Comm. Korean Math. Soc. **12** (1997), No. 1, pp. 17–25

SOME NOTES ON THE GENUS OF MODULAR CURVE $X_0^0(N)$

CHANG HEON KIM AND JA KYUNG KOO

ABSTRACT. We estimate the genus $g(N)$ of modular curve $X_0^0(N)$ and show that $g(N) = 0$ if and only if $1 \leq N \leq 5$.

1. Introduction

Let $\mathfrak{H}$ be the complex upper half plane. Then $SL_2(\mathbb{Z})$ acts on $\mathfrak{H}$ by linear fractional transformation. Let $\mathfrak{H}^*$ be the union of $\mathfrak{H}$ and $\mathbb{P}^1(\mathbb{Q})$ and, for $N \geq 1$, let $\Gamma_0^0(N)$ be a congruence subgroup of $\Gamma(1)$ $(= SL_2(\mathbb{Z}))$ defined by

$$\Gamma_0^0(N) = \left\{ \gamma \in \Gamma(1) \,|\, \gamma \equiv \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \mod N \right\}.$$

The modular curve $\Gamma_0^0(N)\backslash\mathfrak{H}^*$ which is a projective closure of smooth affine curve $\Gamma_0^0(N)\backslash\mathfrak{H}$ is denoted by $X_0^0(N)$. In this article, we shall first directly compute the genus $g(N)$ of the modular curve $X_0^0(N)$ as follows.

THEOREM 1.

$$g(N) = 1 + \frac{N^2}{12}\prod_{p|N}\left(1+\frac{1}{p}\right) - \frac{\alpha_N}{4}\prod_{p|N}\left(1+\left(\frac{-1}{p}\right)\right) - \frac{\beta_N}{3}\prod_{p|N}\left(1+\left(\frac{-3}{p}\right)\right) - \frac{N}{2}\prod_{p|N}\left(1+\frac{1}{p}\right)$$

Received July 13, 1996. Revised October 7, 1996.
1991 AMS Subject Classification: 11F03, 11F11.
Key words and phrases: modular curve, genus, elliptic element, cusp element.
This work was supported in part by Non Directed Research Fund, Korea Research Foundation 1993 and KOSEF Research Grant 95-K3-0101 (RCAA).

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

$$\beta_N = \begin{cases} 0, & \text{if } 3|N \\ 1, & \text{otherwise} \end{cases} \quad \text{and } \left(\frac{\cdot}{p}\right) \text{ is the Legendre symbol.}$$

Next, let $\Gamma_0(N)$ be the Hecke subgroup of elements in $\Gamma(1)$ which are congruent to $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ mod N. Comparing the genus of the curve $X_0(N^2)$ $(= \Gamma_0(N^2)\backslash\mathfrak{H}^*)$ [1], [2], [5] with the above $g(N)$, we are able to derive an interesting identity (Corollary 2). And, using Theorem 1, we shall see later in §2 that $g(N) = 0$ only for the five cases $1 \leq N \leq 5$.

Throughout the article we adopt the following notations:

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

Γ_s the isotropy group of s

2. Proof

Let μ be the index of $\overline{\Gamma}_0^0(N)$ in $\overline{\Gamma}(1)$ as transformation groups. Let ν_2 (resp. ν_3) be the number of $\Gamma_0^0(N)$-inequivalent elliptic points of order 2 (resp. order 3) and ν_∞ be the number of $\Gamma_0^0(N)$-inequivalent cusps. It is well-known ([3] p.68, [4] Ch. IV or [5] Proposition 1.40) that

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

Thus in order to estimate $g(N)$ it is enough to know the explicit values of μ, ν_2, ν_3 and ν_∞. (i) μ:

Observe that $\Gamma_0^0(N)$ is contained in the Hecke subgroup $\Gamma_0(N)$. Put $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then $T^{\mathbb{Z}} = \{T^n \mid n \in \mathbb{Z}\}$ is also contained in $\Gamma_0(N)$. Hence, $\Gamma_0^0(N)T^{\mathbb{Z}} \subseteq \Gamma_0(N)$. Conversely, for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, let n be an integer such that $an \equiv b \mod N$. Since $(a, N) = 1$, such n can be uniquely determined up to mod N. Consider $\gamma T^{-n} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} =$

$\begin{pmatrix} a & -an+b \\ c & -cn+d \end{pmatrix}$. Since $-an + b \equiv 0 \mod N$ and $c \equiv 0 \mod N$, we have $\gamma T^{-n} \in \Gamma_0^0(N)$, i.e., $\gamma \in \Gamma_0^0(N)T^{\mathbb{Z}}$. Hence,

$$\Gamma_0(N) = \Gamma_0^0(N)T^{\mathbb{Z}}. \tag{2}$$

Note that N is the smallest positive integer j such that $T^j \in \Gamma_0^0(N)$. Hence, from (2) we come up with the following right coset decomposition of $\Gamma_0(N)$ with respect to the subgroup $\Gamma_0^0(N)$

$$\Gamma_0(N) = \bigcup_{j=0}^{N-1} \Gamma_0^0(N)T^j. \tag{3}$$

Therefore $[\overline{\Gamma}_0(N) : \overline{\Gamma}_0^0(N)] = [\Gamma_0(N) : \Gamma_0^0(N)] = N$. Now by [5], Proposition 1.43 and the above, we conclude that

$$\begin{aligned} \mu &= [\overline{\Gamma}(1) : \overline{\Gamma}_0^0(N)] \\ &= [\overline{\Gamma}(1) : \overline{\Gamma}_0(N)] \cdot [\overline{\Gamma}_0(N) : \overline{\Gamma}_0^0(N)] \\ &= N \cdot \prod_{p|N} \left(1 + \tfrac{1}{p}\right) \cdot N \\ &= N^2 \cdot \prod_{p|N} \left(1 + \tfrac{1}{p}\right). \end{aligned}$$

(ii) ν_2:

Suppose that there exists an elliptic element γ of order 2 in $\Gamma_0^0(N)$ which is conjugate to $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ under $\Gamma(1)$. Then, for some element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma(1)$,

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} S \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} bd + ac & -b^2 - a^2 \\ c^2 + d^2 & -bd - ac \end{pmatrix}. \tag{4}$$

In order for γ to sit in $\Gamma_0^0(N)$, we must have

$$a^2 + b^2 \equiv 0 \mod N \text{ and } c^2 + d^2 \equiv 0 \mod N. \tag{5}$$

If $2|N$, then both a and b are even or odd. And, so are both c and d. Thus we are forced to have that $1 = ad - bc$ must be even, which is impossible. Therefore, if $2|N$, $\nu_2 = 0$. When $2 \nmid N$, we'll count the number of conjugacy classes of γ in $\Gamma_0^0(N)$, which is equal to ν_2. First, we view γ as an elliptic element in $\Gamma_0(N)$ and consider its conjugacy class in $\Gamma_0(N)$ which is denoted by $\mathcal{C}$, i.e., $\mathcal{C} = \{\sigma\gamma\sigma^{-1} | \sigma \in \Gamma_0(N)\}$. Take $\gamma' \in \mathcal{C} \cap \Gamma_0^0(N)$. By (2), we can write γ' as $\gamma' = \tau T^j \gamma T^{-j} \tau^{-1}$ for some $\tau \in \Gamma_0^0(N)$ and $j \in \mathbb{Z}$. Then $T^j\gamma T^{-j} = \tau^{-1}\gamma'\tau \in \Gamma_0^0(N)$. On the other hand, by matrix computation using (4), we come to have

$$T^j \gamma T^{-j} = \begin{pmatrix} * & -(b+jd)^2 - (a+jc)^2 \\ c^2 + d^2 & * \end{pmatrix}$$

, which implies that $(a+jc)^2 + (b+jd)^2 \equiv 0 \mod N$. Rewrite it as

$$\begin{aligned}(a+jc)^2 + (b+jd)^2 &= (c^2+d^2)j^2 + 2(ac+bd)j + a^2 + b^2 \\ &\equiv 0 \cdot j^2 + 2(ac+bd)j + 0 \mod N \quad \text{by (5).}\end{aligned}$$

It follows from (4) that $(ac+bd, N) = 1$. Therefore, if $a \nmid N$ then $(2(ac+bd), N) = 1$. This claims that $j \equiv 0 \mod N$ with $2 \nmid N$ so that $\tau T^j \in \Gamma_0^0(N)$. Thus, if $2 \nmid N$ then any element in $\mathcal{C} \cap \Gamma_0^0(N)$ is $\Gamma_0^0(N)$-conjugate to γ. It shows that $\nu_2(\Gamma_0(N)) \geq \nu_2(\Gamma_0^0(N))$.

Next, consider an elliptic element σ in $\Gamma_0(N)$ which is conjugate to S. By abuse of notation, we write $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} S \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$ as before. Take an integer j such that $2(ac+bd)j + a^2 + b^2 \equiv 0 \mod N$. When $2 \nmid N$, such j is uniquely determined up to mod N. Now, we consider $T^j\sigma T^{-j}$ which belongs to $\Gamma_0(N)$-conjugacy class of σ. By similar argument to the former case, one sees that $T^j\sigma T^{-j}$ lies in $\Gamma_0^0(N)$. Hence, any $\Gamma_0(N)$-conjugacy class of σ contains an element of $\Gamma_0^0(N)$. This gives us the reverse inequality, that is, $\nu_2(\Gamma_0(N)) \leq \nu_2(\Gamma_0^0(N))$. Therefore we get by [5] Proposition 1.43 that

$$\nu_2 = \begin{cases} 0, & \text{if } 2|N \\ \prod_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right), & \text{otherwise} \end{cases}.$$

(iii) ν_3:

Suppose that there exists an elliptic element γ of order 3 in $\Gamma_0^0(N)$ which is conjugate to $ST = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$. Then for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$, γ can be written in the form

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} ST \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \tag{6}$$

where $A = bd + ac - bc$, $B = -b^2 - a^2 + ab$, $C = c^2 + d^2 - cd$ and $D = -bd - ac + ad$. Since γ belongs to $\Gamma_0^0(N)$, we must have

$$a^2 + b^2 - ab \equiv 0 \mod N \text{ and } c^2 + d^2 - cd \equiv 0 \mod N. \tag{7}$$

First, let's consider the case $3|N$. Since $ad - bc = 1$, $(a, b) = 1 = (c, d)$. Then one of a and b is not a multiple of 3, say $3 \nmid a$. Similarly, one of c and d is not a multiple of 3, say $3 \nmid c$. Let a^{-1} (resp. c^{-1}) be the arithmetic inverse of a (resp. c) mod 3. It follows from (7) that $a^2 + b^2 - ab \equiv 0 \mod 3$. Thus $1 + (a^{-1}b)^2 - (a^{-1}b) \equiv 0 \mod 3$, which is equivalent to $a^{-1}b \equiv -1 \mod 3$. Therefore $b \equiv -a \mod 3$. In a similar way, one can have $d \equiv -c \mod 3$. Then $1 = ad - bc \equiv -ac + ac \equiv 0 \mod 3$, which results in a contradiction. Hence, if $3|N$ then $\nu_3 = 0$.

Next, we think of the case $3 \nmid N$. As in the case of ν_2, let $\mathcal{C}$ be the $\Gamma_0(N)$-conjugacy class of γ and let us consider an element γ' from $\mathcal{C} \cap \Gamma_0^0(N)$. By (2), $\gamma' = \tau T^i \gamma T^{-i} \tau^{-1}$ for some $\tau \in \Gamma_0^0(N)$ and $i \in \mathbb{Z}$. On the other hand, we obtain by (6) that

$$\begin{aligned} T^i \gamma T^{-i} &= \begin{pmatrix} * & -(b + id)^2 - (a + ic)^2 + (a + ic)(b + id) \\ c^2 + d^2 - cd & * \end{pmatrix} \\ &= \begin{pmatrix} * & -Ci^2 + (D - A)i + B \\ C & * \end{pmatrix} \end{aligned}$$

with $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ as in (6). Since $T^i \gamma T^{-i} \in \Gamma_0^0(N)$, we must have $-Ci^2 + (D - A)i + B \equiv 0 \mod N$. The fact that $B, C \equiv 0 \mod N$ yields

$$(D - A)i \equiv 0 \mod N. \tag{8}$$

Now, we consider the congruence relation $(D-A)^2 \equiv (D+A)^2 - 4AD \mod N$. Since γ is conjugate to ST whose trace is 1, $D+A$ (=the trace of γ) must be 1. Also $1 = \det\gamma = AD - BC \equiv AD \mod N$. So, $(D-A)^2 \equiv -3 \mod N$. Therefore if $3 \nmid N$, N is relatively prime to $D-A$. This guarantees that $i \equiv 0 \mod N$ in (8). Hence, $\tau T^i \in \Gamma_0^0(N)$. Since any element from $\mathcal{C} \cap \Gamma_0^0(N)$ is $\Gamma_0^0(N)$-conjugate to γ, we conclude that $\nu_3(\Gamma_0(N)) \geq \nu_3(\Gamma_0^0(N))$. Conversely, let us take an elliptic element σ order 3 of $\Gamma_0(N)$ which is conjugate to ST under $\Gamma(1)$. We can then write it as $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} ST \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with $C \equiv 0 \mod N$. By similar argument as before, $D-A$ must be relatively prime to N. Hence we can choose an integer i such that $(D-A)i + B \equiv 0 \mod N$. And $T^i \sigma T^{-i} \in \Gamma_0^0(N)$. Thus any $\Gamma_0(N)$-conjugacy class of σ contains an elliptic element of $\Gamma_0^0(N)$, which implies $\nu_3(\Gamma_0(N)) \leq \nu_3(\Gamma_0^0(N))$. It then follows from [5] Proposition 1.43 that

$$\nu_3 = \begin{cases} 0, & \text{if } 3|N \\ \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right), & \text{otherwise.} \end{cases}$$

(iv) ν_∞:

Let $s \in \mathbb{P}^1(\mathbb{Q})$ be a cusp and $\xi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element in $\Gamma(1)$ such that $\xi\infty = s$. Then

$$\pm\xi^{-1}\Gamma(1)_s\xi = \left\{ \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^j \right\}_{j\in\mathbb{Z}}$$

and

$$\pm\xi^{-1}\Gamma_0^0(N)_s\xi = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^j \right\}_{j\in\mathbb{Z}}$$

for some $h > 0$. Here h is the smallest integer for which

$$\xi \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \xi^{-1} = \begin{pmatrix} * & a^2h \\ -c^2h & * \end{pmatrix} \text{ belongs to } \Gamma_0^0(N).$$

Therefore, h must be the smallest positive integer such that $a^2h \equiv 0 \mod N$ and $c^2h \equiv 0 \mod N$. From this we come up with

$$h = l.c.m. \left(\frac{N}{(a^2, N)}, \frac{N}{(c^2, N)} \right). \tag{9}$$

But, the fact that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ implies $(a, c) = 1$. Hence, $h = N$ in (9). And

$$[\overline{\Gamma}(1)_s : \overline{\Gamma}_0^0(N)_s] = [\pm\xi^{-1}\Gamma(1)_s\xi : \pm\xi^{-1}\Gamma_0^0(N)_s\xi] = N. \tag{10}$$

Now, let $p : \Gamma_0^0(N)\backslash\mathfrak{H}^* \to \Gamma(1)\backslash\mathfrak{H}^*$ be the natural projection. Let $p^{-1}(\infty) = \{s_1, \ldots, s_{\nu_\infty}\}$ and e_j be the ramification index of p at s_j. Then $e_j = [\overline{\Gamma}(1)_{s_j} : \overline{\Gamma}_0^0(N)_{s_j}] = N$ by (10) and so $\mu = [\overline{\Gamma}(1) : \overline{\Gamma}_0^0(N)] = e_1 + \cdots + e_{\nu_\infty} = N \cdot \nu_\infty$. Therefore, we end up with $\nu_\infty = \mu/N = N \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right)$. □

Let $A_N = \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}$. Since $A_N\Gamma_0^0(N)A_N^{-1} = \Gamma_0(N^2)$, the genus of $X_0^0(N)$ is equal to that of the modular curve $X_0(N^2)$ $(= \Gamma_0(N^2)\backslash\mathfrak{H}^*)$. We can then derive from [5] Proposition 1.43 ([1] Theorem 9.10 ; [2] Theorem 4.2.5 and 4.2.7) the following interesting fact whose elementary proof can be done by multiplicativity of the Euler function φ.

COROLLARY 2.

$$\sum_{\substack{d|N^2 \\ d>0}} \varphi\left(\left(d, \tfrac{N^2}{d}\right)\right) = N \cdot \prod_{p|N} \left(1 + \tfrac{1}{p}\right).$$

PROPOSITION 3. *For $N > 20$, $g(N) > 21$.*

PROOF. It follows from Theorem 1 that

$$g(N) \geq 1 + \tfrac{N^2}{12} \prod_{p|N} \left(1 + \tfrac{1}{p}\right) - \tfrac{1}{4} \prod_{p|N} 2 - \tfrac{1}{3} \prod_{p|N} 2 - \tfrac{N}{2} \prod_{p|N} \left(1 + \tfrac{1}{p}\right).$$

By simplifying the above inequality, we get

$$g(N) \geq 1 + \tfrac{N-6}{12} \cdot N \cdot \prod_{p|N} \left(1 + \tfrac{1}{p}\right) - \tfrac{7}{12} \prod_{p|N} 2. \tag{11}$$

Now let $N = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization. Then $N \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right)$ $= \prod_{i=1}^{r} (p_i^{k_i} + p_i^{k_i - 1})$ is greater than $\prod_{p|N} 2$. Hence, (11) becomes

$$\begin{aligned} g(N) &> 1 + \tfrac{N-6}{12} \cdot N \cdot \prod_{p|N} \left(1 + \tfrac{1}{p}\right) - \tfrac{7}{12} \cdot N \cdot \prod_{p|N} \left(1 + \tfrac{1}{p}\right) \\ &\geq 1 + \tfrac{N-13}{12} \cdot N \cdot \prod_{p|N} \left(1 + \tfrac{1}{p}\right). \end{aligned}$$

Let $l(N) = \frac{N-13}{12} \cdot N \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right)$. Then $l(N) > 22$ for $N \geq 24$. Furthermore by an easy computation we can check that $l(21) = 21\frac{1}{3}$, $l(22) = 27$, $l(23) = 20$. Therefore, the proposition follows.

On the other hand, for $N \leq 20$, Theorem 1 gives the following table:

N	μ	ν_∞	ν_2	ν_3	g	N	μ	ν_∞	ν_2	ν_3	g
1	1	1	1	1	0	11	132	12	0	0	6
2	6	3	0	0	0	12	288	24	0	0	13
3	12	4	0	0	0	13	182	14	2	2	8
4	24	6	0	0	0	14	336	24	0	0	17
5	30	6	2	0	0	15	360	24	0	0	19
6	72	12	0	0	1	16	384	24	0	0	21
7	56	8	0	2	1	17	306	18	2	0	17
8	96	12	0	0	3	18	648	36	0	0	37
9	108	12	0	0	4	19	380	20	0	2	22
10	180	18	0	0	7	20	720	36	0	0	43

REMARK. From the above table and Proposition 3, we conclude that $g(N) = 0$ if and only if $N = 1, 2, 3, 4, 5$. This amounts to saying that the genus of the curve $X_0(N^2)$ is zero only for the five cases $1 \leq N \leq 5$.

References

1. Knapp, A.W., *Elliptic Curves*, Mathematical Notes 40, Princeton University Press, 1992.
2. Miyake, T., *Modular Forms*, Springer-Verlag, 1989.
3. Rankin, R., *Modular Forms and Functions*, Cambridge: Cambridge University press, 1977.
4. Schoeneberg, B., *Elliptic Modular Functions*, Springer-Verlag, 1973.
5. Shimura, G., *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan, No.11., Tokyo Princeton, 1971.

Department of Mathematics
KAIST
Taejon 305-701, Korea