Trigonal modular curves $X_0^*(N)$

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., June 13, 2000)

Abstract: For a positive integer N, let $X_0^*(N)$ denote the quotient curve of $X_0(N)$ by the Atkin–Lehmer involutions. In this paper, we determine the trigonality of $X_0^*(N)$ for all N. It turns out that there are seven values of N for which $X_0^*(N)$ is a non-trivial trigonal curve.

Key words: Modular curve; trigonal curve; Atkin–Lehmer involution.

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

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

For a positive divisor d of N such that $d \neq 1$ and $(d, N/d) = 1$, let $X_0^{+d}(N)$ denote the quotient curve of $X_0(N)$ by the Atkin–Lehner involution W_d corresponding to d; in case $d = N$, this is the curve usually denoted by $X_0^+(N)$. By our previous works [6][7], all the trigonal modular curves $X_0(N)$ and $X_0^{+d}(N)$ have been determined. Here an algebraic curve is said to be *trigonal* if it has a finite morphism of degree 3 to the projective line $\mathbf{P}^1$. It turns out that every trigonal modular curve of type $X_0(N)$ is "trivial" in the sense it has genus at most 4 (see the beginning of Section 2); on the other hand, there do exist non-trivial trigonal modular curves of type $X_0^{+d}(N)$.

Now let $X_0^*(N)$ be the quotient curve of $X_0(N)$ by the group of Atkin–Lehner involutions. By definition, this equals $X_0^+(N)$ when N is a prime power. In this article, we determine the trigonal modular curves $X_0^*(N)$ by an argument analogous to [7]. That is,

Theorem 1. *The curve $X_0^*(N)$ is trigonal of genus $g \geq 5$ if and only if*

$$N = 181, 227, 253, 302, 323, 555 \qquad (g = 5);$$
$$N = 351 \qquad (g = 6).$$

Notation. For a positive integer N, we define $\omega(N)$ to be the number of distinct prime divisors of N, and $\psi(N)$ to be the product $N \prod_q (1 + 1/q)$, where the product runs over the set of distinct prime divisors of N. We also denote, for a (fixed) prime $p \nmid N$, by $\widetilde{X}_0(N)$, $\widetilde{X}_0^*(N)$ the reduction of $X_0(N)$, $X_0^*(N)$ at p respectively.

2. An upper bound for N. An algebraic curve of genus $g \leq 4$ is trigonal, unless $g = 3, 4$ and it is hyperelliptic. On the other hand, any hyperelliptic curve of genus $g \geq 3$ is not trigonal. See [9][3][1] for details. In view of these facts, we first exhibit the values of N for which $X_0^*(N)$ is hyperelliptic of genus $g \geq 3$.

Theorem 2 ([4]). *The curve $X_0^*(N)$ is hyperelliptic of genus $g \geq 3$ if and only if*

$$N = 136, 171, 207, 252, 315 \qquad (g = 3);$$
$$N = 176 \qquad (g = 4);$$
$$N = 279 \qquad (g = 5).$$

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	97	109	113	127	128	139	144	149	151	152
	162	164	169	175	178	179	183	185	187	189
	194	196	203	217	234	236	239	240	245	246
	248	249	258	270	282	290	294	295	303	310
	312	318	329	348	420	429	430	455	462	476
	510									
4	137	148	160	172	173	199	200	201	202	214
	219	224	225	228	242	247	251	254	259	260
	261	262	264	267	273	275	280	300	305	306
	308	311	319	321	322	334	335	341	342	345
	350	354	355	366	370	374	385	395	399	426
	434	483	546	570						

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

This work was supported in part by Grant-in-Aid for JSPS Fellows 11-06151 and by Waseda University Grant for Special Research Projects 2000A-157.

In what follows, we always assume $g^*(N) \geq 5$ and $N \neq 279$. We know from [10, Thm. 2.1] 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 $\mathbf{Q}$. Thus if $X_0^*(N)$ is trigonal, then $X_0(N)$ admits a $\mathbf{Q}$-rational morphism of degree $3 \cdot 2^{\omega(N)}$ to $\mathbf{P}^1$, since the natural projection $X_0(N) \to X_0^*(N)$ has degree $2^{\omega(N)}$ and is defined over $\mathbf{Q}$. This means that, for each prime $p \nmid N$, there is a morphism $\widetilde{X}_0(N) \to \mathbf{P}^1$ over $\mathbf{F}_p$ of degree at most $3 \cdot 2^{\omega(N)}$ ([10, Lem. 5.1]). Ogg's lower bound for $\sharp\widetilde{X}_0(N)(\mathbf{F}_{p^2})$ then tells us:

Lemma 1 ([11]). *The curve $X_0^*(N)$ is not trigonal if there exists a prime p not dividing N such that*

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

Using this, we can find an upper bound for the values of N for which $X_0^*(N)$ is possibly trigonal.

Proposition 2. *The curve $X_0^*(N)$ is not trigonal whenever $N > 4830$.*

Proof. (The proof is essentially the same as the hyperelliptic case; see the argument given in [5, p. 181].) Let p be the smallest prime not dividing N. We will then show that (1) actually holds for all $N > 4830$. Let us write

$$f(N) := \frac{1}{2^{\omega(N)}}\psi(N), \quad g(x) := 12\frac{3x^2+2}{x-1}.$$

Note that $f(N)$ is multiplicative and $g(n)$ is increasing for integers $n \geq 2$. Clearly it suffices to show that

$$f(N) > g(p). \tag{2}$$

First assume that $r := \omega(N) \geq 6$. Let p_i be the i-th prime. Then we have

$$f(N) \geq f(p_1 \cdots p_r) \text{ and } g(p_{r+1}) \geq g(p).$$

Thus we are reduced to show that

$$f(p_1 \cdots p_r) > g(p_{r+1}). \tag{3}$$

Obviously, this holds for $r = 6$. For $r > 6$, this can be shown by induction on r. Indeed, we have $p_{r+1} < 2p_r$ by Chebyshev's theorem, so

$$\frac{g(p_{r+1})}{g(p_r)} = \frac{3{p_{r+1}}^2+2}{3{p_r}^2+2}\frac{p_r-1}{p_{r+1}-1} < \frac{3{p_{r+1}}^2+2}{3{p_r}^2+2} \leq \frac{12{p_r}^2+2}{3{p_r}^2+2} < 4.$$

On the other hand, since $f(N)$ is multiplicative, we have

$$\frac{f(p_1 \cdots p_r)}{f(p_1 \cdots p_{r-1})} = f(p_r) = \frac{1}{2}(p_r+1) > 4.$$

It follows that

$$\frac{f(p_1 \cdots p_r)}{f(p_1 \cdots p_{r-1})} > \frac{g(p_{r+1})}{g(p_r)}.$$

This implies (3), since $f(p_1 \cdots p_{r-1}) > g(p_r)$ by the induction hypothesis.

Assume now that $r < 6$, so $p \leq p_{r+1} \leq p_6 = 13$. Let us define

$$N_0(r) = \max_{1 \leq i \leq r+1}\{N_0(r;i)\},$$

where

$$N_0(r;i) = \begin{cases} 2^r \cdot g(2) - 1 & \text{if } i = 1; \\ 2^r \dfrac{p_1 \cdots p_{i-1}}{\psi(p_1 \cdots p_{i-1})} g(p_i) & \text{if } i > 1. \end{cases}$$

Then clearly (2) holds for all $N > N_0(r)$ such that $\omega(N) = r$, since

$$\psi(N) \geq \begin{cases} N+1 & \text{if } p = 2; \\ N\dfrac{\psi(p_1 \cdots p_{i-1})}{p_1 \cdots p_{i-1}} & \text{if } p = p_i,\ i > 1. \end{cases}$$

More explicitly, the inequality (2) holds for

$$N > \begin{cases} 2^r \cdot 168 - 1 & \text{if } 1 \leq r \leq 4; \\ 5443 & \text{if } r = 5. \end{cases}$$

Note that in the range $N \leq 5443$ there are only seven values of N for which $r = 5$, the largest being $N = 4830$. The assertion follows. □

3. Determination of the trigonal modular curves $X_0^*(N)$. We are now ready to determine the trigonal modular curves $X_0^*(N)$. Before applying the trisecant criterion described in [7, § 2] to the canonical embedding of $X_0^*(N)$, we proceed as follows. To begin with, we check whether $\psi(N) > 128 \cdot 3 \cdot 2^{\omega(N)}$; if this is the case, then $X_0^*(N)$ cannot be trigonal by Zograf's theorem [14, Thm. 5]. If not, we next check whether N satisfies the condition of Lemma 1 (we let p be the smallest prime not dividing N). If this is not the case either, then using Eichler–Shimura congruence relation we count the exact number $\sharp\widetilde{X}_0^*(N)(\mathbf{F}_q)$ for every prime power q such that $(N, q) = 1$ and $q \leq g^2$, and check the inequality $\sharp\widetilde{X}_0^*(N)(\mathbf{F}_q) > 3(q+1)$. For the trace formulas of Hecke operators used in this step, we refer to [8][13]. Now we tabulate the values of N for which

Table I. 137 values for the trisecant criterion and 34 values for the number of fixed points

g	N
5	192 208 212 216 218 226 235 237 250 253
	278 302 323 339 *364* 371 376 377 378 382
	391 396 402 406 407 410 413 414 418 435
	438 440 442 *444* 465 494 *495* 551 555 572
	574 595 630 663 714 770 798 910
6	244 265 272 274 291 297 301 314 327 332
	336 338 351 470 506 561 564 598 609 627
	690 780 858
7	*232* 288 309 324 358 *360* 363 *372* 423 450
	456 *460* 474 490 492 498 *504* 518 525 530
	550 *558* 582 636 638 *660* 870 924
8	*292* *304* *333* 346 362 408 468 480 *520* *532*
	534 540 552 585 606 651 654 665 759 930
	966 *990* 1020 1155

g	N
9	*328* *392* 404 *522* *528* *560* *588* 594 602 618
	642 1110 1122 1140
10	600 612 616 678 *696* 702 708 741 *840* 1050
	1218 1230 1290 1326
11	666 *672* 1302
12	*744* 1170 2310
13	*720* *1260*
14	*1320* 1410 1590 2730
15	810 *1380* 1470
16	900 *1560*
17	*1530*
19	*1680* 3570

Table II. Trigonal modular curves $X_0^*(N)$ of genus $g = g^*(N) \geq 5$ $(\omega(N) \geq 2)$

N	g	Plane model of $X_0^*(N)$
253	5	$(3t^2-7t+6)s^3 - (t^3-5t^2+9t+1)s^2 - (4t^3-9t^2-t-1)s + t(t^3-2t^2-2) = 0$
302	5	$ts^3 + (t^3+2t^2+3)s^2 + (t^4+3t^3+6t^2+5t-2)s - (t^2+2t+2)(t^2+2t+3) = 0$
323	5	$t(t+1)s^3 + (t^3-2t^2-2)s^2 - (3t^3-2)s - (t^4-t^3-3t+1) = 0$
555	5	$(t^2+2t+6)s^3 - (2t^3+13t^2+12t-4)s^2 + (4t^4+12t^3+7t^2-6t-2)s - t^2(4t^2+2t-5) = 0$
351	6	$(t+1)s^3 - 3(t+1)(t^2+2t+3)s^2$ $+ 3(t^5+5t^4+13t^3+19t^2+18t+11)s - (3t^5+24t^4+72t^3+111t^2+76t+34) = 0$

$\omega(N) \geq 2$ and none of the above conditions are satisfied (Table I; 171 values in total). Note that if $4|N$ or $9\|N$, the curve $X_0^*(N)$ has an involution [4]. In this case we also check whether this involution has more than 6 fixed points; if so, then $X_0^*(N)$ is not trigonal (such values in Table I are italicized).

Example. Let N be a positive integer such that $N \leq 4830$ and $r = 5$, i.e., $N = 2310$, 2730, 3570, 3990, 4290, 4620, 4830. Then we see that $X_0^*(N)$ is not trigonal for

$N = 4620, 4830$ by Zograf's theorem;
$N = 4290$ by Lemma 1 ($p = 7$);
$N = 3990$ by the inequality

$$\sharp\widetilde{X}_0^*(N)(\mathbf{F}_{121}) = 376 > 3(121+1).$$

For $N = 2310$, 2730 and 3570, none of the above conditions are satisfied.

Now, as the final step, we determine the trigonality of $X_0^*(N)$ for the remaining 137 values of N by applying the trisecant criterion; the curve $X_0^*(N)$ is trigonal if and only if N is in the list of Theorem 1. Table II gives the plane models of the trigonal modular curves $X_0^*(N)$ of genus $g \geq 5$. We refer to [7, § 3] the method to obtain plane models of such curves.

In each case, we choose t as a function of degree 3 such that $(t)_\infty \geq P_\infty$, where P_∞ 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 the sole singularity of the given plane model.

References

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

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

[3] Hartshorne, R.: Algebraic Geometry. Grad. Texts

in Math., **52**, Springer, Berlin–Heidelberg–New York, pp. 1–496 (1977).
[4] Hasegawa, Y.: Hyperelliptic modular curves $X_0^*(N)$. Acta Arith., **81**, 369–385 (1997).
[5] Hasegawa, Y., and Hashimoto, K.: Hyperelliptic modular curves $X_0^*(N)$ with square-free levels. Acta Arith., **77**, 179–193 (1996).
[6] Hasegawa, Y., and Shimura, M.: Trigonal modular curves. Acta Arith., **88**, 129–140 (1999).
[7] Hasegawa, Y., and Shimura, M.: Trigonal modular curves $X_0^{+d}(N)$. Proc. Japan Acad., **75A**, 172–175 (1999).
[8] Hijikata, H.: Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$. J. Math. Soc. Japan, **26**, 56–82 (1974).
[9] Kleiman, S. L. and Laksov, D.: Another proof of the existence of special divisors. Acta Math., **132**, 163–176 (1974).
[10] Nguyen, K. V., and Saito, M.-H.: D-gonality of modular curves and bounding torsions (preprint).
[11] Ogg, A. P.: Hyperelliptic modular curves. Bull. Soc. Math. France, **102**, 449–462 (1974).
[12] Shimura, M.: Defining equations of modular curves $X_0(N)$. Tokyo J. Math., **18**, 443–456 (1995).
[13] Yamauchi, M.: On the traces of Hecke operators for a normalizer of $\Gamma_0(N)$. J. Math. Kyoto Univ., **13**, 403–411 (1973).
[14] Zograf, P. G.: Small eigenvalues of automorphic Laplacians in spaces of cusp forms (Russian) Automorphic functions and number theory, II. Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI), **134**, 157–168 (1984).