ACTA ARITHMETICA
112.1 (2004)

Bielliptic modular curves $X_1(N)$

by

Daeyeol Jeon and Chang Heon Kim (Seoul)

0. Introduction. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ be the full modular group. For any integer $N \geq 1$, we have subgroups $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$ of Γ defined by matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ congruent modulo N to

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

respectively. We let $X(N), X_1(N), X_0(N)$ be the modular curves defined over $\mathbb{Q}$ associated to $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$ respectively. The X's are compact Riemann surfaces. Denote the genera of $X_1(N), X_0(N)$ by $g_1(N), g_0(N)$ respectively.

A smooth, projective curve X with genus $g(X) \geq 2$ is called *hyperelliptic* (respectively *bielliptic*) if it admits a map $\phi : X \to C$ of degree 2 onto a curve C of genus zero (respectively one).

Harris and Silverman [H-S] showed that if a curve X with $g(X) \geq 2$ defined over a number field K is neither hyperelliptic nor bielliptic, then the set of quadratic points on X,

$$\{P \in X(\overline{K}) : [K(P) : K] \leq 2\}$$

is finite.

Bars [B] determined all the bielliptic modular curves of type $X_0(N)$ and also found all curves $X_0(N)$ which have infinitely many quadratic points over $\mathbb{Q}$.

In this paper, we shall determine all the bielliptic modular curves of type $X_1(N)$. Our result is as follows.

Theorem 0.1. *The curve $X_1(N)$ is bielliptic for exactly* 8 *values of N, namely for $N =$* 13, 16, 17, 18, 20, 21, 22, 24.

2000 *Mathematics Subject Classification*: 11G18, 11G30.

The first author supported by the Brain Korea 21 Project in 2001.

The work of the second author was supported by the Post-doctoral Fellowship Program of Korea Science and Engineering Foundation (KOSEF).

We also discuss the problem of determining all modular curves $X_1(N)$ which have infinitely many quadratic points over $\mathbb{Q}$.

1. Preliminaries. Let $\varDelta$ be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$. Let $X_\varDelta(N)$ be the modular curve defined over $\mathbb{Q}$ associated to the modular group $\varGamma_\varDelta(N)$:

$$\varGamma_\varDelta(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \varGamma \;\middle|\; c \equiv 0 \bmod N,\ (a \bmod N) \in \varDelta \right\}.$$

We always assume that $-1 \in \varDelta$. For $d \mid N$, let π_d be the natural projection from $(\mathbb{Z}/N\mathbb{Z})^*$ to $(\mathbb{Z}/\{d, N/d\}\mathbb{Z})^*$, where $\{d, N/d\}$ is the least common multiple of d and N/d.

THEOREM 1.1 ([K]). *The genus of the modular curve $X_\varDelta(N)$ is*

$$g(X_\varDelta(N)) = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2},$$

where

$$\mu = N \prod_{\substack{p \mid N \\ prime}} \left(1 + \frac{1}{p}\right) \frac{\varphi(N)}{|\varDelta|},$$

$$\nu_2 = |\{(b \bmod N) \in \varDelta \mid b^2 + 1 \equiv 0 \bmod N\}| \cdot \frac{\varphi(N)}{|\varDelta|},$$

$$\nu_3 = |\{(b \bmod N) \in \varDelta \mid b^2 - b + 1 \equiv 0 \bmod N\}| \cdot \frac{\varphi(N)}{|\varDelta|},$$

$$\nu_\infty = \sum_{\substack{d \mid N \\ d > 0}} \frac{\varphi(d) \cdot \varphi(N/d)}{|\pi_d(\varDelta)|}.$$

PROPOSITION 1.2. *Let v be any involution on the compact Riemann surface X, and let $\#$ denote the number of fixed points of v. Then we have the following genus formula*:

$$g(v \backslash X) = \frac{1}{4}\,(2g(X) + 2 - \#).$$

Proof. This follows from the Hurwitz formula. ∎

For an integer a prime to N, let $[a]$ denote the automorphism of $X_1(N)$ represented by $\gamma \in \varGamma_0(N)$ such that $\gamma \equiv \left(\begin{smallmatrix} a & * \\ 0 & * \end{smallmatrix}\right) \bmod N$. Sometimes we regard $[a]$ as a matrix.

For any matrices $A, B \in M_2(\mathbb{Z})$ which give automorphisms on $X_1(N)$, we write $A \equiv B \bmod \varGamma_1(N)$ if $A^{-1}B \in \pm\varGamma_1(N)$. In fact, if $A \equiv B \bmod \varGamma_1(N)$, then A and B define the same automorphism on $X_1(N)$.

For each divisor $d \mid N$ with $(d, N/d) = 1$, consider the matrices of the form

$$\begin{pmatrix} dx & y \\ Nz & dw \end{pmatrix}$$

with $x, y, z, w \in \mathbb{Z}$ and determinant d. They define a unique involution on $X_0(N)$, called the *Atkin–Lehner involution* and denoted by W_d. In particular, if $d = N$, then W_N is called the *full Atkin–Lehner involution.* We also denote by W_d a matrix of the above form.

Now we fix a matrix W_d. By [K-Ko2], W_d belongs to the normalizer of $\Gamma_1(N)$ in $\mathrm{PSL}_2(\mathbb{R})$ and therefore defines an automorphism of $X_1(N)$. For each integer a prime to N, $[a]W_d$ defines a different automorphism of $X_1(N)$. Furthermore W_d, in general, does not give an involution on $X_1(N)$. But when $d = N$, W_N still gives an involution on $X_1(N)$ whose properties are investigated in the following proposition.

PROPOSITION 1.3. *Let $\psi : X_1(N) \to X_0(N)$ be the Galois covering with Galois group $G = (\mathbb{Z}/N\mathbb{Z})^*/\pm 1$.*

(1) *W_N defines an involution on $X_1(N)$ and $[a]W_N \equiv W_N[a^{-1}] \bmod \Gamma_1(N)$ for each $a \in G$.*

(2) *Let $\tau_0 \in X_0(N)$ be a fixed point of W_N. Then the covering ψ is unramified at each inverse image of τ_0. Thus the number of inverse images of τ_0 is equal to the degree of ψ.*

(3) *Let $\tau \in X_1(N)$ be a fixed point of W_N. For each $a \in G$, $[a]\tau$ is also fixed by W_N if and only if $a^2 \equiv \pm 1 \bmod N$.*

(4) *Let $c \in G \setminus G^2$ and $\tau, \tau' \in X_1(N)$ be fixed by W_N and $[c]W_N$ respectively. Then $\psi(\tau) \neq \psi(\tau')$.*

Proof. (1) We can write $W_N = [b]\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ for some $b \in G$. It is easy to check that $[b]\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)[b^{-1}] \bmod \Gamma_1(N)$. Thus $W_N^2 \equiv \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)^2 \bmod \Gamma_1(N)$ defines the identity map on $X_1(N)$ and the relation $[a]W_N \equiv W_N[a^{-1}] \bmod \Gamma_1(N)$ is satisfied.

(2) If $1 \le N \le 4$, then ψ is the trivial covering and thus it is unramified. If $N \ge 5$, then one can show that the coset $\Gamma_0(N)W_N = \Gamma_0(N)\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ has no parabolic elements and can have elliptic elements of order 2. Therefore the fixed points of W_N on $X_0(N)$ are neither elliptic points nor cusp points. Thus ramification does not occur over those points.

(3) is straightforward.

(4) If $\psi(\tau) = \psi(\tau')$, then $\tau' = [b]\tau$ for some $b \in G$. Thus $[b]W_N[b]^{-1}\tau' = \tau'$. Now $[b]^2W_N$ turns out to be $[c]W_N$. This is a contradiction to $c \in G \setminus G^2$. ∎

COROLLARY 1.4. *With the notation of Proposition* 1.3 *and* $N \ge 5$, *let* n *denote the degree of* ψ $(= |G|)$. *Assume that* (1) n *is odd or* (2) n *is even* *and $g_0(N) \leq 1$. Then the numbers of fixed points of W_N on $X_0(N)$ and on $X_1(N)$ are the same.*

Proof. (1) Let $\tau_0 \in X_0(N)$ be a fixed point of W_N. By Proposition 1.3(2), there are n distinct points of $X_1(N)$ lying over τ_0. Since W_N permutes these points and n is odd, at least one of them must be fixed. But by Proposition 1.3(3), exactly one of them is fixed.

(2) First we consider the case $g_0(N) = 1$. The matrix $\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ always has a fixed point on the complex upper half plane $\mathcal{H}$, and hence W_N always has a fixed point on $X_0(N)$. Thus by Proposition 1.2, W_N fixes exactly four points of $X_0(N)$. The fixed points of W_N on $X_1(N)$ certainly lie over those four points. By a suitable choice of $\gamma \in \Gamma_1(N)$ we can form an elliptic element γW_N. Thus W_N has at least one fixed point on $X_1(N)$. Except $N = 24$, the order of G/G^2 is 2. Thus the number of fixed points is less than or equal to 8. Possible numbers are $4, 8, 2$ or 6. From Proposition 1.2 the latter two are impossible. By Proposition 1.3(4), 8 can also be excluded. If $N = 24$, the order of G/G^2 is 4. Thus W_N has at least four fixed points. But for each $c = 5, 7, 11$, $[c]W_N$ also has at least four fixed points. By Proposition 1.3(4), the image sets of their fixed points cannot intersect and so we are done. The case $g_0(N) = 0$ can be proved similarly. ∎

By [O1] we have the following description of cusps. The cusps of $X(N)$ can be regarded as pairs $\pm\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$, where $x, y \in \mathbb{Z}/N\mathbb{Z}$, and are relatively prime, and $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} -x \\ -y \end{smallmatrix}\right)$ are identified; $\Gamma/\Gamma(N)$ operates naturally on the left, and so a cusp of $X_0(N)$ or $X_1(N)$ can be regarded as an orbit of $\Gamma_0(N)/\Gamma(N)$ or $\Gamma_1(N)/\Gamma(N)$. For each $d \mid N$, a cusp of $X_1(N)$ is represented by a pair $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ with x reduced modulo $d = (y, N)$ and $(x, d) = 1$. If $g_1(N) > 0$, then we have $\frac{1}{2}\varphi(d)\varphi(N/d)$ cusps $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ with $d = (y, N)$ and the cusps $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ with a fixed value of $\pm y$ are conjugate, and in particular are rational only if $\varphi(d) = 1$, i.e. $d = 1$ or 2. For each $d \mid N$, a cusp of $X_0(N)$ is represented by a pair $\left(\begin{smallmatrix} x \\ d \end{smallmatrix}\right)$ with x reduced modulo $t = (d, N/d)$. We have $\varphi(t)$ conjugate cusps $\left(\begin{smallmatrix} x \\ d \end{smallmatrix}\right)$ corresponding to d, each with ramification degree $e = t$ in the Galois covering $X_1(N) \to X_0(N)$.

Let $\Gamma_1^*(N)$ be the normalizer of $\overline{\Gamma}_1(N) = \pm\Gamma_1(N)/\pm 1$ in $\mathrm{PSL}_2(\mathbb{R})$. Let $\operatorname{Aut} X_1(N)$ be the group of automorphisms of $X_1(N)$. In [K-Ko2], Kim and Koo showed that $\Gamma_1^*(N)$ is generated by $\overline{\Gamma}_0(N) = \Gamma_0(N)/\pm 1$ and the matrices W_d with $d \mid N$ and $(d, N/d) = 1$. Also Ishii and Momose [I-M] established that $\operatorname{Aut} X_1(N)$ is equal to $\Gamma_1^*(N)/\overline{\Gamma}_1(N)$ for hyperelliptic curves $X_1(N)$, i.e. $N = 13, 16, 18$. Later for square free N, Momose [M] verified that $\operatorname{Aut} X_1(N) = \Gamma_1^*(N)/\overline{\Gamma}_1(N)$. Therefore, for such N, $\operatorname{Aut} X_1(N)$ is generated by $\overline{\Gamma}_0(N)/\overline{\Gamma}_1(N)$ and the automorphisms induced by the matrices W_d.

2. Non-bielliptic curves. For the reader's convenience, in Table 1 we tabulate the genera of $X_1(N)$ for $1 \le N \le 60$ ([K-Ko1]). There is a misprint in the table of [K-Ko1, p. 297]: $g_1(18) = 3$ should be corrected to $g_1(18) = 2$.

We assume that $g_1(N) \ge 2$, i.e. $N = 13$ or $N \ge 16$. We recall that if $X_1(N)$ is a bielliptic curve, there exists an involution v, called a bielliptic involution, such that $v\backslash X_1(N)$ is an elliptic curve. If $g_1(N) \ge 6$, by Proposition 1.2 of [Sch], v is unique, defined over $\mathbb{Q}$, and lies in the center of $\operatorname{Aut} X_1(N)$. Then either v is contained in the Galois group of $X_1(N)$ over $X_0(N)$ or it induces an involution $\widetilde{v}$ on $X_0(N)$ such that $\widetilde{v}\backslash X_0(N)$ is a rational or elliptic curve. In the first case, we must of course have $g_0(N) \le 1$. Now we divide N into 3 cases.

Table 1

N	$g_1(N)$	N	$g_1(N)$	N	$g_1(N)$	N	$g_1(N)$	N	$g_1(N)$	N	$g_1(N)$
1	0	11	1	21	5	31	26	41	51	51	65
2	0	12	0	22	6	32	17	42	25	52	55
3	0	13	2	23	12	33	21	43	57	53	92
4	0	14	1	24	5	34	21	44	36	54	52
5	0	15	1	25	12	35	25	45	41	55	81
6	0	16	2	26	10	36	17	46	45	56	61
7	0	17	5	27	13	37	40	47	70	57	85
8	0	18	2	28	10	38	28	48	37	58	78
9	0	19	7	29	22	39	33	49	69	59	117
10	0	20	3	30	9	40	25	50	48	60	57

Case I: $g_1(N) > 6$ and $g_0(N) = 0$ or 1, i.e. $N = 19, 25, 27, 32, 36, 49$.
Case II: $g_1(N) > 6$ and $g_0(N) \ge 2$.
Case III: $2 \le g_1(N) \le 6$, i.e. $N = 13, 16, 17, 18, 20, 21, 22, 24$.

First we consider the six values of N which belong to Case I.

Lemma 2.1. *$X_1(19)$ is not a bielliptic curve.*

Proof. Note that $\operatorname{Aut} X_1(19)$ is generated by $\overline{\Gamma}_0(19)/\overline{\Gamma}_1(19)$ and W_{19}. First, there is no involution of type $[a]$. By Proposition 1.2 and Corollary 1.4, we have $g(W_{19}\backslash X_1(19)) = 3$. Therefore W_{19} is not a bielliptic involution. ∎

Lemma 2.2. *$X_1(27)$ is not a bielliptic curve.*

Proof. According to [Ke-M1], the only points on $X_1(27)$ that are rational or quadratic over $\mathbb{Q}$ are certain cusps. The bielliptic involution v would be defined over $\mathbb{Q}$ and hence would preserve these points. Let S_d be the set of $\Gamma_1(N)$-inequivalent cusps $\binom{x}{y}$ with $(y, N) = d$. Then S_1 (resp. S_3) consists of rational (resp. quadratic) cusps and it is not changed by v. Under an involution W_{27}, the set S_1 (resp. S_3) is mapped to S_{27} (resp. S_9). Since v commutes with W_{27}, all cusps in S_9 or S_{27} are also preserved by v. Thus v induces an automorphism of $Y_1(27)$ and so comes from an element in the normalizer of $\Gamma_1(27)$. First, there is no involution of $X_1(27)$ of type $[a]$. By Proposition 1.2 and Corollary 1.4, $g(W_{27}\backslash X_1(27)) = 6$. Thus W_{27} is not a bielliptic involution. ∎

Lemma 2.3. *$X_1(25)$ and $X_1(32)$ are not bielliptic.*

Proof. Note that [7] (resp. [15]) induces an involution on $X_1(25)$ (resp. $X_1(32)$). By Theorem 1.1, the genus of $[7]\backslash X_1(25)$ (resp. $[15]\backslash X_1(32)$) is 4 (resp. 5) and $g_1(25) = 12$ (resp. $g_1(32) = 17$). By Proposition 1.2, [7] (resp. [15]) has 10 (resp. 16) fixed points. However, if a curve of genus at least 6 has an involution with more than 8 fixed points, then by Proposition 1.2(b) of [Sch] either this involution is the bielliptic involution or the curve is not bielliptic. Now the assertion follows immediately. ∎

Lemma 2.4. *$X_1(36)$ and $X_1(49)$ are not bielliptic.*

Proof. Suppose that $X_1(36)$ is bielliptic with bielliptic involution v. From Theorem 1.1 one can check that v does not belong to the Galois group of $X_1(36)$ over $X_0(36)$. Let $\widetilde{v}$ be the involution on $X_0(36)$ induced by v. Note that $g_0(36) = 1$ and $g(\widetilde{v}\backslash X_0(36)) = 0$. By Proposition 1.2, $\widetilde{v}$ has 4 fixed points. Since the degree of the covering $X_1(36) \to X_0(36)$ is equal to 6, there are 24 fixed points of v in $X_1(36)$. But this contradicts Proposition 1.2. Thus $X_1(36)$ is not bielliptic. Similarly, $X_1(49)$ is not bielliptic, either. ∎

Now we consider Case II. The image of a bielliptic curve under a finite morphism of curves is either bielliptic, hyperelliptic, elliptic or rational (see [H-S]). Since there is a finite morphism $X_1(N) \to X_0(N)$, we have

Lemma 2.5 (Corollary 3.16 of [B]). *The modular curves $X_1(N)$ are not bielliptic for $N \geq 132$ and for all N in the table below*:

52, 57, 58, 66, 67, 68, 70, 73, 74, 76, 77, 78, 80, 82, 84, 85, 86, 87, 88, 90, 91, 93, 96, 97, 98, 99, 100, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130.

Lemma 2.6. *$X_1(N)$ is not a bielliptic curve for the following N*:

23, 29, 31, 41, 43, 47, 53, 59, 61, 65, 71, 75, 79, 83, 89, 95, 101, 119, 131.

Proof. Let N be one of the numbers of the above list. Then the curve $X_0(N)$ is either hyperelliptic or bielliptic, but not both. From the tables in [B, O2], we know that the hyperelliptic or bielliptic involution is the full Atkin–Lehner involution. Suppose that $X_1(N)$ is bielliptic and let v be the bielliptic involution. Since $g_0(N) \geq 2$, the involution v induces an involution $\widetilde{v}$ on $X_0(N)$ which is the full Atkin–Lehner involution. Then $\widetilde{v}$ maps the cusp $\binom{0}{1}$ to $\binom{1}{0}$. Thus v maps the cusps lying above $\binom{0}{1}$ to the cusps lying above $\binom{1}{0}$. Note that the cusps over $\binom{0}{1}$ are rational but the cusps over $\binom{1}{0}$ are non-rational. This is a contradiction. ∎

Lemma 2.7. *$X_1(N)$ is not a bielliptic curve for the following N*:

$$30,\ 33,\ 35,\ 38,\ 39,\ 42,\ 46,\ 51,\ 55,\ 60,\ 62,\ 69,\ 92,\ 94.$$

Proof. Let N be one of the numbers of the above list. From the tables in [B, O2], we know that any hyperelliptic or bielliptic involution on $X_0(N)$ is equal to one of the Atkin–Lehner involutions W_d with $d \neq 2$. Suppose that $X_1(N)$ is bielliptic and v is the bielliptic involution. Then v induces an involution $\widetilde{v}$ on $X_0(N)$ which is W_d with $d \neq 2$. Note that W_d is represented by a matrix $\left(\begin{smallmatrix} dx & y \\ Nz & dw \end{smallmatrix}\right)$ where $x, y, z, w \in \mathbb{Z}$ and $\det W_d = d$. We can choose $w = 1$ and $(y, d) = 1$. Then $\widetilde{v}$ maps the cusp $\binom{0}{1}$ to $\binom{y}{d}$. Since the cusps lying above $\binom{y}{d}$ are non-rational, v maps rational cusps to non-rational cusps. This gives rise to a contradiction. ∎

Lemma 2.8. *$X_1(N)$ is not a bielliptic curve for the following N*:

$$26,\ 28,\ 34,\ 40,\ 44,\ 45,\ 48,\ 50,\ 54,\ 56,\ 64,\ 72,\ 81.$$

Proof. Let N be one of the numbers of the above list. Suppose that $X_1(N)$ is a bielliptic curve with bielliptic involution v. Let $\widetilde{v}$ be the induced involution on $X_0(N)$. Since $N \neq 37, 63$, every automorphism of $X_0(N)$ is a modular automorphism (see [Ke-M2]). So for our 13 values of N, the possible candidate for $\widetilde{v}$ is also a modular automorphism. Thus v is induced from an element of $\Gamma_1^*(N)$. If v is W_d with $d \neq 2$, we are done by the same arguments as in Lemmas 2.6 and 2.7. For example, if $N = 40$, v can be one of W_5, W_8, W_{40} and so we can apply the rationality argument.

If $N = 54$, v cannot be W_2 since the genus of $W_2 \backslash X_0(56)$ is 2. For $N = 26, 34, 50$, v may happen to be W_2. In these 3 cases we can use the counting argument used in the proof of Lemma 2.4 to show that $X_1(N)$ is not bielliptic, either. ∎

Lemma 2.9. *$X_1(37)$ and $X_1(63)$ are not bielliptic curves.*

Proof. Let N be 37 or 63. Suppose that $X_1(N)$ is bielliptic and v is the bielliptic involution. Let $\widetilde{v}$ be the induced involution on $X_0(N)$.

If $N = 37$, $\operatorname{Aut} X_1(37)$ is generated by $\overline{\Gamma}_0(37)/\overline{\Gamma}_1(37)$ and W_{37} because 37 is square free. Thus the involution $\widetilde{v}$ must be a modular automorphism, and hence equal to W_{37}. By the same argument as in the proof of Lemma 2.6, this is a contradiction.

If $N = 63$, the involution $\widetilde{v}$ must be a bielliptic involution. We can deal with this case by applying the counting argument used in the proof Lemma 2.4 to show that $X_1(63)$ is not bielliptic, either. ∎

3. Bielliptic curves. In this section we will show that for all values of N in Case III, $X_1(N)$ is bielliptic.

LEMMA 3.1. *$X_1(N)$ is a bielliptic curve for $N = 13, 16, 18, 20$.*

Table 2

N	*Some bielliptic involutions*
13	$[a]\left(\begin{smallmatrix} 0 & -1 \\ 13 & 0 \end{smallmatrix}\right) \quad (a = 1, \ldots, 6)$
16	$[a]\left(\begin{smallmatrix} 0 & -1 \\ 16 & 0 \end{smallmatrix}\right) \quad (a = 1, 3, 5, 7)$
18	$[a]\left(\begin{smallmatrix} 0 & -1 \\ 18 & 0 \end{smallmatrix}\right), \quad [7a]W_2\left(\begin{smallmatrix} 0 & -1 \\ 18 & 0 \end{smallmatrix}\right) \quad (a = 1, 5, 7)$
20	$[9], \quad [a]\left(\begin{smallmatrix} 0 & -1 \\ 20 & 0 \end{smallmatrix}\right) \quad (a = 1, 3, 7, 9)$

Proof. From Proposition 1.2 and Corollary 1.4, it follows that $W_N = [a]\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ is a bielliptic involution of $X_1(N)$ for $N = 13, 16, 18, 20$.

For $N = 13, 16, 18$, the curves $X_1(13), X_1(16), X_1(18)$ have genus 2 and so they are hyperelliptic. The hyperelliptic involution u is unique and given by $[5], [7], W_2[7]$, respectively ([I-M]). Because these curves have genus 2, any other involution v must be bielliptic. But since u commutes with every automorphism, uv will be another bielliptic involution. For $N = 20$, since $g([9]\backslash X_1(20)) = g(X_\Delta(20)) = 1$ where $\Delta = \{\pm 1, \pm 9\}$, $[9]$ is also a bielliptic involution of $X_1(20)$. ∎

LEMMA 3.2. *Suppose N is even and congruent to* 2 *modulo* 4. *Then* $W_2[a] \equiv [a]W_2 \bmod \Gamma_1(N)$ *for all $a \in (\mathbb{Z}/N\mathbb{Z})^*$.*

Proof. Say

$$[a] = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad W_2 = \begin{pmatrix} 2x & y \\ Nz & 2w \end{pmatrix}.$$

By a simple calculation, the $(1,1)$-entry of $W_2^{-1}[a]^{-1}W_2[a]$ is equal to $2xw - \frac{1}{2}a^2yzN \bmod N$. Since $4xw - yzN = 2$, $2xw - \frac{1}{2}a^2yzN = 1 + \frac{1}{2}(1-a^2)yzN \equiv 1 \bmod N$. ∎

Consider the case $N = 22$. Take $W_2 = \left(\begin{smallmatrix} 8 & -3 \\ 22 & -8 \end{smallmatrix}\right)$. Then W_2 is an elliptic element and gives an involution on $X_1(22)$. Thus $W_2\tau = \tau$ for some $\tau \in \mathcal{H}$. Note that W_2 defines a bielliptic involution of $X_0(22)$. From Proposition 1.2, we know that the number of fixed points of W_2 in $X_0(22)$ is 2. Let τ_1, τ_2 be the fixed points with $\tau_1 = \tau$. Since the degree of the covering $X_1(22) \to X_0(22)$ is 5 and this covering is unramified, there are five points of $X_1(22)$ lying above τ_i $(i = 1, 2)$. For each $i = 1, 2$, the five points lying above τ_i are represented by $[d]\tau_i$ with $d \in (\mathbb{Z}/22\mathbb{Z})^*$. By the above lemma,

$$W_2[d]\tau_1 = [d]W_2\tau_1 = [d]\tau_1 \quad \text{on } X_1(22).$$

Thus W_2 fixes the five points lying above τ_1. W_2 permutes the five points lying above τ_2 so that at least one of them must be fixed. Let W_2 fix $[d]\tau_2$ for some $d \in (\mathbb{Z}/22\mathbb{Z})^*$. For each $d' \in (\mathbb{Z}/22\mathbb{Z})^*$,

$$\begin{aligned} W_2[d']\tau_2 &= W_2[d'][d]^{-1}[d]\tau_2 = [d'][d]^{-1}W_2[d]\tau_2 \\ &= [d'][d]^{-1}[d]\tau_2 = [d']\tau_2 \quad \text{on } X_1(22). \end{aligned}$$

Thus W_2 fixes exactly 10 points of $X_1(22)$. By Proposition 1.2, W_2 must be a bielliptic involution. Moreover since $g_1(22) = 6$, W_2 is a unique bielliptic involution.

LEMMA 3.3. *$X_1(22)$ is a bielliptic curve. $W_2 = \left(\begin{smallmatrix} 8 & -3 \\ 22 & -8 \end{smallmatrix}\right)$ is the only bielliptic involution.*

LEMMA 3.4. *$X_1(17)$ is a bielliptic curve.* [4] *is the only bielliptic involution.*

Proof. Only [4] is an involution of $X_1(17)$ of type $[a]$. By Theorem 1.1, $g([4]\backslash X_1(17)) = g(X_\Delta(17)) = 1$ where $\Delta = \{\pm 1, \pm 4\}$. Thus [4] is a bielliptic involution of $X_1(17)$. By [M] and [K-Ko2], other involutions must be of type W_{17}. By Proposition 1.2 and Corollary 1.4, we obtain $g(W_{17}\backslash X_1(17)) = 2$. Thus W_{17} is not a bielliptic involution. ∎

LEMMA 3.5. *$X_1(21)$ is a bielliptic curve. All the bielliptic involutions are $W_3 = \left(\begin{smallmatrix} 9 & -4 \\ 21 & -9 \end{smallmatrix}\right)$ and $[8]W_3$.*

Proof. Take $W_3 = \left(\begin{smallmatrix} 9 & -4 \\ 21 & -9 \end{smallmatrix}\right)$. Then W_3 is an elliptic element and it defines an involution on $X_1(21)$. For $a = 1, 2, 4, 5, 8, 10$, we have $[a]W_3 \equiv W_3[a] \bmod \Gamma_1(21)$. By an argument similar to the proof of Lemma 3.2, W_3 has at least six fixed points on $X_1(21)$. By Proposition 1.2, the number of fixed points of W_3 must be 8 or 12. Since $X_1(21)$ is not a hyperelliptic curve, W_3 cannot have twelve fixed points. Thus the number of fixed points of W_3 is 8 and then W_3 is a bielliptic involution. It can be easily seen that $[8]W_3$ also gives an involution on $X_1(21)$ and it is the only involution of type $[a]W_3$ with $a \neq 1$. We can choose a matrix [8] so that $[8]W_3$ is an elliptic element. Similarly $[8]W_3$ gives another bielliptic involution.

By [M] and [K-Ko2], other involutions can be of type $[a]$, W_7 or W_{21}. Write $W_7 = \left(\begin{smallmatrix} 7x & y \\ 21z & 7w \end{smallmatrix}\right)$ and assume $\frac{1}{7}W_7^2 \equiv \pm 1 \bmod \Gamma_1(21)$. Combined with the condition $\det W_7 = 7$, this leads to a contradiction. So W_7 cannot give an involution on $X_1(21)$.

By Proposition 1.2 and Corollary 1.4, the genus of $W_{21}\backslash X_1(21)$ is 2 so that the involution W_{21} cannot be a bielliptic involution.

Among the types $[a]$, only $[8]$ is an involution of $X_1(21)$. By Theorem 1.1, $g([8]\backslash X_1(21)) = 3$. Thus $[8]$ is not a bielliptic involution. ∎

Lemma 3.6. *$X_1(24)$ is a bielliptic curve. Among the modular automorphisms, $[11]$ is the only bielliptic involution.*

Proof. $[5], [7], [11]$ are all the involutions of type $[a]$. Put $\Delta_1 = \{\pm 1, \pm 5\}$, $\Delta_2 = \{\pm 1, \pm 7\}$, $\Delta_3 = \{\pm 1, \pm 11\}$. Then $g(X_{\Delta_1}(24)) = g(X_{\Delta_2}(24)) = 3$ and $g(X_{\Delta_3}(24)) = 1$. Thus $[11]$ is the only bielliptic involution among the above involutions.

Consider the involutions of types W_3, W_8, W_{24}. By Proposition 1.2 and Corollary 1.4, W_{24} cannot be a bielliptic involution. And W_3 does not give an involution on $X_1(24)$. Write $W_8 = \left(\begin{smallmatrix} 8 & -3 \\ 24 & -8 \end{smallmatrix}\right)$. Then W_8 is an elliptic element and gives an involution. For any a prime to 24, a^2 is congruent to 1 mod 24 so that $[a]W_8 \equiv W_8[a] \bmod \Gamma_1(N)$. Thus, for such a, $[a]W_8$ defines an involution on $X_1(24)$. As in the proof of Lemma 3.2, there are at least four fixed points of W_8 in $X_1(24)$. We can choose a matrix $[a]$ so that $[a]W_8$ is an elliptic element for any a prime to 24. Thus each $[a]W_8$ also has at least four fixed points in $X_1(24)$. One can show that Proposition 1.3(4) is also valid for W_8. Thus we conclude that W_8 has exactly four fixed points and so it cannot be a bielliptic involution. ∎

Summarizing the results of the last two sections, we obtain Theorem 0.1.

Remark 3.7. $X_1(N)$ is a bielliptic curve if and only if $2 \le g_1(N) \le 6$.

4. Quadratic points. Let K be a quadratic field over $\mathbb{Q}$ and E an elliptic curve defined over K. Denote by $E_{\text{tors}}(K)$ the group of K-rational torsion points of E. Then one has a complete description of $E_{\text{tors}}(K)$.

Theorem 4.1 ([Ka-Ma],[Ke-M1]). *$E_{\text{tors}}(K)$ is isomorphic to one of the following*:

(i) $\mathbb{Z}/m\mathbb{Z}$ *with* $m \le 16$, *or* $m = 18$,
(ii) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ *with* $k \le 6$,
(iii) $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3l\mathbb{Z}$ *with* $l \le 2$,
(iv) $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

As a corollary we can state the following known result:

Theorem 4.2. *The following are equivalent*:

(a) $N \le 18$, $N \ne 17$.
(b) $g_1(N) \le 2$.
(c) $X_1(N)$ *is rational*, *elliptic or hyperelliptic.*
(d) $X_1(N)$ *has infinitely many quadratic points over* $\mathbb{Q}$.

(e) *$X_1(N)$ has quadratic points over $\mathbb{Q}$ that are not cusps.*

(f) *There exist infinitely many non-isomorphic elliptic curves E with a primitive N-torsion point P such that E is defined over some quadratic number field K (depending on E and P) and P is K-rational.*

(g) *There exists at least one elliptic curve E defined over some quadratic number field K with a K-rational, primitive N-torsion point.*

Proof. (a)⇒(b)⇒(c)⇒(d)⇒(e)⇒(g) and (d)⇒(f)⇒(g) are clear, while (g)⇒(a) follows from Theorem 4.1. ∎

REMARK 4.3. (1) Without the above theorem, our classification of bielliptic curves $X_1(N)$ shows that there are only finitely many N (essentially $N < 25$) for which $X_1(N)$ can have infinitely many quadratic points over $\mathbb{Q}$.

(2) $13, 16, 18$ are the only values of N such that $X_1(N)$ is a bielliptic curve admitting infinitely many quadratic points over $\mathbb{Q}$.

(3) Since a curve X with $g(X) \geq 2$ has infinitely many quadratic points over $\mathbb{Q}$ if and only if X is a hyperelliptic curve or a bielliptic curve over $\mathbb{Q}$ mapping to an elliptic curve E with positive rank, we deduce that all elliptic curves over $\mathbb{Q}$ doubly covered by $X_1(N)$ $(N = 17, 20, 21, 22, 24)$ have rank zero.

Acknowledgments. We thank Dr. Andreas Schweizer for his kind and valuable suggestions concerning the proofs of the results of this paper.

References

[B] F. Bars, *Bielliptic modular curves*, J. Number Theory 76 (1999), 154–165.

[H-S] J. Harris and J. H. Silvermann, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc. 112 (1991), 347–356.

[I-M] N. Ishii and F. Momose, *Hyperelliptic modular curves*, Tsukuba J. Math. 15 (1991), 413–423.

[Ka-Ma] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields* (with an appendix by A. Granville), Columbia University Number Theory Seminar (New York, 1992), Astérisque 228 (1995), 3, 81–100.

[Ke-M1] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 109 (1988), 125–149.

[Ke-M2] —, —, *Automorphism groups of the modular curves $X_0(N)$*, Comp. Math. 65 (1988), 51–80.

[K] C. H. Kim, *On the genus of $X_\Delta(N)$*, preprint.

[K-Ko1] C. H. Kim and J. K. Koo, *On the genus of some modular curves of level N*, Bull. Austral. Math. Soc. 54 (1996), 291–297.

[K-Ko2] —, —, *The normalizer of $\Gamma_1(N)$ in $PSL_2(\mathbb{R})$*, Comm. Algebra 28 (2000), 5303–5310.

[M] F. Momose, *Automorphism groups of the modular curves $X_\Delta(N)$*, preprint.

[O1] A. Ogg, *Rational points on certain elliptic modular curves*, in: Proc. Sympos. Pure Math. 24, Amer. Math. Soc., 1973, 221–231.

[O2] —, *Hyperelliptic modular curves*, Bull. Soc. Math. France 102 (1974), 449–462.

[Sch] A. Schweizer, *Bielliptic Drinfeld modular curves*, Asian J. Math. 5 (2001), 705–720.

KIAS 207-43
Cheongnyangni 2-dong
Dongdaemun-gu
Seoul, 130-722 Korea
E-mail: dyjeon@kias.re.kr
chkim@kias.re.kr

Received on 21.5.2002
and in revised form on 14.2.2003 (4291)