# Trigonal modular curves $X_0^{+d}(N)$

By Yuji HASEGAWA and Mahoro SHIMURA

Department of Mathematical Sciences, Waseda University, 3-4-1 Okubo, Shinjuku-ku, Tokyo 169-8555

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1999)

**1. Introduction.** Let $N$ be a positive integer, and let $X_0(N)$ be the modular curve corresponding to the congruence subgroup

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

In [8], we have determined the trigonal modular curves $X_0(N)$. Here an algebraic curve is said to be *trigonal* if it has a finite morphism of degree 3 to the projective line $\mathbf{P}^1$. According to [8], there are no non-trivial trigonal modular curves of type $X_0(N)$, that is, $X_0(N)$ is of genus at most 4 whenever it is trigonal. In this article, we determine the trigonal modular curves $X_0^{+d}(N) = X_0(N)/\langle W_d \rangle$ with $1 \neq d \| N$ (in case $d = N$ it is usually denoted by $X_0^+(N)$) by an argument analogous to [8]. The main result is

**Theorem 1.**

(i) *The curve $X_0^+(N)$ is trigonal of genus $g \geq 5$ if and only if*

$$N = 122, 146, 181, 227 \qquad (g = 5);$$
$$N = 164 \qquad (g = 6);$$
$$N = 162 \qquad (g = 7).$$

(ii) *If $d \neq N$, then $X_0^{+d}(N)$ is trigonal of genus $g \geq 5$ if and only if*

$$(N, d) = (147, 3) \qquad (g = 5);$$
$$(N, d) = (117, 13) \qquad (g = 6).$$

Consequently, it turns out that there do exist non-trivial trigonal modular curves of type $X_0^{+d}(N)$.

We shall prove this theorem only for $X_0^+(N)$. This is simply because we prefer to avoid the complexity of description. The argument of the next section will of course be applied without modification to the general case.

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

The first author was supported in part by Waseda University Grant for Special Research Projects 98A-637 and Grant-in-Aid for Encouragement of Young Scientists 10740023.

**2. Determination of the trigonal modular curves $X_0^+(N)$.** Let $X$ be an algebraic curve of genus $g$. If $g \leq 2$, then it is trigonal; in fact, it is sub-hyperelliptic. Also, $X$ is trigonal if it is non-hyperelliptic with $g = 3, 4$. On the other hand, any hyperelliptic curve of genus $g \geq 3$ is not trigonal. See [5] [1] or [8, § 1].

Let $W(N)$ be the group of Atkin–Lehner involutions on $X_0(N)$. All the pairs $(N, W')$, with $W'$ a subgroup of $W(N)$, for which $X_0(N)/W'$ is hyperelliptic are determined by [6][7][4]. We record here a specific version.

**Theorem 2.** *The curve $X_0^+(N)$ has a hyperelliptic quotient curve of type $X_0(N)/W'$ of genus $g \geq 3$, if and only if*

$$N = 60, 66, 78, 85, 92, 94, 104, 105, 110, 120, 126,$$
$$136, 165, 171, 176, 195, 207, 252, 279, 315.$$

*In particular, $X_0^+(N)$ itself is hyperelliptic of genus $g \geq 3$ if and only if*

$$N = 60, 66, 85, 104 \qquad (g = 3);$$
$$N = 92, 94 \qquad (g = 4).$$

Given a non-negative integer $g$, it is not difficult to determine the values of $N$ for which the genus $g^+(N)$ of $X_0^+(N)$ is equal to $g$. Thus we obtain:

**Proposition 1.** *The curve $X_0^+(N)$ is trigonal of genus $g = 3$ or 4 if and only if $N$ is in the following list.*

| $g$ | $N$ | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 58 | 76 | 86 | 96 | 97 | 99 | 100 | 109 | 113 | 127 |
| | 128 | 139 | 149 | 151 | 169 | 179 | 239 | | | |
| 4 | 70 | 82 | 84 | 88 | 90 | 93 | 108 | 115 | 116 | 117 |
| | 129 | 135 | 137 | 147 | 155 | 159 | 161 | 173 | 199 | 215 |
| | 251 | 311 | | | | | | | | |

From now on, we always assume $g^+(N) \geq 5$, and $N$ is not in the list of Theorem 2. It is a fact that every trigonal curve over $\mathbf{Q}$ of genus $g \geq 5$ has a $\mathbf{Q}$-rational finite morphism of degree 3 to a rational curve over $\mathbf{Q}$ ([11, Thm. 2.1]). Therefore the argument of [8, § 3] is applicable. To be precise, fix a prime $p$ with $p \nmid N$ and consider the reduction $\widetilde{X}_0(N)$ of $X_0(N)$ at $p$. Then

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

gives a lower bound of the number $\sharp\widetilde{X}_0(N)(\mathbf{F}_{p^2})$ of $\mathbf{F}_{p^2}$-rational points on $\widetilde{X}_0(N)$ ([12][13]). Here $\omega(N)$ is the number of distinct prime divisors of $N$, and $\psi$, $h$, $s$ are defined as in [13]. Suppose that $X_0^+(N)$ is trigonal. Then $X_0(N)$ has a $\mathbf{Q}$-rational finite morphism of degree 6 to $\mathbf{P}^1$, so we have an obvious upper bound $U_p^{(6)}(N) = 6(p^2+1)$ of $\sharp\widetilde{X}_0(N)(\mathbf{F}_{p^2})$. Hence if $X_0^+(N)$ is trigonal, then we must have

$$(*) \qquad L_p(N) \le U_p^{(6)}(N).$$

**Lemma.** *If $N > 335$, there is a prime $p \nmid N$ which does not satisfy the inequality $(*)$.*

The proof is analogous to [8, Lem. 3.2]. The above lemma implies that $X_0^+(N)$ is not trigonal whenever $N > 335$, since in this case $g^+(N) \ge 5$. Hence we assume in the following that $N \le 335$. We first check whether there is a prime $p$ not dividing $N$ which does not satisfy $(*)$. This is indeed the case for

$$N = 160, 170, 182, 189, 190, 196, 198, 200, 208, 216, 220, 222, 224\text{-}226, 228, 230\text{-}232, 234, 236\text{-}238, 240, 242\text{-}246, 248\text{-}250, 254\text{-}256, 258, 260\text{-}262, 264\text{-}268, 270, 272\text{-}276, 278, 280, 282, 284\text{-}288, 290\text{-}292, 294\text{-}306, 308\text{-}310, 312, 314, 316, 318\text{-}330, 332\text{-}335.$$

Next we eliminate the possibility for the following values of $N$ by applying [8, Cor. 4.2]:

$$N = 102, 114, 118, 123, 124, 138, 140\text{-}142, 144, 145, 156, 158, 166, 168, 174, 177, 178, 184, 186, 188, 202, 204\text{-}206, 210, 213, 214.$$

Namely, there is an involution $\gamma$ on $X_0^+(N)$ having more than 6 fixed points for these $N$. Here $\gamma$ can be chosen so that it is of Atkin–Lehner type except for $N = 144$, in which case we set $\gamma = V_2W_{16}$ (see [4, § 2] for notation).

The third step is counting the exact number of rational points over finite fields. To do this, we employ the trace formulas of Hecke operators [9][16]. We see that, for the following values of $N$, there is a prime $p$ with $p \nmid N$ such that

$$\sharp\widetilde{X}_0^+(N)(\mathbf{F}_q) > 3(q+1),$$

where $\widetilde{X}_0^+(N)$ is the reduction of $X_0^+(N)$ at $p$ and $q$ is a power of $p$.

$$N = 154, 163, 172, 185, 187, 192, 194, 201, 209, 211, 212, 217\text{-}219, 221, 223, 229, 233, 235, 241, 247, 253, 257, 259, 269, 271, 277, 281, 283, 289, 293, 307, 313, 317, 331.$$

Finally, we apply the method explained below to determine the trigonality of $X_0^+(N)$ for the remaining values of $N$. The values to be tested are:

$$N = 106, 112, 122, 130, 132\text{-}134, 146, 148, 150, 152, 153, 157, 162, 164, 175, 180, 181, 183, 193, 197, 203, 227, 263.$$

Let $N$ be one of them. In case $N = 180$ we have $g^+(180) = 10$ and it suffices to check the trigonality of $X_0^+(180)/\langle W_4\rangle$, which is of genus 5 ([10, Thm. VII.2][11, Lem. 1.3]). Otherwise we have $g^+(N) \le 8$.

The key of our algorithm is the following fundamental

**Theorem 3.** *Let $X$ be a canonical curve of genus $g \ge 5$. Then $X$ is trigonal if and only if the intersection of all the quadrics passing through $X$ contains a rational scroll. Furthermore, in this case $X$ lies on this scroll, and the $g_3^1$ is cut out by the ruling of the scroll.*

For the proof, see, e.g., [1, III, § 3][14]. In view of the above theorem, we proceed as follows (cf. [8, § 2]). Let $X$ be a canonical curve of genus $g \ge 5$. Let $P$ be a point of $X$ and let $L$ be a line through $P$. After a suitable coordinate change, we may assume $P = (1 : 0 : \cdots : 0)$, so that $L$ is parametrized as $\{(u : v\xi_2 : \cdots : v\xi_g)\}$ for some $(\xi_2 : \cdots : \xi_g) \in \mathbf{P}^{g-2}$. Let $\{Q_i\}_{i=1}^n$, $n = (g-2)(g-3)/2$ be a basis for the quadratic part $I_2$ of the ideal of $X$. Since $P$ is a common zero of the $Q_i$, we have $Q_i(1, vx_2, \ldots, vx_g) = vF_{1i} + v^2F_{2i}$, where the $F_{ji}$ are homogeneous polynomials of degree $j$ in $x_2, \ldots, x_g$. Therefore the line $L$ is contained in $\cap Z(Q_i)$ if and only if $F_{1i}(\xi_2, \ldots, \xi_g) = F_{2i}(\xi_2, \ldots, \xi_g) = 0$ for $1 \le i \le n$. ($Z(F)$ stands for the zero set of a homogeneous polynomial $F$.) We thus have

**Proposition 2.** *Notation being as above, $X$ is trigonal if and only if there is a non-trivial solution for the system of equations $F_{1i} = F_{2i} = 0$, $1 \le i \le n$.*

Returning to our case, a basis $\{Q_i\}$ for $I_2$ is easily computed by using modular forms ([15]). It turns out that the equations in the proposition have a non-trivial solution if and only if $N = 122, 146, 162, 164, 181, 227$; this proves our assertion (for $X_0^+(N)$).

**3. Plane models.** In this section, we give plane models of the trigonal modular curves $X_0^{+d}(N)$ of genus $g \geq 5$.

Let $X$ be a trigonal curve of genus $g$, and let $|D|$ be a $g_3^1$ on $X$. It is known that this is the only $g_3^1$ on $X$ whenever $g \geq 5$ ([1, Chap. III, Exer. B-3]). Note that $|K-D|$ is base-point-free by Clifford's theorem. If $g=5$, then $|K-D|$ is a $g_5^2$, and this linear system realizes $X$ as a plane quintic with one node. Projecting from this node, we get the $g_3^1$. Next set $g=6$. Then $|K-D|$ is a $g_7^3$, so $X$ is represented as a space curve of degree 7. On the other hand, every non-singular space curve of degree 7, not contained in any plane, has genus at most 6. If $Y$ is one such, with genus 6, then $Y$ lies on a non-singular quadric $Q$ as a curve of type $(3,4)$. This means that one of the rulings on $Q$ cuts out the $g_3^1$ on $Y$ (so $Y$ is trigonal). (For the facts on space curves used above, see [5, IV, § 6].) Furthermore, if $|D'|$ is a base-point-free $g_6^2$ on a curve $Y'$ of genus 6, then $Y'$ is trigonal if and only if the map associated to $|D'|$ is either a three-fold covering of a conic ($|D'| = |2D|$), or a birational map to a plane sextic, which has a triple point ($|D'| = |K-D-P| \neq |2D|$ for some $P \in X$). For more information about curves of genera 5, 6, see [1][5]. Finally consider the case $g=7$. Then $|K-2D|$ is a $g_6^2$, which must be base-point-free, since otherwise $X$ would be birational to a plane quintic. We claim that the image of $X$ under the map associated to $|K-2D|$ is a plane sextic with a triple point. This can be shown as follows. Let $\phi$ be the map associated to $|K-2D|$. Note that $\phi$ cannot be a double covering of a plane cubic, since $X$ is not hyperelliptic, nor bielliptic. On the other hand, it cannot be a triple covering of a conic, since $K-2D$ is not linearly equivalent to $2D$. Thus $\phi$ determines a birational map to a plane sextic. Furthermore, since there is a canonical divisor of the form $3D+P_1+P_2+P_3$, $P_1, P_2, P_3 \in X$, this plane curve must have a triple point, which is the image of $P_1$, $P_2$, $P_3$.

Let us now display plane models of trigonal modular curves $X_0^{+d}(N)$. In each case, we choose $t$ as a function of degree 3 such that $(t)_\infty \geq P_\infty$, where $P_\infty$ is the cusp at infinity. If we embed the $(s,t)$-plane in $\mathbf{P}^2$ by $(s,t) \mapsto (s:t:1)$, then $P_\infty = (0:1:0)$. Also, the point $(1:0:0)$ is a singularity of the given plane model. When $g \neq 6$, this is the sole singularity. When $g=6$, there is one more, namely, $(1:1:0)$ (resp. $(0:1:0)$) if $(N,d) = (164,164)$ (resp. $(117,13)$).

Table I. Trigonal modular curves $X_0^+(N)$ of genus $g = g^+(N) \geq 5$

| $N$ | $g$ | Plane model of $X_0^+(N)$ |
|---|---|---|
| 122 | 5 | $(t^2{+}2t{+}2)s^3 + t(t^2{+}3t{+}3)s^2 + (t^4{+}3t^3{+}2t^2{-}2t{-}1)s - t(t{+}1)(t^2{+}3t{+}3) = 0$ |
| 146 | 5 | $(t^2{-}3t{+}3)s^3 + (t{-}1)(t{-}2)s^2 + (t{-}1)(2t^2{-}7t{+}7)s - (t{-}1)(t{-}2)(t^2{-}3t{+}3) = 0$ |
| 181 | 5 | $(t{-}1)s^3 + (t^3{+}2t^2{+}t{-}2)s^2 + t(t^3{-}3t{-}1)s - (t^2{-}t{-}1) = 0$ |
| 227 | 5 | $(4t^2{+}15t{+}17)s^3 + (3t^3{+}9t^2{-}t{-}16)s^2 + (t^4{+}3t^3{-}t^2{-}2t{+}6)s - (t^3{+}t^2{+}1) = 0$ |
| 164 | 6 | $(t^3{+}t{+}1)s^3 - (2t^4{+}t^3{+}3t^2{+}3t{+}1)s^2 + (t{+}1)(t^4{+}2t^2{+}t{+}1)s - (t^2{+}1) = 0$ |
| 162 | 7 | $(t{-}1)(t^2{+}t{+}1)s^3 + 3t(t^3{+}t{-}1)s^2 + 3t(t^2{+}1)(t^2{-}t{+}1)s - (3t^5{-}3t^4{+}t^3{-}3t^2{+}1) = 0$ |

Table II. Trigonal modular curves $X_0^{+d}(N)$ of genus $g = g^{+d}(N) \geq 5$

| $(N,d)$ | $g$ | Plane model of $X_0^{+d}(N)$ |
|---|---|---|
| $(147,3)$ | 5 | $(t^2{-}t{+}1)s^3 - (t^3{-}2t^2{+}4t{-}2)s^2 + (t^4{+}5t^2{-}3t{+}2)s - (t^3{-}2t^2{+}t{-}1) = 0$ |
| $(117,13)$ | 6 | $t(t^2{+}3t{+}3)s^3 - (t{+}1)(t{+}3)(t^2{+}3)s - 3t(t^2{+}3t{+}3) = 0$ |

## References

[ 1 ] E. Arbarello, M. Cornalba, P. A. Griffis, and J. Harris: Geometry of Algebraic Curves, Vol.I. Grundlehren Math. Wiss., **267**, Springer-Verlag, Berlin-Heidelberg-New York, pp. 1–386 (1985).

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

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

[ 4 ] M. Furumoto and Y. Hasegawa: Hyperelliptic quotients of modular curves $X_0(N)$. Tokyo J. Math., **22**, 105–125 (1999).

[ 5 ] R. Hartshorne: Algebraic Geometry. Graduate Text in Math., **52**, Springer-Verlag, Berlin-Heidelberg-New York, pp. 1–496 (1977).

[ 6 ] Y. Hasegawa: Table of quotient curves of modular curves $X_0(N)$ with genus 2. Proc. Japan Acad., **71A**, 235–239 (1995).

[ 7 ] Y. Hasegawa: Hyperelliptic modular curves $X_0^*(N)$. Acta Arith., **81**, 369–385 (1997).

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

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

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

[11] K.V. Nguyen and M.-H. Saito: D-gonality of modular curves and bounding torsions (preprint).

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

[13] A. P. Ogg: Modular functions. The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979) (eds. B. Cooperstein and G. Mason), Proc. Sympos. Pure Math., **37**, Amer. Math. Soc., pp. 521–532 (1980).

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

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

[16] M. Yamauchi: On the traces of Hecke operators for a normalizer of $\Gamma_0(N)$. J. Math. Kyoto Univ., **13**, 403–411 (1973).

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