SOME NON-CONGRUENCE SUBGROUPS AND THE ASSOCIATED MODULAR CURVES

TONGHAI YANG AND HONGBO YIN

Dedicated to Professor Wen-Ching Winnie Li.

ABSTRACT. In this paper, we study two families of normal subgroups of $\Gamma_0(2)$ with abelian quotients and their associated modular curves. They are similar to Fermat groups and Fermat curves in some aspects but very different in other aspects. Almost all of them are non-congruence subngroups. These modular curves are either projective lines or hyperelliptic curves. There are few modular forms of weight 1 for these groups. We also determine their cuspidal divisor class groups and show that these groups are finite.

1. INTRODUCTION

Let $\mathbf{f}_i$ be the three famous Weber functions defined by ([YZ97])

$$\begin{aligned}
\mathbf{f}_0(\tau) &= q^{-\frac{1}{48}}\prod_{n>0}(1+q^{n-\frac{1}{2}}) = \zeta_{48}^{-1}\cdot\frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)},\\
\mathbf{f}_1(\tau) &= q^{-\frac{1}{48}}\prod_{n>0}(1-q^{n-\frac{1}{2}}) = \frac{\eta(\frac{\tau}{2})}{\eta(\tau)},\\
\mathbf{f}_2(\tau) &= \sqrt{2}q^{\frac{1}{24}}\prod_{n>0}(1+q^n) = \sqrt{2}\cdot\frac{\eta(2\tau)}{\eta(\tau)}.
\end{aligned} \tag{1.1}$$

Here $\zeta_n = e^{\frac{2\pi i}{n}}$ is a n-th primitive root of unity, $q = e^{2\pi i\tau}$, and

$$\eta(\tau) = q^{\frac{1}{24}}\prod_{n>0}(1-q^n)$$

Key words and phrases. Non-congruence subgroups, modular curves, modular functions, modular forms.

The first author is partially supported by a NSF grant DMS-1200380 and a Chinese Qian Ren grant. The second author is partially supported by the Chinese Scholarship Council.

is the well-known eta function. They are all modular functions for the main congruence subgroup $\Gamma(48)$ and are 24-th roots of three other Weber functions ($\Delta(\eta)=\eta(\tau)^{24}$)

$$\begin{aligned}\omega_0(\tau)&=q^{-\frac{1}{2}}\prod_{n>0}(1+q^{n-\frac{1}{2}})^{24}=-\frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)},\\ \omega_1(\tau)&=q^{-\frac{1}{2}}\prod_{n>0}(1-q^{n-\frac{1}{2}})^{24}=\frac{\Delta(\frac{\tau}{2})}{\Delta(\tau)},\\ \omega_2(\tau)&=2^{12}q\prod_{n>0}(1+q^{n})^{24}=2^{12}\cdot\frac{\Delta(2\tau)}{\Delta(\tau)}.\end{aligned}\tag{1.2}$$

According to the CM (complex multiplication) theory, the CM values $\mathbf{f}_i(\tau)$ are defined over the ray class field of $\mathbb{Q}(\sqrt{d})$ of modulus 48 for any imaginary quadratic number $\tau\in\mathbb{H}$ of fundamental discriminant $d<0$. A surprising and amusing fact, discovered by Yui and Zagier [YZ97], is that when $d\equiv 1 \pmod 8$ and $3\nmid d$, the number

$$f(\mathcal{O}_d)=(-1)^{\frac{d-1}{8}}\zeta_{48}\mathbf{f}_2(\frac{-1+\sqrt{d}}{2})$$

belongs to the much smaller Hilbert class field of $K_d=\mathbb{Q}(\sqrt{d})$, where $\mathcal{O}_d$ is the ring of integers of K_d. Moreover, they conjectured and Gee proved [Gee99] that the Galois conjugates of $f(\mathcal{O}_d)$ are given by similarly twisted CM values of some $\mathbf{f}_i$ at other ideal classes ([YZ97, Proposition], where they are denoted by $f(Q)$ using the associated binary quadratic forms). A natural question is whether $\mathbf{f}_i$ are actually modular functions for much bigger subgroups of $SL_2(\mathbb{Z})$ (than $\Gamma(48)$). Another question is: why the 24-th roots? What about the N-th roots? In this paper, we study the modular groups, modular curves, and modular forms related to these questions.

Let

$$T=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right),\quad S=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right),\quad B=STS^{-1}=\left(\begin{smallmatrix}1&0\\-2&1\end{smallmatrix}\right).\tag{1.3}$$

Let $\Phi^0(N)$ (N a fixed positive integer) be the subgroup of $\Gamma_0(2)$ generated by its commutator subgroup $\Gamma_0(2)'$, T^N and B^N. Let $\Phi^0_s(N)$ be the subgroup of $\Gamma_0(2)$ generated by $\Phi^0(N)$ and TB^{s+1} for an integer s. Notice that $\Phi^0_0(N)$ is the stabilizer of a N-th root $\omega_2^{\frac{1}{N}}$ (defined in Section 2). Here and throughout this paper, a stabilizer always means the stabilizer in $SL_2(\mathbb{Z})$. We also remark that $\Phi^0_0(24)$, the stabilizer of $\mathbf{f}_2=\omega_2^{\frac{1}{24}}$, is a subgroup of $\Gamma_0(2)$ of index 24 and is thus much bigger than $\Gamma(48)$.

Notice also that groups $\Phi^0(N)$ are similar to the Fermat groups $\Phi(N)$, the subgroup of $\Gamma(2)$ generated by $\Gamma(2)'$, T^{2N}, and B^N, which are well studied by Rohrlich ([Roh76], [Roh77]) and others. They are called the Fermat groups as their associated modular curves are the famous Fermat curves $x^N+y^N=1$. For a subgroup Γ of $SL_2(\mathbb{Z})$ of finite index, its associated modular curve is defined to be $X_\Gamma=\Gamma\backslash\mathbb{H}^*$, where $\mathbb{H}^*$ is the union of the upper half plane $\mathbb{H}$ and the rational projective line $\mathbb{P}^1(\mathbb{Q})$. A cool theorem of Fricke ([Fri86]) and Rohrlich ([Roh76, Appendix]) asserts that $\Phi(N)$ is a congruence subgroup if and only if $N|8$.

The Fermat curve has natural quotients for $-1 \le s < N-1$

$$X_{\Phi_s(N)}: \quad v^N = u(1-u)^s,$$

which are associated to the subgroups of $\Gamma(2)$ generated by $\Phi(N)$ and T^2B^{s+1}, studied by Gross and Rohrlich [GR78], and also one of the authors [Yan96]. For example, Gross and Rohrlich constructed infinitely many quadratic fields of p-rank bigger than zero using these curves. In [Yan96], one of the authors showed that the dimension of the space of weight 1 modular forms for $\Phi_{p-2}(p)$ assumes the maximal possible dimension.

In this paper, we study the modular groups $\Phi^0(N)$ and $\Phi^0_s(N)$ and the associated modular curves $X_{\Phi^0}(N)$ and $X_{\Phi^0_s}(N)$ using similar ideas. Although some results are very similar, others are dramatically different. Although T^2 and B generate a free subgroup of $\Gamma(2)$ of index 2 (missing -1), T and B generate $\Gamma_0(2)$ with relations

$$(TB)^4 = 1, \quad (TB)^2 = -1. \tag{1.4}$$

This is perhaps the main reason for some of the main difference between our results in this paper and those for the Fermat groups. Now we briefly summarize the main results of this paper. In Section 2, we study when these groups are congruence subgroups, following [Roh76], and prove the following theorem which combines Theorems 2.7 and 2.10.

Theorem 1.1. *(1) The group $\Phi^0(N)$ is a congruence subgroup if and only if $N|24$.*
(2) Assume $N|4s$. Then the group $\Phi^0_s(N)$ is a congruence subgroup if and only if $N|24$.

It is easy to check (Lemma 2.8) that $\Phi^0_s(N) = \Phi^0_s(d)$ for $d = \gcd(4s, N)$. So the condition $N|4s$ in (2) of the above theorem is not restrictive. In Section 3, we study the cusps and elliptic points of these groups and compute the genus of the associated modular curves. The main result is the following theorem (restatement of Theorems 3.1 and 3.4), which is quite different from the Fermat curves and their quotients. In particular, we have constructed a family of non-congruence subgroups of $SL_2(\mathbb{Z})$ whose modular curves have genus 0.

Theorem 1.2. *(1) The associated modular curve $X_{\Phi^0(N)}$ has genus 0 or $\frac{N}{2}-1$ depending on whether N is odd or even.*
(2) Assume $N|4s$. Then

(a) *The modular curve $X_{\Phi^0_0(N)}$ has always genus 0.*
(b) *When $N \equiv a \pmod 4$ with $a = 0, 2$, $X_{\Phi^0_{\frac{N}{2}}(N)}$ has genus $\frac{N-a}{4}$.*
(c) *When $N \equiv a \pmod 8$ with $a = 0, 4$, $X_{\Phi^0_{\pm\frac{N}{4}}(N)}$ has genus $\frac{N-a}{8}$.*

We remark that when N is odd, $\Phi^0(N) = \Phi^0_0(N)$. In Section 4, we determine the function fields of these modular curves and give explicit affine equations for these modular curves.

Let $\lambda(\tau)$ be the modular Lambda function for $\Gamma(2)$ given by

$$\lambda(\tau) = -\frac{1}{16}q^{-\frac{1}{2}}\prod_{n\geq 1}(\frac{1-q^{n-\frac{1}{2}}}{1+q^n})^8, \tag{1.5}$$

$$1-\lambda(\tau) = \frac{1}{16}q^{-\frac{1}{2}}\prod_{n\geq 1}(\frac{1+q^{n-\frac{1}{2}}}{1+q^n})^8.$$

In particular, $\lambda(\tau)\neq 0,1$ in the upper half plane. The following theorem is a restatement of Theorems 4.3 and 4.4.

Theorem 1.3. *(1)*

(a) *When N is odd, The function field of $X_{\Phi^0(N)}$ is $\mathbb{C}(\omega_2^{\frac{1}{N}})$. The modular curve $X_{\Phi^0(N)}$ is a projective line.*

(b) *When N is even, The function field of $X_{\Phi^0(N)}$ is $\mathbb{C}(\lambda,\omega_2^{\frac{1}{N}})$. The modular curve $X_{\Phi^0(N)}$ has the following affine equation:*

$$y^2-y=16x^N.$$

(2) Assume $N|4s$.

(a) *When $N|s$, the function field of $X_{\Phi^0_s(N)}$ is $\mathbb{C}(\omega_2^{\frac{1}{N}})$, and $X_{\Phi^0_s(N)}$ is a projective line.*

(b) *When $N|2s$ and $N\nmid s$, the function field of $X_{\Phi^0_s(N)}$ is $\mathbb{C}(\omega_2^{\frac{2}{N}},(1-2\lambda)\omega_2^{\frac{1}{N}})$, and the modular curve $X_{\Phi^0_s(N)}$ has the following affine equation:*

$$y^2=x+64x^{\frac{N}{2}+1}.$$

(c) *When $N|4s$ and $N\nmid 2s$, the function field of $X_{\Phi^0_s(N)}$ is $\mathbb{C}(\omega_2^{\frac{4}{N}},(1-2\lambda)\omega_2^{\frac{2}{N}})$, and the modular curve $X_{\Phi^0_s(N)}$ has the following affine equation:*

$$y^2=x+64x^{\frac{N}{4}+1}.$$

In Section 5, we study the space of modular forms of weight 1 for $\Phi^0(N)$ and $\Phi^0_{\pm\frac{N}{4}}(N)$ when $4|N$ (they are the only ones not containing -1). The space of modular forms of weight 1 is special. For example, its dimension is not covered by the Riemann-Roch theorem and is very small in the congruence subgroup case (see for example [Duk95], [Ser77]). For congruence subgroups, it is also closely related to the complex Galois representations ([DS74], [Ser77]). For non-congruence subgroups, the space could be big as shown in [Yan96] although we don't know the general picture. The following theorem shows that it could also be very small.

Theorem 1.4. *When $4|N$. We have*

$$M_1(\Phi^0(N))=\mathbb{C}\theta(\tau)+\mathbb{C}\theta(\tau+1),\quad S_1(\Phi^0(N))=0,$$

and

$$M_1(\Phi^0_{\pm\frac{N}{4}}(N))=\begin{cases}0 & \text{if } \frac{N}{4} \text{ is even,}\\ \mathbb{C}(\theta(\tau)+\theta(\tau+1)) & \text{if } \frac{N}{4} \text{ is odd,}\end{cases}$$

$$S_1(\Phi^0_{\pm\frac{N}{4}}(N)) = 0.$$

Here

$$\theta(\tau) = (\sum_{n\in\mathbb{Z}} q^{\frac{n^2}{2}})^2$$

is a modular form of weight 1 *for the free subgroup of* $\Gamma(2)$ *generated by* T^2 *and* B.

Notice that the dimensions do not depend on N at all. The method can also be used to construct spaces of modular and cusp forms of any weight without modification, which we also do in Section 5 (Theorems 5.5 and 5.6).

Finally, we study the cuspidal divisor class groups for these modular curves following suggestion of David Rohrlich in Section 6. For a subgroup Γ of $SL_2(\mathbb{Z})$ of finite index, let $X^0_\Gamma = \Gamma\backslash\mathbb{H}$ be the open modular curve of Γ. Let $\mathscr{D}^\infty$ be the free abelian group of degree 0 divisors supported on the cusps $X_\Gamma - X^0_\Gamma = \Gamma\backslash\mathbb{P}^1(\mathbb{Q})$, and let $\mathscr{F}^\infty$ be its subgroup of the divisors $\mathrm{Div}(f)$ for some modular function f whose divisor is supported on the cusps. Let $\mathrm{CL}(\Gamma) = \mathscr{D}^\infty/\mathscr{F}^\infty$ be the cuspidal divisor class group associated to Γ. A natural question is to determine this concrete divisor class group. A well-known theorem of Manin ([Man72]) and Drinfeld ([Dri73]) asserts that $\mathrm{CL}(\Gamma)$ is always a finite group when Γ is a congruence subgroup. Rohrlich proved ([Roh76], [Roh77]) that $\mathrm{CL}(\Gamma)$ is also finite for every Fermat group. In Section 6, we show that $\mathrm{CL}(\Gamma)$ are finite for $\Gamma = \Phi^0(N)$ and $\Phi^0_s(N)$, and determine their group structures (Theorems 6.3 and 6.4).

It is a pleasure to dedicate this paper to Professor Wen-Ching Winnie Li, who is inspirational and has a lot of positive influence to one of the authors (T.Y.). We thank David Rohrlich for his very helpful comments and suggestions. In particular, Section 6 is added at his suggestion. We thank Matija Kazalicki and the anonymous referee for their comments. Finally, we thank the referee and his/her friend for patiently checking and correcting numerous English errors in the previous version.

2. Non-congruence subgroups

In this section, we will study the subgroups $\Phi^0(N)$ and $\Phi^0_s(N)$ and determine when they are congruence subgroups. We need some preparations.

Let Γ be a subgroup of $SL_2(\mathbb{Z})$ with finite index and let f be a modular function of Γ. Let c be a cusp of Γ, and let m be the smallest positive integer such that $\gamma T^m\gamma^{-1} \in \Gamma$ and $\gamma\infty = c$. Then $\mathrm{order}^\Gamma_c f$ is defined to be the number $k/2$ such that

$$(\gamma \circ f)(\tau) = f(\gamma(\tau)) = \sum_{n\geq k} a_n q^{\frac{n}{2m}}, \quad a_k \neq 0. \tag{2.1}$$

We write $\mathrm{order}_c f$ instead of $\mathrm{order}^\Gamma_c f$ if Γ is clear. The three functions ω_i do not vanish in the upper half plane and satisfy

$$S \circ (\omega_0, \omega_1, \omega_2) = (\omega_0, \omega_2, \omega_1), \quad T \circ (\omega_0, \omega_1, \omega_2) = (-\omega_1, -\omega_0, \omega_2). \tag{2.2}$$

As in [Roh76, section 1], we take the logarithm of ω_2 by

$$\log\omega_2 = 12\log 2 + 2\pi i\tau + 24\sum_{n>0}\log(1+q^n).$$

Here log denotes the principal branch of the logarithm. We define

$$\omega_2^{\frac{1}{N}} := e^{\frac{1}{N}\log\omega_2} = 2^{\frac{12}{N}} q^{\frac{1}{N}} \prod_{n\geq 1}(1+q^n)^{\frac{24}{N}}. \tag{2.3}$$

We similarly define $\omega_i^{\frac{1}{N}}$ for $i = 0, 1$. Using (2.2), we can understand $\omega_i^{\frac{1}{N}}$ once we understand $\omega_2^{\frac{1}{N}}$. It is thus enough to focus on $\omega_2^{\frac{1}{N}}$ in this paper.

Suppose f is modular with respect to Γ, holomorphic and never zero in the upper half plane. Then Proposition 1.1 in [Roh76] states that

$$\frac{1}{2\pi i}(\gamma T^m \gamma^{-1} \circ (\log f) - \log f) = \mathrm{order}_{\gamma\infty} f. \tag{2.4}$$

Here m is the same as defined just before (2.1).

Lemma 2.1. *The function $\omega_2^{\frac{1}{N}}$ is a modular function for the subgroup $\Phi_0^0(N)$ and thus for $\Phi^0(N)$. Furthermore, $\Phi_0^0(N)$ is the stabilizer of $\omega_2^{\frac{1}{N}}$. In particular, $\Phi_0^0(24)$ is the stabilizer of $\mathbf{f}_2$.*

Proof. We have that

$$T \circ \log(\omega_2) = \log\omega_2 + 2\pi i \cdot \mathrm{order}_\infty \omega_2 = \log\omega_2 + 2\pi i,$$
$$B \circ \log(\omega_2) = \log\omega_2 + 2\pi i \cdot \mathrm{order}_0 \omega_2 = \log\omega_2 - 2\pi i.$$

It is easy to see from this that

$$T \circ \omega_2^{\frac{1}{N}} = \zeta_N \omega_2^{\frac{1}{N}}, \quad B \circ \omega_2^{\frac{1}{N}} = \zeta_N^{-1} \omega_2^{\frac{1}{N}}.$$

So

$$TB \circ \omega_2^{\frac{1}{N}} = BT \circ \omega_2^{\frac{1}{N}} = \omega_2^{\frac{1}{N}}, \quad T^N \circ \omega_2^{\frac{1}{N}} = B^N \circ \omega_2^{\frac{1}{N}} = \omega_2^{\frac{1}{N}},$$

and

$$\alpha \circ \omega_2^{\frac{1}{N}} = \omega_2^{\frac{1}{N}}$$

for $\alpha \in \Gamma_0(2)'$. The function $\omega_2^{\frac{1}{N}}$ is a modular function for the subgroup $\Phi_0^0(N)$.

From (2.2), we can see that the stabilizer of ω_2 (in $SL_2(\mathbb{Z})$) is generated by T and B, and hence $\Gamma_0(2)$. Since

$$\Gamma_0(2)/\Phi_0^0(N) = \{1, T, \cdots, T^{N-1}\}$$

and T^k changes $\omega_2^{\frac{1}{N}}$ unless $N|k$, the stabilizer of $\omega_2^{\frac{1}{N}}$ is $\Phi_0^0(N)$. □

Lemma 2.2. *We have $SL_2(\mathbb{Z})^{ab} \cong \mathbb{Z}/12$. In particular, $-1 \notin SL_2(\mathbb{Z})'$.*

Proof. It is a well-known fact. Indeed, we have abstractly

$$SL_2(\mathbb{Z}) \cong \langle x, y : x^2 = y^3 = -1 \rangle$$

with $x = S$ and $y = ST$. So $SL_2(\mathbb{Z})^{ab}$ is the abelian group generated by x and y with the same condition as above, i.e., $x^2 = y^3 = -1$. Now the conclusion is clear. □

One character $\chi : SL_2(\mathbb{Z}) \to \mu_{12}$ is given by

$$\eta^2(\gamma z) = \chi(\gamma)(cz+d)\eta^2(z), \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

So $\eta^2(z)$ is a cusp form of $SL_2(\mathbb{Z})$ of weight 1 with character χ.

Lemma 2.3. *We have*

(1) *If* $N \equiv 1, 3 \pmod 4$, *then* $TB \in \Phi^0(N)$ *and* $-1 \in \Phi^0(N)$.
(2) *If* $N \equiv 2 \pmod 4$, *then* $TB \notin \Phi^0(N)$ *and* $-1 \in \Phi^0(N)$.
(3) *If* $N \equiv 0 \pmod 4$, *then* $TB \notin \Phi^0(N)$ *and* $-1 \notin \Phi^0(N)$.

Proof. First notice that $(TB)^2 = -1$ and $(TB)^3 = -TB$.

Case 1. We first assume $N \equiv 1, 3 \pmod 4$. There exist integers x, y with $xN + 4y = 1$. So

$$TB = (TB)^{xN+4y} = (TB)^{xN} \in (T^N B^N)^x \Gamma_0(2)' \subset \Phi^0(N).$$

Case 2. Next we assume $N \equiv 2 \pmod 4$. Then we have $xN + 4y = 2$ for some integers x, y, and so

$$-1 = (TB)^2 = (TB)^{xN+4y} = (TB)^{xN} \in (T^N B^N)^x \Gamma_0(2)' \subset \Phi^0(N).$$

In this case, T^N, B^N, and $\Gamma_0(2)'$ stabilize ω_0, but TB changes ω_0 to ω_1. So TB cannot belong to $\Phi^0(N)$.

Case 3. Finally we assume $N \equiv 0 \pmod 4$. If $-1 \in \Phi^0(N)$, then

$$-1 = T^{kN} B^{lN} X = T^{(k-l)N} (TB)^{lN} X' = T^{(k-l)N} X'$$

for some $X, X' \in \Gamma_0(2)'$. By Lemma 2.2, it follows that $k - l \neq 0$. Then $T^{(k-l)N} = -(X')^{-1}$. Choose n such that $(k-l)N$ and n are coprime. Then $T^{(k-l)N}$ changes $\omega_2^{\frac{1}{n}}$ while $-(X')^{-1}$ fixes $\omega_2^{\frac{1}{n}}$, which is a contradiction. So $-1 \notin \Phi^0(N)$ and TB of course cannot be in $\Phi^0(N)$. □

Lemma 2.4. *We have*

$$\Gamma_0(2)/\Phi^0(N) \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & \text{if } N \equiv 1, 3 \pmod 4, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} & \text{if } N \equiv 2 \pmod 4, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} & \text{if } N \equiv 0 \pmod 4. \end{cases}$$

Proof. Every element of $\Gamma_0(2)$ can be written as a product of T and B. So the elements of $\Gamma_0(2)/\Gamma_0(2)'$ can be written as $T^m B^n = T^{m-n}(TB)^n$. Thus $G = \Gamma_0(2)/\Phi^0(N)$ is abelian and generated by T and TB with properties $T^N = 1$ and $(TB)^4 = 1$. Since T^n does not fix $\omega_2^{\frac{1}{N}}$ for any $1 \leq n \leq N-1$ and $\Phi^0(N)$ fixes $\omega_2^{\frac{1}{N}}$, T has exactly order N. The order of $TB \in G$ is 1, 2, or 4 according to N being odd, 2 (mod 4), or 0 (mod 4) by Lemma 2.3. Finally, we note that if $T^m(TB)^n = 1$ in G, then $N|m$ as TB fixes $\omega_2^{\frac{1}{N}}$. □

Corollary 2.5. *For a subgroup Γ of $SL_2(\mathbb{Z})$, we write $\overline{\Gamma}$ for its image in $SL_2(\mathbb{Z})/\pm 1$. Then we have*

$$\overline{\Gamma_0(2)}/\overline{\Phi^0(N)} \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & \text{if } N \equiv 1 \pmod 2, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} & \text{if } N \equiv 0 \pmod 2. \end{cases}$$

and

$$\overline{\Phi^0(N)}\backslash\overline{\Gamma_0(2)}/\Gamma_\infty \cong \begin{cases} \{1\} & \text{if } N \equiv 1 \pmod 2, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } N \equiv 0 \pmod 2. \end{cases}$$

Here

$$\Gamma_\infty = \{ \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\}.$$

Proof. Note that every element of $\Gamma_0(2)/\Phi^0(N)$ can be written as $(TB)^n T^m$ and -1 does not belong to $\Phi^0(N)$ when $N \equiv 0 \pmod 4$. □

Remark 2.6. From the proof of Lemma 2.4, we can see that $\Gamma_0(2)'$ has infinite index in $\Gamma_0(2)$ because $T^m \notin \Gamma_0(2)'$ for any integer m.

Theorem 2.7. *$\Phi^0(N)$ is a congruence subgroup if and only if $N|24$.*

Proof. We follow the method of Rohrlich [Roh76, Appendix] closely in the proof. Suppose $\Phi^0(N)$ is a congruence subgroup, i.e., $\Gamma(2^r M) \subset \Phi^0(N)$ for some integers $r \geq 1$ and positive odd integer M. Since $\Gamma_0(2)/\Phi^0(N)$ is abelian, the surjective map

$$\Gamma_0(2)/\Gamma(2^r M) \to \Gamma_0(2)/\Phi^0(N)$$

factors through $(\Gamma_0(2)/\Gamma(2^r M))^{ab}$.

Step 1: First we prove the following claim: when M is odd and $r \geq 1$ is an integer,

(*) $(\Gamma_0(2)/\Gamma(2^r M))^{ab}$ is a quotient of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Since $\Gamma_0(2)/\Gamma(2^r M) \cong \Gamma_0(2)/\Gamma(2^r) \times \Gamma(1)/\Gamma(M)$, we have

$$(\Gamma_0(2)/\Gamma(2^r M))^{ab} \cong (\Gamma_0(2)/\Gamma(2^r))^{ab} \times (\Gamma(1)/\Gamma(M))^{ab}.$$

Rohlrlich proved in [Roh76] that

(1) $(\Gamma(2)/\Gamma(2^r))^{ab}$ is a quotient of $(\Gamma(2)/\Gamma(16))^{ab} = (\mathbb{Z}/8\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$. Moreover, they are equal for $r \geq 4$.

(2) we have

$$(\Gamma(1)/\Gamma(M))^{ab} \cong \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{if } 3|M, \\ 1 & \text{if } 3 \nmid M. \end{cases}$$

So to prove the claim (*), it is enough to prove $(\Gamma_0(2)/\Gamma(2^r))^{ab}$ is a quotient of $(\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$. Rohlrlich proved [Roh76, Page 98] that $\Gamma(2)'\Gamma(2^r) = \Gamma(2)'\Gamma(16)$ for $r \geq 4$, which implies $\Gamma_0(2)'\Gamma(2^r) = \Gamma_0(2)'\Gamma(16)$. So we have

$$(\Gamma_0(2)/\Gamma(2^r))^{ab} = (\Gamma_0(2)/\Gamma(16))^{ab}$$

for $r \geq 4$ since

$$(\Gamma_0(2)/\Gamma(16))^{ab} = \Gamma_0(2)/\Gamma_0(2)'\Gamma(16)$$

and

$$(\Gamma_0(2)/\Gamma(2^r))^{ab} = \Gamma_0(2)/\Gamma_0(2)'\Gamma(2^r).$$

Now to prove the claim (*), it suffices to verify that

$$(\Gamma_0(2)/\Gamma(16))^{ab} = (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}).$$

Since

$$T^8 = (TB)^8 B^{-8} = B^{-8} \mod \Gamma_0(2)',$$

we have $T^8 \in \Gamma_0(2)'\Phi(8)$. As a result, $\Phi^0(8) = \Gamma_0(2)'\Phi(8)$. It was proved by Rohrlich that $\Phi(8) = \Gamma(2)'\Gamma(16)$ [Roh76, Page 100](Note that in Rorhlich's thesis, he defined -1 in $\Phi(8)$ while we did not), so

$$\Phi^0(8) = \Gamma_0(2)'\Phi(8) = \Gamma_0(2)'\Gamma(16),$$

and thus

$$(\Gamma_0(2)/\Gamma(16))^{ab} = \Gamma_0(2)/(\Gamma_0(2)'\Gamma(16)) = \Gamma_0(2)/\Phi^0(8) = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$$

by Lemma 2.4. The claim (*) is true.

Step 2: Next assume $\Gamma(2^r M) \subset \Phi^0(N)$ for some $r \geq 1$ and M odd. Then $\Gamma_0(2)/\Phi^0(N)$ is a quotient of $(\Gamma_0(2)/\Gamma(2^r M))^{ab}$. So $\Gamma_0(2)/\Phi^0(N)$ is a quotient of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. By Lemma 2.4, we have $N|24$.

Step 3: Finally we prove that $\Phi^0(24)$ is a congruence subgroup. Recall that $\Phi_0^0(24)$ is the stabilizer of $\mathbf{f}_2$ (Lemma 2.1). Since $\mathbf{f}_2$ is a modular function for $\Gamma(48)$, we have $\Gamma_0(2)'\Gamma(48) \subset \Phi_0^0(24)$. Since $T^{24} = (TB)^{24}B^{-24} = B^{-24} \mod \Gamma_0(2)'$, we obtain

$$\Phi^0(24) = \langle \Gamma_0(2)', B^{24} \rangle \subset \Gamma_0(2)'\Gamma(48) \subset \Phi_0^0(24).$$

Notice that $\Phi_0^0(24)/\Phi^0(24)$ is cyclic of order 4, generated by TB. On the other hand, we have by Lemma 2.3

$$-1 \notin \Phi^0(8) = \Gamma_0(2)'\Gamma(16).$$

So $-1 \notin \Gamma_0(2)'\Gamma(48)$ and TB has also order 4 in $\Phi_0^0(24)/\Gamma_0(2)'\Gamma(48)$. Therefore

$$\Phi^0(24) = \Gamma_0(2)'\Gamma(48) \tag{2.5}$$

is a congruence subgroup.

□

Lemma 2.8. *Let $d = gcd(4s, N)$. Then $\Phi_s^0(N) = \Phi_s^0(d)$. Furthermore, if d is odd, then $\Phi_s^0(N) = \Phi^0(d)$.*

Proof. Since $(TB)^4 = 1$, we have $B^{4s} = (TB^{s+1})^4 \mod \Gamma_0(2)'$. Thus $B^{4s} \in \Phi_s^0(N)$. There are integers a and b such that $d = 4as + bN$, and so $B^d = B^{4as}B^{bN} \in \Phi_s^0(N)$. As a result,

$$T^d = (TB^{s+1})^d B^{-d(s+1)} \mod \Gamma_0(2)' \in \Phi_s^0(N).$$

Thus $\Phi_s^0(N) = \Phi_s^0(d)$. When d is odd,

$$(TB)^4 = 1 \mod \Phi_s^0(d) \quad \text{and} \quad T^d = B^d = 1 \mod \Phi_s^0(d)$$

imply that $TB = 1 \mod \Phi_s^0(d)$. On the other hand, $TB^{s+1} = 1 \mod \Phi^0(d)$. Therefore $\Phi_s^0(d) = \Phi_0^0(d) = \Phi^0(d)$ by Lemma 2.3. □

By this lemma, we may and will assume $N|4s$.

Lemma 2.9. *Assume $N|4s$. Then $\Phi_s^0(N)$ has only four possibilities: $\Phi_0^0(N), \Phi_{\frac{N}{2}}^0(N)$, and $\Phi_{\pm\frac{N}{4}}^0(N)$. More precisely,*

(1) *When $N|s$, we have that $\Phi_s^0(N) = \Phi_0^0(N)$, and*
$$\overline{\Gamma_0(2)}/\overline{\Phi_0^0(N)} \cong \Gamma_0(2)/\Phi_0^0(N) \cong \mathbb{Z}/N\mathbb{Z}.$$
(2) *When $N|2s$ and $N \nmid s$, we have that $\Phi_s^0(N) \cong \Phi_{\frac{N}{2}}^0(N)$, $TB \notin \Phi_s^0(N)$, $-1 \in \Phi_s^0(N)$ and*
$$\overline{\Gamma_0(2)}/\overline{\Phi_s^0(N)} \cong \Gamma_0(2)/\Phi_s^0(N) \cong \mathbb{Z}/N\mathbb{Z}.$$
(3) *When $N|4s$ and $N \nmid 2s$, we have that $\Phi_s^0(N) \cong \Phi_{\frac{N}{4}}^0(N)$ or $\Phi_{-\frac{N}{4}}^0(N)$, neither TB nor -1 is in $\Phi_s^0(N)$ and*
$$\Gamma_0(2)/\Phi_s^0(N) \cong \mathbb{Z}/N\mathbb{Z},$$
$$\overline{\Gamma_0(2)}/\overline{\Phi_s^0(N)} \cong \mathbb{Z}/(N/2)\mathbb{Z}.$$

Proof. (1) If $N|s$, then $TB = TB^{s+1} \mod \Phi^0(N)$ and $\Phi_0^0(N) = \Phi_s^0(N)$. The isomorphisms follow easily from Corollary 2.5.

(2) Assume $N|2s$ and $N \nmid s$. Then $s = \frac{N}{2}(2k+1)$,
$$TB^{s+1} = TB^{\frac{N}{2}+1}B^{Nk} \in \Phi_{\frac{N}{2}}^0(N),$$
and
$$TB^{\frac{N}{2}+1} = TB^{s+1}B^{-Nk} \in \Phi_s^0(N).$$
So $\Phi_s^0(N) \cong \Phi_{\frac{N}{2}}^0(N)$.

To prove the isomorphisms, first notice that $T = B^{-s-1} \mod \Phi_s^0(N)$, so $\Gamma_0(2)/\Phi_s^0(N)$ is cyclic and generated by B (of order at most N). Next, $\Phi_s^0(N) \subset \Phi_s^0(\frac{N}{2})$ and by (1)
$$\Gamma_0(2)/\Phi_s^0(\frac{N}{2}) \cong \mathbb{Z}/(N/2)\mathbb{Z}.$$
So B has order at least $N/2$. Now the isomorphism follows from the claim $TB \notin \Phi_s^0(N)$. Consider the function $(1-2\lambda)\omega_2^{\frac{1}{N}}$. It is invariant under the action of T^N, B^N and $TB^{\frac{N}{2}+1}$. But $TB \circ (1-2\lambda)\omega_2^{\frac{1}{N}} = -(1-2\lambda)\omega_2^{\frac{1}{N}}$. Then $TB \notin \Phi_{\frac{N}{2}}^0(N)$. This proves (2).

(3) The case $N|4s$ and $N \nmid 2s$ can be proved similarly. In this case, $s = \frac{N}{4}(4k \pm 1)$,
$$TB^{s+1} = TB^{\pm\frac{N}{4}+1}B^{Nk} \in \Phi_{\pm\frac{N}{4}}^0(N),$$
and
$$TB^{\pm\frac{N}{4}+1} = TB^{s+1}B^{-Nk} \in \Phi_s^0(N).$$
So $\Phi_s^0(N) \cong \Phi_{\pm\frac{N}{4}}^0(N)$.

To prove the isomorphisms, first notice that $T = B^{-s-1} \mod \Phi_s^0(N)$, so $\Gamma_0(2)/\Phi_s^0(N)$ is cyclic and generated by B (of order at most N). Next, $\Phi_s^0(N) \subset \Phi_s^0(\frac{N}{2})$ and by (2)
$$\Gamma_0(2)/\Phi_s^0(\frac{N}{2}) \cong \mathbb{Z}/(N/2)\mathbb{Z}.$$

So B has order at least $N/2$. Now the isomorphism follows from the claim $-1 \notin \Phi_s^0(N)$. By Lemma 2.3, it follows that $-1 \notin \Phi^0(N)$. If $-1 \in \Phi_s^0(N)$, then

$$-1 = (TB^{\pm\frac{N}{4}+1})^n \mod \Phi^0(N)$$

with $1 \leq n \leq 3$. Consider the function $\omega_2^{\frac{1}{N}}$. It is invarient under the action of $\Phi^0(N)$ and -1. But $(TB^{\pm\frac{N}{4}+1})^n \circ \omega_2^{\frac{1}{N}} = \zeta_N^{\pm\frac{nN}{4}}\omega_2^{\frac{1}{N}}$. Then $-1 \notin \Phi_s^0(N)$. This proves (3).

□

Theorem 2.10. *We assume $N|4s$. Then $\Phi_s^0(N)$ is a congruence subgroup if and only if $N|24$.*

Proof. When $N|24$, we have that $\Phi_s^0(N) \supset \Phi^0(N)$ is a congruence subgroup. When $N \nmid 24$, it follows that $\Gamma_0(2)/\Phi_s^0(N)$ cannot be a quotient of $(\Gamma_0(2)/\Gamma(2^rM))^{ab}$ by Lemma 2.9 and Claim (*) in the proof of Theorem 2.7. So $\Phi_s^0(N)$ is not a congruence subgroup. □

3. The genus of the modular curves

For a subgroup Γ of $SL_2(\mathbb{Z})$ of finite index, let $X_\Gamma = \Gamma\backslash\mathbb{H}^*$ be the associated projective modular curve as in the introduction. We first recall that the well-known formula for the genus $g(X_\Gamma)$ of X_Γ as given by ([Shi94, Theorem 1.40])

$$g(X_\Gamma) = 1 + \frac{d}{12} - \frac{e_2(\Gamma)}{4} - \frac{e_3(\Gamma)}{3} - \frac{e_\infty(\Gamma)}{2}. \tag{3.1}$$

Here $d = [\overline{SL_2(\mathbb{Z})} : \bar{\Gamma}]$, e_2 and e_3 are the numbers of elliptic points of $\bar{\Gamma}$ of order 2 and 3 respectively, and e_∞ is the number of cusps of $\bar{\Gamma}$.

Theorem 3.1. *The genus of $X_{\Phi^0(N)}$ is 0 or $\frac{N}{2}-1$ depending on whether N is odd or even.*

Proof. First Corollary 2.5 implies

$$d = [\overline{SL_2(\mathbb{Z})} : \overline{\Phi^0(N)}] = \begin{cases} 3N & \text{if } N \equiv 1 \pmod 2, \\ 6N & \text{if } N \equiv 0 \pmod 2. \end{cases}$$

Next the same lemma implies that

$$e_\infty = |\overline{\Phi^0(N)}\backslash\overline{\Gamma_0(2)}/\Gamma_\infty| + |\overline{\Phi^0(N)}\backslash\overline{\Gamma_0(2)}/S\Gamma_\infty S^{-1}| = \begin{cases} 2 & \text{if } N \equiv 1 \pmod 2, \\ 4 & \text{if } N \equiv 0 \pmod 2. \end{cases}$$

Since $\overline{\Gamma_0(2)}$ has no elliptic point of order 3, neither has its subgroup $\Phi^0(N)$. So $e_3 = 0$. Finally, $\overline{\Gamma_0(2)}$ has exactly one elliptic point $\tau_0 = \overline{\Gamma_0(2)}^{\frac{i+1}{2}}$ of order 2 with stabilizer $G_0 = \langle TB\rangle$. Since TB has order 1 or 2 in $\overline{\Gamma_0(2)}/\overline{\Phi^0(N)}$ depending on N being odd or even by Lemma 2.3, $\overline{\Phi^0(N)}^{\frac{1+i}{2}}$ is an elliptic point of order 2 exactly when N is odd. Since $\Phi^0(N)$ is a normal subgroup of $\Gamma_0(2)$, $\overline{\Phi^0(N)}$ has exactly $[\overline{\Gamma_0(2)} : \overline{\Phi^0(N)}]$ elliptic points of order 2 or none depending on whether N is odd or even. So we have by Corollary 2.5

$$e_2 = \begin{cases} N & \text{if } N \equiv 1 \pmod 2, \\ 0 & \text{if } N \equiv 0 \pmod 2. \end{cases}$$

Now our theorem follows from the genus formula (3.1). □

Remark 3.2. It is interesting to compare Theorem 3.1 with the Fermat groups extensively studied by Rohrlich ([Roh76], [Roh77]). The N-th Fermat group $\Phi(N)$ is the subgroup of $\Gamma(2)$ generated by $\Gamma(2)'$ and T^{2N} and B^N. The associated modular curve is the Fermat curve $X_{\Phi(N)} : x^N + y^N = 1$. Its genus is always $\frac{(N-1)(N-2)}{2}$.

Now consider the modular curve $X_{\Phi_s^0(N)}$ and assume without loss of generosity that $N|4s$ by Lemma 2.8.

Lemma 3.3. *Consider the modular curve $X_{\Phi_s^0(N)}$ with $N|4s$. Then $e_3 = 0$. Moreover,*

$$d = [\overline{SL_2(\mathbb{Z})} : \overline{\Phi_s^0(N)}] = \begin{cases} 3N & \text{if } N|2s, \\ \frac{3N}{2} & \text{if } N \nmid 2s. \end{cases} \tag{3.2}$$

$$e_2 = \begin{cases} N & \text{if } N|s, \\ 0 & \text{if } N \nmid s. \end{cases} \tag{3.3}$$

$$e_\infty = \begin{cases} 2 & \text{if } N|s, \\ 2 & \text{if } N|2s, N \nmid s, \text{and } N \equiv 0 \mod 4 \text{ or} \\ & N|4s, N \nmid 2s \text{ and } N \equiv 0 \mod 8, \\ 3 & \text{if } N|2s, N \nmid s, \text{and } N \equiv 2 \mod 4 \text{ or} \\ & N|4s, N \nmid 2s \text{ and } N \equiv 4 \mod 8. \end{cases} \tag{3.4}$$

Proof. Formula (3.2) follows from Lemma 2.9. To show (3.3), note that $\Gamma_0(2)$ has exactly one elliptic point $\tau_0 = \Gamma_0(2)\frac{i+1}{2}$ of order 2 with stabilizer $G_0 = \langle TB \rangle$. By Lemma 2.9, $TB \in \Phi_s^0(N)$ exactly when $N|s$. So $\frac{i+1}{2}$ gives an elliptic point of order 2 for $\Phi_s^0(N)$ exactly when $N|s$. Because $\Phi_s^0(N)$ is a normal subgroup of $\Gamma_0(2)$, the preimages of τ_0 in $X_{\Phi_s^0(N)}$ are either all elliptic points or all non-elliptic points. This proves (3.3). Finally, we verify (3.4) case by case.

(1) When $N|s$, $\Phi_s^0(N) = \Phi_0^0(N)$. In this case, both $\{B^n \mid 0 \le n \le N-1\}$ and $\{T^n \mid 0 \le n \le N-1\}$ can be considered as a set of representations of $\overline{\Phi_s^0(N)}\backslash\overline{\Gamma_0(2)}$. The set $\{B^n \mid 0 \le n \le N-1\}$ fixes 0 and the set $\{T^n \mid 0 \le n \le N-1\}$ fixes ∞. So $X_{\Phi_s^0(N)}$ has two cusps 0 and ∞.

(2) When $N|2s$ and $N \nmid s$, and $N \equiv 2 \mod 4$, we have ($(TB)^2 = -1$)

$$T^{\frac{N}{2}} = (TB)^{\frac{N}{2}+1}T^{-1}B^{-\frac{N}{2}-1} = 1 \mod \Phi_{\frac{N}{2}}^0(N),$$

and

$$B^{\frac{N}{2}} = TB \mod \Phi_{\frac{N}{2}}^0(N).$$

It follows from Lemma 2.9 that $TB \notin \Phi_{\frac{N}{2}}^0(N)$, then

$$\{B^n \mid 0 \le n \le N-1\}$$

and

$$\{(TB)^i T^n \mid 0 \le n \le \frac{N}{2} - 1, i = 0, 1\}$$

can be chosen to be two representative sets of $\overline{\Phi_s^0(N)}\backslash\overline{\Gamma_0(2)}$. The set $\{B^n \mid 0 \leq n \leq N-1\}$ fixes 0 and the set $\{(TB)^iT^n \mid 0 \leq n \leq \frac{N}{2}-1, i=0,1\}$ acts on ∞ with the orbit $\{\infty, \frac{1}{2}\}$. So $X_{\Phi_s^0(N)}$ has 3 cusps.

(3) When $N|2s$ and $N \nmid s$, and $N \equiv 0 \mod 4$, we have

$$T^{\frac{N}{2}} = (TB)^{\frac{N}{2}+1}T^{-1}B^{-\frac{N}{2}-1} = TB \mod \Phi^0_{\frac{N}{2}}(N),$$

and

$$B^{\frac{N}{2}} = (TB)^{-1} \mod \Phi^0_{\frac{N}{2}}(N).$$

By Lemma 2.9, it follows that $TB \notin \Phi^0_{\frac{N}{2}}(N)$, then both T and B have order N in $\overline{\Phi_s^0(N)}\backslash\overline{\Gamma_0(2)}$. The situation is similar to (1).

(4) When $N|4s$ and $N \nmid 2s$, and $N \equiv 4 \mod 8$, we have

Case 1 If $\Phi_s^0(N) \cong \Phi^0_{\frac{N}{4}}(N)$, then

$$T^{\frac{N}{4}} = (TB)^{\frac{N}{4}+1}T^{-1}B^{-\frac{N}{4}-1} = \pm 1 \mod \Phi^0_{\frac{N}{4}}(N),$$

and

$$B^{\frac{N}{4}} = (TB)^{-1} \mod \Phi^0_{\frac{N}{4}}(N).$$

Case 2 If $\Phi_s^0(N) \cong \Phi^0_{-\frac{N}{4}}(N)$, then

$$T^{-\frac{N}{4}} = (TB)^{-\frac{N}{4}+1}T^{-1}B^{\frac{N}{4}-1} = \pm 1 \mod \Phi^0_{-\frac{N}{4}}(N),$$

and

$$B^{\frac{N}{4}} = TB \mod \Phi^0_{-\frac{N}{4}}(N).$$

By Lemma 2.9, it follows that $TB, -1 \notin \Phi^0_{\pm\frac{N}{4}}(N)$. In both cases,

$$\{B^n \mid 0 \leq n \leq \frac{N}{2}-1\}$$

and

$$\{(TB)^iT^n \mid 0 \leq n \leq \frac{N}{4}-1, i=0,1\}$$

can be chosen to be two representative sets of $\overline{\Phi_s^0(N)}\backslash\overline{\Gamma_0(2)}$. The set $\{B^n \mid 0 \leq n \leq \frac{N}{2}-1\}$ fixes 0 and the set $\{(TB)^iT^n \mid 0 \leq n \leq \frac{N}{4}-1, i=0,1\}$ acts on ∞ with the orbit $\{\infty, \frac{1}{2}\}$. So $X_{\Phi_s^0(N)}$ has 3 cusps.

(5) When $N|4s$ and $N \nmid 2s$, and $N \equiv 0 \mod 8$, we have

Case 1 If $\Phi_s^0(N) \cong \Phi^0_{\frac{N}{4}}(N)$, then

$$T^{\frac{N}{4}} = (TB)^{\frac{N}{4}+1}T^{-1}B^{-\frac{N}{4}-1} = \pm TB \mod \Phi^0_{\frac{N}{4}}(N),$$

and

$$B^{\frac{N}{4}} = (TB)^{-1} \mod \Phi^0_{\frac{N}{4}}(N).$$

Case 2 If $\Phi_s^0(N) \cong \Phi^0_{-\frac{N}{4}}(N)$, then

$$T^{\frac{N}{4}} = (TB)^{-\frac{N}{4}+1}T^{-1}B^{\frac{N}{4}-1} = \pm TB \mod \Phi^0_{-\frac{N}{4}}(N),$$

and

$$B^{\frac{N}{4}} = TB \mod \Phi^0_{-\frac{N}{4}}(N).$$

By Lemma 2.9, it follows that $TB, -1 \notin \Phi^0_{-\frac{N}{4}}(N)$. Then in both cases, T and B have order $\frac{N}{2}$ in $\overline{\Phi_s^0(N)}\backslash\overline{\Gamma_0(2)}$. The situation is similar to (1).

□

Combining Lemma 3.3 and Formula (3.1), we obtain the following theorem.

Theorem 3.4. *We have the following:*

(1) *The modular curve $X_{\Phi_0^0(N)}$ has always genus 0.*
(2) *When $N \equiv a \pmod 4$ with $a = 0, 2$, $X_{\Phi^0_{\frac{N}{2}}(N)}$ has genus $\frac{N-a}{4}$.*
(3) *When $N \equiv a \pmod 8$ with $a = 0, 4$, $X_{\Phi^0_{\pm\frac{N}{4}}(N)}$ has genus $\frac{N-a}{8}$.*

4. Modular functions and explicit equations

In this section, we determine the modular functions for $\Phi^0(N)$ and $\Phi_s^0(N)$. As a consequence, we give explicit affine equations for the associated modular curves. It turns out that they are either projective lines or hyperelliptic curves. Recall that the function field of $X(2) = X_{\Gamma(2)}$ is generated by the lambda function $\lambda(\tau)$ (see (1.5)), which has value 0, 1, and ∞ at the cusps 0, 1, and ∞, respectively.

Lemma 4.1. *If N is even, then $\Phi^0(N) \subset \Gamma(2)$ and $[\overline{\Gamma(2)} : \overline{\Phi^0(N)}] = N$.*

Proof. It is easy to check $T \circ \lambda = 1 - \lambda$ by the the product expansion (1.5). It is also clear that $B \circ \lambda = \lambda$ as $B \in \Gamma(2)$. So λ is invariant under $\Gamma_0(2)'$ and thus $\Gamma_0(2)' \subset \Gamma(2)$. If N is even, then $T^N, B^N \in \Gamma(2)$, so $\Phi^0(N) \subset \Gamma(2)$. By Corollary 2.5 and the fact that $[\overline{\Gamma_0(2)} : \overline{\Gamma(2)}] = 2$, we get $[\overline{\Gamma(2)} : \overline{\Phi^0(N)}] = N$. □

Lemma 4.2. *The modular functions $\omega_2^{\frac{n}{N}}$ are linearly independent over $\mathbb{C}(\lambda)$ for $0 \le n \le N-1$.*

Proof. Assume

$$\sum_{0\le n\le N-1} f_n(\lambda)\omega_2^{\frac{n}{N}} = 0.$$

Letting B act on the equation $N-1$ times, we get a linear system of equations:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_N^{-1} & \zeta_N^{-2} & \cdots & \zeta_N^{-(N-1)} \\ 1 & \zeta_N^{-2} & \zeta_N^{-4} & \cdots & \zeta_N^{-2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_N^{-(N-1)} & \zeta_N^{-2(N-1)} & \cdots & \zeta_N^{-(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} f_0(\lambda) \\ f_1(\lambda)\omega_2^{\frac{1}{N}} \\ f_1(\lambda)\omega_2^{\frac{2}{N}} \\ \vdots \\ f_{N-1}(\lambda)\omega_2^{\frac{N-1}{N}} \end{pmatrix} = 0.$$

The determinant of the matrix is nonzero, so $f_n(\lambda) = 0$ for all n.

□

Theorem 4.3. *The function field of $X_{\Phi^0(N)}$ is $\mathbb{C}(\omega_2^{\frac{1}{N}})$ or $\mathbb{C}(\lambda, \omega_2^{\frac{1}{N}})$ depending on whether N is odd or even. In particular, when N is odd, $X_{\Phi^0(N)}$ is isomorphic to the projective line $\mathbb{P}^1$, and when N is even, it is hyperelliptic with affine equation*

$$X_{\Phi^0(N)}: \quad y^2 - y = 16x^N.$$

Proof. It is well known that the function fields of $X_{\Gamma_0(2)}$ and $X_{\Gamma(2)}$ are $\mathbb{C}(\omega_2)$ and $\mathbb{C}(\lambda)$, respectively. Lemma 2.1 asserts that $\omega_2^{\frac{1}{N}}$ is a rational function on $X_{\Phi^0(N)}$.

When N is odd, the cover map $\phi_1 : X_{\Phi^0(N)} \to X_{\Gamma_0(2)}$ has

$$\deg(\phi_1) = [\overline{\Gamma_0(2)} : \overline{\Phi^0(N)}] = N = [\mathbb{C}(\omega_2^{\frac{1}{N}}) : \mathbb{C}(\omega_2)].$$

So $\mathbb{C}(\omega_2^{\frac{1}{N}})$ is the function field of $X_{\Phi^0(N)}$.

When N is even, the cover map $\phi_2 : X_{\Phi^0(N)} \to X_{\Gamma(2)}$ has

$$\deg\ \phi_2 = [\overline{\Gamma(2)} : \overline{\Phi^0(N)}] = N = [\mathbb{C}(\lambda, \omega_2^{\frac{1}{N}}) : \mathbb{C}(\lambda)].$$

So $\mathbb{C}(\lambda, \omega_2^{\frac{1}{N}})$ is the function field of $X_{\Phi^0(N)}$.

It is clear that $X_{\Phi^0(N)}$ is isomorphic to the projective line $\mathbb{P}^1$ when N is odd. We assume that N is even. By (1.2) and (1.5), one can see that

$$\begin{aligned}
\omega_2(\lambda - 1)\lambda &= 16 \prod_{n\geq 1} (1 - q^{n-\frac{1}{2}})^8 (1 + q^{n-\frac{1}{2}})^8 (1 + q^n)^8 \\
&= 16 \prod_{n\geq 1} (1 - q^{2n-1})^8 (1 + q^n)^8 \\
&= 16 \prod_{n\geq 1} \frac{(1 - q^n)^8}{(1 - q^{2n})^8} (1 + q^n)^8 \\
&= 16.
\end{aligned}$$

Thus,

$$\omega_2 = \frac{16}{(\lambda - 1)\lambda}. \tag{4.1}$$

Let $x = \omega_2^{-\frac{1}{N}}$ and $y = \lambda$, then we get

$$y^2 - y = 16x^N.$$

□

Similarly, we have

Theorem 4.4. *Assume $N|4s$. Then the function field of $X_{\Phi_s^0(N)}$ is given by*

$$\mathbb{C}(\Phi_s^0(N)) = \begin{cases} \mathbb{C}(\omega_2^{\frac{1}{N}}) & \text{if } N|s, \\ \mathbb{C}(\omega_2^{\frac{2}{N}}, (1-2\lambda)\omega_2^{\frac{1}{N}}) & \text{if } N|2s, N\nmid s, \\ \mathbb{C}(\omega_2^{\frac{4}{N}}, (1-2\lambda)\omega_2^{\frac{2}{N}}) & \text{if } N|4s, N\nmid 2s. \end{cases}$$

Moreover, $X_{\Phi_0^0(N)}$ is isomorphic to the projective line $\mathbb{P}^1$, $X_{\Phi^0_{\frac{N}{2}}(N)}$ is isomorphic to the curve

$$y^2 = x + 64x^{\frac{N}{2}+1},$$

and $X_{\Phi^0_{\pm\frac{N}{4}}(N)}$ is isomorphic to the curve

$$y^2 = x + 64x^{\frac{N}{4}+1}.$$

Proof. (1) By Lemma 2.9, $\overline{\Gamma_0(2)}/\overline{\Phi_0^0(N)} \cong \mathbb{Z}/N\mathbb{Z}$. Then $[\mathbb{C}(\Phi_s^0(N)) : \mathbb{C}(\Gamma_0(2))] = N$. So it is clear that $\mathbb{C}(\Phi_0^0(N)) = \mathbb{C}(\omega_2^{\frac{1}{N}})$ and that $X_{\Phi_0^0(N)}$ is isomorphic to the projective line $\mathbb{P}^1$.

(2) We have

$$\begin{aligned} T\circ\lambda &= (1-\lambda), \qquad T\circ(1-\lambda) = \lambda, \\ B\circ\lambda &= \lambda, \quad \text{and} \quad B\circ(1-\lambda) = (1-\lambda). \end{aligned}$$

Since N is even, it is easy to check that $(1-2\lambda)\omega_2^{\frac{1}{N}}$ is invariant under the action of T^N, B^N and $TB^{\frac{N}{2}+1}$. But $B^{\frac{N}{2}}\circ(1-2\lambda)\omega_2^{\frac{1}{N}} = -(1-2\lambda)\omega_2^{\frac{1}{N}}$. Thus $(1-2\lambda)\omega_2^{\frac{1}{N}}$ is a modular form for $\Phi^0_{\frac{N}{2}}(N)$, but not a modular form for $\Phi^0_{\frac{N}{2}}(\frac{N}{2})$.

By Lemma 2.9,

$$\overline{\Phi^0_{\frac{N}{2}}(\frac{N}{2})}/\overline{\Phi^0_{\frac{N}{2}}(N)} = \mathbb{Z}/2\mathbb{Z}.$$

So

$$[\mathbb{C}(\Phi^0_{\frac{N}{2}}(N)) : \mathbb{C}(\Phi^0_{\frac{N}{2}}(\frac{N}{2}))] = 2.$$

We know that $\mathbb{C}(\Phi^0_{\frac{N}{2}}(\frac{N}{2})) = \mathbb{C}(\omega_2^{\frac{2}{N}})$ by (1). So

$$\mathbb{C}(\Phi^0_{\frac{N}{2}}(N)) = \mathbb{C}(\omega_2^{\frac{2}{N}}, (1-2\lambda)\omega_2^{\frac{1}{N}}).$$

Let $x = \omega_2^{-\frac{2}{N}}$ and $y = (1-2\lambda)\omega_2^{\frac{2}{N}}$. Then by (4.1) we get

$$xy^2 = 1 + 64x^{\frac{N}{2}}.$$

Replacing y by y/x, we get the equation in the theorem.

(3) It is easy to check that $(1-2\lambda)\omega_2^{\frac{2}{N}}$ is invariant under the action of T^N, B^N, and $TB^{\pm\frac{N}{4}+1}$. Since $B^{\frac{N}{4}}\circ(1-2\lambda)\omega_2^{\frac{2}{N}} = -(1-2\lambda)\omega_2^{\frac{2}{N}}$, it follows that $(1-2\lambda)\omega_2^{\frac{2}{N}}$ is a modular function for $\Phi^0_{\pm\frac{N}{4}}(N)$ but not a modular function for $\Phi^0_{\pm\frac{N}{4}}(\frac{N}{4})$.

By Lemma 2.9,

$$\overline{\Phi^0_{\pm\frac{N}{4}}(\frac{N}{4})}/\overline{\Phi^0_{\pm\frac{N}{4}}(N)} = \mathbb{Z}/2\mathbb{Z}.$$

So

$$[\mathbb{C}(\Phi^0_{\pm\frac{N}{4}}(N)) : \mathbb{C}(\Phi^0_{\pm\frac{N}{4}}(\frac{N}{4}))] = 2.$$

We know that $\mathbb{C}(\Phi^0_{\pm\frac{N}{4}}(\frac{N}{4})) = \mathbb{C}(\omega_2^{\frac{4}{N}})$ by (1). So

$$\mathbb{C}(\Phi^0_{\pm\frac{N}{4}}(N)) = \mathbb{C}(\omega_2^{\frac{4}{N}}, (1-2\lambda)\omega_2^{\frac{2}{N}}).$$

Let $x = \omega_2^{-\frac{4}{N}}$ and $y = (1-2\lambda)\omega_2^{\frac{4}{N}}$. Then we have by (4.1)

$$xy^2 = 1 + 64x^{\frac{N}{4}}.$$

Replacing y by y/x, we get the equation in the theorem. □

Remark 4.5. In Theorem 4.4 (3), $\Phi^0_{\frac{N}{4}}(N)$ and $\Phi^0_{-\frac{N}{4}}(N)$ are two different groups but have the same function field. This is not a contradiction. We have

$$\Phi^0_{\frac{N}{4}}(N)/\Phi^0(N) = \langle TB^{\frac{N}{4}+1}\rangle,$$

and

$$\Phi^0_{-\frac{N}{4}}(N)/\Phi^0(N) = \langle TB^{-\frac{N}{4}+1}\rangle = \langle TB^{\frac{N}{4}+1}B^{-\frac{N}{2}}\rangle.$$

On the other hand, $B^{\frac{N}{2}} = -1 \mod \Phi^0(N)$. So the projections from $X_{\Phi^0(N)}$ to $X_{\Phi^0_{\frac{N}{4}}(N)}$ and $X_{\Phi^0_{-\frac{N}{4}}(N)}$ are the same.

Remark 4.6. Since the modular curves $X_{\Phi^0(N)}$ and $X_{\Phi^0_s(N)}$ are either projective lines or hyperelliptic curves, their genera are easy to compute. This would give another proof of Theorem 1.2.

5. Modular forms for $\Phi^0(N)$

As mentioned in Section 1, the space of modular forms of weight 1 is mysterious in general. Its dimension is not known in general although it is expected to be very small for congruence subgroups. In this section, we study the question for $\Phi^0(N)$ and $\Phi^0_{\pm\frac{N}{4}}(N)$ for $4|N$ and prove Theorem 1.4. Actually we will mainly focus on the case $\Phi^0(N)$ until the end. Since the method is general, we obtain a basis for the space of modular (respectively cusp) forms of any integral weight $k \geq 1$.

Recall that the theta function $\theta(\tau)$ defined in Theorem 1.4 is a weight one holomorphic modular form for $\Delta = \langle T^2, B\rangle \subset \Gamma(2)$. Notice that $\Gamma(2) = \Delta \times \{\pm 1\}$. It is well known that θ has a unique zero at the cusp 1 of order $\frac{1}{2}$ (see for example [Yan96]).

There are four cusps $\{0, 1, \infty, \frac{1}{2}\}$ for $\Phi^0(N)$. The branched cover $X_{\Phi^0(N)} \to X_{\Gamma(2)}$ ramifies exactly at the cusps: 0 and 1 are totally ramified with ramification index N while ∞ and $\frac{1}{2}$ lie above ∞ with ramification index $\frac{N}{2}$. We list the orders of the modular functions of $\Phi^0(N)$ at the cusps as follows:

TABLE 1. Orders of functions at cusps

	0	1	∞	$\frac{1}{2}$
$\lambda(\tau)$	N	0	$-\frac{N}{2}$	$-\frac{N}{2}$
$\frac{1}{1-\lambda(\tau)}$	0	$-N$	$\frac{N}{2}$	$\frac{N}{2}$
$\omega_2^{\frac{1}{N}}$	-1	-1	1	1
$\frac{\lambda^l\omega_2^{\frac{n}{N}}}{(1-\lambda)^m}$	$Nl-n$	$-mN-n$	$n+\frac{N}{2}(m-l)$	$n+\frac{N}{2}(m-l)$

Recall that $\Phi^0(N)\subset\Gamma(2)$. We have the following lemma similar to [Yan96, Corollary 1.2].

Lemma 5.1. *Assume $4|N$ and let k be a positive integer. The map $h\to h\theta^k$ gives isomorphisms*

$$H^0(X_{\Phi^0(N)},\mathcal{O}(\frac{N}{2}k\cdot 1))\cong M_k(\Phi^0(N)),$$
$$H^0(X_{\Phi^0(N)},\mathcal{O}(-1\cdot 0+(\frac{N}{2}k-1)\cdot 1-1\cdot\frac{1}{2}-1\cdot\infty)\cong S_k(\Phi^0(N)).$$

Here $\frac{N}{2}k\cdot 1$ means that the divisor is supported at the cusp 1 with multiplicity $\frac{N}{2}k$. For a divisor D, the associated line bundle is denoted by $\mathcal{O}(D)$.

Lemma 5.2. *Any modular (meromorphic) function f of $\Phi^0(N)$ with poles only at the cusp 1 can be written as*

$$\frac{\sum_{0\le n\le N-1}f_n(\lambda)\omega_2^{\frac{n}{N}}}{(1-\lambda)^m}$$

for some $m\ge 0$ and some polynomials $f_n(\lambda)$ of λ.

Proof. By Theorem 4.3, we can write

$$f=\frac{\sum_{n=0}^{N-1}f_n(\lambda)\omega_2^{\frac{n}{N}}}{g(\lambda)},$$

where $g(\lambda)$ and $f_n(\lambda)$ are all polynomials on λ with the common divisor 1. Suppose $g(\lambda)\neq c(1-\lambda)^m$ for some $m\ge 0$ and some $c\neq 0$, $g(\lambda)=0$ has a root $\lambda_0=\lambda(\tau_0)\neq 1$.

If $\lambda_0=0$, then τ_0 is the cusp 0 for $\Gamma(2)$. Since $\omega_2^{\frac{1}{N}}$ has a pole at the cusp 0, we see that $f_n(\lambda)$ are all multiples of λ, contradicting to the assumption that they are prime to g.

So we may assume $\lambda(\tau_0)=\lambda_0\neq 0$. Then the point $\tau_0\in X(2)$ is unique.
For $0\le i\le N-1$, let

$$\tau_i=B^i(\tau_0),\quad \alpha_i=\omega_2^{\frac{1}{N}}(\tau_i),\ \text{and}\ \lambda_i=\lambda(\tau_i).$$

Then $\lambda_i=\lambda_0$, and that all α_i are distinct. Indeed, $\tau_i\in X_{\Phi^0(N)}$ are distinct preimages of τ_0 as the projection $X_{\Phi^0(N)}\to X(2)$ is unramified outside cusps. If $\alpha_i=\alpha_j$, then

$$\lambda(\tau_i)=\lambda(\tau_j)\ \text{and}\ \omega_2^{\frac{1}{N}}(\tau_i)=\omega_2^{\frac{1}{N}}(\tau_j),$$

which imply that $\tau_i = \tau_j \in X_{\Phi^0(N)}$. By assumption that f has only one pole at the cusp 1 and $g(\lambda(\tau_i)) = g(\lambda_0) = 0$, we see that

$$\sum f_n(\lambda_0)\alpha_i^n = 0, \quad 0 \le i \le N-1.$$

So $f_n(\lambda_0) = 0$ for all n, again contradicting to the assumption that f_n and g are relatively prime. This proves the lemma.

□

It is clear from Lemma 5.2 that any function $f \in H^0(X_{\Phi^0(N)}, \mathcal{O}(\frac{N}{2}k \cdot 1))$ can be written as a linear combination of monomials $\frac{\lambda^l \omega_2^{\frac{n}{N}}}{(1-\lambda)^m}$. From Table 1, we can see that

$$\frac{\lambda^l \omega_2^{\frac{n}{N}}}{(1-\lambda)^m} \in H^0(X_{\Phi^0(N)}, \mathcal{O}(\frac{N}{2}k \cdot 1))$$

if and only if l, m, and n satisfy the following inequalities:

$$Nl - n \ge 0, \tag{5.1}$$

$$-Nm - n + \frac{N}{2}k \ge 0, \tag{5.2}$$

$$-\frac{N}{2}l + n + \frac{N}{2}m \ge 0. \tag{5.3}$$

Lemma 5.3. *Assume $f \in H^0(X_{\Phi^0(N)}, \mathcal{O}(\frac{N}{2}k \cdot 1))$, then f can be written as*

$$f = \sum c_{l,m,n} \frac{\lambda^l \omega_2^{\frac{n}{N}}}{(1-\lambda)^m},$$

with (l, m, n) satisfying the inequalities (5.1)—(5.3).

Proof. By Lemma 5.2, we write f as

$$f = \frac{\sum_{0 \le n \le N-1} f_n(\lambda)\omega_2^{\frac{n}{N}}}{(1-\lambda)^p} = \sum_{0 \le n \le N-1} h_n(\tau).$$

where $h_n(\tau) = \frac{f_n(\lambda)\omega_2^{\frac{n}{N}}}{(1-\lambda)^p}$. We also assume $f_n(\lambda) = g_n(\lambda)\lambda^{a_n}(1-\lambda)^{b_n}$, with $g_n(0) \neq 0$ and $g_n(1) \neq 0$.

(I) Let

$$t_n = \text{order}_0 h_n(\tau) = Na_n - n.$$

Because $0 \le n \le N-1$, it follows that $t_j = t_i$ if and only if $j = i$. Then $\text{order}_0 f \ge 0$ if and only if $t_n \ge 0$ for every n, i.e.

$$Na_n - n \ge 0. \tag{5.4}$$

(II) Let

$$r_n = \text{order}_1 h_n(\tau) = Nb_n - n - pN.$$

We have that $r_j = r_i$ if and only if $j = i$, since $0 \le n \le N-1$. Then $\text{order}_1 f \ge -\frac{N}{2}k$ if and only if $r_n \ge -\frac{N}{2}k$ for every n, i.e.

$$Nb_n - n - pN \ge -\frac{N}{2}k. \tag{5.5}$$

(III) Let

$$s_n = \text{order}_\infty h_n(\tau) = \text{order}_{\frac{1}{2}} h_n(\tau) = \frac{N}{2}p - \frac{N}{2}\text{deg} f_n + n.$$

Then $s_i = s_j$ with $i > j$ if and only if $i = j + \frac{N}{2}$ and $\text{deg} f_i(\lambda) = \text{deg} f_j(\lambda) + 1$, since $0 \le n \le N-1$. Assume that s_k is the smallest number in $\{s_n\}$. If $s_j > s_k$ for any $j \ne k$, then $\text{order}_\infty f \ge 0$ if and only if $s_n \ge 0$ for every n, i.e.

$$\frac{N}{2}p - \frac{N}{2}\text{deg} f_n + n \ge 0. \tag{5.6}$$

Otherwise, without loss of generality, we can assume that $s_{k+\frac{N}{2}} = s_k$. We prove $s_k \ge 0$ also in this case. If $s_k < 0$, assume the Fourier expansions of h_k and $h_{k+\frac{N}{2}}$ at infinity are

$$\sum_{n \ge s_k} c_n q^{\frac{n}{N}} \text{ and } \sum_{n \ge s_{k+\frac{N}{2}}} d_n q^{\frac{n}{N}},$$

where $c_{s_k} \ne 0$ and $d_{s_{k+\frac{N}{2}}} \ne 0$. Because $B \circ h_k = \zeta_N^{-k} h_k$ and $B \circ h_{k+\frac{N}{2}} = \zeta_N^{-k-\frac{N}{2}} h_{k+\frac{N}{2}}$, the Fourier expansions of h_k and $h_{k+\frac{N}{2}}$ at $\frac{1}{2}$ are

$$\zeta_N^{-k} \sum_{n \ge s_k} c_n q^{\frac{n}{N}} \text{ and } \zeta_N^{-k-\frac{N}{2}} \sum_{n \ge s_{k+\frac{N}{2}}} d_n q^{\frac{n}{N}}.$$

Since $\text{order}_\infty f = \text{order}_{\frac{1}{2}} f \ge 0$, we must have $c_{s_k} + d_{s_{k+\frac{N}{2}}} = 0$ and $\zeta_N^{-k} c_{s_k} + \zeta_N^{-k-\frac{N}{2}} d_{s_{k+\frac{N}{2}}} = 0$. This is impossible ($N \ge 4$). So we must have $s_k \ge 0$. As a result, $s_n \ge 0$ for every n, i.e. (5.6) is always true.

Now write $f = \sum c_{l,m,n} \frac{\lambda^l \omega_2^{\frac{n}{N}}}{(1-\lambda)^m}$ with $m = p - b_n$. Then $a_n \le l \le \text{deg} f_n - b_n$. By (5.4)–(5.6), l, m, and n satisfy (5.1)–(5.3).

□

Lemma 5.4. $\left\{ \frac{\omega_2^{\frac{n}{N}}}{(1-\lambda)^m} \mid 0 \le m \le d \right\}$ *is maximal linearly independent in the set*

$$\left\{ \frac{\lambda^l \omega_2^{\frac{n}{N}}}{(1-\lambda)^m} \mid 0 \le l \le m, 0 \le m \le d \right\}$$

over $\mathbb{C}$.

Proof. $\left\{\frac{\lambda^l\omega_2^{\frac{n}{N}}}{(1-\lambda)^m} \mid 0\le l\le m, 0\le m\le d\right\}=\emptyset$ if and only if $\left\{\frac{\omega_2^{\frac{n}{N}}}{(1-\lambda)^m} \mid 0\le m\le d\right\}=\emptyset$. We assume that both sets are nonempty.

Since $\frac{\lambda^l\omega_2^{\frac{n}{N}}}{(1-\lambda)^m}=\frac{\lambda^l(1-\lambda)^{d-m}\omega_2^{\frac{n}{N}}}{(1-\lambda)^d}$, there is a correspondence between

$$\left\{\frac{\lambda^l\omega_2^{\frac{n}{N}}}{(1-\lambda)^m} \mid 0\le l\le m, 0\le m\le d\right\} \tag{5.7}$$

and

$$\left\{\lambda^l(1-\lambda)^{d-m} \mid 0\le l\le m+b, 0\le m\le d\right\}, \tag{5.8}$$

which keeps the linear relationship over $\mathbb{C}$.

The degree of λ in (5.8) is between 0 and d. So there are at most $d+1$ linearly independent elements over $\mathbb{C}$ in (5.8). There are $d+1$ elements in

$$\left\{\frac{\omega_2^{\frac{n}{N}}}{(1-\lambda)^m} \mid 0\le m\le d\right\}$$

and they are obviously linearly independent over $\mathbb{C}$. Then it is maximal linearly independent over $\mathbb{C}$ in (5.7).

□

Theorem 5.5. *We have a basis $\{f_i\theta^k\}$ for the space $M_k(\Phi^0(N))$ $(4|N)$ of modular forms of weight k for $\Phi^0(N)$, where $\{f_i\}$ is a basis for $H^0(X_{\Phi^0(N)},\mathcal{O}(\frac{N}{2}k\cdot 1))$ given below.*

1. *If k is even, a basis of $H^0(X_{\Phi^0(N)},\mathcal{O}(\frac{N}{2}k\cdot 1))$ is given by the union of the following three sets of elements:*
   - (a) $\left\{\frac{1}{(1-\lambda)^m} \mid 0\le m\le\frac{k}{2}\right\}$,
   - (b) $\left\{\frac{\lambda}{(1-\lambda)^m}\omega_2^{\frac{n}{N}} \mid 1\le m\le\frac{k}{2}-1, 0<n<\frac{N}{2}\right\}$,
   - (c) $\left\{\frac{\lambda}{(1-\lambda)^m}\omega_2^{\frac{n}{N}} \mid 0\le m\le\frac{k}{2}-1, \frac{N}{2}\le n\le N-1\right\}$.
2. *If k is odd, a basis of $H^0(X_{\Phi^0(N)},\mathcal{O}(\frac{N}{2}k\cdot 1))$ is given by the union of the following four sets of elements:*
   - (a) $\left\{\frac{1}{(1-\lambda)^m} \mid 0\le m\le\frac{k-1}{2}\right\}$,
   - (b) $\left\{\frac{\lambda}{(1-\lambda)^m}\omega_2^{\frac{n}{N}} \mid 1\le m\le\frac{k-1}{2}, 0<n<\frac{N}{2}\right\}$,
   - (c) $\left\{\frac{\lambda}{(1-\lambda)^m}\omega_2^{\frac{1}{2}} \mid 0\le m\le\frac{k-1}{2}\right\}$,
   - (d) $\left\{\frac{\lambda}{(1-\lambda)^m}\omega_2^{\frac{n}{N}} \mid 0\le m\le\frac{k-1}{2}-1, \frac{N}{2}<n\le N-1\right\}$.
3. *We have for $k>0$*

$$\dim M_k(\Phi^0(N)) = (k-1)(\frac{N}{2}-2)+2k.$$

In particular, $\dim M_1(\Phi^0(N)) = 2$.

Proof. The equations (5.1)–(5.3) and $m \geq 0$ imply that

$$0 \leq m \leq \frac{k}{2} - \frac{n}{N}, \tag{5.9}$$

$$\frac{n}{N} \leq l \leq m + \frac{2n}{N}. \tag{5.10}$$

Let

$$S_n = \left\{ \frac{\lambda^l \omega_2^{\frac{n}{N}}}{(1-\lambda)^m} \mid (l,m) \quad \text{satisfy} \quad (5.10) \quad \text{and} \quad (5.10) \right\}.$$

Then Lemmas 5.2 and 5.3 imply that

$$S = \bigcup_{n=0}^{N-1} S_n$$

generates the vector space $H^0(X_{\Phi^0(N)}, \mathcal{O}(\frac{N}{2}k \cdot 1))$. Let T_n be a maximal linearly independent subset of S_n. It follows from Lemma 4.2 that $T = \bigcup T_n$ is also linearly independent and thus a basis of $H^0(X_{\Phi^0(N)}, \mathcal{O}(\frac{N}{2}k \cdot 1))$. In the following, we try to find such a set T_n for each $0 \leq n \leq N-1$.

(**i**) Assume k is even. We divide this into three cases.

(1) $n = 0$, then $0 \leq m \leq \frac{k}{2}$ and $0 \leq l \leq m$. By Lemma 5.4,

$$\left\{ \frac{1}{(1-\lambda)^m} \mid 0 \leq m \leq \frac{k}{2} \right\}$$

is maximal linearly independent. There are $\frac{k}{2}+1$ linearly independent elements in this case.

(2) $0 < n < \frac{N}{2}$, then $0 \leq m \leq \frac{k}{2} - 1$ and $1 \leq l \leq m$. By Lemma 5.4,

$$\left\{ \frac{\lambda \omega_2^{\frac{n}{N}}}{(1-\lambda)^m} \mid 1 \leq m \leq \frac{k}{2} - 1 \right\}$$

is maximal linearly independent for each fixed n. There is a total of $(\frac{k}{2}-1)(\frac{N}{2}-1)$ linearly independent elements in this case.

(3) $\frac{N}{2} \leq n \leq N-1$, then $0 \leq m \leq \frac{k}{2} - 1$ and $1 \leq l \leq m+1$. By Lemma 5.4,

$$\left\{ \frac{\lambda \omega_2^{\frac{n}{N}}}{(1-\lambda)^m} \mid 0 \leq m \leq \frac{k}{2} - 1 \right\}$$

is maximal linearly independent for each fixed n. There is a total of $\frac{k}{2} \cdot \frac{N}{2}$ linearly independent elements in this case.

Putting the elements together, we have the basis in the theorem. Moreover,

$$\begin{aligned}\dim M_k(\Phi^0(N)) &= \frac{k}{2}+1+(\frac{k}{2}-1)(\frac{N}{2}-1)+\frac{k}{2}\cdot\frac{N}{2}\\ &= (k-1)(\frac{N}{2}-2)+2k.\end{aligned}$$

(**ii**) Assume that k is odd. We divide this into four cases.

(1) $n=0$, then $0\le m\le \frac{k-1}{2}$ and $0\le l\le m$. By Lemma 5.4,

$$\left\{\frac{1}{(1-\lambda)^m}\mid 0\le m\le\frac{k-1}{2}\right\}$$

is maximal linearly independent. There are $\frac{k-1}{2}+1$ linearly independent elements in this case.

(2) $0<n<\frac{N}{2}$, then $0\le m\le\frac{k-1}{2}$ and $1\le l\le m$. By Lemma 5.4,

$$\left\{\frac{\lambda\omega_2^{\frac{n}{N}}}{(1-\lambda)^m}\mid 1\le m\le\frac{k-1}{2}\right\}$$

is maximal linearly independent for each fixed n. There is a total of $\frac{k-1}{2}(\frac{N}{2}-1)$ linearly independent elements in this case.

(3) $n=\frac{N}{2}$, then $0\le m\le\frac{k-1}{2}$ and $1\le l\le m+1$. By Lemma 5.4,

$$\left\{\frac{\lambda\omega^{\frac{1}{2}}}{(1-\lambda)^m}\mid 0\le m\le\frac{k-1}{2}\right\}$$

is maximal linearly independent. There is a total of $\frac{k-1}{2}+1$ linearly independent elements in this case.

(4) $\frac{N}{2}<n\le N-1$, then $0\le m\le\frac{k-1}{2}-1$ and $1\le l\le m+1$. By Lemma 5.4,

$$\left\{\frac{\lambda\omega_2^{\frac{n}{N}}}{(1-\lambda)^m}\mid 0\le m\le\frac{k-1}{2}-1\right\}$$

is maximal linearly independent for each fixed n. There is a total of $\frac{k-1}{2}(\frac{N}{2}-1)$ linearly independent elements in this case.

Putting the elements together, we have the basis in the theorem. Moreover,

$$\begin{aligned}\dim M_k(\Phi^0(N)) &= \frac{k-1}{2}+1+\frac{k-1}{2}(\frac{N}{2}-1)+\frac{k-1}{2}+1+\frac{k-1}{2}(\frac{N}{2}-1)\\ &= (k-1)(\frac{N}{2}-2)+2k.\end{aligned}$$

□

Similarly we have the following theorem by replacing $\ge$ with $>$ in (5.1)–(5.3).

Theorem 5.6. *We have a basis $\{f_i\theta^k\}$ for the space $S_k(\Phi^0(N))$ $(4|N)$ of cusp forms of weight k for $\Phi^0(N)$, where $\{f_i\}$ is a basis for $H^0(X_{\Phi^0(N)},\mathcal{O}(-1\cdot 0+(\frac{N}{2}k-1)\cdot 1-1\cdot\frac{1}{2}-1\cdot\infty)$ given below.*

(1) *If k is even, a basis of $H^0(X_{\Phi^0(N)}, \mathcal{O}(-1\cdot 0 + (\frac{N}{2}k-1)\cdot 1 - 1\cdot\frac{1}{2} - 1\cdot\infty)$ is given by the union of the following three sets of elements:*
   (a) $\left\{\frac{1}{(1-\lambda)^m} \mid 2\le m\le \frac{k}{2}-1\right\}$,
   (b) $\left\{\frac{\lambda}{(1-\lambda)^m}\omega_2^{\frac{n}{N}} \mid 1\le m\le \frac{k}{2}-1, 0<n\le\frac{N}{2}\right\}$,
   (c) $\left\{\frac{\lambda}{(1-\lambda)^m}\omega_2^{\frac{n}{N}} \mid 0\le m\le \frac{k}{2}-1, \frac{N}{2}<n\le N-1\right\}$.

(2) *If k is odd, a basis of $H^0(X_{\Phi^0(N)}, \mathcal{O}(-1\cdot 0 + (\frac{N}{2}k-1)\cdot 1 - 1\cdot\frac{1}{2} - 1\cdot\infty)$ is given by the union of the following four sets of elements:*
   (a) $\left\{\frac{1}{(1-\lambda)^m} \mid 2\le m\le \frac{k-1}{2}\right\}$,
   (b) $\left\{\frac{\lambda}{(1-\lambda)^m}\omega_2^{\frac{n}{N}} \mid 1\le m\le \frac{k-1}{2}, 0<n<\frac{N}{2}\right\}$,
   (c) $\left\{\frac{\lambda}{(1-\lambda)^m}\omega_2^{\frac{1}{2}} \mid 1\le m\le \frac{k-3}{2}\right\}$,
   (d) $\left\{\frac{\lambda}{(1-\lambda)^m}\omega_2^{\frac{n}{N}} \mid 0\le m\le \frac{k-1}{2}-1, \frac{N}{2}<n\le N-1\right\}$.

In particular,

$$\dim S_k(\Phi^0(N)) = \begin{cases} 0 & \text{if } k=1,\\ \frac{N}{2}-1 & \text{if } k=2,\\ (k-1)(\frac{N}{2}-2)+2k-4 & \text{if } k>2.\end{cases}$$

Remark 5.7. By Theorem 3.1, the genus of $X_{\Phi^0(N)}$ is $\frac{N}{2}-1$ in the case where $4|N$. Note that in this case the four cusps of $X_{\Phi^0(N)}$ are all regular and there are no elliptic points for $\Phi^0(N)$ in this case. The formulas in Theorem 5.5 and 5.6 are the same as the general dimension formulas in [Shi94].

For $\delta = \begin{pmatrix} a & b\\ c & d\end{pmatrix} \in SL_2(\mathbb{Z})$ and $f(\tau)$ a modular form of weight k, we define the slash operator $f|\delta = (c\tau+d)^{-k} f(\delta\tau)$ as usual.

Proof of Theorem 1.4: Since $\Phi^0(N) \subset \Phi^0_{\pm\frac{N}{4}}(N)$, it follows that

$$S_1(\Phi^0_{\pm\frac{N}{4}}(N)) \subset S_1(\Phi^0(N)) \quad \text{and} \quad M_1(\Phi^0_{\pm\frac{N}{4}}(N)) \subset M_1(\Phi^0(N)).$$

Then it follows from from Theorem 5.6 that

$$S_1(\Phi^0(N)) = S_1(\Phi^0_{\pm\frac{N}{4}}(N)) = 0$$

.

By Theorem 5.5, we have

$$M_1(\Phi^0(N)) = \mathbb{C}\theta \oplus \mathbb{C}\lambda\omega_2^{\frac{1}{2}}\theta.$$

So $f = C_1\theta + C_2\lambda\omega_2^{\frac{1}{2}}\theta \in M_1(\Phi^0_{\pm\frac{N}{4}}(N))$ if and only if $f|(TB^{\pm\frac{N}{4}+1}) = f$. It can be checked ([Rad73, chapter 10]) that (our θ equals $(\theta_3(0,\tau))^2$ in [Rad73, chapter 10])

$$\theta|(TB^{\pm\frac{N}{4}+1}) = \theta|T,$$
$$(\lambda\omega_2^{\frac{1}{2}}\theta)|(TB^{\pm\frac{N}{4}+1}) = \epsilon(1-\lambda)\omega_2^{\frac{1}{2}}(\theta|T), \quad \epsilon = (-1)^{\frac{N}{4}}.$$

Recall the following product expansions of θ and $\theta|T$ from [Rad73, chapter 10]:

$$\theta = \prod_{n\geq 1}(1-q^n)^2(1+q^{n-\frac{1}{2}})^4, \tag{5.11}$$
$$\theta|T = \prod_{n\geq 1}(1-q^n)^2(1-q^{n-\frac{1}{2}})^4.$$

By (1.5), (4.1), and (5.11) we have

$$\theta|T = -\frac{1}{4}\lambda\omega_2^{\frac{1}{2}}\theta,$$
$$(1-\lambda)\omega_2^{\frac{1}{2}}(\theta|T) = -\frac{1}{4}\lambda(1-\lambda)\omega_2\theta = 4\theta.$$

So $f|(TB^{\pm\frac{N}{4}+1}) = f$ becomes

$$C_1\theta + C_2\lambda\omega_2^{\frac{1}{2}}\theta = -\frac{1}{4}C_1\lambda\omega_2^{\frac{1}{2}}\theta + \epsilon 4C_2\theta,$$

i.e.,

$$C_1 = 4\epsilon C_2 \quad \text{and} \quad C_2 = -\frac{1}{4}C_1.$$

When $\epsilon = 1$, we see that $C_1 = C_2 = 0$. When $\epsilon = -1$, we see that $C_1 = -4C_2$, and

$$\theta(\tau) - \frac{1}{4}(\lambda\omega_2^{\frac{1}{2}}\theta)(\tau) = \theta(\tau) + \theta(\tau+1) \in M_1(\Phi^0_{\pm\frac{N}{4}}(N)).$$

This proves Theorem 1.4.

6. Cuspidal divisor class groups

In this section, we study and determine the divisor class groups $\mathrm{CL}(\Phi^0(N))$ and $\mathrm{CL}(\Phi^0_s(N))$ defined in the introduction. In particular, we prove that they are finite. Let us first consider the group $\Phi^0(N)$. We may assume that N is even as the odd case is trivial. Let

$$h_1 = \lambda\omega_2^{\frac{1}{2}} + 4 \quad \text{and} \quad h_2 = -(1-\lambda)\omega_2^{\frac{1}{2}} + 4, \tag{6.1}$$
$$h_3 = -\lambda\omega_2^{\frac{1}{2}} + 4 \quad \text{and} \quad h_4 = (1-\lambda)\omega_2^{\frac{1}{2}} + 4.$$

Lemma 6.1. *The functions h_i are in $\mathscr{F}^\infty$ for $i = 1, 2, 3, 4$. In fact, we have the following table:*

TABLE 2. Orders of h_i

	0	1	∞	$\frac{1}{2}$
h_1	0	$-\frac{N}{2}$	$\frac{N}{2}$	0
h_2	$-\frac{N}{2}$	0	$\frac{N}{2}$	0
h_3	0	$-\frac{N}{2}$	0	$\frac{N}{2}$
h_4	$-\frac{N}{2}$	0	0	$\frac{N}{2}$

Proof. It is easy to see that T exchanges h_1 and h_2, h_3 and h_4 while B exchanges h_1 and h_3, h_2 and h_4. So it suffices to check the lemma for h_1. Clearly, since $h_1(0) = 4$, we have $\text{order}_0 h_1 = 0$. It is also clear that $\text{order}_1 h_1 = -\frac{N}{2}$. It is easy to check using (1.2) and (1.5) that

$$h_1 = 32q^{\frac{1}{2}} + ...,$$

and we find that $\text{order}_\infty h_1 = \frac{N}{2}$. On the other hand, $\lambda\omega_2^{\frac{1}{2}} \circ B = -\lambda\omega_2^{\frac{1}{2}}$, and thus $h_1(\frac{1}{2}) = 8 \neq 0$. So the behavior of h_1 at the cusps is given as in Table 2. Furthermore, it is clear that h_1 has no poles in the open modular curve $X^0_{\Phi^0(N)}$, and $\deg \text{Div}(h_1) = 0$. Therefore h_1 has no zeros in the open modular curve $X^0_{\Phi^0(N)}$ either. So $h_1 \in \mathscr{F}^\infty$. □

By Lemma 6.1, we know that h_i has no zeros and no poles in the upper half plane. So for each positive integer $c > 1$, there is a c-th root function $h_i^{\frac{1}{c}} = e^{\frac{1}{c}\log h_i}$ which is holomorphic in the upper half plane. Here by (1.2) and (1.5), $\log h_i$ has the expansion near the infinity as follows :

$$\begin{aligned}
\log(h_1) &= \log 32 + \pi i\tau + \log(1 + a_2 q + a_3 q^{\frac{3}{2}} + \cdots),\\
\log(h_2) &= \pi i + \log 32 + \pi i\tau + \log(1 + b_2 q + b_3 q^{\frac{3}{2}} + \cdots),\\
\log(h_3) &= \log 8 + \log(1 + c_1 q^{\frac{1}{2}} + c_2 q + c_3 q^{\frac{3}{2}} + \cdots),\\
\log(h_4) &= \log 8 + \log(1 + d_1 q^{\frac{1}{2}} + d_2 q + d_3 q^{\frac{3}{2}} + \cdots),
\end{aligned}$$

the log that appears on the right hand side is given by the Taylor series (convergent when $\text{Im}(\tau) \gg 0$). By definition, we have the following transforming relations:

$$\begin{aligned}
T \circ h_1^{\frac{1}{c}} = h_2^{\frac{1}{c}} \quad \text{and} \quad T \circ h_2^{\frac{1}{c}} = \zeta_c h_1^{\frac{1}{c}},\\
T \circ h_3^{\frac{1}{c}} = h_4^{\frac{1}{c}} \quad \text{and} \quad T \circ h_4^{\frac{1}{c}} = h_3^{\frac{1}{c}},
\end{aligned}$$

and

$$\begin{aligned}
B \circ h_1^{\frac{1}{c}} = c_1 h_3^{\frac{1}{c}} \quad \text{and} \quad B \circ h_3^{\frac{1}{c}} = c_2 h_1^{\frac{1}{c}},\\
B \circ h_2^{\frac{1}{c}} = c_3 h_4^{\frac{1}{c}} \quad \text{and} \quad B \circ h_4^{\frac{1}{c}} = c_4 h_3^{\frac{1}{c}}.
\end{aligned}$$

for some constants c_1, c_2, c_3, and c_4. Evaluating the above equations at the cusps ∞ and $\frac{1}{2}$, we get $c_1 = \zeta_{2c}^{-1}$, $c_2 = 1$, $c_3 = \zeta_{2c}^{-1}$, and $c_4 = 1$. For example, since $B\infty = -\frac{1}{2}$,

$$B \circ \log h_1(\infty) = \log h_1(-\frac{1}{2}) = -\pi i + \log h_1(\frac{1}{2}).$$

On the other hand, it is easy to see that $\log h_3(\infty) = \log h_1(\frac{1}{2})$. So $B \circ h_1^{\frac{1}{c}}(\infty) = \zeta_{2c}^{-1} h_3^{\frac{1}{c}}(\infty)$, and therefore $c_1 = \zeta_{2c}^{-1}$.

Lemma 6.2. *Assume that N is even. Then all of the modular functions on $X_{\Phi^0(N)}$ with divisors supporting at cusps are products of integral powers of λ, $h_1 = \lambda\omega_2^{\frac{1}{2}} + 4$, and $\omega_2^{\frac{1}{N}}$.*

Proof. Notice that the divisors of λ, h_1, and ω_2 span a rank three lattice in $\mathscr{D}^\infty$, which is itself a free abelian group of rank three (as $X_{\Phi^0(N)}$ has four cusps). So $\mathrm{CL}(\Phi^0(N))$ is a finite abelian group. In particular, every f in $\mathscr{F}^\infty$ can be written as a product $f = (\lambda^a h_1^b \omega_2^d)^{\frac{1}{c}}$ for some integers a, b, c, and d with $c \geq 1$. Writing

$$x = \lambda^{\frac{1}{c}}, \quad y = (1-\lambda)^{\frac{1}{c}}, \quad \text{and} \quad z = \omega_2^{\frac{1}{c}}.$$

It follows from [Roh76, Pages 12-13] that

$$T \circ x = y, \quad T \circ y = \zeta_c^{-1} x, \quad \text{and} \quad T \circ z = \zeta_c z,$$
$$B \circ x = \zeta_c x, \quad B \circ y = y, \quad \text{and} \quad B \circ z = \zeta_c^{-1} z.$$

Now it is easy to check

$$T^{-1}B^{-1}TB \circ f = \zeta_c^a f, \quad T^{-1}BTB^{-1} \circ f = \zeta_c^{-a} f, \quad \text{and} \quad B^{-1}TBT^{-1} \circ f = \zeta_c^{-a-b} f.$$

This implies that $a \equiv b \equiv 0 \pmod{c}$. Now it is easy to see that $\frac{d}{c}$ is an element of $\frac{1}{N}\mathbb{Z}$, and this proves the lemma. □

Theorem 6.3. *We have*

$$\mathrm{CL}(\Phi^0(N)) = \begin{cases} 0 & \text{if } N \text{ is odd,} \\ (\mathbb{Z}/\frac{N}{2}\mathbb{Z})^2 & \text{if } N \text{ is even.} \end{cases}$$

Proof. If N is odd, then $X_{\Phi^0(N)}$ has genus zero and $\mathrm{CL}(\Phi^0(N))$ is automatically trivial. Directly, $X_{\Phi^0(N)}$ has two cusps $\{0, \infty\}$ and the divisor of $\omega_2^{\frac{1}{N}}$ is $\infty - 0$.

If N is even, then there are four cusps $\{0, 1, \infty, \frac{1}{2}\}$. We identify for convenience

$$\mathscr{D}^\infty \cong \{x = (x_i) \in \mathbb{Z}^4 : \sum x_i = 0\}$$

and

$$x_1 \cdot 0 + x_2 \cdot 1 + x_3 \cdot \infty + x_4 \cdot \frac{1}{2} \mapsto (x_1, x_2, x_3, x_4).$$

Then the divisors of λ, $\lambda\omega_2^{\frac{1}{2}} + 4$, and $\omega_2^{\frac{1}{N}}$ are $a = (N, 0, -\frac{N}{2}, -\frac{N}{2})$, $b = (0, -\frac{N}{2}, \frac{N}{2}, 0)$, and $c = (-1, -1, 1, 1)$, respectively. By Lemma 6.2, it follows that $\mathscr{F}^\infty$ is generated by a, b and c. Let $a' = a + \frac{N}{2}$. Then it is easy to see that

$$\mathrm{CL}(\Phi^0(N)) \cong (\mathbb{Z}/\frac{N}{2}\mathbb{Z})^2$$

is generated by $\frac{2}{N}a'$ and $\frac{2}{N}b$. □

For the groups $\Phi_s^0(N)$, the number of cusps is listed in Lemma 3.3.

Theorem 6.4. *We have*

$$\mathrm{CL}(\Phi_s^0(N)) = \begin{cases} 0 & \text{if } N|s, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } N|2s, N\nmid s, \text{and } N\equiv 0 \mod 4, \\ \mathbb{Z}/4\mathbb{Z} & \text{if } N|4s, N\nmid 2s \text{ and } N\equiv 0 \mod 8, . \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z} & \text{if } N|2s, N\nmid s, \text{and } N\equiv 2 \mod 4, \\ \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z} & \text{if } N|4s, N\nmid 2s \text{ and } N\equiv 4 \mod 8. \end{cases}$$

Proof. We briefly verify the case where $N|2s, N\nmid s$, and $N\equiv 2 \mod 4$, and we leave the other cases to the reader. Recall that $\mathbb{C}(X_{\Phi_s^0(N)}) = \mathbb{C}(\omega_2^{\frac{2}{N}}, (1-2\lambda)\omega_2^{\frac{1}{N}})$ by Theorem 4.3. However $(1-2\lambda)\omega_2^{\frac{1}{N}}$ is not in $\mathscr{F}^\infty$ as it has zeros in the upper-half plane. On the other hand, we have Table 3 above. Combining this table with argument in Theorem 6.3, we can show that $(1-2\lambda)\omega_2^{\frac{1}{2}}-8$ is in $\mathscr{F}^\infty$, and that $\mathscr{F}^\infty$ is generated by $\omega_2^{\frac{2}{N}}$ and $(1-2\lambda)\omega_2^{\frac{1}{2}}-8$. This verifies the special case. We leave the details to the reader. □

Table 3. Orders of functions at cusps

	0	∞	$\frac{1}{2}$
$\omega_2^{\frac{2}{N}}$	-4	2	2
$(1-2\lambda)\omega_2^{\frac{1}{2}}-8$	$-N$	N	0

We note that in the case where $N|4s, N\nmid 2s$ and $N\equiv 4 \mod 8$, one set of generators of $\mathscr{F}^\infty$ is $\{\omega_2^{\frac{4}{N}}, (1-2\lambda)\omega_2^{\frac{1}{2}}-8\}$.

References

[Dri73] V. G. Drinfel′d. Two theorems on modular curves. *Funkcional. Anal. i Priložen.*, 7(2):83–84, 1973.

[DS74] P. Deligne and J.-P. Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530 (1975), 1974.

[Duk95] W. Duke. The dimension of the space of cusp forms of weight one. *Internat. Math. Res. Notices*, (2):99–109, 1995.

[Fri86] R. Fricke. Ueber die substitutionsgruppen, welche zu den aus dem legendre'schesn integralmodul $k^2(\omega)$ gezogenen wurzeln gehören. *Math. Ann.*, 28:99–118, 1886.

[Gee99] A. Gee. Class invariants by Shimura's reciprocity law. *J. Théor. Nombres Bordeaux*, 11(1):45–72, 1999. Les XXèmes Journées Arithmétiques (Limoges, 1997).

[GR78] B. H. Gross and D. E. Rohrlich. Some results on the Mordell-Weil group of the Jacobian of the Fermat curve. *Invent. Math.*, 44(3):201–224, 1978.

[Man72] Ju. I. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.

[Rad73] H. Rademacher. *Topics in analytic number theory*. Springer-Verlag, New York-Heidelberg, 1973. Edited by E. Grosswald, J. Lehner and M. Newman, Die Grundlehren der mathematischen Wissenschaften, Band 169.

[Roh76] D. E. Rohrlich. *Modular functions and the Fermat curves*. ProQuest LLC, Ann Arbor, MI, 1976. Thesis (Ph.D.)–Yale University.

[Roh77] D. E. Rohrlich. Points at infinity on the Fermat curves. *Invent. Math.*, 39(2):95–127, 1977.

[Ser77] J.-P. Serre. Modular forms of weight one and Galois representations. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 193–268. Academic Press, London, 1977.

[Shi94] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Yan96] T. H. Yang. Cusp forms of weight 1 associated to Fermat curves. *Duke Math. J.*, 83(1):141–156, 1996.

[YZ97] N. Yui and D. Zagier. On the singular values of Weber modular functions. *Math. Comp.*, 66(220):1645–1662, 1997.

Department of Mathematics, University of Wisconsin Madison, Van Vleck Hall, Madison, WI 53706, USA

E-mail address: thyang@math.wisc.edu

School of Mathematics, Shandong University, Jinan 250100, P.R.China

E-mail address: yhb2004@mail.sdu.edu.cn