TAIWANESE JOURNAL OF MATHEMATICS
Vol. 20, No. 6, pp. 1275–1293, December 2016
DOI: 10.11650/tjm.20.2016.6547
This paper is available online at http://journal.tms.org.tw

Notes on Weierstrass Points of Modular Curves $X_0(N)$

Bo-Hae Im, Daeyeol Jeon* and Chang Heon Kim

Abstract. We give conditions for when the fixed points by the partial Atkin-Lehner involutions on $X_0(N)$ are Weierstrass points as an extension of the result by Lehner and Newman [18]. Furthermore, we complete their result by determining whether the fixed points by the full Atkin-Lehner involutions on $X_0(N)$ are Weierstrass points or not.

1. Introduction

Let $\mathfrak{H}$ be the complex upper half plane and Γ be a congruence subgroup of the full modular group $\mathrm{SL}_2(\mathbb{Z})$. Denote by $X(\Gamma)$ the modular curve obtained by compactifying the quotient $\Gamma \setminus \mathfrak{H}$. We can view $X(\Gamma)$ as a compact Riemann surface analytically. For each positive integer N, we let $\Gamma_0(N)$ be the Hecke subgroup of $\mathrm{SL}_2(\mathbb{Z})$ defined by

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

and let $X_0(N) := X(\Gamma_0(N))$.

We recall the definitions of a Weierstrass point of a compact Riemann surface and its Weierstrass weight as in [1]. One says that a point P of a compact Riemann surface X of genus $g := g(X) \geq 2$ is *a Weierstrass point* of X if there is a holomorphic differential ω (not identically zero) with a zero of order $\geq g$ at P. If $P \in X$ and $\omega_1, \omega_2, \ldots, \omega_g$ form a basis for the holomorphic differentials on X with the property that

$$0 = \mathrm{ord}_P(\omega_1) < \mathrm{ord}_P(\omega_2) < \cdots < \mathrm{ord}_P(\omega_g),$$

Received July 8, 2015; Accepted April 29, 2016.
Communicated by Yi-Fan Yang.
2010 *Mathematics Subject Classification.* Primary: 14H55; Secondary: 11F06, 11G18.
Key words and phrases. Weierstrass points, Modular curves.
Bo-Hae Im was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2014R1A1A2053748).
Daeyeol Jeon was was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2014R1A1A2056390).
Chang Heon Kim was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2015R1D1A1A01057428).
*Corresponding author.

then *the Weierstrass weight of* P is the non-negative integer defined by

$$\mathrm{wt}(P) := \sum_{j=1}^{g} (\mathrm{ord}_P(\omega_j) - j + 1).$$

Note that $\mathrm{wt}(P) > 0$ if and only if P is a Weierstrass point of X.

The Weierstrass points of modular curves have been studied by many authors: Lehner and Newman [18] gave conditions for when the cusp at infinity is a Weierstrass point of $X_0(N)$ for $N = 4n, 9n$ and Atkin [2] gave conditions for the case of $N = p^2n$ where p is a prime ≥ 5. Also, Ogg [22], Kohnen [16, 17] and Kilger [14] gave some conditions for when the cusp at infinity is not a Weierstrass point of $X_0(N)$ for certain N. And Ono [23] and Rohrlich [24] investigated Weierstrass points of $X_0(p)$ for various primes p. Recently in [13] we investigated Weierstrass points on coverings of $X_0(N)$.

The Weierstrass points have been illustrated as an important class in number theory. For example, they are connected to supersingular j-invariants and polynomials as demonstrated, for instance, in the works of Ahlgren and Ono [1] and El-Guindy [9] on that topic.

The main purpose of this paper is to give some conditions of being the Weierstrass points of $X_0(N)$. To describe our main result in this paper more precisely, we recall the definition of the Atkin-Lehner involution. We call a positive divisor Q of N with $\gcd(Q, N/Q) = 1$ an *exact divisor* of N and denote it by $Q \parallel N$. For each $Q \parallel N$, consider the matrices of the form $\begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix}$ with $x, y, z, w \in \mathbb{Z}$ and determinant Q. Then such a matrix defines a unique involution on $X_0(N)$ which is called the *Atkin-Lehner involution* and denoted by W_Q. If $Q = N$, then W_Q is called the *full Atkin-Lehner involution*, and otherwise it is said to be a *partial Atkin-Lehner involution*. Sometimes we regard W_Q as a matrix.

Lehner and Newman [18] have shown that the fixed points by the full Atkin-Lehner involution on $X_0(N)$ are Weierstrass points except possibly for finitely many N which are listed in Lemma 3.3. In order to obtain the result, they have applied Schöneberg's Theorem [25, Satz 1]. Our main result in this paper is to determine explicitly when the fixed points by the partial Atkin-Lehner involutions on $X_0(N)$ are Weierstrass points as an extension of the result by Lehner and Newman [18]. Also in this paper we give an algorithm to generate $\Gamma_0(N)$-inequivalent fixed points by the full Atkin-Lehner involution and we provide a computational method which can take care of the exceptional cases listed in Lemma 3.3 which are not covered by Lehner and Newman [18].

This paper is organized as follows. In Section 2, we recall the formula [10, Remark 2] for the number of fixed points on $X_0(N)$ by the Atkin-Lehner involutions and explain algorithmically how to generate $\Gamma_0(N)$-inequivalent fixed points of $X_0(N)$ by the full Atkin-Lehner involution W_N. In Section 3, we give conditions for when fixed points by

the Atkin-Lehner involutions are Weierstrass points. We apply the formula [10, Remark 2] of the number of fixed points on $X_0(N)$ by the Atkin-Lehner involutions and Schöneberg's Theorem [25, Satz 1], and we give some new formulae for the number of fixed points when the so-called *elliptic condition* (Definition 3.9) is satisfied and apply them to obtain the conditions for Weierstrass points. In Section 4, we consider the exceptional cases which are not determined solely by Schöneberg's Theorem [25, Satz 1] and the formula given in [10, Remark 2], and we give a computational explanation of how to determine whether they are Weierstrass points or not.

2. Fixed points by Atkin-Lehner involutions

Let $X_0^{+Q}(N)$ be the quotient space of $X_0(N)$ by W_Q. Let $g_0(N)$ and $g_0^{+Q}(N)$ be the genera of $X_0(N)$ and $X_0^{+Q}(N)$ respectively. Then $g_0^{+Q}(N)$ is computed by the Riemann-Hurwitz formula as follows:

$$g_0^{+Q}(N) = \frac{1}{4}(2g_0(N) + 2 - \nu(Q)),$$

where $\nu(Q) := \nu(Q; N)$ is the number of fixed points on $X_0(N)$ by W_Q. We recall the formula for $\nu(Q)$.

Proposition 2.1. [10, Remark 2] *For each $Q \parallel N$, $\nu(Q)$ is given by*

$$\begin{aligned}
\nu(Q) = &\left(\prod_{p|N/Q} c_1(p)\right) h(-4Q) \\
&+ \begin{cases} \left(\prod_{p|N/Q} c_2(p)\right) h(-Q), & \text{if } 4 \le Q \equiv 3 \pmod 4, \\ 0, & \text{otherwise} \end{cases} \\
&+ \begin{cases} \prod_{p|N/2} \left(1 + \left(\frac{-4}{p}\right)\right), & \text{if } Q = 2, \\ 0, & \text{otherwise} \end{cases} \\
&+ \begin{cases} \prod_{p|N/3} \left(1 + \left(\frac{-3}{p}\right)\right), & \text{if } Q = 3, \\ 0, & \text{otherwise} \end{cases} \\
&+ \begin{cases} \prod_{p^k|N/Q} \left(p^{[\frac{k}{2}]} + p^{[\frac{k-1}{2}]}\right), & \text{if } Q = 4, \\ 0, & \text{otherwise} \end{cases}
\end{aligned} \tag{2.1}$$

where $h(-d)$ is the class number of primitive quadratic forms of discriminant $-d$, $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol and the functions $c_i(p)$ are defined as follows: for $i = 1, 2$,

$$c_i(p) = \begin{cases} 1 + \left(\frac{-Q}{p}\right), & \text{if } p \neq 2 \text{ and } Q \equiv 3 \pmod 4, \\ 1 + \left(\frac{-4Q}{p}\right), & \text{if } p \neq 2 \text{ and } Q \not\equiv 3 \pmod 4, \end{cases}$$

$$c_1(2) = \begin{cases} 1, & \text{if } Q \equiv 1 \pmod 4 \text{ and } 2 \parallel N, \\ 0, & \text{if } Q \equiv 1 \pmod 4 \text{ and } 4 \mid N, \\ 2, & \text{if } Q \equiv 3 \pmod 4 \text{ and } 2 \parallel N, \\ 3 + \left(\frac{-Q}{2}\right), & \text{if } Q \equiv 3 \pmod 4 \text{ and } 4 \parallel N, \\ 3\left(1 + \left(\frac{-Q}{2}\right)\right), & \text{if } Q \equiv 3 \pmod 4 \text{ and } 8 \mid N, \end{cases}$$

$$c_2(2) = 1 + \left(\frac{-Q}{2}\right), \quad \text{if } Q \equiv 3 \pmod 4.$$

Next we give an algorithm to find $\Gamma_0(N)$-inequivalent fixed points of W_N on $X_0(N)$.

For a positive integer d congruent to 0 or 3 modulo 4, we denote by $\mathcal{Q}_d$ the set of positive definite integral binary quadratic forms

$$Q(x, y) = [a, b, c] := ax^2 + bxy + cy^2$$

with discriminant $-d = b^2 - 4ac$. Then $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{Q}_d$ by

$$Q \circ \gamma(x, y) = Q(px + qy, rx + sy)$$

where $\gamma = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. We say that a quadratic form $[a, b, c] \in \mathcal{Q}_d$ is *primitive* if $\gcd(a, b, c) = 1$. A primitive positive definite form $[a, b, c]$ is said to be *reduced* if

$$|b| \le a \le c, \quad \text{and} \quad b \ge 0 \quad \text{if either } |b| = a \text{ or } a = c. \tag{2.2}$$

Let $\mathcal{Q}_d^\circ \subset \mathcal{Q}_d$ be the subset of primitive forms. Then $\mathrm{SL}_2(\mathbb{Z})$ also acts on $\mathcal{Q}_d^\circ$. As is well known, there is a one-to-one correspondence between the set of classes $\mathcal{Q}_d^\circ/\mathrm{SL}_2(\mathbb{Z})$ and the set of reduced forms.

Now for a fixed positive integer N we let d be a positive integer such that $-d$ is congruent to a square modulo $4N$. We choose an integer β with $-d \equiv \beta^2 \pmod{4N}$. Then we define

$$\mathcal{Q}_{d,N}^\circ = \{[aN, b, c] \in \mathcal{Q}_d \mid \gcd(a, b, c) = 1\}$$

and

$$\mathcal{Q}_{d,N,\beta}^\circ = \left\{[aN, b, c] \in \mathcal{Q}_{d,N}^\circ \mid b \equiv \beta \pmod{2N}\right\}.$$

Then $\Gamma_0(N)$ acts on both $\mathcal{Q}_{d,N}^\circ$ and $\mathcal{Q}_{d,N,\beta}^\circ$. For $Q = [aN, b, c] \in \mathcal{Q}_{d,N}^\circ$, we define $Q|W_N = [cN, -b, a]$. We observe that this defines an action of W_N on the set $\mathcal{Q}_{d,N}^\circ/\Gamma_0(N)$.

Assume that $N \ge 5$ and W_N fixes $\Gamma_0(N)\tau \in X_0(N)$ for some $\tau \in \mathfrak{H}$. This means that $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) W_N\tau = \tau$ for some $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \Gamma_0(N)$. Thus τ satisfies a quadratic equation

$$NsX^2 - (r + qN)X + p = 0,$$

whose discriminant D is given by $D=(r+qN)^2-4psN=(r'-q)^2N^2-4N$ where $r=r'N$. Since $D\le 0$, we come up with $(r'-q)^2N\le 4$. Since we have assumed that $N\ge 5$, we must have $r'-q=0$ and therefore $D=-4N$. Thus one has $D=4q^2N^2-4psN=-4N$, which gives $\gcd(p,qN)=1$ and hence $\gcd(s,-2qN,p)=1$ or 2. If $\gcd(s,-2qN,p)=2$, then both p and s should be even. It then follows from $ps-q^2N=1$ that $N\equiv 3 \pmod 4$. Now we set $Q_\tau:=[sN,-2qN,p]$. Then we see that

$$Q_\tau\in\mathcal{Q}^\circ_{4N,N,0}\quad\text{or}\quad\frac{1}{2}Q_\tau\in\mathcal{Q}^\circ_{N,N,N}$$

where the latter case may happen only if $N\equiv 3 \pmod 4$. Let $\mathcal{F}_N$ be the set of the fixed points of W_N on $X_0(N)$ and let

$$\mathcal{G}_N:=\begin{cases}\mathcal{Q}^\circ_{4N,N,0}/\Gamma_0(N)\cup\mathcal{Q}^\circ_{N,N,N}/\Gamma_0(N), & \text{if } N\equiv 3 \pmod 4,\\ \mathcal{Q}^\circ_{4N,N,0}/\Gamma_0(N), & \text{otherwise,}\end{cases}$$

where the union is disjoint. Now we define a map $\phi\colon\mathcal{F}_N\to\mathcal{G}_N$ by

$$\phi(\Gamma_0(N)\tau)=\begin{cases}Q_\tau, & \text{if } (s,-2qN,p)=1,\\ \frac{1}{2}Q_\tau, & \text{if } (s,-2qN,p)=2.\end{cases}$$

Then we can easily check that ϕ is well-defined.

On the other hand, given a quadratic form $Q\in\mathcal{Q}^\circ_{4N,N,0}/\Gamma_0(N)$ or $Q\in\mathcal{Q}^\circ_{N,N,N}/\Gamma_0(N)$ we can find a fixed point $\Gamma_0(N)\tau\in X_0(N)$ such that $Q=\phi(\Gamma_0(N)\tau)$. Thus the map ϕ is surjective.

Now we deduce from [11, Proposition in p. 505] that the natural maps

$$\begin{aligned}&\mathcal{Q}^\circ_{4N,N,0}/\Gamma_0(N)\to\mathcal{Q}^\circ_{4N}/\operatorname{SL}_2(\mathbb{Z}),\\ &\mathcal{Q}^\circ_{N,N,N}/\Gamma_0(N)\to\mathcal{Q}^\circ_{N}/\operatorname{SL}_2(\mathbb{Z})\quad(\text{when } N\equiv 3 \pmod 4)\end{aligned}\tag{2.3}$$

are well-defined and bijective.

From [10], we have the following formula for the number of fixed points of W_N on $X_0(N)$:

$$\nu(N)=\#\mathcal{F}_N=\delta_N h(-4N),$$

where $h(-4N)$ denotes $\#\mathcal{Q}^\circ_{4N}/\operatorname{SL}_2(\mathbb{Z})$ and

$$\delta_N=\begin{cases}2, & \text{if } N\equiv 7 \pmod 8,\\ \frac{4}{3}, & \text{if } N\equiv 3 \pmod 8 \text{ and } N>3,\\ 1, & \text{otherwise.}\end{cases}$$

Since it is well-known that

$$h(-4N)=\begin{cases}h(-N), & \text{if } N\equiv 7 \pmod 8,\\ 3h(-N), & \text{if } N\equiv 3 \pmod 8 \text{ and } N>3,\end{cases}\tag{2.4}$$

we have $\#\mathcal{F}_N = \#\mathcal{G}_N$, and hence ϕ is a bijection.

Now we will find $\Gamma_0(N)$-inequivalent fixed points in $\mathcal{F}_N$ by finding $\Gamma_0(N)$-inequivalent quadratic forms in $\mathcal{G}_N$ which can be obtained by pulling back the reduced forms in $\mathcal{Q}_{4N}^{\circ}/\operatorname{SL}_2(\mathbb{Z})$ and $\mathcal{Q}_N^{\circ}/\operatorname{SL}_2(\mathbb{Z})$ through the maps (2.3). Before providing an algorithm, we need the following lemma.

Lemma 2.2. *For a fixed positive integer N we let d be a positive integer such that $-d$ is congruent to a square modulo $4N$. We choose an integer β with $-d \equiv \beta^2 \pmod{4N}$. Then the following statements are true.*

(1) *Given a primitive quadratic form $Q \in \mathcal{Q}_d^{\circ}$ there exists a quadratic form $[a,b,c]$ which is $\operatorname{SL}_2(\mathbb{Z})$-equivalent with Q and $\gcd(a,N)=1$.*

(2) *Let K be a solution to the linear congruence equation $2aX+b \equiv -\beta \pmod{2N}$ and set $[A,B,C] := [a,b,c] \circ \left(\begin{smallmatrix} K & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Then $[A,B,C]$ belongs to $\mathcal{Q}_{d,N,\beta}$.*

Proof. (1) follows from [7, Lemma 2.3 and Lemma 2.25].

(2) First we note that b and β have the same parity since $-d = b^2 - 4ac$ and $-d \equiv \beta^2 \pmod{4N}$. Thus we obtain that $2 = \gcd(2a, 2N) \mid (-\beta - b)$, which guarantees that the linear congruence $2aX + b \equiv -\beta \pmod{2N}$ is solvable. Since $B = -2aK - b \equiv \beta \pmod{2N}$ and $C = a$, we must have

$$-4Aa = -4AC = -d - B^2 \equiv \beta^2 - B^2 \equiv 0 \pmod{4N},$$

which yields that $N \mid A$ since $\gcd(a,N) = 1$. Hence one has $[A,B,C] \in \mathcal{Q}_{d,N,\beta}$, as desired. □

Now we summarize the procedures explained in the above as the following algorithm.

Algorithm 2.3. *The following steps implement an algorithm to find $\Gamma_0(N)$-inequivalent fixed points of W_N:*

Step 1. *Set $(d,\beta) = (4N, 0)$ or $(d,\beta) = (N,N)$ (when $N \equiv 3 \pmod 4$).*

Step 2. *Starting from a reduced form Q^{red} satisfying (2.2) we first find a quadratic form $[a,b,c]$ which is $\operatorname{SL}_2(\mathbb{Z})$-equivalent with Q^{red} and $\gcd(a,N)=1$.*

Step 3. *Set $[A,B,C] := [a,b,c] \circ \left(\begin{smallmatrix} K & -1 \\ 1 & 0 \end{smallmatrix}\right)$ where K is a solution to the linear congruence equation $2aX+b \equiv -\beta \pmod{2N}$. Then $[A,B,C]$ belongs to $\mathcal{Q}_{d,N,\beta}$.*

Step 4. *Let $\tau = \frac{-B+\sqrt{-d}}{2A}$. Then $\Gamma_0(N)\tau$ gives a fixed point of W_N.*

3. Weierstrass point on $X_0(N)$ arising from the fixed points of Atkin-Lehner involutions

First, we recall Schöneberg's Theorem [25, Satz 1] as follows.

Theorem 3.1. [25] *Let g be the genus of the modular curve $X(\Gamma)$ of a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ and let M be an element of the normalizer of Γ in $\mathrm{SL}_2(\mathbb{R})$ and p be the exponent of M modulo Γ. Let g^* be the genus of the quotient space $X(\Gamma)/\langle M\rangle$ by the subgroup $\langle M\rangle$ generated by M modulo Γ. Then τ is a Weierstrass point on $X(\Gamma)$ provided that*

$$g^* \neq \lfloor g/p \rfloor.$$

($\lfloor x \rfloor$ denotes the largest integer not greater than x.)

By using the formula in Proposition 2.1 and Schöneberg's Theorem [25, Satz 1], we have the following:

Lemma 3.2. *Let τ be a fixed point of W_Q on $X_0(N)$ with $g_0(N) > 1$. If $\nu(Q) > 4$, then τ is a Weierstrass point of $X_0(N)$.*

Proof. By Theorem 3.1, τ is a Weierstrass point of $X_0(N)$ if

$$g_0(N) - 2g_0^{+Q}(N) > 1$$

which is equivalent to that $\nu(Q) > 4$. □

Note that $\nu(N) = \delta_N h(-4N)$ and there exist only finitely many N such that $h(-4N) \leq 4$. By using these facts, Lehner and Newman [18] have shown that the fixed points of W_N are Weierstrass points on $X_0(N)$ except possibly for finitely many N. However they didn't specify such possible N's, and hence we list them in Lemma 3.3. By Proposition 3.11 which we will prove later, we have the following:

Lemma 3.3. *The fixed points of W_N are Weierstrass points on $X_0(N)$ with $g_0(N) > 1$ except possibly for the following values for N:*

> 22, 28, 30, 33, 34, 37, 40, 42, 43, 45, 46, 48, 52, 57, 58, 60, 64, 67, 70, 72, 73, 78, 82, 85, 88, 93, 97, 100, 102, 112, 130, 133, 142, 148, 163, 177, 190, 193, 232, 253.

All of the forty possible exceptions in Lemma 3.3 turn out to be true exceptions (see Section 4).

From now on, if $Q \parallel N$ and $N = QM$, we always assume $M > 1$. By Proposition 2.1 and Lemma 3.2 we have the following results.

Lemma 3.4. *Let $2 \parallel N$ and $N = 2M$. Then we have the following.*

(1) $\nu(2) = 0$ *if and only if M has a prime factor p with $p \equiv 7 \pmod 8$ or prime factors q, r with $q \equiv 3 \pmod 8$ and $r \equiv 5 \pmod 8$.*

(2) *If $\nu(2) \neq 0$, then*

$$\nu(2) = \delta_{0,s_2} 2^{s_0+s_1} + \delta_{0,s_1} 2^{s_0+s_2},$$

where s_0, s_1 and s_2 are the numbers of prime factors p of M with $p \equiv 1 \pmod 8$, $p \equiv 3 \pmod 8$ and $p \equiv 5 \pmod 8$ respectively, and $\delta_{i,j}$ is the Kronecker delta function.

Proof. Since $h(-8) = 1$,

$$\nu(2) = \prod_{p|M} \left(1 + \left(\frac{-8}{p}\right)\right) + \prod_{p|M} \left(1 + \left(\frac{-4}{p}\right)\right).$$

Since

$$\left(\frac{-8}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 3 \pmod 8, \\ -1, & \text{if } p \equiv 5, 7 \pmod 8, \end{cases}$$

and

$$\left(\frac{-4}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

our result follows. □

Lemma 3.5. *Let $3 \parallel N$ and $N = 3M$. Then we have the following.*

(1) $\nu(3) = 0$ *if and only if $8 \mid M$ or M has a prime factor p with $p \equiv 5$ or $11 \pmod{12}$.*

(2) *If $\nu(3) \neq 0$, then*

$$\nu(3) = 2^{s+1},$$

where s is the number of prime factors p of M with $p \equiv 1$ or $7 \pmod{12}$.

Proof. If $8 \mid M$, then $\nu(3) = 0$ because $\left(\frac{-3}{2}\right) = -1$. Suppose $8 \nmid M$. Since $h(-12) = 1$,

$$\nu(3) = \prod_{p|M} \left(1 + (-1)^{p-1}\left(\frac{-3}{p}\right)\right) + \prod_{p|M} \left(1 + \left(\frac{-3}{p}\right)\right).$$

Since

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 7 \pmod{12}, \\ -1, & \text{if } p \equiv 5, 11 \pmod{12} \end{cases}$$

for an odd prime p, the condition of $\nu(3) > 0$ follows. If $\nu(3) > 0$, then

$$\nu(3) = 2 \prod_{p|M} \left(1 + \left(\frac{-3}{p}\right)\right) = 2^{s+1}.$$

□

Lemma 3.6. *Let $4 \parallel N$ and $N = 4M$. Then W_4 has always a fixed point on $X_0(N)$. Let s and t denote the numbers of prime factors p of M with $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$ respectively. Then we have the following:*

$$\nu(4) = \begin{cases} \prod_{p^k \| M} \left(p^{\left[\frac{k}{2}\right]} + p^{\left[\frac{k-1}{2}\right]} \right), & \text{if } t > 0, \\ \prod_{p^k \| M} \left(p^{\left[\frac{k}{2}\right]} + p^{\left[\frac{k-1}{2}\right]} \right) + 2^s, & \text{if } t = 0. \end{cases}$$

Proof. It follows directly from Proposition 2.1. □

By using Lemmas 3.4, 3.5 and 3.6, we have the following result:

Theorem 3.7. *Let $Q \parallel N$ and $N = QM$. Suppose $\nu(Q) > 0$. Then the fixed points of W_Q are Weierstrass points of $X_0(N)$ for each of the followings:*

(1) *$Q = 2$; $s_0 > 1$ and $s_1 = s_2 = 0$, $s_0 + s_1 > 2$ or $s_0 + s_2 > 2$ where s_0, s_1 and s_2 are the numbers of prime factors p, q and r of M with $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$ and $r \equiv 5 \pmod 8$ respectively.*

(2) *$Q = 3$; $s > 1$ where s is the number of prime factors p of M with $p \equiv 1, 7 \pmod{12}$.*

(3) *$Q = 4$; M is not a square-free integer with $M \neq 9$ or M is square-free and $6s + 4t > 11$ where s and t are the numbers of prime factors p and q of M with $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ respectively.*

Proof. (1) and (2) follow immediately from Lemmas 3.4 and 3.5.

For (3), if M is not a square-free integer with $M \neq 9$, then one can check easily that $\nu(4) > 4$ by Lemma 3.6. If M is square-free, then by Lemma 3.6

$$\nu(4) = \begin{cases} 2^{s+t}, & \text{if } t > 0, \\ 2^{s+1}, & \text{if } t = 0. \end{cases}$$

One can check easily that $\nu(4) > 4$ if and only if $6s + 4t > 11$. □

Now we deal with the case when $Q > 4$. For that we need the following result.

Proposition 3.8. *Let $Q \parallel N$ and $N = QM$. If $Q > 3$, then the following statements are equivalent.*

(1) *W_Q has a fixed point on $X_0(N)$.*

(2) *W_Q can be defined by a matrix of the form $\begin{pmatrix} Qx & y \\ Nz & -Qx \end{pmatrix}$ with $\det(W_Q) = Q$.*

(3) *$X^2 \equiv -Q \pmod N$ has a solution.*

(4) $\left(\frac{-Q}{p}\right) = 1$ *for any odd prime* $p \mid M$, *and* $Q \equiv 3 \pmod 4$ *if* $4 \parallel M$ *and* $Q \equiv 7 \pmod 8$ *if* $8 \mid M$.

Proof. (1)⇒(2): Suppose $W_Q = \begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix}$ with $\det(W_Q) = Q$ and W_Q has a fixed point on $X_0(N)$. Then there exists $\tau \in \mathfrak{H}$ such that $W_Q\tau = \gamma\tau$ for some $\gamma \in \Gamma_0(N)$. Since $\gamma^{-1}W_Q$ defines the same partial Atkin-Lehner involution, one may assume that $W_Q\tau = \tau$ by changing coefficients x, y, z, w of W_Q. Then the matrix W_Q is elliptic, and hence $|x + w|\sqrt{Q} < 2$. Since $Q > 3$, $x + w = 0$ and the result follows.

(2)⇒(3): Suppose $W_Q = \begin{pmatrix} Qx & y \\ Nz & -Qx \end{pmatrix}$ with $\det(W_Q) = Q$. Then $\det(W_Q) = -(Qx)^2 - Nyz = Q$, and hence Qx is a solution of $X^2 \equiv -Q \pmod N$.

(3)⇒(2): Suppose $X^2 \equiv -Q \pmod N$ has a solution, say x_0. Since $\gcd(Q, M) = 1$, one can choose Q' so that $QQ' \equiv 1 \pmod M$. Then $QQ'x_0$ is a solution of $X^2 \equiv -Q \pmod N$ which is divisible by Q. Letting $x = Q'x_0$, $(Qx)^2 = -Q - Nyz$ for some y, z, and hence the matrix $\begin{pmatrix} Qx & y \\ Nz & -Qx \end{pmatrix}$ has $\det(W_Q) = Q$.

(2)⇒(1): Since $W_Q = \begin{pmatrix} Qx & y \\ Nz & -Qx \end{pmatrix}$ with $\det(W_Q) = Q$ is elliptic, it has a fixed point in $\mathfrak{H}$, and hence has one on $X_0(N)$.

(3)⇔(4): It follows from [6, Theorem 9.13]. □

Definition 3.9. For $Q \parallel N$, if one of the equivalent statements of Proposition 3.8 is satisfied, then we call that $(N; Q)$ satisfies the *elliptic condition*.

From Propositions 2.1 and 3.8, we have the following:

Lemma 3.10. *Let* $Q \parallel N$ *and* $N = QM$. *Suppose* $Q > 4$ *and* $(N; Q)$ *satisfies the elliptic condition. Then the following holds: Let* s *be the number of prime divisors of* M *and*

$$\alpha_N = \begin{cases} 1, & \text{if } 2 \nmid N \text{ or } 2 \parallel N, \\ 2, & \text{if } 4 \parallel N, \\ 3, & \text{if } 8 \mid N. \end{cases}$$

(1) *If* $Q \equiv 7 \pmod 8$ *or* $Q \equiv 3 \pmod 8$ *and* N *is odd, then*

$$\nu(Q) = 2^s(\alpha_N h(-4Q) + h(-Q)).$$

(2) *If* $Q \equiv 1 \pmod 4$ *and* N *is even, then*

$$\nu(Q) = 2^{s-1}h(-4Q).$$

(3) *If* Q *is even, or* $Q \equiv 3 \pmod 8$ *and* N *is even, or* $Q \equiv 1 \pmod 4$ *and* N *is odd, then*

$$\nu(Q) = 2^s h(-4Q).$$

Proof. If Q is even, then M is odd, and hence $c_1(p) = 2$ for all $p \mid M$. Thus $\nu(Q) = 2^s h(-4Q)$. This equality holds for the cases of $Q \equiv 1 \pmod 4$ and N is odd because M is odd. If $Q \equiv 1 \pmod 4$ and N is even, then M is even and $c_1(2) = 1$. Thus $\nu(Q) = 2^{s-1} h(-4Q)$. Consider the case $Q \equiv 3 \pmod 4$. If N is odd, then so is M, and $c_1(p) = c_2(p) = 2$ for all $p \mid M$. Thus $\nu(Q) = 2^s(h(-4Q) + h(-Q))$. If $Q \equiv 7 \pmod 8$ and N is even, then M is even, and $c_1(2) = 2\alpha_N$, $c_2(2) = c_i(p) = 2$ for all odd prime $p \mid M$ and $i = 1, 2$. Thus $\nu(Q) = 2^s(\alpha_N h(-4Q) + h(-Q))$. If $Q \equiv 3 \pmod 8$ and N is even, then M is even, and $c_2(2) = 0$, $c_1(p) = 2$ for all $p \mid M$. Thus $\nu(Q) = 2^s h(-4Q)$. □

For getting the condition that $\nu(Q) > 4$, we need to determine the values for Q with small $h(-Q)$ and $h(-4Q)$. Recall that if d_K is the (fundamental) discriminant of an imaginary quadratic field K, then $h(d_K)$ is equal to the class number of K, i.e., $h(d_K) = h(\mathcal{O}_K)$ where $\mathcal{O}_K$ is the ring of integers of K and $h(\mathcal{O}_K)$ is the order of the ideal class group of $\mathcal{O}_K$. On the other hand, if $d = f^2 d_K$ is the discriminant of a primitive quadratic form with $f > 1$, then $h(d) = h(\mathcal{O})$ where $\mathcal{O}$ is the order of conductor f in K (cf. [7]). Note that d is a fundamental discriminant if and only if one of the following statements holds:

- $d \equiv 1 \pmod 4$ and d is square-free,
- $d = 4m$ where $m \equiv 2$ or $3 \pmod 4$ and m is square-free.

The complete list of fundamental discriminants of class number 1 is as follows:

$$-3, -4, -7, -8, -11, -19, -43, -67, -163. \tag{3.1}$$

This is accomplished independently by Heegner [12], Baker [3] and Stark [26]. The non-fundamental discriminants of class number 1 are as follows:

$$-12, -16, -27, -28. \tag{3.2}$$

Thus $h(-Q) = 1$ if and only if $Q \in S_1$, where

$$S_1 = \{3, 4, 7, 8, 11, 12, 16, 19, 27, 28, 43, 67, 163\}.$$

The determination of fundamental discriminants of class number 2 was done again by Baker [4] and Stark [27].

Now consider the condition that $\nu(Q) > 4$. Due to (2.4) and Lemma 3.10, it suffices to determine the values for Q such that $h(-Q) = 1$ and $h(-4Q) = 2, 3, 4$. For the purpose, we refer to a paper by Klaise [15] in which all the orders of class number 2 and 3 are

determined and an algorithm to find all orders of class number up to 100 is suggested. Let

$$\begin{aligned}
S_2 &= \{5, 6, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 37, 58\}, \\
S_3 &= \{11, 19, 23, 27, 31, 43, 67, 163\}, \\
S_4 &= \{14, 17, 20, 21, 24, 30, 32, 33, 34, 36, 39, 40, 42, 45, 46, 48, 49, \\
&\qquad 52, 55, 57, 60, 63, 64, 70, 72, 73, 78, 82, 85, 88, 93, 97, 100, 102, \\
&\qquad 112, 130, 133, 142, 148, 177, 190, 193, 232, 253\}.
\end{aligned}$$

By using the result in [15] and some computations of the orders of class number 4 we have the following:

Proposition 3.11. *The list of Q with $h(-4Q) = 2, 3, 4$ is completely determined as follows:*

$$h(-4Q) = i \quad \text{if and only if} \quad Q \in S_i \text{ for } i = 2, 3, 4.$$

By Proposition 3.11, we have the following result:

Theorem 3.12. *Let $Q \parallel N$ and $N = QM$. Suppose that $Q > 4$ and (N, Q) satisfies the elliptic condition. Let s denote the number of prime divisors of M.*

(1) *When $Q \equiv 7 \pmod 8$ or $Q \equiv 3 \pmod 8$ and N is odd,*

   (a) *if $Q \neq 7$, then all the fixed points of W_Q on $X_0(N)$ are Weierstrass points, and*

   (b) *if $Q = 7$ and $4 \mid N$ or $s > 1$, then all the fixed points of W_7 on $X_0(N)$ are Weierstrass points.*

(2) *When $Q \equiv 1 \pmod 4$ and N is even,*

   (a) *if $Q \notin S_2 \cup S_4$, then all the fixed points of W_Q on $X_0(N)$ are Weierstrass points, and*

   (b) *if $Q \in S_2$ and $s > 2$ or $Q \in S_4$ and $s > 1$, then all the fixed points of W_Q on $X_0(N)$ are Weierstrass points.*

(3) *In other cases,*

   (a) *if $Q \notin S_2$, then all the fixed points of W_Q on $X_0(N)$ are Weierstrass points, and*

   (b) *if $Q \in S_2$ and $s > 1$, then all the fixed points of W_Q on $X_0(N)$ are Weierstrass points.*

Proof. (1) From Lemma 3.10, we need to consider Q such that $h(-4Q)+h(-Q)=2$. By Proposition 3.11, one can check that the only $Q=7$ such that $h(-4Q)+h(-Q)=2$. In the case of $Q=7$, if $4 \mid N$ or $s>1$, then $\nu(7)>4$, and hence the result follows.

(2) From Lemma 3.10, we need to consider Q such that $h(-4Q) \leq 4$. By Proposition 3.11, one can check that there doesn't exist $Q \equiv 1 \pmod 4$ such that $h(-4Q)=1,3$, and hence the result follows.

(3) From Lemma 3.10, we need to consider Q such that $h(-4Q) \leq 2$. However by Proposition 3.11 one can check that there doesn't exist such a Q so that $h(-4Q)=1$ in these cases. Therefore the result follows. □

4. Computations for the exceptional cases

In this section, we completely determine when the fixed points of the full Atkin-Lehner involution W_N are Weierstrass points on $X_0(N)$ including the exceptional cases listed in Lemma 3.3. From now on, we always assume that N is one of those integer values. Let $\tau \in \mathfrak{H}^* := \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ and $[\tau] := \Gamma_0(N)\tau \in X_0(N)$. Let $\{f_1, f_2, \ldots, f_g\}$ be a basis of the cuspform space $S_2(N)$ of weight 2 on $\Gamma_0(N)$, where g is the genus of $X_0(N)$. Then the differentials $\omega_i := f_i\, dz$ form a basis for the holomorphic differentials on $X_0(N)$. Then the order $\mathrm{ord}_{[\tau]}(\omega_i)$ has certain relation with $\mathrm{ord}_{[\tau]}(f_i)$ depending on the types of $[\tau]$ (see [20]). In particular, $[\tau]$ is an ordinary point, i.e., it is non-cuspidal and non-elliptic, then $\mathrm{ord}_{[\tau]}(\omega_i) = \mathrm{ord}_{[\tau]}(f_i)$. We will compute the Weierstrass weight of $[\tau]$ by using the f_i. In general, it is very difficult to construct f_i explicitly, and hence we will use the Fourier expansions at the infinite cusp ∞ of the f_i which can be easily computed by using the computer algebra system Sage [28].

Following the work of Rohrlich [24] as summarized on [23, p. 113], we have the following result:

Lemma 4.1. *Let $[\tau]$ be a point of $X_0(N)$, and let $\{f_1, f_2, \ldots, f_g\}$ be a basis of the cusp form space $S_2(N)$ of weight 2 on $\Gamma_0(N)$. Then $[\tau]$ is a Weierstrass point of $X_0(N)$ if and only if the vanishing order of $W_N(f_1, \ldots, f_g)(dz)^{g(g+1)/2}$ at $[\tau]$ is nonzero, where*

$$W_N(f_1, \ldots, f_g) = \begin{vmatrix} f_1 & f_2 & \cdots & f_g \\ f_1' & f_2' & \cdots & f_g' \\ \cdots & \cdots & \cdots & \cdots \\ f_1^{(g-1)} & f_2^{(g-1)} & \cdots & f_g^{(g-1)} \end{vmatrix}$$

is the Wronskian of $f_1, f_2, \ldots, f_g$. In particular, if $[\tau]$ is an ordinary point, then it is a Weierstrass point if and only if $W_N(f_1, \ldots, f_g)(\tau) = 0$.

Now we estimate the value $f_i^{(j-1)}(\tau)$ using the Fourier expansion of $f_i = \sum_{n=1}^{\infty} a_i(n)q^n$ at ∞ where $z \in \mathfrak{H}$ and $q = e^{2\pi iz}$. Note that

$$f_i^{(j-1)}(\tau) = \sum_{n=1}^{\infty} (2\pi in)^{j-1} a_i(n) q^n \Big|_{z=\tau}. \tag{4.1}$$

Since $\left|e^{2\pi i\tau}\right| = e^{-2\pi \operatorname{Im}(\tau)}$, we need to find $\tau' \in [\tau]$ whose imaginary part is as big as possible for the fast convergence of the right side of (4.1). We will consider an algorithm to find $\tau' \in [\tau]$ so that $\operatorname{Im}(\tau')$ is the biggest. Note that $\operatorname{Im}(\alpha(\tau)) = \frac{\operatorname{Im}(\tau)}{|c\tau+d|}$ for $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Thus it suffices to find a pair (c, d) with $c \equiv 0 \pmod{N}$ and $\gcd(c, d) = 1$ so that $|c\tau + d|$ is the smallest. Let $\tau = x + iy$ with $x, y \in \mathbb{R}$. Since $|c\tau + d|^2 = (cx + d)^2 + (cy)^2 \leq 1$, there are only finitely many such pairs (c, d) because $|c| \leq \frac{1}{|y|}$ and $|cx + d| \leq 1$.

We summarize the procedures explained in the above as the following algorithm.

Algorithm 4.2. *The following steps implement an algorithm to find $\tau' \in [\tau]$ so that $\operatorname{Im}(\tau')$ is the biggest.*

Step 1. *Set $m = [1/|y|]$ the largest integer not greater than $1/|y|$.*

Step 2. *For each c with $-m \leq c \leq m$ and $c \equiv 0 \pmod{N}$, set $l_c = [-1 - cx]$ and $u_c = [1 - cx]$.*

Step 3. *Pick a pair (c_0, d_0) so that $|c_0\tau + d_0|$ is the smallest among $|c\tau + d|$ where $-m \leq c \leq m$ and $l_c \leq d \leq u_c$ with $\gcd(c, d) = 1$.*

Step 4. *Set $\tau' = \frac{\operatorname{Im}(\tau)}{|c_0\tau+d_0|}$.*

We list the genera of $X_0(N)$ and the fixed points of W_N in Table 4.1 by using Algorithms 2.3 and 4.2. By using Lemma 4.1, we can confirm that there are no Weierstrass points on $X_0(N)$ arising from the fixed points of W_N. We have used SAGE [28], MAPLE [19], and MATHEMATICA [29] for the numerical computations.

Table 4.1: Fixed points by W_N on $X_0(N)$.

N	$g(X_0(N))$	fixed points by W_N
22	2	$\frac{1}{\sqrt{-22}}, -\frac{6}{13} + \frac{\sqrt{-22}}{286}$
28	2	$\frac{1}{2\sqrt{-7}}, -\frac{8}{11} + \frac{\sqrt{-7}}{154}$
30	3	$\frac{1}{\sqrt{-30}}, \frac{8}{17} + \frac{\sqrt{-30}}{510}, \frac{4}{13} + \frac{\sqrt{-30}}{390}, \frac{2}{11} + \frac{\sqrt{-30}}{330}$
33	3	$\frac{1}{\sqrt{-33}}, \frac{1}{2} + \frac{\sqrt{-33}}{66}, \frac{9}{14} + \frac{\sqrt{-33}}{462}, -\frac{2}{7} + \frac{\sqrt{-33}}{231}$
34	3	$\frac{1}{\sqrt{-34}}, \frac{9}{19} + \frac{\sqrt{-34}}{646}, -\frac{4}{5} + \frac{\sqrt{-34}}{170}, \frac{4}{5} + \frac{\sqrt{-34}}{170}$

37	2	$\frac{1}{\sqrt{-37}}, \frac{1}{2} + \frac{\sqrt{-37}}{74}$
40	3	$\frac{1}{2\sqrt{-10}}, -\frac{6}{11} + \frac{\sqrt{-10}}{220}, -\frac{8}{13} + \frac{\sqrt{-10}}{260}, \frac{5}{7} + \frac{\sqrt{-10}}{140}$
42	5	$\frac{1}{\sqrt{-42}}, \frac{11}{23} + \frac{\sqrt{-42}}{966}, \frac{11}{17} + \frac{\sqrt{-42}}{714}, -\frac{2}{13} + \frac{\sqrt{-42}}{546}$
43	3	$\frac{1}{\sqrt{-43}}, -\frac{3}{4} + \frac{\sqrt{-43}}{172}, \frac{3}{4} + \frac{\sqrt{-43}}{172}, \frac{1}{2} + \frac{\sqrt{-43}}{86}$
45	3	$\frac{1}{3\sqrt{-5}}, \frac{1}{2} + \frac{\sqrt{-5}}{30}, \frac{11}{14} + \frac{\sqrt{-5}}{210}, \frac{4}{7} + \frac{\sqrt{-5}}{105}$
46	5	$\frac{1}{\sqrt{-46}}, \frac{12}{25} + \frac{\sqrt{-46}}{1150}, \frac{3}{5} + \frac{\sqrt{-46}}{230}, -\frac{3}{5} + \frac{\sqrt{-46}}{230}$
48	3	$\frac{1}{4\sqrt{-3}}, -\frac{13}{19} + \frac{\sqrt{-3}}{228}, -\frac{7}{13} + \frac{\sqrt{-3}}{156}, -\frac{1}{7} + \frac{\sqrt{-3}}{84}$
52	5	$\frac{1}{2\sqrt{-13}}, -\frac{13}{17} + \frac{\sqrt{-13}}{442}, \frac{4}{7} + \frac{\sqrt{-13}}{182}, -\frac{4}{7} + \frac{\sqrt{-13}}{182}$
57	5	$\frac{1}{\sqrt{-57}}, \frac{1}{2} + \frac{\sqrt{-57}}{114}, -\frac{15}{22} + \frac{\sqrt{-57}}{1254}, -\frac{4}{11} + \frac{\sqrt{-57}}{627}$
58	6	$\frac{1}{\sqrt{-58}}, \frac{15}{31} + \frac{\sqrt{-58}}{1798}$
60	7	$\frac{1}{2\sqrt{-15}}, \frac{15}{23} + \frac{\sqrt{-15}}{690}, \frac{14}{19} + \frac{\sqrt{-15}}{570}, \frac{10}{17} + \frac{\sqrt{-15}}{510}$
64	3	$\frac{1}{8\sqrt{-1}}, -\frac{9}{17} + \frac{\sqrt{-1}}{136}, -\frac{4}{5} + \frac{\sqrt{-1}}{40}, \frac{4}{5} + \frac{\sqrt{-1}}{40}$
67	5	$\frac{1}{\sqrt{-67}}, -\frac{3}{4} + \frac{\sqrt{-67}}{268}, \frac{3}{4} + \frac{\sqrt{-67}}{268}, \frac{1}{2} + \frac{\sqrt{-67}}{134}$
70	9	$\frac{1}{\sqrt{-70}}, \frac{18}{37} + \frac{\sqrt{-70}}{2590}, \frac{15}{19} + \frac{\sqrt{-70}}{1330}, \frac{12}{17} + \frac{\sqrt{-70}}{1190}$
72	5	$\frac{1}{6\sqrt{-2}}, \frac{9}{19} + \frac{\sqrt{-2}}{228}, -\frac{2}{17} + \frac{\sqrt{-2}}{204}, \frac{3}{11} + \frac{\sqrt{-2}}{132}$
73	5	$\frac{1}{\sqrt{-73}}, \frac{1}{2} + \frac{\sqrt{-73}}{146}, \frac{4}{7} + \frac{\sqrt{-73}}{511}, -\frac{4}{7} + \frac{\sqrt{-73}}{511}$
78	11	$\frac{1}{\sqrt{-78}}, \frac{20}{41} + \frac{\sqrt{-78}}{3198}, \frac{19}{29} + \frac{\sqrt{-78}}{2262}, -\frac{16}{19} + \frac{\sqrt{-78}}{1482}$
82	9	$\frac{1}{\sqrt{-82}}, \frac{21}{43} + \frac{\sqrt{-82}}{3526}, \frac{5}{7} + \frac{\sqrt{-82}}{574}, -\frac{5}{7} + \frac{\sqrt{-82}}{574}$
85	7	$\frac{1}{\sqrt{-85}}, \frac{1}{2} + \frac{\sqrt{-85}}{170}, \frac{13}{22} + \frac{\sqrt{-85}}{1870}, -\frac{2}{11} + \frac{\sqrt{-85}}{935}$
88	9	$\frac{1}{2\sqrt{-22}}, -\frac{12}{23} + \frac{\sqrt{-22}}{1012}, -\frac{12}{19} + \frac{\sqrt{-22}}{836}, -\frac{10}{13} + \frac{\sqrt{-22}}{572}$
93	9	$\frac{1}{\sqrt{-93}}, \frac{1}{2} + \frac{\sqrt{-93}}{186}, -\frac{23}{34} + \frac{\sqrt{-93}}{3162}, \frac{11}{17} + \frac{\sqrt{-93}}{1581}$
97	7	$\frac{1}{\sqrt{-97}}, \frac{1}{2} + \frac{\sqrt{-97}}{194}, -\frac{6}{7} + \frac{\sqrt{-97}}{679}, \frac{6}{7} + \frac{\sqrt{-97}}{679}$
100	7	$\frac{1}{10\sqrt{-1}}, -\frac{22}{29} + \frac{\sqrt{-1}}{290}, \frac{6}{13} + \frac{\sqrt{-1}}{130}, \frac{7}{13} + \frac{\sqrt{-1}}{130}$
102	15	$\frac{1}{\sqrt{-102}}, \frac{26}{53} + \frac{\sqrt{-102}}{5406}, -\frac{25}{37} + \frac{\sqrt{-102}}{3774}, \frac{19}{23} + \frac{\sqrt{-102}}{2346}$
112	11	$\frac{1}{4\sqrt{-7}}, -\frac{15}{29} + \frac{\sqrt{-7}}{812}, \frac{13}{23} + \frac{\sqrt{-7}}{644}, -\frac{7}{11} + \frac{\sqrt{-7}}{308}$
130	17	$\frac{1}{\sqrt{-130}}, \frac{33}{67} + \frac{\sqrt{-130}}{8710}, -\frac{25}{31} + \frac{\sqrt{-130}}{4030}, \frac{16}{23} + \frac{\sqrt{-130}}{2990}$
133	11	$\frac{1}{\sqrt{-133}}, \frac{1}{2} + \frac{\sqrt{-133}}{266}, -\frac{15}{26} + \frac{\sqrt{-133}}{3458}, \frac{11}{13} + \frac{\sqrt{-133}}{1729}$
142	17	$\frac{1}{\sqrt{-142}}, \frac{36}{73} + \frac{\sqrt{-142}}{10366}, -\frac{10}{11} + \frac{\sqrt{-142}}{1562}, \frac{10}{11} + \frac{\sqrt{-142}}{1562}$
148	17	$\frac{1}{2\sqrt{-37}}, -\frac{31}{41} + \frac{\sqrt{-37}}{3034}, -\frac{10}{19} + \frac{\sqrt{-37}}{1406}, \frac{10}{19} + \frac{\sqrt{-37}}{1406}$
163	13	$\frac{1}{\sqrt{-163}}, -\frac{3}{4} + \frac{\sqrt{-163}}{652}, \frac{3}{4} + \frac{\sqrt{-163}}{652}, \frac{1}{2} + \frac{\sqrt{-163}}{326}$
177	19	$\frac{1}{\sqrt{-177}}, \frac{1}{2} + \frac{\sqrt{-177}}{354}, \frac{41}{62} + \frac{\sqrt{-177}}{10974}, \frac{10}{31} + \frac{\sqrt{-177}}{5487}$

190	27	$\frac{1}{\sqrt{-190}}, \frac{48}{97}+\frac{\sqrt{-190}}{18430}, -\frac{26}{43}+\frac{\sqrt{-190}}{8170}, \frac{26}{29}+\frac{\sqrt{-190}}{5510}$
193	15	$\frac{1}{\sqrt{-193}}, \frac{1}{2}+\frac{\sqrt{-193}}{386}, -\frac{8}{11}+\frac{\sqrt{-193}}{2123}, \frac{8}{11}+\frac{\sqrt{-193}}{2123}$
232	27	$\frac{1}{2\sqrt{-58}}, -\frac{30}{59}+\frac{\sqrt{-58}}{6844}, \frac{23}{37}+\frac{\sqrt{-58}}{4292}, \frac{23}{31}+\frac{\sqrt{-58}}{3596}$
253	23	$\frac{1}{\sqrt{-253}}, \frac{1}{2}+\frac{\sqrt{-253}}{506}, -\frac{31}{34}+\frac{\sqrt{-253}}{8602}, -\frac{14}{17}+\frac{\sqrt{-253}}{4301}$

Among the values of N in Table 4.1, we give a list of some Weierstrass points which can be determined by Schöneberg's Theorem [25, Satz 1] or the cases when the 0 or ∞-cusps are Weierstrass points in the following table. We refer to [5, 21] for computing the genera of the quotient spaces of $X_0(N)$ by involutions. In the following table, $U = \left(\begin{smallmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{smallmatrix}\right)$ and μ is the unique hyperelliptic involution of $X_0(37)$.

Table 4.2: Some Weierstrass points on $X_0(N)$.

N	$g(X_0(N))$	some Weierstrass points
22	2	fixed points by W_{11}
28	2	fixed points by W_7
30	3	fixed points by W_{15}
33	3	fixed points by W_{11}
37	2	fixed points by μ
40	3	fixed points by $\left(\begin{smallmatrix} -10 & 1 \\ -120 & 10 \end{smallmatrix}\right)$
42	5	fixed points by W_{14}
46	5	fixed points by W_{23}
48	3	fixed points by $\left(\begin{smallmatrix} -6 & 1 \\ -48 & 6 \end{smallmatrix}\right)$
58	6	fixed points by W_{29}
60	7	fixed points by W_{15}, W_{20}, W_5U and $W_5W_4UW_4$
64	3	0 and ∞ cusps
70	9	fixed points by W_{14} and W_{35}
72	5	fixed points by U
78	11	fixed points by W_{26} and W_{39}
82	9	fixed points by W_{41}
88	9	fixed points by $W_{11}U$ and $W_{11}W_8UW_8$
100	7	0 and ∞ cusps, fixed points by W_4, U and W_4UW_4
102	15	fixed points by W_{17} and W_{51}

112	11	fixed points by W_7, W_7U and $W_7W_{16}UW_{16}$
130	17	fixed points by W_{26} and W_{65}
133	11	fixed points by W_{19}
177	19	fixed points by W_{59}
190	27	fixed points by W_{19} and W_{95}
232	27	fixed points by $W_{29}UW_8UW_8$
253	23	fixed points by W_{11}

Acknowledgments

We would like to thank KIAS (Korea Institute for Advanced Study) for its hospitality while we have worked on this result. Daeyeol Jeon would like to thank Brown University for its hospitality during his sabbatical year. Finally, we thank anonymous referees for their helpful comments, which made significant improvements of this paper.

References

[1] S. Ahlgren and K. Ono, *Weierstrass points on $X_0(p)$ and supersingular j-invariants*, Math. Ann. **325** (2003), no. 2, 355–368. https://doi.org/10.1007/s00208-002-0390-9

[2] A. O. L. Atkin, *Weierstrass points at cusps of* $\Gamma_0(n)$, Ann. of Math. (2) **85** (1967), no. 1, 42–45. https://doi.org/10.2307/1970524

[3] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika **13** (1966), no. 2, 204–216. https://doi.org/10.1112/s0025579300003971

[4] ———, *Imaginary quadratic fields with class number* 2, Ann. of Math. (2) **94** (1971), no. 1, 139–152. https://doi.org/10.2307/1970739

[5] F. Bars, *Bielliptic modular curves*, J. Number Theory **76** (1999), no. 1, 154–165. https://doi.org/10.1006/jnth.1998.2343

[6] D. Burton, *Elementary Number Theory*, McGRAW-Hill, 2011.

[7] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*, John Wiley & Sons, Inc., New York, 1989. https://doi.org/10.5860/choice.27-5799

[8] C. Delaunay, *Critical and ramification points of the modular parametrization of an elliptic curve*, J. Théor. Nombres Bordeaux **17** (2005), no. 1, 109-124. https://doi.org/10.5802/jtnb.480

[9] A. El-Guindy, *Weierstrass points on $X_0(pM)$ and supersingular j-invariants*, J. London Math. Soc. (2) **70** (2004), no. 1, 1-22. https://doi.org/10.1112/s0024610704005496

[10] M. Furumoto and Y. Hasegawa, *Hyperelliptic quotients of modular curves $X_0(N)$*, Tokyo J. Math. **22** (1999), no. 1, 105-125. https://doi.org/10.3836/tjm/1270041616

[11] B. Gross, W. Kohnen and D. Zagier, *Heegner points and derivatives of L-series II*, Math. Ann. **278** (1987), no. 1-4, 497–562. https://doi.org/10.1007/bf01458081

[12] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), no. 3, 227-253. https://doi.org/10.1007/bf01174749

[13] B.-H. Im, D. Jeon and C. H. Kim, *Weierstrass points on certain modular groups*, J. Number Theory **160** (2016), 586-602. https://doi.org/10.1016/j.jnt.2015.09.018

[14] K. Kilger, *Weierstrass points on $X_0(p\ell)$ and arithmetic properties of Fourier coefficients of cusp forms*, Ramanujan J. **17** (2008), no. 3, 321–330. https://doi.org/10.1007/s11139-007-9018-8

[15] J. Klaise, *Orders in quadratic imaginary fields of small class number*, preprint.

[16] W. Kohnen, *Weierstrass points at cusps on special modular curves*, Abh. Math. Sem. Univ. Hamburg **73** (2003), no. 1, 241–251. https://doi.org/10.1007/bf02941280

[17] ———, *A short remark on Weierstrass points at infinity on $X_0(N)$*, Monatsh. Math. **143** (2004), no. 2, 163–167. https://doi.org/10.1007/s00605-003-0054-1

[18] J. Lehner and M. Newman, *Weierstrass points of $\Gamma_0(N)$*, Ann. of Math. (2) **79** (1964), no. 2, 360–368. https://doi.org/10.2307/1970550

[19] Maple (Version 16). Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.

[20] J. S. Milne, *Modular Functions and Modular Forms*. http://www.jmilne.org/math/CourseNotes/MF110.pdf

[21] A. P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462.

[22] ———, *On the Weierstrass points of $X_0(N)$*, Illinois J. Math. **22** (1978), no. 1, 31–35.

[23] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS Regional Conference Series in Mathematics **102**, American Mathematical Society, Providence, RI. 2004. https://doi.org/10.1090/cbms/102

[24] D. E. Rohrlich, *Weierstrass points and modular forms*, Illinois J. Math. **29** (1985), no. 1, 131–141.

[25] B. Schöneberg, *Über die Weierstrass-Punkte in den Körpern der elliptischen Modulfunktionen*, Abh. Math. Sem. Univ. Hamburg **17** (1951), no. 1, 104–111. https://doi.org/10.1007/bf02950745

[26] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14** (1967), no. 1, 1–27. https://doi.org/10.1307/mmj/1028999653

[27] ———, *On complex quadratic fields with class-number two*, Math. Comp. **29** (1975), 289–302. https://doi.org/10.1090/s0025-5718-1975-0369313-x

[28] W. Stein, *Sage: Open Source Mathematical Software (Version 3.1.2)*, The Sage Group, 2008. Available at http://www.sagemath.org.

[29] Wolfram Research, Inc., Mathematica, Version 10, Champaign, IL (1999).

Bo-Hae Im
Department of Mathematical Sciences, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, South Korea
E-mail address: bohaeim@gmail.com

Daeyeol Jeon
Department of Mathematics education, Kongju National University, 56 Gongjudaehak-ro, Gongju-si, Chungcheongnam-do 314-701, South Korea
E-mail address: dyjeon@kongju.ac.kr

Chang Heon Kim
Department of Mathematics, Sungkyunkwan University, Suwon 440-746, South Korea
E-mail address: chhkim@skku.edu