ACTA ARITHMETICA
LXXXVIII.2 (1999)

Trigonal modular curves

by

Yuji Hasegawa and Mahoro Shimura (Tokyo)

0. Introduction. For a positive integer N, let $X_0(N)$ (over $\mathbb{C}$) be the modular curve corresponding to the modular group $\Gamma_0(N)$. It is known that there are only finitely many values of N for which $X_0(N)$ is *sub-hyperelliptic*, i.e., it admits a two-fold covering onto the projective line $\mathbb{P}^1$. These values are explicitly determined by Ogg [13].

A smooth projective curve C defined over an algebraically closed field k is called *d-gonal* if there exists a finite morphism $C \to \mathbb{P}^1$ over k of degree d. Thus, C is sub-hyperelliptic if and only if it is 2-gonal. Also, in the rest of the paper, we will use "trigonal", "tetragonal", "pentagonal" to mean "d-gonal" for $d = 3$, 4, 5, respectively.

Recently, Nguyen and Saito [12] proved an analogue of the strong Uniform Boundedness Conjecture for elliptic curves defined over function fields of dimension one; if a base curve is d-gonal, they gave a bound of the orders of torsions of Mordell–Weil groups in term of d uniformly by connecting the problem with the problem of bounding the level N of d-gonal modular curves $X_0(N)/\mathbb{C}$. Therefore it is an interesting problem to give a sharp bound for the level N of d-gonal modular curves. In fact, there is a result of Zograf [17] which gives a linear bound of the level N of d-gonal modular curves $X_0(N)/\mathbb{C}$; see Theorem 4.3. (Nguyen and Saito [12] also gave a bound of N by a quartic polynomial in d by employing a purely algebraic method.)

In this paper, we prove that $X_0(N)$ is trigonal if and only if it is of genus $g \le 2$ or is non-hyperelliptic of genus $g = 3, 4$ (Theorem 3.3; see also Remark 1.3). As a consequence, we have $N \le 81$ if $X_0(N)$ is trigonal. Also we will show that $N \le 191$ (resp. $N \le 197$) if $d = 4$ (resp. $d = 5$) (Proposition 4.4). These give a highly sharpened upper bound for $3 \le d \le 5$ (cf. [17], [12]).

1991 *Mathematics Subject Classification*: Primary 11F11; Secondary 11F03, 11G30, 14E20, 14H25.

This research was supported in part by Waseda University Grant for Special Research Projects 97A-166.

Let us explain the outline of the proof of our result for the trigonal case. Recall first that $X_0(N)$ has the canonical $\mathbb{Q}$-structure, having good reduction outside N ([7]). Let $g = g(X_0(N))$ be the genus of $X_0(N)$. It is a general fact that a non-hyperelliptic curve of genus 3 or 4 is necessarily trigonal; see Remark 1.3. Hence we may assume that $g \geq 5$. In this case, if $X_0(N)$ is trigonal, then there exists a finite morphism $X_0(N) \to \mathbb{P}^1$ of degree 3 *defined over* $\mathbb{Q}$ by the results of Nguyen and Saito [12] (see Theorem 1.6). Suppose $X_0(N)$ is a trigonal curve of genus $g \geq 5$. Let p be a (fixed) prime number not dividing N, so that $X_0(N)$ has good reduction at p. Denote by $\widetilde{X}_0(N)$ the reduction modulo p of $X_0(N)$. Then, again by [12] (see Lemma 1.8), there is a finite morphism $\widetilde{X}_0(N) \to \mathbb{P}^1$ over $\mathbb{F}_p$ of degree at most 3, so we have an upper bound $U_p^{(3)}(N)$ of the number $\sharp\widetilde{X}_0(N)(\mathbb{F}_{p^2})$ of the $\mathbb{F}_{p^2}$-rational points of $\widetilde{X}_0(N)$. On the other hand, Ogg [13] gave a lower bound $L_p(N)$ of this number. The explicit formulas of $U_p^{(3)}(N)$ and $L_p(N)$ will be given in Section 3. If $N > 155$, then the genus of $X_0(N)$ is at least 8, and there is a prime $p \nmid N$ such that $L_p(N) > U_p^{(3)}(N)$. This means that $X_0(N)$ is not trigonal if $N > 155$. Furthermore, from the previous result of the second author [16], we know that there are no trigonal modular curves $X_0(N)$ with $g = 5, 6$. We may thus assume that $g \geq 7$ and $N \leq 155$. Now, by calculating the exact number $\sharp\widetilde{X}_0(N)(\mathbb{F}_{p^2})$ by means of the trace formula of Hecke operators [6], we see that there are only 14 values of N for which the inequality $\sharp\widetilde{X}_0(N)(\mathbb{F}_{p^2}) \leq U_p^{(3)}(N)$ holds for all $p \nmid N$. Finally, by applying a criterion for the trigonality (Section 2), we conclude that $X_0(N)$ is also non-trigonal for these 14 cases. Therefore $X_0(N)$ is a trigonal curve without sub-hyperelliptic covering if and only if it is a non-hyperelliptic curve of genus $g = 3$ or 4.

Notation. For an algebraic curve C, we denote by $g = g(C)$ the genus of C. For a positive integer N, let $\omega(N)$ be the number of the distinct prime divisors of N, and let $\psi(N) = N\prod_{q|N}(1 + 1/q)$, where the product runs over the set of distinct prime divisors of N. For any set S, the cardinality of S is denoted by $\sharp S$.

1. Generalities for d-gonal algebraic curves. In this section, we review some facts on the d-gonality of algebraic curves. We refer to [1], [5], [12] for basic references.

DEFINITION 1.1. A smooth projective curve C defined over an algebraically closed field k is called *d-gonal* if there exists a finite morphism $C \to \mathbb{P}^1$ over k of degree d.

Borrowing a terminology of linear systems, a curve is d-gonal if and only if it has a *base-point-free* g_d^1. It is a fact that if $d \geq \frac{1}{2}g + 1$, then any curve of genus g has a g_d^1; on the other hand, for $d < \frac{1}{2}g + 1$, there exist curves of genus g with no g_d^1 (see [8]).

REMARK 1.2. Any curve of genus $g \le 2$ is sub-hyperelliptic. If C is sub-hyperelliptic of $g \ge 2$, then it is called *hyperelliptic*. There exist hyperelliptic curves of arbitrary genus $g \ge 2$.

REMARK 1.3. Let C be an algebraic curve. If $g = g(C) \le 2$, then by the Riemann–Roch Theorem we find a base-point-free g_3^1, hence C is trigonal (in case $g = 2$, take any ordinary point P and consider the divisor $3(P)$). If C is non-hyperelliptic with $g = 3, 4$, then it is also trigonal, just as mentioned above. Moreover, any hyperelliptic curve with genus $g \ge 3$ is *not* trigonal (see [1, Chap. I, Exer. D-9]).

It is also known that a non-hyperelliptic curve of genus $g \ge 5$ has at most one g_3^1 ([1, Chap. III, Exer. B-3]).

EXAMPLE 1.4 ([5, Chap. IV, Ex. 5.5.2]). Let C be a non-hyperelliptic curve of genus $g(C) = 3$. Then its canonical embedding (see the beginning of the next section) is a plane quartic curve. Projecting from any point of C to $\mathbb{P}^1$, we obtain a g_3^1. Thus C has infinitely many g_3^1's.

Let C be a non-hyperelliptic curve of genus $g(C) = 4$. Then its canonical embedding in $\mathbb{P}^3$ is contained in a unique irreducible quadric surface Q, and is the complete intersection of Q with an irreducible cubic surface. Let k be an algebraically closed field. An irreducible quadric surface in $\mathbb{P}^3$ is isomorphic over k to either $\operatorname{Proj} k[x_0, x_1, x_2, x_3]/(x_0x_1 - x_2^2)$ or $\operatorname{Proj} k[x_0, x_1, x_2, x_3]/(x_0x_1 - x_2x_3)$. The former is a quadric cone, and the latter is a ruled surface $\mathbb{P}^1 \times \mathbb{P}^1$. If Q is a quadric cone, then the one family of lines on Q cuts out a unique g_3^1 on C. If Q is a ruled surface, then each of the two families of lines on Q cuts out a g_3^1 on C, and these two are the only ones.

PROPOSITION 1.5 ([11], [12]). *Let C_1, C_2 be smooth projective curves over an algebraically closed field k, and assume that there is a finite morphism $C_1 \to C_2$ over k. If C_1 is d-gonal, so is C_2.*

Now let k be any perfect field. Given a curve C over k, one may ask whether a d-gonal morphism can also be defined over k. Of course, it is possible to choose a k-rational d-gonal morphism for some d. Here we require d to be minimal, meaning that there are no d'-gonal morphisms $C \to \mathbb{P}^1$ over an algebraic closure of k with $d' < d$. The answer is affirmative when $g(C)$ is large compared with d.

THEOREM 1.6 ([12]). *Let C be a smooth projective curve defined over a perfect field k. Assume that C is d-gonal* (*over an algebraic closure of k*). *Then there exists a smooth projective curve C' defined over k and a finite* *morphism $C \to C'$ over k of degree d' dividing d such that*

$$g(C') \le (d/d' - 1)^2.$$

Corollary 1.7. *Notation being as above, assume further that d is a prime, and that $g(C) > (d-1)^2$. Then there exists a rational curve C' defined over k and a finite morphism $C \to C'$ of degree d over k.*

The following lemma treats the reduction of morphisms.

Lemma 1.8 ([12]). *Let C_1, C_2 be smooth projective curves defined over $\mathbb{Q}$ both of which are geometrically irreducible, and let $f : C_1 \to C_2$ be a finite morphism of degree d which is also defined over $\mathbb{Q}$. Assume that C_1 has good reduction at a prime p.*

(i) *If $g(C_2) \ge 1$, then C_2 has good reduction at p and f induces a finite morphism*

$$\widetilde{f} : \widetilde{C}_1 \to \widetilde{C}_2$$

of degree d over $\mathbb{F}_p$, where $\widetilde{C}_i$ $(i = 1, 2)$ denotes the reduction of C_i at p.

(ii) *If $g(C_2) = 0$, then we obtain a finite morphism*

$$\widetilde{f}' : \widetilde{C}_1 \to \widetilde{C}_2'$$

of degree $d' \le d$ over $\mathbb{F}_p$, where $\widetilde{C}_1$ is as in (i), *and $\widetilde{C}_2'$ is a smooth rational curve over $\mathbb{F}_p$.*

2. Criterion for trigonality. Let C be a non-hyperelliptic curve of genus $g \ge 3$ defined over an algebraically closed field. The *canonical embedding* of C is the embedding

$$C \ni P \mapsto (\omega_1(P) : \ldots : \omega_g(P)) \in \mathbb{P}^{g-1}$$

determined by the canonical linear system. Its image is called a *canonical curve*.

Theorem 2.1 (Petri's Theorem [1], [14]). *Let C be a canonical curve of genus $g \ge 4$ defined over an algebraically closed field. Then the ideal $I(C)$ of C is generated by some quadratic polynomials, unless C 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.*

Hence, to obtain a minimal generating system of the ideal $I(C)$ of C, we have only to compute the relations of the $\omega_i\omega_j$ and the $\omega_i\omega_j\omega_k$ $(1 \le i, j, k \le g)$, and to eliminate those cubic relations arising from quadratic relations. A canonical curve C is trigonal if and only if it is *non*-isomorphic to a smooth plane quintic and a minimal generating system of $I(C)$ contains a cubic polynomial. (It can be shown that a smooth plane quintic curve has no g_3^1; see [5, Chap. IV, Exer. 5.6].)

Step I. *Computing the generators of degree 2.* The number of monomials $\omega_i\omega_j$ of degree 2 is

$$\binom{g+2-1}{2} = \frac{g(g+1)}{2}.$$

All the $\omega_i\omega_j$ are contained in the space $\Gamma(C, (\Omega^1)^{\otimes 2})$, where Ω^1 is the canonical sheaf on C. By the Riemann–Roch Theorem, we compute

$$\dim \Gamma(C, (\Omega^1)^{\otimes 2}) = 2(2g-2) - g + 1 = 3(g-1).$$

Therefore there are

$$\frac{g(g+1)}{2} - 3(g-1) = \frac{1}{2}(g-2)(g-3)$$

linear relations among the $\omega_i\omega_j$. Let $Q_1, \ldots, Q_{(g-2)(g-3)/2}$ be a system of quadratic generators of $I(C)$ obtained in this way.

Step II. *Computing the generators of degree 3.* By an analogous argument as in Step I, we see that there are

$$\binom{g+3-1}{3} - 5(g-1) = \frac{(g-3)(g^2+6g-10)}{6}$$

linear relations among the $\omega_i\omega_j\omega_k$. Put $L = \Gamma(C, (\Omega^1)^{\otimes 3})$, and let L' be the subspace of L generated by the x_iQ_j $(1 \le i \le g;\ 1 \le j \le (g-2)(g-3)/2)$, where x_i is the ith homogeneous coordinate of $\mathbb{P}^{g-1}$. Then the number of cubic generators is given by

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

The curve C is trigonal only if the above difference is non-zero. In fact, if C is trigonal, then this quantity equals $g-3$ (1, [Chap. III, Exer. I-6]).

Now consider the modular curve $X_0(N)$ (over $\mathbb{C}$). Let $S_2(N)$ be the space of cuspforms of weight 2 on $\Gamma_0(N)$, and Ω^1 the canonical sheaf on $X_0(N)$. Then, as is well known, the space $S_2(N)$ is canonically isomorphic to $H^0(X_0(N), \Omega^1)$ via the map $f(z) \mapsto \omega_f := 2\pi\sqrt{-1}f(z)dz$. Thus, if $X_0(N)$ is non-hyperelliptic of genus $g \ge 3$, then the canonical embedding may be written as

$$\Phi : X_0(N) \ni z \mapsto (f_1(z) : f_2(z) : \ldots : f_g(z)) \in \mathbb{P}^{g-1},$$

where $\langle f_1, f_2, \ldots, f_g\rangle$ is a basis of $S_2(N)$. We regard $X_0(N)$ as a canonical curve under Φ. Since $\Gamma_0(N)$ contains $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, every element $f(z)$ of $S_2(N)$ is expanded to a Fourier series $f(z) = \sum_{n=1}^{\infty} a_n \exp(2\pi\sqrt{-1}\,nz)$. It is convenient to use this series expression for computing generators of the ideal of $X_0(N)$. To calculate sufficiently many Fourier coefficients of the f_i, one can make use of the trace formula of Hecke operators [6].

Example 2.2 (cf. [16]). The modular curve $X_0(42)$ is of genus 5 and non-hyperelliptic [13]. Let $f_1(z), f_3(z), f_5(z)$ be newforms of levels $N = 14$, 21, 42, respectively, and put $f_2(z) = f_1(3z)$, $f_4(z) = f_3(2z)$. Then $\langle f_1, \ldots, f_5\rangle$ forms a basis of $S_2(42)$. The sequences $\{a_n^{(i)}\}_{n=1}^{\infty}$ of Fourier coefficients of f_i $(1 \le i \le 5)$ are as follows.

f_1: $\{1, -1, -2, 1, 0, 2, 1, -1, 1, 0, 0, -2, -4, -1, 0,$
$1, 6, -1, 2, 0, -2, 0, 0, 2, -5, 4, 4, 1, -6, 0, \ldots\}$,

f_2: $\{0, 0, 1, 0, 0, -1, 0, 0, -2, 0, 0, 1, 0, 0, 0,$
$0, 0, 2, 0, 0, 1, 0, 0, -1, 0, 0, 1, 0, 0, 0, \ldots\}$,

f_3: $\{1, -1, 1, -1, -2, -1, -1, 3, 1, 2, 4, -1, -2, 1, -2,$
$1, -6, -1, 4, 2, -1, -4, 0, 3, -1, 2, 1, 1, -2, 2, \ldots\}$,

f_4: $\{0, 1, 0, -1, 0, 1, 0, -1, 0, -2, 0, -1, 0, -1, 0,$
$3, 0, 1, 0, 2, 0, 4, 0, -1, 0, -2, 0, 1, 0, -2, \ldots\}$,

f_5: $\{1, 1, -1, 1, -2, -1, -1, 1, 1, -2, -4, -1, 6, -1, 2,$
$1, 2, 1, -4, -2, 1, -4, 8, -1, -1, 6, -1, -1, -2, 2, \ldots\}$.

An elementary calculation of linear algebra shows that three quadratic generators of the ideal of $X_0(42)$ are given by

$$\begin{cases} Q_1 : 2x_1^2 + 6x_1x_2 + 4x_3x_4 - x_3x_5 + 2x_4x_5 - x_5^2, \\ Q_2 : -x_1^2 + 9x_2^2 + x_3x_5 - 2x_4x_5, \\ Q_3 : 4x_1^2 + 3x_3^2 + 20x_3x_4 - 2x_3x_5 + 12x_4^2 + 4x_4x_5 - 5x_5^2, \end{cases}$$

where we obtain the relations $Q_i(f_1, \ldots, f_5) = 0$ by assigning x_i to f_i. Since after some calculation we find that the dimension of L' (see Step II) is exactly 15, it follows that there are no essential cubic generators. Therefore $X_0(42)$ is not trigonal.

3. Trigonal modular curves. In this section, we will give a complete list of trigonal modular curves $X_0(N)$. To begin with, we make use of the trick essentially due to Ogg [13]. Note that $X_0(N)$ has at least one $\mathbb{Q}$-rational point, which is the image of the point $\sqrt{-1}\infty$ at infinity. Therefore if $X_0(N)$ has a finite morphism to a rational curve C' over $\mathbb{Q}$, then C' is necessarily isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1$. Suppose $X_0(N)$ has a d-gonal morphism over $\mathbb{Q}$. Since $X_0(N)$ has good reduction at each $p \nmid N$, and since the reduced curve $\widetilde{X}_0(N)$ at p has a $\mathbb{F}_p$-rational point, we have a finite morphism $\widetilde{X}_0(N) \to \mathbb{P}^1$ defined over $\mathbb{F}_p$ of degree at most d (Lemma 1.8). Since clearly $\sharp\mathbb{P}^1(\mathbb{F}_{p^2}) = 1 + p^2$, we have

$$\sharp\widetilde{X}_0(N)(\mathbb{F}_{p^2}) \le U_p^{(d)}(N) := d(p^2 + 1). \tag{1}$$

This gives an upper bound for $\sharp\widetilde{X}_0(N)(\mathbb{F}_{p^2})$. A lower bound of this number, found by Ogg, is described by $\psi(N) = N\prod(1 + 1/q)$ and $\omega(N)$.

LEMMA 3.1 ([13]). *For a prime p with $p \nmid N$, put*

$$L_p(N) := \frac{p-1}{12}\psi(N) + 2^{\omega(N)}.$$

Then

$$\sharp \widetilde{X}_0(N)(\mathbb{F}_{p^2}) \geq L_p(N). \tag{2}$$

Suppose now $X_0(N)$ is a trigonal curve of genus $g \geq 5$. Then we see from Corollary 1.7 that there exists a finite morphism $X_0(N) \to \mathbb{P}^1$ defined over $\mathbb{Q}$ of degree three. Therefore we must have

$$\frac{p-1}{12}\psi(N) + 2^{\omega(N)} = L_p(N) \leq U_p^{(3)}(N) = 3(p^2+1). \tag{3}$$

LEMMA 3.2. *If $N > 155$, there is a prime $p \nmid N$ which does not satisfy* (3).

Proof. It is sufficient to show that there is a prime $p \nmid N$ satisfying

$$\psi(N) > \frac{12}{p-1}(3(p^2+1) - 2^{\omega(N)}).$$

The proof is divided into the following five cases:

(i) $2 \nmid N$ and $N > 155$; take $p = 2$.
(ii) $2 \mid N$, $3 \nmid N$ and $N > 112$; take $p = 3$.
(iii) $(2 \cdot 3) \mid N$, $5 \nmid N$ and $N > 111$; take $p = 5$.
(iv) $(2 \cdot 3 \cdot 5) \mid N$, $7 \nmid N$ and $N > 119$; take $p = 7$.
(v) $(2 \cdot 3 \cdot 5 \cdot 7) \mid N$; take $p = p_0$, the smallest prime not dividing N.

Assume that $2 \nmid N$ and $N > 155$. Then

$$\psi(N) \geq N + 1 > 156 = \frac{12}{2-1}(3(2^2+1) - 2) \geq \frac{12}{2-1}(3(2^2+1) - 2^{\omega(N)}).$$

This proves the lemma for the case (i). The other cases can be treated in the same manner. (For the case (v), note that $p_0 < 2q_0$ for the largest prime q_0 dividing N.) ∎

Note that $g(X_0(N)) \geq 8$ for all $N > 155$ (equality holds only when $N = 169$). Hence we conclude from Lemma 3.2 that $X_0(N)$ is not trigonal if $N > 155$. Since we see from the list of defining equations given in [16] that there are no trigonal modular curves with genus $g = 5, 6$ ([1]), we may assume that $X_0(N)$ is of genus $g \geq 7$. Then by [13] it is also non-hyperelliptic. There are 84 values of $N \leq 155$ for which $X_0(N)$ is of genus $g \geq 7$. More precisely, we have $g \geq 7$ for all $N \geq 82$ but $N = 121$, and if $N \leq 81$, then $g \geq 7$ for $N = 60, 62, 66, 68–70, 74, 76–78, 80$. Now use the trace formula of Hecke

([1]) The list given in [16] misses the case $N = 121$ ($g = 6$). We have checked, using the method of Section 2, that $X_0(121)$ is not trigonal.

operators [6] to calculate $\sharp\widetilde{X}_0(N)(\mathbb{F}_{p^2})$. Then we find that

$$\sharp\widetilde{X}_0(N)(\mathbb{F}_{p^2}) \le U_p^{(3)}(N)$$

for all $p \nmid N$ only for the following 14 values of N:

$$N = 60, 62, 74, 77, 78, 83, 87, 89, 90, 92, 101, 103, 125, 131. \tag{4}$$

For $N = 78$ and 90, the curve $X_0(N)$ has a non-hyperelliptic quotient curve $X_0(N)/\langle w\rangle$ of genus $g = 5$ for some Atkin–Lehner involution w ([3], [4]). Note, by Proposition 1.5, that checking trigonality of $X_0(N)$ reduces to that of $X_0(N)/\langle w\rangle$. Finally, using the algorithm explained in Section 2, we find that the ideal of $X_0(N)$ (or rather $X_0(N)/\langle w\rangle$ when $N = 78, 90$), viewed as a canonical curve, is generated by quadratic polynomials for all N given in (4). Therefore $X_0(N)$ is not trigonal whenever $g \ge 5$.

Theorem 3.3. *The modular curve $X_0(N)$ is a non-sub-hyperelliptic trigonal curve if and only if*

$$N = 34, 43, 45, 64 \qquad (g = 3);$$
$$N = 38, 44, 53, 54, 61, 81 \qquad (g = 4).$$

For each of the above cases, let us determine the minimal degree of a number field over which there is a trigonal morphism $X_0(N) \to \mathbb{P}^1$. For a construction of a g_3^1 on $X_0(N)$, we refer to Example 1.4. If $X_0(N)$ is of genus $g = 3$, then the projection from a $\mathbb{Q}$-rational cusp yields a trigonal morphism $X_0(N) \to \mathbb{P}^1$ over $\mathbb{Q}$. Next consider the case $g = 4$. Let Q be an irreducible quadric surface over $\mathbb{Q}$ in $\mathbb{P}^3$. After a suitable coordinate change (over $\mathbb{Q}$), it is given by

$$\begin{cases} ax^2 + by^2 + cz^2 + dw^2 = 0, & a, b, c, d \in \mathbb{Q}^* \quad \text{or} \\ ax^2 + by^2 + cz^2 = 0, & a, b, c \in \mathbb{Q}^*. \end{cases}$$

It is then clear that Q is isomorphic over some elementary 2-extension of $\mathbb{Q}$ of degree at most 4 to either a ruled surface given by $xy - zw = 0$ or a quadric cone given by $xy - z^2 = 0$. It follows that for a curve C over $\mathbb{Q}$ of genus $g = 4$, a trigonal morphism $C \to \mathbb{P}^1$ is defined over either $\mathbb{Q}$, a quadratic field, or a biquadratic field.

Returning to our cases, it turns out that the only one of the six cases lies on a quadric cone ($N = 81$), and in this case, the unique trigonal morphism is defined over $\mathbb{Q}$. We also note that $X_0(81)$ is a superelliptic curve (see the table below). For the other, the curve $X_0(N)$ lies on a ruled surface over

$$k(N) = \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-15}),\ \mathbb{Q},\ \mathbb{Q}(\sqrt{-1})$$

according as $N = 38, 44, 53, 54, 61$. Table 1 gives a plane model of $X_0(N)$ over $k(N)$, which reflects the trigonality of the curve, for $g = 4$ (here we put $k(81) = \mathbb{Q}$).

Table 1. Trigonal modular curves of genus $g = 4$

N	Plane model of $X_0(N)/k(N)$
38	$(20t^3 - 22t^2 + 8t - 1)s^3 - (132t^3 - 159t^2 + 62t - 8)s^2$ $+ (288t^3 - 372t^2 + 159t - 22)s - 4(54t^3 - 72t^2 + 33t - 5) = 0$
44	$((2 + 3\sqrt{-2})t^2 - 8\sqrt{-2})ts^3 - (3(6 - 5\sqrt{-2})t^2 - 8\sqrt{-2})s^2$ $- (8\sqrt{-2}t^2 + 3(6 + 5\sqrt{-2}))ts + (8\sqrt{-2}t^2 + (2 - 3\sqrt{-2})) = 0$
53	$((65 + 17\sqrt{-15})t^2 + 30(10 - \sqrt{-15})t - 90\sqrt{-15})ts^3$ $+ 2(5(10 - \sqrt{-15})t^3 - (45 + 68\sqrt{-15})t^2 - 375t + 45\sqrt{-15})s^2$ $- 2(5\sqrt{-15}t^3 + 125t^2 + (45 - 68\sqrt{-15})t - 15(10 + \sqrt{-15}))s$ $+ (10\sqrt{-15}t^2 + 10(10 + \sqrt{-15})t + (65 - 17\sqrt{-15})) = 0$
54	$(t^3 + 8)s^3 - t^3 + 1 = 0$
61	$(3\sqrt{-1}t^2 + 2(2 + 3\sqrt{-1})t + 4\sqrt{-1})ts^3$ $+ (2(2 + 3\sqrt{-1})t^3 + (4 + 11\sqrt{-1})t^2 - 4\sqrt{-1})s^2$ $+ (4\sqrt{-1}t^3 + (4 - 11\sqrt{-1})t + 2(2 - 3\sqrt{-1}))s$ $- (4\sqrt{-1}t^2 - 2(2 - 3\sqrt{-1})t + 3\sqrt{-1}) = 0$
81	$s^3 = t^6 + 9t^3 + 27$

REMARK 3.4. The plane model of $X_0(38)/\mathbb{Q}(\sqrt{-3})$ given above arises from a model of $X_0(38)/\mathbb{Q}$ obtained by twisting $X_0(38)$, furnished with the canonical $\mathbb{Q}$-structure, by $\mathbb{Q}(\sqrt{-3})$.

For $N = 38, 44, 53, 61$, we see from [3, Table 5] that the modular curve $X_0(N)$ (with canonical $\mathbb{Q}$-structure) has a g_4^1 over $\mathbb{Q}$.

4. Some remarks and results for $d = 4, 5$. Let C be an algebraic curve having non-trivial automorphism γ. Then there is a criterion for the d-gonality of C in terms of the number of fixed points of γ.

LEMMA 4.1 ([10]). *Let C be a smooth projective curve defined over an algebraically closed field k, and let γ be an automorphism of C of prime order p. Let S be the set of fixed points of γ. Suppose $f : C \to \mathbb{P}^1$ gives a d-gonal morphism such that $\gamma^* f \neq f$. Then*

$$2d \geq \frac{1}{p-1} \deg R,$$

where R is the ramification divisor of the natural projection $C \to C/\langle\gamma\rangle$.

Proof. (See also [9, Lemma 1.11].) For a function $f: C \to \mathbb{P}^1$, let $\mathrm{div}(f)$ be the divisor of f. Changing f to $(f-\alpha)/(f-\beta)$ for suitable $\alpha, \beta \in k$ if necessary, we may assume that f has a pole or zero at no $P \in S$. Suppose $\mathrm{div}(\gamma^* f) = \mathrm{div}(f)$. Then $\gamma^* f = \zeta f$ for some root of unity ζ in k. By our assumption that $\gamma^* f \neq f$, we find that $\zeta \neq 1$. But then for $P \in S$ we would have

$$\gamma^* f(P) = f(\gamma P) = f(P) \neq \zeta f(P) = \gamma^* f(P),$$

which is impossible. Therefore $\mathrm{div}(\gamma^* f) \neq \mathrm{div}(f)$, in other words, the function $\gamma^*(f)/f$ is non-constant. On the other hand, since γ is of prime order, we see from [15, VI, Cor. to Prop. 7] that the degree of the ramification divisor satisfies the equality

$$\deg R = (p-1) \sum_{Q \in S} \mathrm{ord}_Q(\gamma^*(t_Q) - t_Q),$$

where t_Q is a local parameter at Q and ord_Q is the normalized valuation at Q. Now since

$$\mathrm{ord}_Q\left(\frac{\gamma^*(f)}{f} - 1\right) \geq \mathrm{ord}_Q(\gamma^*(t_Q) - t_Q)$$

for all $Q \in S$, we see that

$$2d \geq \deg\left(\mathrm{div}\left(\frac{\gamma^*(f)}{f} - 1\right)_0\right) \geq \sum_{Q \in S} \mathrm{ord}_Q(\gamma^*(t_Q) - t_Q) = \frac{1}{p-1}\deg R,$$

as desired (here $\mathrm{div}(*)_0$ is the divisor of zeros). ■

Corollary 4.2. *Under the assumption and notation of Lemma* 4.1, *assume further that* γ *is an involution* (*i.e.*, γ *is of order* 2). *Then*

$$g(C) \leq 2g(C/\langle\gamma\rangle) + d - 1.$$

Let us consider the modular curve $X_0(N)$. Corollary 4.2 often gives a nice tool, since $\mathrm{Aut}\, X_0(N)$ contains an elementary 2-abelian group of order $2^{\omega(N)}$ consisting of the Atkin–Lehner involutions on $X_0(N)$ ([2]). For example, we have as an application an alternative proof of Theorem 3.3 (by admitting that there are no trigonal modular curves of genera $g = 5, 6$). Namely, if N is listed in (4), then we see from [3, Table 5] that $X_0(N)$ has an Atkin–Lehner involution with more than 6 fixed points. The method explained in Section 2 is still needed for $g = 5, 6$.

Let us consider the problem of bounding the level N of d-gonal modular curves $X_0(N)$. In fact, we know the following general result of Zograf:

Theorem 4.3 ([17, Thm. 5]). *Let* X_Γ *be the algebraic curve corresponding to a congruence subgroup* $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ *of index*

$$n = [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma].$$

If X_Γ *is* d-*gonal*, *then*

$$n < 128d. \tag{5}$$

Let $\Gamma = \Gamma_0(N)$. The estimate (5) may be improved by a detailed analysis for individual d. For instance, if $d = 1$, then $N \leq 25$ from the genus formula, and if $d = 2$, then $N \leq 71$ by [13]. Theorem 3.3 gives $N \leq 81$ when $d = 3$. Now we consider the cases of $d = 4, 5$.

Let $d = 4$. Then $X_0(N)$ is *tetragonal* but not d'-gonal with $d' \leq 3$ for

$$\begin{aligned}
g = 5:&\quad N = 42, 51, 52, 55, 56, 57, 63, 65, 67, 72, 73, 75,\\
g = 6:&\quad N = 58, 79, 121,\\
g = 7:&\quad N = 60, 62, 68, 69, 77, 80, 83, 85, 89, 91, 98, 100,\\
g = 8:&\quad N = 74, 101, 103, 125,\\
g = 9:&\quad N = 66, 70, 87, 95, 96, 107,\\
g = 10:&\quad N = 92,\\
g = 11:&\quad N = 78, 94, 104, 111, 119, 131,\\
g = 13:&\quad N = 143,\\
g = 14:&\quad N = 167,\\
g = 16:&\quad N = 191,\\
g = 17:&\quad N = 142.
\end{aligned}$$

We note that each of them has an involution v induced by a linear fractional transformation (i.e., an element of the normalizer of $\Gamma_0(N)$ in $\mathrm{GL}_2^+(\mathbb{Q})$) such that the quotient curve $X_0(N)/\langle v\rangle$ is sub-hyperelliptic of non-zero genus (see [3], [4]). Since we see from Theorem 1.6 that every tetragonal curve of genus $g \geq 10$ has a tetragonal morphism over $\mathbb{Q}$, we can prove a statement analogous to Lemma 3.2. Now combining this observation with Corollary 4.2 we find, besides the above list, the possible values of N for which $X_0(N)$ may be tetragonal but not d'-gonal with $d' \leq 3$:

$$N = 76, 82, 84, 88, 90, 93, 97, 99, 106, 108, \\ 109, 113, 115, 128, 133, 137, 157, 169. \tag{6}$$

Next we let $d = 5$. Then again imitating the method explained in Section 3 and using Lemma 4.1, we find the possible values of N for which $X_0(N)$ may be *pentagonal* but not d'-gonal with $d' \leq 4$; N is either one of the above eighteen values (6) or one of the following:

$$N = 86, 112, 117, 122, 136, 144, 147, 148, 153, 162, 163, 180, 181, 187, 193, 197.$$

In particular, we have $N \leq 197$ in this case. Our result is summarized as follows.

Proposition 4.4. *Let $d = 3, 4$ or 5, and assume that $X_0(N)$ is d-gonal. Then*

$$\begin{cases} N \leq 81 & \text{if } d = 3,\\ N \leq 191 & \text{if } d = 4,\\ N \leq 197 & \text{if } d = 5.\end{cases}$$

We note that for $d = 5$, we have not obtained any essentially pentagonal modular curve yet (i.e., not d'-gonal with $d' \leq 4$); thus our bound $N \leq$

197 given above may or may not be the best possible, while $X_0(81)$ (resp. $X_0(191)$) is trigonal (resp. tetragonal).

References

[1] E. Arbarello *et al.*, *Geometry of Algebraic Curves*, Vol. I, Grundlehren Math. Wiss. 267, Springer, 1985.

[2] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. 185 (1970), 134–160.

[3] A. O. L. Atkin and D. J. Tingley, *Numerical tables on elliptic curves*, in: Modular Functions of One Variable IV, B. Birch and W. Kuyk (eds.), Lecture Notes in Math. 476, Springer, 1975, 74–144.

[4] M. Furumoto and Y. Hasegawa, *Hyperelliptic quotients of modular curves* $X_0(N)$, Tokyo J. Math., to appear.

[5] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. 52, Springer, 1977.

[6] H. Hijikata, *Explicit formula of the traces of Hecke operators for* $\Gamma_0(N)$, J. Math. Soc. Japan 26 (1974), 56–82.

[7] J. Igusa, *Kroneckerian model of fields of elliptic modular functions*, Amer. J. Math. 81 (1959), 561–577.

[8] S. L. Kleiman and D. Laksov, *Another proof of the existence of special divisors*, Acta Math. 132 (1974), 163–176.

[9] F. Momose, *p-torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 96 (1984), 139–165.

[10] F. Momose and S. Yamada, *Another estimate of the level of d-gonal modular curves*, preprint.

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

[12] K. V. Nguyen and M.-H. Saito, *D-gonality of modular curves and bounding torsions*, preprint.

[13] A. P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France 102 (1974), 449–462.

[14] B. Saint-Donat, *On Petri's analysis of the linear system of quadrics through a canonical curve*, Math. Ann. 206 (1973), 157–175.

[15] J. P. Serre, *Local Fields*, Grad. Texts in Math. 67, Springer, 1979.

[16] M. Shimura, *Defining equations of modular curves* $X_0(N)$, Tokyo J. Math. 18 (1995), 443–456.

[17] P. G. Zograf, *Small eigenvalues of automorphic Laplacians in spaces of cusp forms*, in: Automorphic Functions and Number Theory, II, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) 134 (1984), 157–168 (in Russian).

Department of Mathematics
Waseda University
3-4-1, Okubo Shinjuku-ku, Tokyo, 169-8555 Japan
E-mail: hase@mse.waseda.ac.jp
shimshim@mse.waseda.ac.jp

Received on 15.7.1997
and in revised form on 23.10.1998 (3224)