BULL. AUSTRAL. MATH. SOC. 11G30, 14H55
VOL. 54 (1996) [291–297]

ON THE GENUS OF SOME MODULAR CURVES OF LEVEL N

CHANG HEON KIM AND JA KYUNG KOO

We estimate the genus of the modular curves $X_1(N)$.

INTRODUCTION

Let $\mathfrak{h}$ be the complex upper half plane. Then $SL_2(\mathbb{Z})$ acts on $\mathfrak{h}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = (az+b)/(cz+d)$. Let $\mathfrak{h}^*$ be the union of $\mathfrak{h}$ and $\mathbb{P}^1(\mathbb{Q})$, and let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ $(=\Gamma(1))$, which is a Fuchsian group of the first kind and contains a principal congruence subgroup $\Gamma(N)$ for some positive integer N. Then the modular curve $\Gamma\backslash\mathfrak{h}^*$ is a projective closure of the affine curve $\Gamma\backslash\mathfrak{h}$, which we denote by X_Γ, with genus g_Γ. In this article, we shall determine the genus $g(N)$ of the modular curve $X_1(N)$ $(= X_{\Gamma_1(N)})$ when $\Gamma = \Gamma_1(N)$ for $N = 1, 2, 3, \cdots$. Here, we denote by $\Gamma_1(N)$ the group of elements in $\Gamma(1)$ which are congruent to $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ mod N.

THEOREM 1. *The genus $g(N)$ of $X_1(N)$ is given by*

$$g(N) = \begin{cases} 0, & \text{if } 1 \leqslant N \leqslant 4 \\ 1 + \dfrac{N^2}{24} \prod\limits_{p|N} \left(1 - \dfrac{1}{p^2}\right) - \dfrac{1}{4} \sum\limits_{d|N,\, d>0} \varphi(d)\varphi\left(\frac{N}{d}\right), & \text{otherwise} \end{cases}$$

where φ is the Euler's phi function.

We shall see later in §1 that $g(N) = 0$ only for the eleven cases $1 \leqslant N \leqslant 10$ and $N = 12$.

Throughout the article we adopt the following notation:

$\overline{\Gamma}$ is the inhomogeneous congruence group $(= \Gamma / \pm I)$

Γ_s is the isotropy group of s

$\Gamma(N) = \{\gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv I \mod N\}$

$\Gamma_0(N)$ is the Hecke subgroup $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid c \equiv 0 \mod N\right\}$

$\sigma_0(N)$ is the number of positive divisors of N.

Received 8th November, 1995
Supported by KOSEF Research Grant 95-K3-0101 (RCAA).

1. Proof

Let μ be the index of $\overline{\Gamma}_1(N)$ in $\overline{\Gamma}(1)$. Let ν_2 (respectively ν_3) be the number of $\overline{\Gamma}_1(N)$–inequivalent elliptic points of order 2 (respectively order 3) and ν_∞ be the number of $\overline{\Gamma}_1(N)$–inequivalent cusps. It is well-known [**1**, p.68, **2**, Chapter IV] or [**3**, Proposition 1.40] that

$$(*) \qquad g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}.$$

Thus, in order to estimate g it is enough to know the explicit values of μ, ν_2, ν_3 and ν_∞.

(i) μ :

For the congruence subgroup $\Gamma_0(N)$ of $\Gamma(1)$, we know [**3**, Proposition 1.43] that

$$(1.1) \qquad [\overline{\Gamma}(1) : \overline{\Gamma}_0(N)] = N \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

Note that $\Gamma_1(N)$ is the kernel of the surjective homomorphism f_N from $\Gamma_0(N)$ to $(\mathbb{Z}/N\mathbb{Z})^\times$ defined by $f_N\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = d \mod N$. This yields

$$[\Gamma_0(N) : \Gamma_1(N)] = \varphi(N) = N \cdot \prod_{p|N} \left(1 - \frac{1}{p}\right).$$

Since $-1 \in \Gamma_0(N)$ and $-1 \notin \Gamma_1(N)$ except for $N = 1, 2$,

$$(1.2) \qquad [\overline{\Gamma}_0(N) : \overline{\Gamma}_1(N)] = \begin{cases} N \cdot \prod_{p|N} \left(1 - \frac{1}{p}\right), & \text{if } N = 1,2 \\ \frac{N}{2} \cdot \prod_{p|N} \left(1 - \frac{1}{p}\right), & \text{otherwise.} \end{cases}$$

By (1.1) and (1.2),

$$\mu = [\overline{\Gamma}(1) : \overline{\Gamma}_1(N)] = \begin{cases} 1, & \text{if } N = 1 \\ 3, & \text{if } N = 2 \\ \frac{N^2}{2} \cdot \prod_{p|N} \left(1 - \frac{1}{p^2}\right), & \text{otherwise.} \end{cases}$$

(ii) ν_2 and ν_3 :

Recall that $\gamma \in \Gamma(1)$ is an elliptic element if and only if $|tr(\gamma)| < 2$. If $\gamma \in \Gamma_1(N)$, then $\gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N$. Hence, $tr(\gamma)$ lies in $2 + N\mathbb{Z}$. Thus $\Gamma_1(N)$ has no elliptic element unless $N = 1,2,3$. If $N = 1$, $\Gamma_1(1) = \Gamma(1)$ so that $\nu_2 = \nu_3 = 1$. If $N = 2$, $\Gamma_1(2) = \Gamma_0(2)$ and hence, by [**3**, Proposition 1.43], $\nu_2 = 1$ and $\nu_3 = 0$. If $N = 3$, then $\overline{\Gamma}_1(3) = \overline{\Gamma}_0(3)$. Again, by the same argument, $\nu_2 = 0$ and $\nu_3 = 1$. We summarise the above by

$$\nu_2 = \begin{cases} 1, & \text{if } N = 1,2 \\ 0, & \text{otherwise} \end{cases}$$

and

$$\nu_3 = \begin{cases} 1, & \text{if } N = 1,3 \\ 0, & \text{otherwise.} \end{cases}$$

(iii) ν_∞ :

First, we consider all pairs

$$\text{(1.3)} \qquad \{c, d\} \text{ of positive integers satisfying } (c,d) = 1,\ d \mid N,\ 0 < c \leqslant N/d$$
$$\text{(or } c \text{ in any set of representatives for } \mathbb{Z} \bmod (N/d)).$$

For each pair $\{c, d\}$, take a and b so that $ad - bc = 1$ and fix them. Then the elements $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfying (1.3) form a set of representatives for $\Gamma_0(N)\backslash\Gamma(1)$. Also, the number of double cosets in $\Gamma_0(N)\backslash\Gamma(1)/\Gamma_s$ for any fixed cusp s gives the number of $\Gamma_0(N)$-inequivalent cusps. Take s to be 0. Then we see that it is the number of pairs $\{c, d\}$ satisfying (1.3) modulo the equivalence $\sim$ defined by $\{c, d\} \sim \{c', d'\}$ if $\begin{pmatrix} * & * \\ c' & d' \end{pmatrix} = \begin{pmatrix} * & * \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$ for some $m \in \mathbb{Z}$. From the last equality, we come up with $d = d'$ and $c' = c + dm$. Therefore, for fixed d

$$\text{(1.4)} \qquad \text{there are exactly } \varphi((d, N/d)) \text{ inequivalent pairs.}$$

Now choose a pair $\{c, d\}$ satisfying (1.3) and $\xi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ from $\Gamma(1)$. Put $s = b/d$. Then $\xi \cdot 0 = s$. We want to estimate the index $[\overline{\Gamma}_0(N)_s : \overline{\Gamma}_1(N)_s]$. Suppose that $\pm\xi^{-1}\Gamma_0(N)_s\xi = \left\{\pm\begin{pmatrix} 1 & 0 \\ h_1 & 1 \end{pmatrix}^n\right\}_{n\in\mathbb{Z}}$ for some $h_1 > 0$ and $\pm\xi^{-1}\Gamma_1(N)_s\xi = \left\{\pm\begin{pmatrix} 1 & 0 \\ h_2 & 1 \end{pmatrix}^n\right\}_{n\in\mathbb{Z}}$ for some $h_2 > 0$. Recall that h_1 (respectively h_2) is the smallest positive integer h such that

$$\text{(1.5)} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ h & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 + bdh & -b^2h \\ d^2h & 1 - bdh \end{pmatrix} \in \pm\Gamma_0(N)$$
$$\text{(respectively } \pm\Gamma_1(N)).$$

If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ h & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$ belongs to $-\Gamma_1(N)$, then by taking the trace we have $2 = -2 \mod N$; hence N divides 4, that is, $N = 1, 2, 4$. In what follows, we assume that $N \neq 1, 2, 4$. The cases $N = 1, 2, 4$ will be dealt with separately. By (1.5), h_1 is the smallest positive integer h such that $d^2 h \equiv 0 \mod N$ and h_2 is the smallest positive integer h such that

$$d^2 h \equiv 0 \equiv bdh \mod N. \tag{1.6}$$

Clearly, $h_1 = N/(d^2, N)$. Let h_1' be the smallest positive integer such that $bdh' \equiv 0 \mod N$. Since $d \mid N$, we are forced to get

$$h_1' = \frac{N/d}{(b, N/d)}. \tag{1.7}$$

Then $h_2 = l.c.m(h_1, h_1')$. Observe that $(d^2, N) = (d, N) \cdot ((d, N), N/(d, N)) = d \cdot (d, N/d)$ because N is divisible by d. Using this we are able to rewrite h_1 as

$$h_1 = \frac{N}{(d^2, N)} = \frac{N}{d \cdot (d, N/d)} = \frac{N}{d} \cdot \frac{1}{(d, N/d)}. \tag{1.8}$$

Since $(b, N/b) \mid b$, $(d, N/d) \mid d$ and $(b, d) = 1$, by (1.7) and (1.8) we have $h_2 = l.c.m.(h_1, h_1') = N/d$. Thus

$$\begin{aligned}[\overline{\Gamma}_0(N)_s : \overline{\Gamma}_1(N)_s] &= [\pm\xi^{-1}\Gamma_0(N)_s\xi : \pm\xi^{-1}\Gamma_1(N)_s\xi] \\ &= [h_1\mathbb{Z} : h_2\mathbb{Z}] = \frac{h_2}{h_1} \\ &= \frac{N/d}{N/d \cdot 1/(d, N/d)} = (d, N/d).\end{aligned} \tag{1.9}$$

Now consider the natural projection $p : \overline{\Gamma}_1(N)\backslash\mathfrak{h}^* \to \overline{\Gamma}_0(N)\backslash\mathfrak{h}^*$. Let $p^{-1}(s) = \{s_1, \dots s_h\}$ and let e_k be the ramification index of p at s_k. Then by [**3**, Proposition 1.37], $e_k = [\overline{\Gamma}_0(N)_{s_k} : \overline{\Gamma}_1(N)_{s_k}]$ for $k = 1, \dots, h$. Furthermore, $\overline{\Gamma}_1(N) \triangleleft \overline{\Gamma}_0(N)$ implies that $e_1 = \cdots = e_h$ and

$$[\overline{\Gamma}_0(N) : \overline{\Gamma}_1(N)] = e_1 h = (d, N/d) \cdot h \tag{1.10}$$

by (1.9). Here h is the number of elements of $p^{-1}(s)$ which is equal to the number of those in $p^{-1}(b/d)$ depending only on d. By (1.4), given d, there are $\varphi((d, N/d))$

$\overline{\Gamma}_0(N)$-inequivalent cusps with the same d. Therefore, we have

$$\begin{aligned}
\nu_\infty &= \sum_{d|N} \varphi((d, N/d))h \\
&= \sum_{d|N} \varphi((d, N/d))(d, N/d)^{-1}\varphi(N)/2 \text{ by (1.10)} \\
&= \sum_{d|N} \frac{\varphi(d)\varphi(N/d)}{\varphi(d\cdot(N/d))}\frac{\varphi(N)}{2} \quad \text{using the fact that } \varphi(n_1)\varphi(n_2) = \varphi(n_1 n_2)\frac{\varphi((n_1, n_2))}{(n_1, n_2)} \\
&= \frac{1}{2}\sum_{d|N} \varphi(d)\varphi(N/d).
\end{aligned}$$

Next, we deal with the cases $N = 1, 2, 4$. If $N = 1$, $\Gamma_1(1) = \Gamma(1)$; hence $\nu_\infty = 1$. If $N = 2$, $\Gamma_1(2) = \Gamma_0(2)$, and so by [**3**, Proposition 1.43], $\nu_\infty = 2$. If $N = 4$, $\overline{\Gamma}_1(4) = \overline{\Gamma}_0(4)$, and again by the same Proposition 1.43 in [**3**], $\nu_\infty = 3$. In summary,

$$\nu_\infty = \begin{cases} 1, & \text{if } N = 1 \\ 2, & \text{if } N = 2 \\ 3, & \text{if } N = 4 \\ \frac{1}{2}\sum_{d|N} \varphi(d)\varphi(N/d), & \text{otherwise .} \end{cases}$$

Substituting (i), (ii) and (iii) into the formula $(*)$, we get the theorem.

PROPOSITION 2. *For $N > 20$, $g(N) > 1$.*

PROOF: It follows from Theorem 1 that $g(N) = 1 + (N^2/24)\prod_{p|N}(1 - 1/p^2) - (1/4)\sum_{d|N,\, d>0}\varphi(d)\varphi(N/d)$. Notice that $N \cdot \prod_{p|N}(1 - 1/p) = \varphi(N)$ and $\varphi(d)\varphi(N/d) = \varphi(N)\cdot(\varphi((d, N/d)))/((d, N/d)) \leqslant \varphi(N)$. Then $g(N) \geqslant 1 + (1/24)\Big(N \cdot \prod_{p|N}(1 + 1/p)\cdot\varphi(N) - 6\sigma_0(N)\cdot\varphi(N)\Big)$. We will show that for $N > 20$

$$N \cdot \prod_{p|N}\left(1 + \frac{1}{p}\right) \geqslant 6 \cdot \sigma_0(N), \tag{1.11}$$

where the equality holds if and only if N is square-free. Put $q(N) = \left(N \cdot \prod_{p|N}\left(1 + \frac{1}{p}\right)\right)/(\sigma_0(N))$ and $f_p(k) = (p^k + p^{k-1})/(k+1)$. We must show $q(N) \geqslant 6$. Then for $k \geqslant 1$,

$$\frac{d}{dk}f_p(k) = \frac{(p^k + p^{k-1})((\log p)(k+1) - 1)}{(k+1)^2} > 0$$

indicates that

$$f_p(k_1) < f_p(k_2) \quad \text{for} \quad k_1 < k_2. \tag{1.12}$$

Also it is easy to see that

$$f_{p_1}(k) < f_{p_2}(k) \quad \text{for} \quad p_1 < p_2. \tag{1.13}$$

For $1 \leqslant k \leqslant 5$, f_p has the following values:

k	f_2	f_3	f_5	f_7	f_{11}
1	1.5	2	3	4	6
2	2	4	10	$18\frac{2}{3}$	44
3	3	9	37.5	98	363
4	4.8	21.6	150	548.8	3194.4
5	8	54	625	$3201\frac{1}{3}$	29282

Let $N = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorisation. Then $q(N) = f_{p_1}(k_1) \cdots f_{p_r}(k_r)$. Let $r(N)$ be the number of distinct primes dividing N. If $r(N) \geqslant 3$,

$$q(N) \geqslant f_2(1)f_3(1)f_5(1) = 9 > 6 \quad \text{by (1.12), (1.13) and the table.}$$

If $r(N) = 1$ or 2, we can check the inequality as follows:

(i) $r(N) = 2,\ 2 \nmid N$: $q(N) > f_3(1)f_5(1) = 6$.

(ii) $r(N) = 2,\ 2^3 \mid N$: Since $r(N) = 2$, there exists an odd prime p dividing N. Then $q(N) \geqslant f_2(3)f_3(1) = 6$. In this case, N is not square-free and so we have strict inequality in (1.11).

(iii) $r(N) = 2,\ 2 \mid N,\ (15, N) = 1$: Since $r(N) = 2$ and $3 \nmid N, 5 \nmid N$, there exists an odd prime $p \geqslant 7$ dividing N. Then $q(N) > f_2(1)f_7(1) = 6$.

(iv) $r(N) = 2,\ 2^2 \mid \mid N,\ 3^2 \mid N$: $q(N) \geqslant f_2(2)f_3(2) > 6$.

(v) $r(N) = 2,\ 2^2 \mid \mid N,\ 5^2 \mid N$: $q(N) \geqslant f_2(2)f_5(2) > 6$.

(vi) $r(N) = 2,\ 2 \mid \mid N,\ 3^3 \mid N$: $q(N) \geqslant f_2(1)f_3(3) > 6$.

(vii) $r(N) = 2,\ 2 \mid \mid N,\ 5^2 \mid N$: $q(N) \geqslant f_2(1)f_5(2) > 6$.

(viii) $r(N) = 1,\ N = p^k,\ p \geqslant 11$: $q(N) > f_{11}(1) \geqslant 6$.

(ix) $r(N) = 1,\ N = 7^k,\ k \geqslant 2$: $q(N) \geqslant f_7(2) > 6$.

(x) $r(N) = 1,\ N = 5^k,\ k \geqslant 2$: $q(N) \geqslant f_5(2) > 6$.

(xi) $r(N) = 1,\ N = 3^k,\ k \geqslant 3$: $q(N) \geqslant f_3(3) > 6$.

(xii) $r(N) = 1,\ N = 2^k,\ k \geqslant 5$: $q(N) \geqslant f_2(5) > 6$.

This completes the proof. ∎

For $N \leqslant 20$, Theorem 1 gives the following table :

N	μ	ν_∞	ν_2	ν_3	g
1	1	1	1	1	0
2	3	2	1	0	0
3	4	2	0	1	0
4	6	3	0	0	0
5	12	4	0	0	0
6	12	4	0	0	0
7	24	6	0	0	0
8	24	6	0	0	0
9	36	8	0	0	0
10	36	8	0	0	0
11	60	10	0	0	1
12	48	10	0	0	0
13	84	12	0	0	2
14	72	12	0	0	1
15	96	16	0	0	1
16	96	14	0	0	2
17	144	16	0	0	5
18	108	14	0	0	3
19	180	18	0	0	7
20	144	20	0	0	3

REMARK. From this table and Proposition 2, we conclude that $g(N) = 0$ if and only if $N = 1, \ldots, 10$ and 12.

REFERENCES

[1] R. Rankin, *Modular forms and functions* (Cambridge, Cambridge University press, 1977).

[2] B. Schoeneberg, *Elliptic modular functions* (Springer-Verlag, Berlin, Heidelberg, New York, 1973).

[3] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan **11** (Princeton, Tokyo, 1971).

Department of Mathematics
Korea Advanced Institute of Science and Technology
Taejon 305-701
Korea