. Denote by $s = \binom{x}{y}$ a cusp in $X_1(N)$. Then

$$e_p(s) = e_{p_1}(s)e_{p_2}(p_1 s) \quad \text{and} \quad e_p(s) = (N/d, d) \quad \text{with } d=(y,N)$$

where e's denote ramification indices ([O2, Proposition 2]). Now we claim that

$$e_{p_1}(s) = |\Delta|/|\pi_d(\Delta)|.$$

Note that the group $G = \Gamma_\Delta(N)/\pm\Gamma_1(N)$ is isomorphic to $\Delta/\{\pm1\}$. Each element $\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right) \in \Gamma_\Delta(N)$ acts on $\binom{x}{y}$ as $\binom{ax}{a^{-1}y}$. Then $\binom{x}{y}$ and $\binom{ax}{a^{-1}y}$ represent the same cusp on $X_1(N)$ if and only if $ax \equiv \pm x \bmod d$ and $ay \equiv \pm y \bmod N$, i.e., $a \equiv \pm 1 \bmod d$ and $\bmod N/d$.

Recall that $\{\cdot,\cdot\}$ denotes least common multiple. Let $H = \{a \bmod N \in \Delta/\{\pm1\} \mid a \equiv 1 \bmod \{d, N/d\}\}$. Since H is the kernel of the natural map $\Delta/\{\pm1\} \to (\mathbb{Z}/\{d,N/d\})^*/\{\pm1\}$, the cardinality of H is equal to $|\Delta|/|\pi_d(\Delta)|$. We can view H as a subgroup of G. Then G/H has the same cardinality as the set of orbits Gs. Since the elements of Gs are the cusps in $X_1(N)$ lying over the cusp $p_1(s)$ in $X_\Delta(N)$, the ramification index of s in $X_1(N)$ is equal to the cardinality of H. By the claim we come up with

$$\begin{aligned}\nu_\infty &= \sum_{\substack{d\mid N\\ d>0}} \frac{\deg p_2}{e_{p_2}}\,\varphi((d,N/d)) \qquad \text{since } p_2 \text{ is a Galois covering}\\ &= \sum_{\substack{d\mid N\\ d>0}} \frac{\varphi(N)}{|\Delta|}\,\frac{|\Delta|}{|\pi_d(\Delta)|}\,\frac{1}{(N/d,d)}\,\varphi((d,N/d))\\ &= \sum_{\substack{d\mid N\\ d>0}} \varphi(d)\varphi(N/d)/|\pi_d(\Delta)|.\end{aligned}$$

The last equality can be shown by using the fact that

$$\varphi(n_1)\varphi(n_2) = \varphi(n_1 n_2)\,\frac{\varphi((n_1, n_2))}{(n_1, n_2)}. \ \blacksquare$$

2. Hyperelliptic modular curves. If a curve X is 2-gonal, we call it *sub-hyperelliptic.* Also if X is sub-hyperelliptic of genus $g \geq 2$, then it is called *hyperelliptic.*

PROPOSITION 2.1 ([Ne, N-S]). *Let X_1 and X_2 be smooth projective curves over an algebraically closed field k, and assume that there is a finite morphism $X_1 \to X_2$ over k. If X_1 is d-gonal, so is X_2.*

The best general lower bound for the gonality of a modular curve seems to be the one that is obtained in the following way.

Let λ_1 be the smallest positive eigenvalue of the Laplacian operator on the Hilbert space $L^2(X_\Gamma)$ where X_Γ is the modular curve corresponding to a congruence subgroup Γ of $\Gamma(1)$, and let D_Γ be the index of $\overline{\Gamma}$ in $\overline{\Gamma}(1)$. Abramovich [A] shows the following inequality:

$$\lambda_1 D_\Gamma \leq 24\,\mathrm{Gon}(X_\Gamma).$$

Using the best known lower bound for λ_1, due to Henry Kim and Peter Sarnak, as reported on page 18 of [B-G-G-P], i.e., $\lambda_1 > 0.238$, we get the following result.

THEOREM 2.2. *Let X_Γ be the modular curve corresponding to a congruence subgroup Γ of index $D_\Gamma := [\overline{\Gamma}(1) : \overline{\Gamma}]$. Then*

$$D_\Gamma < \frac{12000}{119}\,\mathrm{Gon}(X_\Gamma).$$

In the following, we call the inequality in Theorem 2.2 *Abramovich's bound.*

Ishii and Momose [I-M] asserted that there existed no hyperelliptic modular curves $X_\Delta(N)$ with $\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^*$. But we get the following result.

THEOREM 2.3. *There exists a unique hyperelliptic modular curve of the form $X_\Delta(N)$ with $\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^*$, namely $X_{\Delta_1}(21)$ where Δ_1 is in Table* 1.

REMARK 2.4. In [I-M] the mistake concerned Atkin–Lehner involutions on $X_\Delta(N)$. The Atkin–Lehner involutions define a unique involution on $X_0(N)$ but this does not hold for $X_\Delta(N)$.

To prove Theorem 2.3, we need some preparations.

Let X be a smooth projective curve of genus $g \geq 2$ and $\Omega^1(X)$ the space of holomorphic differential forms on X. Then $\Omega^1(X)$ gives rise to a line bundle, called the *canonical bundle*, which in certain situations gives an embedding into projective space.

Let $\omega_1, \dots, \omega_g$ be a basis for $\Omega^1(X)$. Viewing X as a Riemann surface, we may choose a finite covering of open sets, with local parameters z on each set, such that we can locally write $\omega_i = f_i(z)dz$. Then we get the well-defined map

$$\phi : X \to \mathbb{P}^{g-1}, \quad P \mapsto (\omega_1(P) : \cdots : \omega_g(P)).$$

Note that $(\omega_1(P) : \cdots : \omega_g(P)) = (f_1(P) : \cdots : f_g(P))$. The above map is called the *canonical map*. Let $\overline{X}$ denote the image of X under the canonical map. It is well-known that if X is not hyperelliptic then the canonical map is injective.

If X is a hyperelliptic curve of genus $g \geq 3$, then the image $\overline{X}$ under the canonical map is a smooth curve which is isomorphic to $\mathbb{P}^1$ and which is described by $(g-1)(g-2)/2$ quadratic equations (see §2 of [Ga]).

Therefore it is possible to distinguish between hyperelliptic and non-hyperelliptic curves by examining their images under the canonical map.

Now we consider the modular curves $X_\Delta(N)$ of genus $g = g_\Delta(N) \geq 3$. Let $S^2_\Delta(N)$ denote the space of cusp forms of weight 2. Suppose $\{f_1, \dots, f_g\}$ is a basis of $S^2_\Delta(N)$. Then the canonical map may be written as

$$X_\Delta(N) \ni P \mapsto (f_1(P) : \cdots : f_g(P)) \in \mathbb{P}^{g-1}.$$

One can get such a basis and their Fourier coefficients from [St]. Then to obtain a system of quadratic generators of $I(\overline{X_\Delta(N)})$, we only have to compute the relations of the $f_i f_j$ $(1 \leq i, j \leq g)$. If $X_\Delta(N)$ is not hyperelliptic, then there exist exactly $(g-2)(g-3)/2$ linear relations among the $f_i f_j$ (see §2 of [H-S1]).

Now we are ready to prove Theorem 2.3. By Proposition 2.1 it suffices to consider $X_\Delta(N)$ when $X_0(N)$ is sub-hyperelliptic. If $g_0(N) \leq 2$, then one can find all $X_\Delta(N)$ for such N in Table 1. The other cases can be found in Table 2.

First applying Abramovich's bound we get the following result:

LEMMA 2.5. *The modular curves $X_{\Delta_i^\dagger}$ and $X_{\Delta_i^\ddagger}$ in Tables* 1 *and* 2 *are not hyperelliptic.*

REMARK 2.6. The notations $\Delta_i^\dagger$ and $\Delta_i^\ddagger$ in the tables mean that Abramovich's bound does not hold for $X_{\Delta_i^\dagger}(N)$ and $X_{\Delta_i^\ddagger}(N)$ when $\mathrm{Gon}(X_{\Gamma_{\Delta_i^\dagger}(N)})$ ≤ 2 and $\mathrm{Gon}(X_{\Gamma_{\Delta_i^\ddagger}(N)}) \leq 3$ respectively.

Now we prove that $X_{\Delta_1}(21)$ is a hyperelliptic curve in two different ways.

Proof 1. The space $S^2_{\Delta_1}(21)$ is of dimension 3 and from [St] we can get a basis consisting of three newforms, as follows:

$$f_1 = q - q^2 + q^3 - q^4 - 2q^5 - q^6 - q^7 + 3q^8 + q^9 + 2q^{10} + \cdots,$$
$$f_2 = q - q^3 - 2q^4 + 2q^6 - 2q^7 + 4q^{10} + 2q^{11} + q^{13} - 2q^{14} - \cdots,$$
$$f_3 = 2q^2 - q^3 - 2q^4 - 2q^5 + q^7 + q^9 + 4q^{10} + 2q^{11} + q^{13} - \cdots.$$

By using the computer algebra system MAPLE we get a quadratic generator of the ideal $I(\overline{X_{\Delta_1}(21)})$:

$$Q\ :\ x_1^2 - x_2^2 - x_3^2 + x_2x_3$$

where we obtain the relation $Q(f_1, f_2, f_3) = 0$ by assigning x_i to f_i. But this means that $X_{\Delta_1}(21)$ is hyperelliptic by the above criterion. ■

Proof 2. In [J-K1] it is proved that $X_1(21)$ is *bielliptic*, i.e., it admits a map of degree 2 to an elliptic curve, and all the bielliptic involutions on $X_1(21)$ are $W_3 = \left(\begin{smallmatrix} 9 & -4 \\ 21 & -9 \end{smallmatrix}\right)$ and $[8]W_3$ where $[a]$ denotes the automorphism of $X_1(N)$ represented by $\gamma \in \Gamma_0(N)$ such that $\gamma \equiv \left(\begin{smallmatrix} a & * \\ 0 & * \end{smallmatrix}\right) \bmod N$. Note that for bielliptic curves of genus 5 all bielliptic involutions commute with each other [Sch, Lemma 4.4]. Let G be the group generated by the two bielliptic involutions of $X_1(21)$. Then we can determine the genus of the quotient $G\backslash X_1(21)$ by the four-group rule [F] as follows:

$$\begin{aligned} g(X_1(21)) = g(W_3\backslash X_1(21)) &+ g([8]W_3\backslash X_1(21)) \\ &+ g([8]\backslash X_1(21)) - 2g(G\backslash X_1(21)). \end{aligned}$$

Thus $G\backslash X_1(21)$ is rational, and hence we get a Galois covering $X_1(21) \to \mathbb{P}^1$ with Galois group G. Since $[8]\backslash X_1(21)$ is the same as $X_{\Delta_1}(21)$, we conclude that $X_{\Delta_1}(21)$ is hyperelliptic. ■

To show that no other curve $X_\Delta(N)$ is hyperelliptic it suffices to consider $X_\Delta(N)$ for the maximal subgroups Δ. For example, the modular curve $X_{\Delta_1}(30)$ is of genus 5 and has a basis of $S^2_{\Delta_1}(30)$ which consists of two old forms and three new forms:

$$f_1 = q - q^2 - q^3 - q^4 + q^5 + q^6 + 3q^8 + q^9 - q^{10} - \cdots,$$
$$f_2 = q^2 - q^4 - q^6 - q^8 + q^{10} + q^{12} + 3q^{16} + q^{18} - q^{20} - \cdots,$$
$$f_3 = q - q^2 + q^3 + q^4 - q^5 - q^6 - 4q^7 - q^8 + q^9 + q^{10} + \cdots,$$
$$f_4 = q - q^4 - 2q^5 + q^6 - q^9 - q^{10} + 2q^{11} + 2q^{14} + q^{15} + \cdots,$$
$$f_5 = q^2 - q^3 + q^5 - 2q^7 - q^8 - 2q^{10} + q^{12} + 6q^{13} + 2q^{15} - \cdots.$$

By using MAPLE we get three quadratic generators of $I(\overline{X_{\Delta_1}(30)})$:

$$\begin{cases} x_4^2 - x_5^2 - x_1x_3 + 2x_2x_3 - 4x_4x_5, \\ x_3^2 - 2x_5^2 + 2x_1x_2 - x_1x_3 + 2x_2x_3 - 4x_4x_5, \\ x_1^2 + 4x_2^2 - 2x_5^2 + 2x_1x_2 - x_1x_3 + 2x_2x_3 - 4x_4x_5. \end{cases}$$

This means that $X_{\Delta_1}(30)$ is not hyperelliptic. A case by case calculation of the quadratic generators of $I(\overline{X_\Delta(N)})$ for maximal subgroups Δ in Tables 1 and 2 finishes the proof of Theorem 2.3.

3. Trigonal modular curves. In this section we determine all trigonal modular curves $X_\Delta(N)$. Combining Theorem 2.3 with Proposition 2.1 it suffices to consider the modular curves $X_\Delta(N)$ with $g_\Delta(N) \geq 5$ in Tables 1 and 3 which contain all the intermediate modular curves between $X_1(N)$ and $X_0(N)$ such that $X_0(N)$ is trigonal.

Applying Abramovich's bound we get the following result.

Lemma 3.1. *None of the modular curves $X_{\Delta_i^\ddagger}(N)$ in Tables* 1 *and* 3 *is trigonal.*

We make use of the method due to Hasegawa and Shimura [H-S1].

Theorem 3.2 (Petri's theorem). *Let X be a canonical curve of genus $g \geq 4$ defined over an algebraically closed field. Then the ideal $I(X)$ of X is generated by some quadratic polynomials, unless X is trigonal or isomorphic to a smooth plane quintic curve, in which cases it is generated by some quadratic and (at least one) cubic polynomials.*

Let $X_\Delta(N)$ be of genus $g_\Delta(N) \geq 5$ and $\{f_1, \ldots, f_g\}$ a basis of $S_\Delta^2(N)$. Then to obtain a minimal generating system of the ideal $I(\overline{X_\Delta(N)})$, we only have to compute the relations of the f_if_j and the $f_if_jf_k$ $(1 \leq i, j, k \leq g)$, and to eliminate those cubic relations arising from quadratic relations. By Petri's theorem, $X_\Delta(N)$ is trigonal if and only if it is not isomorphic to a smooth plane quintic curve, and a minimal generating system of $I(\overline{X_\Delta(N)})$ contains a cubic polynomial. Let $Q_1, \ldots, Q_{(g-2)(g-3)/2}$ be a system of quadratic generators of $I(\overline{X_\Delta(N)})$. Since there are $(g-3)(g^2+6g-10)/6$ linear relations among the $f_if_jf_k$, the number of cubic generators among the minimal generating system is

$$\frac{(g-3)(g^2+6g-10)}{6} - \dim L'$$

where L' is generated by x_iQ_j $(1 \leq i \leq g;\ 1 \leq j \leq (g-2)(g-3)/2)$. Thus $X_\Delta(N)$ is trigonal only if the above difference is non-zero.

Example 3.3. The curve $X_{\Delta_1}(32)$ is of genus 5 and not hyperelliptic. By the exact same method as in the computation of $X_{\Delta_1}(30)$ (see §2) we get three quadratic generators of $I(\overline{X_{\Delta_1}(32)})$:

$$\begin{cases} x_1^2 + x_2^2 + x_3^2 + 8x_5^2 + 2x_2x_3 + 4x_2x_4 - 4x_2x_5 - 8x_4x_5, \\ -x_2x_3 - x_2x_4 - x_2x_5 - x_3x_4 + x_3x_5, \\ x_4^2 - x_5^2 + x_2x_5 + x_3x_4 + 2x_4x_5. \end{cases}$$

By a simple calculation we find that the dimension of L' is exactly 15; it follows that there are no essential cubic generators. Therefore $X_{\Delta_1}(30)$ is not trigonal.

Following the same method as in the above example we calculate the remaining cases to get the following result.

THEOREM 3.4. *The modular curve $X_\Delta(N)$ is trigonal if and only if it is of genus $g_\Delta(N) \leq 2$ or not hyperelliptic with $g_\Delta(N) = 3, 4$. This happens exactly for all the curves $X_\Delta(N)$ of genus $g_\Delta(N) \leq 4$ in Table* 1 *except* $X_{\Delta_1}(21)$.

Acknowledgments. We thank Andreas Schweizer for suggesting the second proof of Theorem 2.3. We also thank Enrique González-Jiménez for the comment on the lost hyperelliptic curve $X_{\Delta_1}(21)$.

Appendix

Table 1. List of $X_\Delta(N)$ and their genera $g_\Delta(N)$ when $X_0(N)$ are of genus $g_0(N) \leq 2$

N	$\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^*$	$g_\Delta(N)$
$1 \leq N \leq 12$	–	–
13	$\Delta_1 = \{\pm 1, \pm 5\}$	0
13	$\Delta_2 = \{\pm 1, \pm 3, \pm 4\}$	0
14	–	–
15	$\Delta_1 = \{\pm 1, \pm 4\}$	1
16	$\Delta_1 = \{\pm 1, \pm 7\}$	0
17	$\Delta_1 = \{\pm 1, \pm 4\}$	1
17	$\Delta_2 = \{\pm 1, \pm 2, \pm 4, \pm 8\}$	1
18	–	–
19	$\Delta_1 = \{\pm 1, \pm 7, \pm 8\}$	1
20	$\Delta_1 = \{\pm 1, \pm 9\}$	1
21	$\Delta_1 = \{\pm 1, \pm 8\}$	3
21	$\Delta_2 = \{\pm 1, \pm 4, \pm 5\}$	1
22	–	–
23	–	–
24	$\Delta_1 = \{\pm 1, \pm 5\}$	3
24	$\Delta_2 = \{\pm 1, \pm 7\}$	3

Table 1 (cont.)

N	$\{\pm1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^*$	$g_\Delta(N)$
24	$\Delta_3 = \{\pm1, \pm11\}$	1
25	$\Delta_1 = \{\pm1, \pm7\}$	4
25	$\Delta_2 = \{\pm1, \pm4, \pm6, \pm9, \pm11\}$	0
26	$\Delta_1 = \{\pm1, \pm5\}$	4
26	$\Delta_2 = \{\pm1, \pm3, \pm9\}$	4
27	$\Delta_1 = \{\pm1, \pm8, \pm10\}$	1
28	$\Delta_1 = \{\pm1, \pm13\}$	4
28	$\Delta_2 = \{\pm1, \pm3, \pm9\}$	4
29	$\Delta_1^\dagger = \{\pm1, \pm12\}$	8
29	$\Delta_2 = \{\pm1, \pm4, \pm5, \pm6, \pm7, \pm9, \pm13\}$	4
31	$\Delta_1 = \{\pm1, \pm5, \pm6\}$	6
31	$\Delta_2 = \{\pm1, \pm2, \pm4, \pm8, \pm15\}$	6
32	$\Delta_1 = \{\pm1, \pm15\}$	5
32	$\Delta_2 = \{\pm1, \pm7, \pm9, \pm15\}$	1
36	$\Delta_1^\dagger = \{\pm1, \pm17\}$	7
36	$\Delta_2 = \{\pm1, \pm11, \pm13\}$	3
37	$\Delta_1^\ddagger = \{\pm1, \pm6\}$	16
37	$\Delta_2^\dagger = \{\pm1, \pm10, \pm11\}$	10
37	$\Delta_3 = \{\pm1, \pm6, \pm8, \pm10, \pm11, \pm14\}$	4
37	$\Delta_4 = \{\pm1, \pm3, \pm4, \pm7, \pm9, \pm10, \pm11, \pm12, \pm16\}$	4
49	$\Delta_1^\ddagger = \{\pm1, \pm18, \pm19\}$	19
49	$\Delta_2 = \{\pm1, \pm6, \pm8, \pm13, \pm15, \pm20, \pm22\}$	3
50	$\Delta_1^\ddagger = \{\pm1, \pm7\}$	22
50	$\Delta_2 = \{\pm1, \pm9, \pm11, \pm19, \pm21\}$	4

Table 2. List of $X_\Delta(N)$ and their genera $g_\Delta(N)$ when $X_0(N)$ are hyperelliptic and $g_0(N) > 2$

N	$\{\pm1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^*$	$g_\Delta(N)$
30	$\Delta_1 = \{\pm1, \pm11\}$	5
33	$\Delta_1^\dagger = \{\pm1, \pm10\}$	11
33	$\Delta_2 = \{\pm1, \pm2, \pm4, \pm8, \pm16\}$	5
35	$\Delta_1^\dagger = \{\pm1, \pm6\}$	13
35	$\Delta_2 = \{\pm1, \pm11, \pm16\}$	9
35	$\Delta_3 = \{\pm1, \pm6, \pm8, \pm13\}$	7
35	$\Delta_4 = \{\pm1, \pm4, \pm6, \pm9, \pm11, \pm16\}$	5
39	$\Delta_1^\dagger = \{\pm1, \pm14\}$	17
39	$\Delta_2^\dagger = \{\pm1, \pm16, \pm17\}$	9
39	$\Delta_3 = \{\pm1, \pm5, \pm8, \pm14\}$	9

Table 2 (cont.)

N	$\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^*$	$g_\Delta(N)$
39	$\Delta_4 = \{\pm 1, \pm 4, \pm 10, \pm 14, \pm 16, \pm 17\}$	5
40	$\Delta_1^\dagger = \{\pm 1, \pm 31\}$	9
40	$\Delta_2^\dagger = \{\pm 1, \pm 9\}$	13
40	$\Delta_3^\dagger = \{\pm 1, \pm 11\}$	13
40	$\Delta_4 = \{\pm 1, \pm 9, \pm 11, \pm 19\}$	5
40	$\Delta_5 = \{\pm 1, \pm 3, \pm 9, \pm 13\}$	7
40	$\Delta_6 = \{\pm 1, \pm 7, \pm 9, \pm 17\}$	7
41	$\Delta_1^\dagger = \{\pm 1, \pm 9\}$	21
41	$\Delta_2^\dagger = \{\pm 1, \pm 3, \pm 9, \pm 14\}$	11
41	$\Delta_3 = \{\pm 1, \pm 4, \pm 10, \pm 16, \pm 18\}$	11
41	$\Delta_4 = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 8, \pm 9, \pm 10, \pm 16, \pm 18, \pm 20\}$	5
46	–	–
47	–	–
48	$\Delta_1^\dagger = \{\pm 1, \pm 7\}$	19
48	$\Delta_2^\dagger = \{\pm 1, \pm 17\}$	19
48	$\Delta_3^\dagger = \{\pm 1, \pm 23\}$	19
48	$\Delta_4 = \{\pm 1, \pm 11, \pm 13, \pm 23\}$	5
48	$\Delta_5 = \{\pm 1, \pm 7, \pm 17, \pm 23\}$	7
48	$\Delta_6 = \{\pm 1, \pm 5, \pm 19, \pm 23\}$	7
59	–	–
71	$\Delta_1^\dagger = \{\pm 1, \pm 5, \pm 14, \pm 17, \pm 25\}$	36
71	$\Delta_2^\dagger = \{\pm 1, \pm 20, \pm 23, \pm 26, \pm 30, \pm 32, \pm 34\}$	26

Table 3. List of $X_\Delta(N)$ and their genera $g_\Delta(N)$ when $X_0(N)$ are trigonal but not sub-hyperelliptic

N	$\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^*$	$g_\Delta(N)$
34	$\Delta_1 = \{\pm 1, \pm 13\}$	9
34	$\Delta_2 = \{\pm 1, \pm 9, \pm 13, \pm 15\}$	5
38	$\Delta_1 = \{\pm 1, \pm 7, \pm 11\}$	10
43	$\Delta_1^\ddagger = \{\pm 1, \pm 6, \pm 7\}$	15
43	$\Delta_2 = \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 11, \pm 16, \pm 21, \pm 22\}$	9
44	$\Delta_1^\ddagger = \{\pm 1, \pm 21\}$	16
44	$\Delta_2 = \{\pm 1, \pm 5, \pm 7, \pm 9, \pm 19\}$	8
45	$\Delta_1^\ddagger = \{\pm 1, \pm 19\}$	21
45	$\Delta_2 = \{\pm 1, \pm 14, \pm 16\}$	9
45	$\Delta_3 = \{\pm 1, \pm 8, \pm 17, \pm 19\}$	11
45	$\Delta_4 = \{\pm 1, \pm 4, \pm 11, \pm 14, \pm 16, \pm 19\}$	5
53	$\Delta_1^\ddagger = \{\pm 1, \pm 23\}$	40

Table 3 (cont.)

N	$\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^*$	$g_\Delta(N)$
53	$\Delta_2 = \{\pm 1, \pm 4, \pm 6, \pm 7, \pm 9, \pm 10, \pm 11, \pm 13, \pm 15, \pm 16, \pm 17, \pm 24, \pm 25\}$	8
54	$\Delta_1^\ddagger = \{\pm 1, \pm 17, \pm 19\}$	10
61	$\Delta_1^\ddagger = \{\pm 1, \pm 11\}$	56
61	$\Delta_2^\ddagger = \{\pm 1, \pm 13, \pm 14\}$	36
61	$\Delta_3^\ddagger = \{\pm 1, \pm 3, \pm 9, \pm 20, \pm 27\}$	26
61	$\Delta_4^\ddagger = \{\pm 1, \pm 11, \pm 13, \pm 14, \pm 21, \pm 29\}$	16
61	$\Delta_5 = \{\pm 1, \pm 3, \pm 8, \pm 9, \pm 11, \pm 20, \pm 23, \pm 24, \pm 27, \pm 28\}$	12
64	$\Delta_1^\ddagger = \{\pm 1, \pm 31\}$	37
64	$\Delta_2^\ddagger = \{\pm 1, \pm 15, \pm 17, \pm 31\}$	13
64	$\Delta_3 = \{\pm 1, \pm 7, \pm 9, \pm 15, \pm 17, \pm 23, \pm 25, \pm 31\}$	5
81	$\Delta_1^\ddagger = \{\pm 1, \pm 26, \pm 28\}$	46
81	$\Delta_2^\ddagger = \{\pm 1, \pm 8, \pm 10, \pm 17, \pm 19, \pm 26, \pm 28, \pm 35, \pm 37\}$	10

References

[A] D. Abramovich, *A linear lower bound on the gonality of modular curves*, Int. Math. Res. Not. 1996, no. 20, 1005–1011.

[B-G-G-P] M. H. Baker, E. González-Jiménez, J. González and B. Poonen, *Finiteness results for modular curves of genus at least* 2, Amer. J. Math. 127 (2005), 1325–1387.

[F] C. R. Ferenbaugh, *The genus-zero problem for $n|h$-type groups*, Duke Math. J. 72 (1993), 31–63.

[Ga] S. D. Galbraith, *Equations for modular curves*, D. Phil. Thesis, Oxford, 1996.

[H-S1] Y. Hasegawa and M. Shimura, *Trigonal modular curves*, Acta Arith. 88 (1999), 129–140.

[H-S2] —, —, *Trigonal modular curves $X_0^{+d}(N)$*, Proc. Japan Acad. Ser. A Math. Sci. 75 (1999), no. 9, 172–175.

[H-S3] —, —, *Trigonal modular curves $X_0^*(N)$*, ibid. 76 (2000), no. 6, 83–86.

[I-M] N. Ishii and F. Momose, *Hyperelliptic modular curves*, Tsukuba J. Math. 15 (1991), 413–423.

[J-K1] D. Jeon and C. H. Kim, *Bielliptic modular curves $X_1(N)$*, Acta Arith. 112 (2004), 75–86.

[J-K2] —, —, *Bielliptic modular curves $X_1(M, N)$*, Manuscripta Math. 118 (2005), 455–466.

[J-K-S] D. Jeon, C. H. Kim and A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. 113 (2004), 291–301.

[Ne] M. Newman, *Conjugacy, genus and class number*, Math. Ann. 196 (1972), 198–217.

[N-S] K. V. Nguyen and M.-H. Saito, *d-gonality of modular curves and bounding torsions*, math.AG/9603024.

[O1] A. Ogg, *Modular Forms and Dirichlet Series*, Benjamin, 1969.

[O2] —, *Rational points on certain elliptic modular curves*, in: Proc. Sympos. Pure Math. 24, Amer. Math. Soc., 1973, 221–231.

[Sch] A. Schweizer, *Bielliptic Drinfeld modular curves*, Asian J. Math. 5 (2001), 705–720.
[St] W. A. Stein, http://modular.fas.harvard.edu.

Department of Mathematics Education
Kongju National University
182 Shinkwan-dong
Kongju, Chungnam, 314-701 Korea
E-mail: dyjeon@kongju.ac.kr

Department of Mathematics
Seoul Women's University
126 Kongnung 2-dong, Nowon-gu
Seoul, 139-774 Korea
E-mail: chkim@swu.ac.kr

Received on 10.1.2007 (5364)