Equations associated to Principal Congruence Subgroups of Level Ten or less, or Twelve

Takashi Niwa

Introduction

The purpose of this paper is to find equations associated to given compact Riemann surfaces. Though all compact Riemann surfaces are obtained by algebraic equations, it is very difficult to give concrete equations for compact Riemann surfaces. Kuribayashi showed in [Ku] that if a compact Riemann surface X has an automorphism τ such that the genus of $X/\langle\tau\rangle$ is zero, an equation of X is given by the following formula

$$y^p = \prod_{i=1}^{r}(x-a_i)^{m_i}.$$

Here, p is the order of the automorphism τ and r is given by the number of branched points of the natural projection $X \to X/\langle\tau\rangle$. We consider this formula in §1 and call it a "semi-hyperelliptic curve". Girondo and Gonzâlez-Diez [GG] give the values of the exponents m_i for prime number p by considering the rotation number of the automorphism τ. Using their idea, we obtain the values of the exponents m_i for all natural numbers p. We also obtain some conditions of a_i.

In §2, we consider the compactification of $\mathbb{H}/\Gamma_q$, where

$$\Gamma_q = \left\{ \begin{pmatrix} qa+1 & qb \\ qc & qd+1 \end{pmatrix} \in SL\,(2,\mathbb{Z}) \mid a,b,c,d \in \mathbb{Z} \right\}$$

is the principal congruence subgroup of level $q \in \mathbb{N}$. We denote these compact Riemann surfaces by X_q. It is well known that X_7 is the Klein's quartic [Kl]. We see that there is an automorphism τ of X_q such that the genus of $X_q/\langle\tau\rangle$ is zero, for $q \leq 10$ or $q = 12$.

In §3, we consider equations of X_q. We remark that the equations are known. For $q \leq 5$, equations of X_q is $y = 0$ since the genus of X_q is zero so that X_q is isomorphic to the Riemann sphere. An equation of X_6 is an elliptic curve

$$y^2 = x^3 - 1$$

since X_6 has an automorphism of order 3 with fixed points. The Klein's quartic X_7 is given by the classical equation

$$y^7 = x(x-1)^2.$$

Furthermore, equations for prime numbers q are given in [II], and Ishida gives equations for all natural numbers q in [Is]. They consider a family of modular functions

$$X_r(\tau) = \exp\left(2\pi\sqrt{-1}\cdot\frac{(r-1)(q-1)}{4q}\right)\prod_{s=0}^{q-1}\frac{K_{r,s}(\tau)}{K_{1,s}(\tau)}$$

for $r \in \mathbb{Z}$ which aren't divided by q. Here, $K_{u,v}(\tau)$ is Klein forms of level q which defined by the following infinite product expansion

$$K_{u,v}(\tau) = \exp\left(\pi\sqrt{-1}v(u-1)\right) q'^{\frac{u(u-1)}{2}}(1-q'') \prod_{n=1}^{\infty} \left(1-q'^n q''\right)\left(1-q'^n q''^{-1}\right)\left(1-q'^n\right)^{-2},$$

where $q' = \exp\left(2\pi\sqrt{-1}\tau\right)$ and $q'' = \exp\left(2\pi\sqrt{-1}(u\tau+v)\right)$. They show that $X_3(\tau)$ is integral over $\mathbb{Q}\left[X_2(\tau)^{\varepsilon_q}\right]$, where ε_q is 1 or 2 according to whether q is odd or even and then, get equations of X_q. Recently, Yang gives another way to get the equations in [Ya] by generalizing Dedekind η-functions. Then we give a new approach to get equations of X_q for $q \leq 10$ or $q = 12$, which are semi-hyperelliptic curves. The advantage of our way is that it is resolved in a more simplyer way. By using a method of §1, we give equations of these X_q except for values of constant numbers a_i. It is done by computing rotation numbers of parallel displacement.

In §4, we get an equation of X_8 completely including constant numbers a_i. The equation is

$$y^8 = x^2(x-1)(x+1).$$

We determine a_i from the automorphism group of X_8 agree with the one of the compact Riemann surface defined by an equation which we get in §3. We consider automorphisms in the projective space because it is difficult to consider them on algebraic curves in $\mathbb{C}^2$.

1 Properties of semi-hyperelliptic curves

We recall that a relation between algebraic functions and compact Riemann surfaces. Let

$$F(x,y) = \sum_{i=0}^{p} a_i(x) \cdot y^i \in \mathbb{C}[x,y]$$

be an irreducible polynomial. If $p \geq 1$, there exists a compact Riemann surface X_F which contains the connected Riemann surface

$$\left\{ (x,y) \in \mathbb{C}^2 \,|\, F(x,y) = 0, F_y(x,y) \neq 0, a_p(x) \neq 0 \right\}, \tag{1.1}$$

which is an open Riemann surface with finitely many complementary points. The first projection $(x,y) \mapsto x$ is a holomorphic function and admits a holomorphic extension $X_F \to \hat{\mathbb{C}}$. X_F is uniquely determined by $F(x,y)$ up to conformal maps. Conversely, all compact Riemann surface X has an irreducible polynomial $F(x,y)$ such that X_F is isomorphic to X. It is shown by considering the meromorphic function field. Let $\mathcal{M}(X)$ be the meromorphic function field of X. $\mathcal{M}(X)$ is an algebraic function field of one variable. In other words, there exists an element $f \in \mathcal{M}(X) \setminus \mathbb{C}$ such that the extension $\mathbb{C}(f) \subset \mathcal{M}(X)$ is finite. It is known that

$$[\mathcal{M}(X) : \mathbb{C}(f)] = \deg(f)$$

and if $g \in \mathcal{M}(X)$ is injective on the generic fiber of f, we get $\mathcal{M}(X) = \mathbb{C}(f,g)$. There is an irreducible polynomial $F(x,y)$ such that $F\left(f(x), g(x)\right) \equiv 0$ on X. X is isomorphic to X_F by extension of

$$X \ni x \mapsto \left(f(x), g(x)\right) \in X_F.$$

Our purpose is to find such irreducible polynomials concretely to given especial compact Riemann surfaces. Let ζ_p be a primitive p-th root of unity. The following proposition motivates us to the main theorem of this paper.

Proposition 1.1. *Let X be a compact Riemann surface which has an automorphism τ of order p such that the genus of $X/\langle\tau\rangle$ is zero. Then an equation of X is given by a semi-hyperelliptic curve*

$$y^p = \prod_{i=1}^{r}(x-a_i)^{m_i} \tag{1.2}$$

and τ corresponds to $(x,y)\mapsto(x,\zeta_p y)$ on this semi-hyperelliptic curve.

Proof. Let τ^* be an automorphism on $\mathcal{M}(X)$ defined by $\tau^*(f)=f\circ\tau$. Since

$$\mathcal{M}(X)^{\langle\tau^*\rangle} = \{\, f\in\mathcal{M}(X)\,|\,\tau^*(f)=f\,\}$$

is isomorphic to $\mathcal{M}(X/\langle\tau\rangle)$, there is a meromorphic function $\mathbf{x}\in\mathcal{M}(X)$ such that $\mathcal{M}(X)^{\langle\tau^*\rangle}=\mathbb{C}(\mathbf{x})$. One can easily see that the degree of $\mathbf{x}$ is p and then $[\mathcal{M}(X):\mathbb{C}(\mathbf{x})]=p<\infty$. We regard the automorphism τ^* as an endomorphism of the vector space $\mathcal{M}(X)$ over the field $\mathbb{C}(\mathbf{x})$. We claim that the minimal polynomial of τ^* is $t^p-1\in\mathbb{C}(\mathbf{x})[t]$. Since $(\tau^*)^p=\mathrm{id}$, it suffices to show the minimality of the degree. We assume that

$$a_0(\mathbf{x})+a_1(\mathbf{x})\,\tau^*+\cdots+a_{p-1}(\mathbf{x})(\tau^*)^{p-1}=0\,, \tag{1.3}$$

where $a_0(\mathbf{x}),\cdots,a_{p-1}(\mathbf{x})\in\mathbb{C}(\mathbf{x})$. We should show $a_l(\mathbf{x})\equiv 0$ for all $l=0,\cdots,p-1$. We take a point $P\in X$ such that P, $\tau(P)$, $\cdots$, $\tau^{p-1}(P)$ differ from each other and $a_l(\mathbf{x})(P)$ is finite for all l. We also take meromorphic functions f_j for $j=1,\cdots,p$ such that $f_j\left(\tau^l(P)\right)=j^l$. The reason of the existence of f_j is shown by the next theorem. For a proof, see [Fr] for example.

Theorem 1.2. *Let X be a compact Riemann surface and $S\subset X$ be a finite subset. Assume that for each $s\in S$ a complex number $a_s\in\mathbb{C}$ is given. Then there is a meromorphic function $f\in\mathcal{M}(X)$ such that $f(s)=a_s$ for all $s\in S$.*

By substituting $f_j(P)$ for (1.3), we have

$$a_0(\mathbf{x})(P)+a_1(\mathbf{x})(P)\cdot j+\cdots+a_{p-1}(\mathbf{x})(P)\cdot j^{p-1}=0.$$

This means that at most $(p-1)$-th degree polynomial has p distinct solution, then we have $a_l(\mathbf{x})(P)=0$. Since this argument is held for all such points $P\in X$, we have $a_l(\mathbf{x})\equiv 0$. Therefore, the minimal polynomial of τ^* is t^p-1.

By Cayley-Hamilton theorem, ζ_p is an eigenvalue of τ^*. We take an eigenvector $\mathbf{y}\in\mathcal{M}(X)$, that is, $\tau^*(\mathbf{y})=\zeta_p\mathbf{y}$. By $\tau^*(\mathbf{y}^p)=\mathbf{y}^p$, we get $\mathbf{y}^p=\dfrac{a(\mathbf{x})}{b(\mathbf{x})}\in\mathbb{C}(\mathbf{x})$. Replacing $\mathbf{y}$ with $\dfrac{\mathbf{y}}{b(\mathbf{x})}$, we can assume $\mathbf{y}^p$ is an element of $\mathbb{C}[\mathbf{x}]$. We can also assume $\mathbf{y}^p$ is a monic polynomial in $\mathbf{x}$ by replacing $\mathbf{y}$ with $c\mathbf{y}$ for a suitable non-zero constant c. Furthermore, since $\mathbf{y}$ is injective on the generic fiber of $\mathbf{x}$, we have $\mathcal{M}(X)=\mathbb{C}(\mathbf{x},\mathbf{y})$. Then we conclude that an equation of X is given by the semi-hyperelliptic curve (1.2).

We finally check the behavior of τ on this semi-hyperelliptic curve. Let

$$\Phi : X\ni P\longmapsto(\mathbf{x}(P),\,\mathbf{y}(P))\in\{\,\text{The compact Riemann surface given by (1.2)}\,\}$$

be an isomorphism and $(x, y) = (\mathbf{x}(P), \mathbf{y}(P))$. By

$$\begin{aligned}\Phi \circ \tau \circ \Phi^{-1}(x, y) &= \Phi \circ \tau(P) \\ &= (\mathbf{x} \circ \tau(P), \mathbf{y} \circ \tau(P)) \\ &= (\mathbf{x}(P), \zeta_p \mathbf{y}(P)) \\ &= (x, \zeta_p y)\end{aligned}$$

we have that τ corresponds to $(x, y) \mapsto (x, \zeta_p y)$. □

Remark 1.3. *The irreducibility of*

$$y^p - \prod_{i=1}^{r}(x - a_i)$$

is shown by the behavior of τ on the semi-hyperelliptic curve. If it is a reducible polynomial, the map $(x, y) \mapsto (x, \zeta_p y)$ is not defined on a compact Riemann surface defined by $y^{p'} = \prod_{i=1}^{r'}(x - a'_i)$, here $p' < p$.

By repeating the replacement of y to $(x - a_i)y$, we can assume $1 \leq m_i < p$. Our next goal is to determine r, m_i and a_i in the definition of a semi-hyperelliptic curve. To do this, we have to consider some properties of a semi-hyperelliptic curve. Let X be a compact Riemann surface defined by (1.2) and we see that how X is done its compactification. By (1.1), X is obtained by the compactification of

$$\left\{ (x, y) \in \mathbb{C}^2 \,|\, y^p = \prod_{i=1}^{r}(x - a_i)^{m_i}, y \neq 0 \right\} \tag{1.4}$$

and thus, points which are related to $(a_i, 0)$ and infinity points are added. To see that how to add points to the curve (1.4) by compactification, we shall define a chart φ_P around each point P.

Let $\gcd(a, b)$ be the greatest common divisor of a and b.

If $P = (a_i, 0)$, we consider

$$\varphi_P^{-1}(t) = \left(t^{\frac{p}{\gcd(p,m_i)}} + a_i,\ t^{\frac{m_i}{\gcd(p,m_i)}} \sqrt[p]{\prod_{k \neq i} \left(t^{\frac{p}{\gcd(p,m_i)}} + a_i - a_k \right)^{m_k}} \right)$$

defined in a small disc. Then the branch order of the first projection $X \ni (x, y) \mapsto x \in \hat{\mathbb{C}}$ at $(a_i, 0)$ is $\frac{p}{\gcd(p,m_i)}$. To be the degree of this projection is p, we have to add $\gcd(p, m_i)$ points $(a_{i,1}, 0), \cdots, (a_{i,\gcd(p,m_i)}, 0)$. We sometimes use simply notation $a_{i,l}$ instead of $(a_{i,l}, 0)$. We also use $(a_i, 0)$ if $\gcd(p, m_i) = 1$. We see the branch order of $\tau : (x, y) \mapsto (x, \zeta_p y)$ at $a_{i,l}$ is $\frac{p}{\gcd(p,m_i)}$ by considering the natural projection $X \to X/\langle\tau\rangle$.

If P is a infinity point, we also consider

$$\varphi_P^{-1}(t) = \begin{cases} \left(t^{-\frac{p}{\gcd(p,m)}},\ t^{-\frac{m}{\gcd(p,m)}} \sqrt[p]{\prod_{i=1}^{r} \left(1 - a_i t^{\frac{p}{\gcd(p,m)}} \right)^{m_i}} \right) & (\, 0 < |t| < \varepsilon \,) \\ \infty & (\, t = 0 \,) \ , \end{cases}$$

where m is $\sum_{i=1}^{r} m_i$. Since the branch order of the first projection at a infinity point is $\frac{p}{\gcd(p,m)}$, we also need to add $\gcd(p,m)$ points $\infty_1, \cdots, \infty_{\gcd(p,m)}$ and the branch order of τ at ∞_l is $\frac{p}{\gcd(p,m)}$. In particular, the infinity points are non-branched points of τ if and only if m is divided by p.

In Proposition 1.1, we take Ψ be an isomorphism from $X/\langle\tau\rangle$ to $\hat{\mathbb{C}}$ and let $Q_1, \cdots, Q_s \in X/\langle\tau\rangle$ be the branched values of the natural projection $X \to X/\langle\tau\rangle$. By composing Ψ with a Möbius transformation if necessary, we can assume $\Psi(Q_i)$ is contained in $\mathbb{C}$ for all i. By the next commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\text{The natural projection}} & X/\langle\tau\rangle \\ {\scriptstyle\Phi}\downarrow & & \downarrow{\scriptstyle\Psi} \\ X' & \xrightarrow[\text{The first projection}]{} & \hat{\mathbb{C}} \end{array}$$

where X' is the compactification of (1.4), we have

$$\Psi\left(\{Q_1, \cdots, Q_s\}\right) = \{a_1, \cdots, a_r\}\,.$$

Thus, we can assume $r = s, \Psi(Q_i) = a_i$ and the infinity points are non-branched points of τ. By the following facts, we obtain conditions about m_i. Under the assumption of Proposition 1.1, let $P_{1,1}, \cdots, P_{1,n_1}, \cdots, P_{r,1}, \cdots, P_{r,n_r}$ be the branched points of τ, where $P_{i,1}, \cdots, P_{i,n_i}$ are τ equivalent points. Namely, $\tau(P_{i,1}) = P_{i,2}, \tau(P_{i,2}) = P_{i,3}, \cdots, \tau(P_{i,n_i}) = P_{i,1}$. Then the Riemann surface X is given by

$$y^p = \prod_{i=1}^{r} \left(x - \Psi\left([P_{i,1}]\right)\right)^{m_i}$$

and the exponents m_i are satisfied with $\gcd(p, m_i) = n_i$ for all i and $\sum_{i=1}^{r} m_i$ is divided by p.

In order to completely determine m_i, we define the "rotation number" (cf. [GG]). Let X be a Riemann surface which has an automorphism τ of order p, and a point $P \in X$ be fixed. Take n to be the smallest natural number such that $\tau^n(P) = P$ and φ to be a τ-invariant chart around P centered at the origin. Then $\varphi \circ \tau^n \circ \varphi^{-1}$ is an automorphism of a small disk fixing the origin with order $\frac{p}{n}$. Hence, it is of the form

$$\varphi \circ \tau^n \circ \varphi^{-1}(t) = \zeta_{\frac{p}{n}}^{k} \cdot t\,. \tag{1.5}$$

Here, k is the integer with $0 \le k < \frac{p}{n}$. We call the pair of n and k a rotation number of τ at P, and we denote it by $\mathcal{R}_\tau(P) = \mathcal{R}(n,k)$.

Remark 1.4. *The number k is independent of the choice of the chart φ, and we see that $\mathcal{R}_\tau(P) = \mathcal{R}_\tau(P')$ if P and P' are τ equivalent.*

We often consider the rotation number at branched points of the natural projection $X \to X/\langle\tau\rangle$. Actually, we simply have $\mathcal{R}_\tau(P) = \mathcal{R}(p,0)$ if P is a non-branched point of this projection. On other hand, if P is a fixed point of τ, we have $n = 1$ and the rotation number's concept, for these points, is only the exponent k of (1.5).

For getting exponents m_i, we consider the rotation number at $a_{i,l}$ of a semi-hyperelliptic curve (1.2).

Lemma 1.5. *Let X be a semi-hyperelliptic curve and τ be an automorphism $(x,\, y) \mapsto (x,\, \zeta_p y)$ of X as before. Let k be a unique number satisfying $k \cdot \frac{m_i}{\gcd(p,m_i)} \equiv 1$ mod $\frac{p}{\gcd(p,m_i)}$ with $1 \leq k < \frac{p}{\gcd(p,m_i)}$. Then*

$$\mathcal{R}_\tau(a_{i,l}) = \mathcal{R}(\gcd(p, m_i), k).$$

Proof. The existence and uniqueness of k are shown by an elementary argument. Indeed, if a and b are coprime integers, the equation $ak + bl = 1$ has a unique number solution k with $1 \leq k < b$ for the suitable integer l.

It is clear that the smallest number n with $\tau^n(a_{i,l}) = a_{i,l}$ is $\gcd(p, m_i)$ since we add $\gcd(p, m_i)$ points $a_{i,1}, \cdots, a_{i,\gcd(p,m_i)}$ to (1.4). Then by

$$\begin{aligned}
&\varphi_{a_{i,l}} \circ \tau^{\gcd(p,m_i)} \circ \varphi_{a_{i,l}}^{-1}(t) \\
&= \left(\varphi_{a_{i,l}} \circ \tau^{\gcd(p,m_i)}\right) \left(\left(t^{\frac{p}{\gcd(p,m_i)}} + a_i,\, t^{\frac{m_i}{\gcd(p,m_i)}} \sqrt[p]{\prod_{k \neq i} \left(t^{\frac{p}{\gcd(p,m_i)}} + a_i - a_k \right)^{m_k}} \right) \right) \\
&= \varphi_{a_{i,l}} \left(t^{\frac{p}{\gcd(p,m_i)}} + a_i,\, \zeta_{\frac{p}{\gcd(p,m_i)}} \cdot t^{\frac{m_i}{\gcd(p,m_i)}} \sqrt[p]{\prod_{k \neq i} \left(t^{\frac{p}{\gcd(p,m_i)}} + a_i - a_k \right)^{m_k}} \right) \\
&= \zeta^k_{\frac{p}{\gcd(p,m_i)}} \cdot t \ ,
\end{aligned}$$

we have $\mathcal{R}_\tau(a_{i,l}) = \mathcal{R}(\gcd(p, m_i),\, k)$. □

From above results, we obtain the next theorem.

Theorem 1.6. *Let X be a compact Riemann surface which has an automorphism τ of order p such that the genus of $X/\langle\tau\rangle$ is zero. $P_{1,1}, \cdots, P_{1,n_1}, \cdots, P_{r,1}, \cdots, P_{r,n_r}$ are all branched points of τ, where $P_{i,1}, \cdots, P_{i,n_i}$ are τ equivalent points and the rotation numbers are given by $\mathcal{R}_\tau(a_{i,l}) = \mathcal{R}(n_i, k_i)$ for all i. If we take unique numbers m_i such that $n_i = \gcd(p, m_i)$ and $k_i \cdot \frac{m_i}{n_i} \equiv 1$ mod $\frac{p}{n_i}$ with $1 \leq m_i < p$, an equation of X is a semi-hyperelliptic curve given by*

$$y^p = \prod_{i=1}^{r} (x - a_i)^{m_i}$$

and τ corresponds to $(x, y) \mapsto (x, \zeta_p y)$. Furthermore, if we take an isomorphism Ψ from $X/\langle\tau\rangle$ to $\hat{\mathbb{C}}$, a_i is given by $\Psi([P_{i,1}])$.

The existence and uniqueness of m_i are shown by the same argument as in the proof of Lemma 1.5. Of course, $\sum_{i=1}^{r} m_i$ is divided by p in this case. Finally, we give a remark about normalization. By composing a suitable Möbius transformation to Ψ, we get a normalized equation of X, namely

$$y^p = x^{m_1}(x-1)^{m_2}(x-a_3')^{m_3} \cdots (x - a_{r-1}')^{m_{r-1}}.$$

Therefore, if $r \leq 3$, we immediately determine an equation completely, which corresponds to X_q for $q \leq 7$.

2 The genus of quotient compact Riemann surfaces of X_q

In this section, we see that there is an automorphism τ of X_q such that the genus of $X_q/\langle\tau\rangle$ is zero for $q \leq 10$ or $q = 12$.

Let $\hat{\mathbb{H}}$ be $\mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$, and we give a unique topology of $\hat{\mathbb{H}}$ such that it satisfies the following properties.

1) The topology induced by $\hat{\mathbb{H}}$ gives the usual topology on $\mathbb{H}$.
2) Elements of $SL(2,\mathbb{Z})$ acts continuously on $\hat{\mathbb{H}}$.
3) A subset of $\hat{\mathbb{H}}$ is a neighborhood of ∞ if and only if it contains a set $\{ z \in \mathbb{H} : \mathrm{Im}\, z > C \} \cup \{\infty\}$ for a positive number $C > 0$.

Since $X_q = \overline{\mathbb{H}/\Gamma_q}$ is isomorphic to $\hat{\mathbb{H}}/\Gamma_q$, we redefined X_q by $\hat{\mathbb{H}}/\Gamma_q$. We take an automorphism τ_n of X_q given by $[z] \mapsto [z+n]$, where n is a positive divisor of q. It is grad if the genus of $X_q/\langle\tau_n\rangle$ is zero.

Remark 2.1. *We naturally think that the genus of $X_q/\langle\tau\rangle$ decreases as the order of $\tau \in \mathrm{Aut}(X_q)$ increases* [1]*. The order of automorphisms of X_q is at most q for $q \geq 7$, and the remainder of q divided by 4 isn't 2 or q is divided by 3 (see Proposition A.3 in appendix). For example, $q = 7, 8, 9, 11, 12, 13, 15, \cdots$. The order of the automorphism $\tau_1 : [z] \mapsto [z+1]$ reaches the bound for these q. Thus, taking τ_n, especially τ_1, from automorphisms of X_q is reasonable.*

For getting the genus of $X_q/\langle\tau_n\rangle$, we define some notations first.

Notation 2.2. *For $\Gamma \subset SL(2,\mathbb{Z})$, we define $\tilde{\Gamma}$ by $\Gamma \cup -\Gamma$ and for $\hat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$, we define next notations.*

$$S_q := \hat{\mathbb{Q}}/\Gamma_q\,,\ h_q := \#S_q\,,\ R_q := \left[SL(2,\mathbb{Z}) : \tilde{\Gamma}_q\right]$$

Let X_q^n be $\hat{\mathbb{H}}/\Gamma_q^n$, which is isomorphic to $X_q/\langle\tau_n\rangle$, where

$$\Gamma_q^n := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \mid a \equiv d \equiv 1,\, c \equiv 0 \pmod{q},\, b \equiv 0 \pmod{n} \right\}.$$

We also define

$$S_q^n := \hat{\mathbb{Q}}/\Gamma_q^n\,,\ h_q^n := \#S_q^n\,,\ R_q^n := \left[SL(2,\mathbb{Z}) : \tilde{\Gamma}_q^n\right]\,.$$

We set g_q and g_q^n be the genera of X_q and X_q^n, respectively.

Finally, for a natural number $q \in \mathbb{N}$, let $\mathcal{P}(q)$ be the set consisting of all primes l which divides q. For example, $\mathcal{P}(12) = \{2, 3\}$.

The next theorem is well known. For a proof, see [Fr] or [Si] for example.

Theorem 2.3. *For $q \geq 3$, we have*

$$R_q = \frac{q^3}{2} \prod_{l \in \mathcal{P}(q)} \left(1 - \frac{1}{l^2}\right)\,,\ h_q = \frac{q^2}{2} \prod_{l \in \mathcal{P}(q)} \left(1 - \frac{1}{l^2}\right)\,,\ g_q = 1 + \frac{(q-6)q^2}{24} \prod_{l \in \mathcal{P}(q)} \left(1 - \frac{1}{l^2}\right)\,.$$

We remark that $R_q = \#PSL(2, \mathbb{Z}/q\mathbb{Z})$. Before getting g_q^n, we evaluate R_q^n and h_q^n. It is because we have $g_q^n = 1 - \frac{h_q^n}{2} + \frac{R_q^n}{12}$ if Γ_q^n acts freely on $\mathbb{H}$. Actually, Γ_q^n acts freely on $\mathbb{H}$ for $q \geq 4$.

[1] Of coures, there are opposite cases. For example, see table 7 in appendix.

Proposition 2.4. *For $q \geq 3$, we have*

$$R_q^n = \frac{nq^2}{2} \prod_{l \in \mathcal{P}(q)} \left(1 - \frac{1}{l^2}\right).$$

Proof. We get it by $\left[SL(2,\mathbb{Z}) : \tilde{\Gamma}_q\right] = \left[SL(2,\mathbb{Z}) : \tilde{\Gamma}_q^n\right] \cdot \left[\tilde{\Gamma}_q^n : \tilde{\Gamma}_q\right]$ and $\left[\tilde{\Gamma}_q^n : \tilde{\Gamma}_q\right] = \left[\Gamma_q^n : \Gamma_q\right] = \frac{q}{n}$. $\square$

Then we consider h_q^n. Let Γ be a subgroup of finite index of $SL(2,\mathbb{Z})$ and κ be an element of $\hat{\mathbb{Q}}$. We take $N \in SL(2,\mathbb{Z})$ such that $N(\infty) = \kappa$. Then there is a positive number R such that

$$\left\{ M \in N^{-1}\tilde{\Gamma}N \,|\, M(\infty) = \infty \right\} = \left\{ \pm \begin{pmatrix} 1 & mR \\ 0 & 1 \end{pmatrix} | \, m \in \mathbb{Z} \right\}.$$

We call R the width of κ and use the notation $\mathcal{W}_\Gamma(\kappa)$ [Fr].

Remark 2.5. *This definition is independent of the choice of N since if we take another N', it satisfies $N' = N\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ for some $b \in \mathbb{Z}$. Moreover, it depends only on the Γ-equivalence class. It is because if κ and κ' are satisfied $\gamma(\kappa) = \kappa'$ for some $\gamma \in \Gamma$, we have $\gamma N(\infty) = \kappa'$ and then $N^{-1}\tilde{\Gamma}N = (\gamma N)^{-1}\tilde{\Gamma}(\gamma N)$. Therefore, we can define the width of elements of $\hat{\mathbb{Q}}/\Gamma$ in a natural way and we use the same notation.*

Lemma 2.6. *Let Γ and Γ' be subgroups of finite index of $SL(2,\mathbb{Z})$ and each of them contains the negative unit matrix. Set Γ to be a subgroup of Γ' and p to be $[\Gamma' : \Gamma]$. Let us take an element from $\hat{\mathbb{Q}}/\Gamma'$ and let κ denote its representative. We consider the quotient of the stabilizer of κ in Γ' determined by Γ. Let $\kappa_1, \cdots, \kappa_h$ denote representatives of this quotient's elements. Then*

$$p \cdot \mathcal{W}_{\Gamma'}(\kappa) = \sum_{i=1}^{h} \mathcal{W}_\Gamma(\kappa_i).$$

Proof. Let $SL(2,\mathbb{Z})_\kappa$ and Γ'_κ be subgroups of $SL(2,\mathbb{Z})$ and Γ', respectively. Each of them fixes κ. Since $\mathcal{W}_{\Gamma'}(\kappa) = [SL(2,\mathbb{Z})_\kappa : \Gamma'_\kappa]$, we take $N_1, \cdots, N_{\mathcal{W}_{\Gamma'}(\kappa)}$ which are the set of left cosets of Γ'_κ in $SL(2,\mathbb{Z})_\kappa$. For $i = 1, \cdots, h$, let $SL(2,\mathbb{Z})_{\kappa_i}$ and Γ_{κ_i} be subgroups of $SL(2,\mathbb{Z})$ and Γ such that they fix κ_i, respectively. Since $\mathcal{W}_\Gamma(\kappa_i) = \left[SL(2,\mathbb{Z})_{\kappa_i} : \Gamma_{\kappa_i}\right]$, we also take $N_{i,1}, \cdots, N_{i,\mathcal{W}_\Gamma(\kappa_i)}$ which are the set of left cosets of Γ_{κ_i} in $SL(2,\mathbb{Z})_{\kappa_i}$. Then by letting $A_1, \cdots, A_p$ denote the set of left cosets of Γ in Γ' and $M, M_1, \cdots, M_h$ satisfy $M(\kappa) = M_1(\kappa_1) = \cdots = M_h(\kappa_h) = \infty$, we claim that

$$\bigoplus_{\mu,\,\nu} M N_\mu A_\nu \Gamma = \bigoplus_{i,j} M_i N_{i,j} \Gamma. \tag{2.1}$$

We prove (2.1) in several steps.

Step 1: $MN_\mu A_\nu \Gamma \cap MN_{\mu'} A_{\nu'} \Gamma = \phi$.
We assume $MN_\mu A_\nu \Gamma \cap MN_{\mu'} A_{\nu'} \Gamma \neq \phi$. We should show $\mu = \mu'$ and $\nu = \nu'$. There is $\gamma \in \Gamma$ such that

$$MN_\mu A_\nu = MN_{\mu'} A_{\nu'} \gamma \Leftrightarrow N_{\mu'}^{-1} N_\mu = A_{\nu'} \gamma A_\nu^{-1}.$$

Since $A_{\nu'} \gamma A_\nu^{-1} \in \Gamma'$, we get $N_{\mu'}^{-1} N_\mu \in \Gamma'_\kappa$ and so $\mu = \mu'$. We also get $\nu = \nu'$ by $A_\nu \Gamma \cap A_{\nu'} \Gamma \neq \phi$.

Step 2: $M_iN_{i,j}\Gamma \cap M_{i'}N_{i',j'}\Gamma = \phi$.
We assume $M_iN_{i,j}\Gamma \cap M_{i'}N_{i',j'}\Gamma \neq \phi$. We should show $i = i'$ and $j = j'$. There is $\gamma \in \Gamma$ such that

$$M_iN_{i,j} = M_{i'}N_{i',j'}\gamma \Leftrightarrow N_{i',j'}^{-1}M_{i'}^{-1}M_iN_{i,j} = \gamma\,.$$

Then we get

$$\gamma(\kappa_i) = N_{i',j'}^{-1}M_{i'}^{-1}M_iN_{i,j}(\kappa_i) = N_{i',j'}^{-1}M_{i'}^{-1}(\infty) = \kappa_{i'}$$

and so $i = i'$. Since $N_{i,j}\Gamma \cap N_{i,j'}\Gamma \neq \phi$, we also get $N_{i,j}\Gamma_{\kappa_i} \cap N_{i,j'}\Gamma_{\kappa_i} \neq \phi$ and so $j = j'$.
Step 3: The left-hand side is contained in the right-hand side.
It is sufficient to prove that $MN_\mu A_\nu$ is contained in the right-hand side. We take $\gamma \in \Gamma$ and i such that $A_\nu^{-1}(\kappa) = \gamma(\kappa_i)$. Since $M_i^{-1}MN_\mu A_\nu\gamma \in SL(2,\mathbb{Z})_{\kappa_i}$, there is j such that $M_i^{-1}MN_\mu A_\nu\gamma \in N_{i,j}\Gamma_{\kappa_i} \subset N_{i,j}\Gamma$. Then we have $MN_\mu A_\nu \in M_iN_{i,j}\Gamma$.
Step 4: The right-hand side is contained in the left-hand side.
It is sufficient to prove that $M_iN_{i,j}$ is contained in the left-hand side. We take $\gamma \in \Gamma$ such that $\gamma(\kappa) = \kappa_i$. Since $M^{-1}M_iN_{i,j}\gamma \in SL(2,\mathbb{Z})_\kappa$, there is μ such that $M^{-1}M_iN_{i,j}\gamma \in N_\mu\Gamma'_\kappa \subset N_\mu\Gamma'$. Then there is ν such that $M_iN_{i,j} \in MN_\mu A_\nu\Gamma$.

Thus, the equation (2.1) is shown and the proof is completed. □

In special case $\Gamma' = SL\,(2,\mathbb{Z})$, we get

Corollary 2.7. *Let Γ be a subgroup of finite index of $SL\,(2,\mathbb{Z})$. Then*

$$\left[SL\,(2,\mathbb{Z}) : \tilde{\Gamma}\right] = \sum_{\kappa\in\hat{\mathbb{Q}}/\Gamma} \mathcal{W}_\Gamma(\kappa)\,.$$

We then evaluate h_q^n by using a width.

Notation 2.8. *Let p be a natural number and $\prod_{i=1}^k p_i^{r_i}$ be the prime factorization of it. We define a multiplicative function $\mathcal{N}(p)$ by*

$$\mathcal{N}(p) := \prod_{i=1}^{k}\left(1 + r_i\cdot\frac{p_i-1}{p_i+1}\right)\,.$$

Here, we note that $\mathcal{N}(1)$ is 1.

Proposition 2.9. *For $q \geq 5$, we have*

$$h_q^n = \frac{nq\cdot\mathcal{N}\left(\frac{q}{n}\right)}{2}\prod_{l\in\mathcal{P}(q)}\left(1-\frac{1}{l^2}\right)\,.$$

Proof. Let p be $\frac{q}{n}$. We split the proof into several steps.
Step 1: We describe by $\frac{x}{z}$ a representative of $\kappa \in S_q^n$, where x and z are coprime integers. We claim that

$$\mathcal{W}_{\Gamma_q^n}(\kappa) = \frac{q}{\gcd(p,z)}\,.$$

Here, we note that ∞ is $\frac{1}{0}$ and $\gcd(p,0)$ is defined to be p.

Let k be $\gcd(p,z)$ and p', z' are coprime integers such that $p = kp', z = kz'$. We take $N = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$ and consider elements of $N^{-1}\Gamma_q^n N$ such that ∞ is fixed. By

$$\begin{pmatrix} w & -y \\ -z & x \end{pmatrix} \begin{pmatrix} -qxz'R+1 & np'x^2R \\ -qzz'R & qxz'R+1 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & np'R \\ 0 & 1 \end{pmatrix}$$

we have $\mathcal{W}_{\Gamma_q^n}(\kappa) \leq np'$. Then we should show $\mathcal{W}_{\Gamma_q^n}(\kappa) \geq np'$.

We consider all the elements in $N^{-1}\Gamma_q^n N$ which fix ∞. Since

$$\begin{pmatrix} w & -y \\ -z & x \end{pmatrix} \begin{pmatrix} 1 & nb \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} \equiv \begin{pmatrix} nzwb+1 & nw^2b \\ -nz^2b & -nzwb+1 \end{pmatrix} \pmod{q}, \tag{2.2}$$

we see that $nzwb$ is a multiple of q, that is, wb is divided by p'. If not, $nzwb \equiv -2 \equiv 2$ in modular q by diagonal components of (2.2). It is a contradiction with $q \geq 5$. Thus, by (1,2) component of (2.2), we have $\mathcal{W}_{\Gamma_q^n}(\kappa) \geq np'$.

Remark 2.10. *The condition $q \geq 5$ in Proposition 2.9 is owing to Step 1. Indeed, we have*

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^{-1} \begin{pmatrix} -4m+1 & 2m \\ -8m & 4m+1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2m \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^{-1} \begin{pmatrix} -4m-1 & 2m+1 \\ -8m-4 & 4m+3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2m+1 \\ 0 & 1 \end{pmatrix}.$$

Thus, we obtain

$$\left\{ M \in \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^{-1} \tilde{\Gamma}_4^1 \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \mid M(\infty) = \infty \right\} = \left\{ \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \mid m \in \mathbb{Z} \right\}.$$

This implies $\mathcal{W}_{\Gamma_4^1}\left(\frac{1}{2}\right) = 1 \neq 2 = \frac{4}{\gcd(4,2)}$.

Step 2: Let $\prod_{i=1}^k p_i^{r_i}$ be the prime factorization of p. For p and $0 \leq j_i \leq r_i$, we define

$$\mathcal{N}_1(j_i) = \mathcal{N}_1(p, p_i^{j_i}) := \begin{cases} 1 & (\, j_i = 0\,) \\ (p_i+1)p_i^{j_i-1} & (\, 1 \leq j_i \leq r_i\,). \end{cases}$$

We claim that the number of elements of S_q such that the denominators of their representative is divided by $\prod_{i=1}^k p_i^{j_i}$ is

$$\frac{h_q}{\prod_{i=1}^k \mathcal{N}_1(j_i)}.$$

Let H_m be the subgroup of $SL(2,\mathbb{Z})$ such that these (2,1) entries are dividid by natural number m. It is sufficient to prove that

$$\left[SL(2,\mathbb{Z}) : H_{\prod_{i=1}^k p_i^{j_i}} \right] = \prod_{i=1}^k \mathcal{N}_1(j_i).$$

We get it by

$$SL\,(2,\mathbb{Z}) = H_{p_1} \oplus \left(\bigoplus_{l=0}^{p_1-1} \begin{pmatrix} l & -1 \\ 1 & 0 \end{pmatrix} H_{p_1} \right), \quad H_{p_1} = \bigoplus_{l=0}^{p_1^{j_1-1}-1} \begin{pmatrix} 1 & 0 \\ lp_1 & 1 \end{pmatrix} H_{p_1^{j_1}}$$

and so on.

Step 3: For p, we define

$$\mathcal{N}_2(j_i) = \mathcal{N}_2(p, p_i^{j_i}) := \begin{cases} \frac{p_i}{p_i+1} & (\, j_i = 0\,) \\ \frac{(p_i-1)p_i^{j_i}}{p_i+1} & (\, 1 \le j_i \le r_i - 1\,) \\ \frac{p_i^{r_i+1}}{p_i+1} & (\, j_i = r_i\,)\,. \end{cases}$$

Let A, whose width of its element with respect to Γ_q^n [2] is $n\prod_{i=1}^k p_i^{j_i}$, be the subset of S_q. We claim that

$$\#A = \frac{h_q}{p} \prod_{i=1}^{k} \mathcal{N}_2(j_i)\,.$$

For elements of A, by Step 1, the denominators of representatives are divided by $\prod_{i=1}^k p_i^{r_i-j_i}$ and are not divided by $p_s^{r_s-j_s+1}\prod_{i\neq s} p_i^{r_i-j_i}$ for all $s = s_1, \cdots, s_\mu$ and for positive j_s. By Step 2, we get

$$\begin{aligned} \#A &= \frac{h_q}{\prod_{i=1}^k \mathcal{N}_1(r_i-j_i)} - \sum_{s_\nu} \frac{h_q}{\mathcal{N}_1(r_s-j_s+1)\prod_{i\neq s}\mathcal{N}_1(r_i-j_i)} \\ &\quad + \sum_{s_\nu,\, s_{\nu'}} \frac{h_q}{\mathcal{N}_1(r_{s_1}-j_{s_1}+1)\mathcal{N}_1(r_{s_2}-j_{s_2}+1)\prod_{i\neq s_1,s_2}\mathcal{N}_1(r_i-j_i)} \\ &\quad - \cdots + (-1)^\mu \sum_{s_1,\ldots,s_\mu} \frac{h_q}{\prod_{\nu=1}^\mu \mathcal{N}_1(r_{s_\nu}-j_{s_\nu}+1)\cdot\prod_{i\neq s_1,\cdots,s_\mu}\mathcal{N}_1(r_i-j_i)} \\ &= \frac{h_q}{p}\prod_{i=1}^k \mathcal{N}_2(j_i)\,. \end{aligned} \tag{2.3}$$

The last equality is showed as follows. We assume that $n\prod_{i=1}^k p_i^{j_i} = np_{h+1}^{j_{h+1}}\cdots p_{h+l}^{j_{h+l}}\cdot p_{h+l+1}^{r_{h+l+1}}\cdots p_k^{r_k}$ and $1 \le j_{h+t} < r_{h+t}$ for all $t = 1, \cdots, l$.

$$\begin{aligned} &\#A \\ &= \frac{h_q}{(p_1+1)p_1^{r_1-1}\cdots(p_h+1)p_h^{r_h-1}(p_{h+1}+1)p_{h+1}^{r_{h+1}-j_{h+1}-1}\cdots(p_{h+l}+1)p_{h+l}^{r_{h+l}-j_{h+l}-1}} \\ &\quad - \frac{h_q}{(p_1+1)p_1^{r_1-1}\cdots(p_h+1)p_h^{r_h-1}(p_{h+1}+1)p_{h+1}^{r_{h+1}-i_{h+1}}(p_{h+2}+1)p_{h+2}^{r_{h+2}-j_{h+2}-1}\cdots(p_{h+l}+1)p_{h+l}^{r_{h+l}-j_{h+l}-1}} \\ &\quad - \cdots - \frac{h_q}{(p_1+1)p_1^{r_1-1}\cdots(p_h+1)p_h^{r_h-1}(p_{h+1}+1)p_{h+1}^{r_{h+1}-j_{h+1}-1}\cdots(p_{h+l-1}+1)p_{h+l-1}^{r_{h+l-1}-j_{h+l-1}-1}(p_{h+l}+1)p_{h+l}^{r_{h+l}-j_{h+l}}} \end{aligned}$$

[2] By taking a representative of elements of S_q, we may consider the its width with respect to Γ_q^n by a natural way.

$$
\begin{aligned}
&- \frac{h_q}{(p_1+1)p_1^{r_1-1}\cdots(p_h+1)p_h^{r_h-1}(p_{h+1}+1)p_{h+1}^{r_{h+1}-j_{h+1}-1}\cdots(p_{h+l}+1)p_{h+l}^{r_{h+l}-j_{h+l}-1}(p_{h+l+1}+1)} \\
&- \cdots - \frac{h_q}{(p_1+1)p_1^{r_1-1}\cdots(p_h+1)p_h^{r_h-1}(p_{h+1}+1)p_{h+1}^{r_{h+1}-j_{h+1}-1}\cdots(p_{h+l}+1)p_{h+l}^{r_{h+l}-j_{h+l}-1}(p_k+1)} \\
&+ \cdots \\
&+ (-1)^{k-h}\frac{h_q}{(p_1+1)p_1^{r_1-1}\cdots(p_h+1)p_h^{r_h-1}(p_{h+1}+1)p_{h+1}^{r_{h+1}-j_{h+1}}\cdots(p_{h+l}+1)p_{h+l}^{r_{h+l}-j_{h+l}}(p_{h+l+1}+1)\cdots(p_k+1)}
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{h_q}{p}\cdot\frac{p_1\cdots p_h\, p_{h+1}^{j_{h+1}+1}\cdots p_{h+l}^{j_{h+l}+1}\, p_{h+l+1}^{r_{h+l+1}}\cdots p_k^{r_k}}{(p_1+1)\cdots(p_{h+l}+1)} - \frac{h_q}{p}\cdot\frac{p_1\cdots p_h\, p_{h+1}^{j_{h+1}}p_{h+2}^{j_{h+2}+1}\cdots p_{h+l}^{j_{h+l}+1}\, p_{h+l+1}^{r_{h+l+1}}\cdots p_k^{r_k}}{(p_1+1)\cdots(p_{h+l}+1)} \\
&\quad - \cdots - \frac{h_q}{p}\cdot\frac{p_1\cdots p_h\, p_{h+1}^{j_{h+1}+1}\cdots p_{h+l-1}^{j_{h+l-1}+1}p_{h+l}^{j_{h+l}}\, p_{h+l+1}^{r_{h+l+1}}\cdots p_k^{r_k}}{(p_1+1)\cdots(p_{h+l}+1)} \\
&\quad - \frac{h_q}{p}\cdot\frac{p_1\cdots p_h\, p_{h+1}^{j_{h+1}+1}\cdots p_{h+l}^{j_{h+l}+1}\, p_{h+l+1}^{r_{h+l+1}}\cdots p_k^{r_k}}{(p_1+1)\cdots(p_{h+l}+1)(p_{h+l+1}+1)} - \cdots - \frac{h_q}{p}\cdot\frac{p_1\cdots p_h\, p_{h+1}^{j_{h+1}+1}\cdots p_{h+l}^{j_{h+l}+1}\, p_{h+l+1}^{r_{h+l+1}}\cdots p_k^{r_k}}{(p_1+1)\cdots(p_{h+l}+1)(p_k+1)} \\
&\quad + \cdots \\
&\quad + (-1)^{k-h}\frac{h_q}{p}\cdot\frac{p_1\cdots p_h\, p_{h+1}^{j_{h+1}}\cdots p_{h+l}^{j_{h+l}}\, p_{h+l+1}^{r_{h+l+1}}\cdots p_k^{r_k}}{(p_1+1)\cdots(p_k+1)}
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{h_q}{p}\cdot\frac{p_1\cdots p_h\, p_{h+1}^{j_{h+1}}\cdots p_{h+l}^{j_{h+l}}\, p_{h+l+1}^{r_{h+l+1}}\cdots p_k^{r_k}}{(p_1+1)\cdots(p_k+1)}\cdot\big\{\, p_{h+1}\cdots p_{h+l}\,(p_{h+l+1}+1)\cdots(p_k+1) \\
&\quad - p_{h+2}\cdots p_{h+l}\,(p_{h+l+1}+1)\cdots(p_k+1) - \cdots - p_{h+1}\cdots p_{h+l-1}\,(p_{h+l+1}+1)\cdots(p_k+1) \\
&\quad - p_{h+1}\cdots p_{h+l}\,(p_{h+l+2}+1)\cdots(p_k+1) - \cdots - p_{h+1}\cdots p_{h+l}\,(p_{h+l+1}+1)\cdots(p_{k-1}+1) \\
&\quad + \cdots + (-1)^{k-h}\,\big\} \\
&= \frac{h_q}{p}\cdot\frac{p_1\cdots p_h\, p_{h+1}^{j_{h+1}}\cdots p_{h+l}^{j_{h+l}}\, p_{h+l+1}^{r_{h+l+1}}\cdots p_k^{r_k}}{(p_1+1)\cdots(p_k+1)}\cdot(p_{h+1}-1)\cdots(p_{h+l}-1)\cdot(p_{h+l+1}+1-1)\cdots(p_k+1-1) \\
&= \frac{h_q}{p}\prod_{i=1}^{k}\mathcal{N}_2(j_i)
\end{aligned}
$$

Example 2.11. *Let q be a semiprime number p_1p_2. We consider elements of $S_{p_1p_2}$ such that their width is p_1p_2 with respect to $\Gamma^1_{p_1p_2}$. By Step 1, the width of $\kappa = \left[\frac{x}{z}\right] \in S_{p_1p_2}$ is p_1p_2 with respect to $\Gamma^1_{p_1p_2}$ if and only if $\gcd(p_1p_2, z) = 1$. The denominator z is not divided p_1 and p_2. By Step 2 and the following calculation, we count the number of such κ:*

$$
\begin{aligned}
&h_{p_1p_2} - \frac{h_{p_1p_2}}{\mathcal{N}_1(p_1p_2, p_1)} - \frac{h_{p_1p_2}}{\mathcal{N}_1(p_1p_2, p_2)} + \frac{h_{p_1p_2}}{\mathcal{N}_1(p_1p_2, p_1)\cdot\mathcal{N}_1(p_1p_2, p_2)} \\
=&h_{p_1p_2} - \frac{h_{p_1p_2}}{p_1+1} - \frac{h_{p_1p_2}}{p_2+1} + \frac{h_{p_1p_2}}{(p_1+1)(p_2+1)} \\
=&\frac{h_{p_1p_2}\cdot p_1p_2}{(p_1+1)(p_2+1)}
\end{aligned}
$$

$$= \frac{h_{p_1p_2}}{p_1p_2} \mathcal{N}_2(p_1p_2, p_1) \cdot \mathcal{N}_2(p_1p_2, p_2).$$

This equation is corresponding to (2.3) in Step 3.

Step 4: For p, we define

$$\mathcal{N}_3(j_i) = \mathcal{N}_3(p, p_i^{j_i}) := \begin{cases} \frac{p_i}{p_i+1} & (\, j_i = 0,\, r_i\,) \\ \frac{p_i-1}{p_i+1} & (\, 1 \le j_i \le r_i - 1\,)\,. \end{cases}$$

Let B, whose width of its element is $n\prod_{i=1}^{k} p_i^{j_i}$, be the subset of S_q^n. We claim that

$$\#B = \frac{h_q}{p} \prod_{i=1}^{k} \mathcal{N}_3(j_i)\,.$$

It is shown by Lemma 2.6. Indeed, we have

$$p \cdot n \prod_{i=1}^{k} p_i^{j_i} \cdot \#B = q \cdot \#A \;\Leftrightarrow\; \#B = \frac{h_q}{p} \prod_{i=1}^{k} \mathcal{N}_3(j_i)\,.$$

Step 5: In this final step, we claim that

$$h_q^n = \sum_{j_1,\cdots,j_k} \frac{h_q}{p} \prod_{i=1}^{k} \mathcal{N}_3(j_i) = \frac{nq \cdot \mathcal{N}(p)}{2} \prod_{l \in \mathcal{P}(q)} \left(1 - \frac{1}{l^2}\right)$$

and complete the proof.

It is sufficient to prove that

$$\sum_{j_1,\cdots,j_k} \prod_{i=1}^{k} \mathcal{N}_3(j_i) = \mathcal{N}(p)$$

and we show it by induction on k. For $k = 1$, we get

$$\begin{aligned} \sum_{j=0}^{r} \mathcal{N}_3(j) &= 2 \cdot \frac{p}{p+1} + (r-1) \cdot \frac{p-1}{p+1} \\ &= 1 + r \cdot \frac{p-1}{p+1} \\ &= \mathcal{N}(p)\ . \end{aligned}$$

We assume that the claim is held for $k-1$. Then we have

$$\begin{aligned}\sum_{j_1,\cdots,j_k}\prod_{i=1}^{k}\mathcal{N}_3(j_i) &= \sum_{j_k=0}^{r_k}\left(\sum_{j_1,\cdots,j_{k-1}}\prod_{i=1}^{k-1}\mathcal{N}_3(j_i)\right)\cdot\mathcal{N}_3(j_k)\\ &= \sum_{j_k=0}^{r_k}\mathcal{N}\left(\prod_{i=1}^{k-1}p_i^{r_i}\right)\cdot\mathcal{N}_3(j_k)\\ &= \mathcal{N}\left(\prod_{i=1}^{k-1}p_i^{r_i}\right)\cdot\mathcal{N}(p_k^{r_k})\\ &= \mathcal{N}(p)\end{aligned}$$

and the proof. □

We recall that $g_q^n = 1-\frac{h_q^n}{2}+\frac{R_q^n}{12}$ and then we obtain the next theorem and table 1.

Theorem 2.12. *For $q\geq 5$, we have*

$$g_q^n = 1+\frac{\left(q-6\mathcal{N}\left(\frac{q}{n}\right)\right)nq}{24}\prod_{l\in\mathcal{P}(q)}\left(1-\frac{1}{l^2}\right).$$

q	$1\sim 5$	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	$\cdots$
g_q	0	1	3	5	10	13	26	25	50	49	73	81	133	109	196	169	$\cdots$
g_q^1	0	0	0	0	0	0	1	0	2	1	1	2	5	2	7	3	$\cdots$

Table 1: Genera of X_q and X_q^1

By considering whether $q-6\mathcal{N}(q)$ is negative or by table 1, we have the next corollary .

Corollary 2.13. *For $q\leq 10$ or $q=12$, X_q has an automorphisms τ such that the genus of $X_q/\langle\tau\rangle$ is zero. In particular, X_q is a semi-hyperelliptic curve.*

The next section, we find equations of X_q except for constant numbers by using Theorem 1.6 for these q.

3 Equations of X_q

We consider rotation numbers of the automorphism $\tau_n : X_q \ni [z]\mapsto [z+n]\in X_q$. Since Γ_q^n acts freely on $\mathbb{H}$ for $q\geq 4$, it is sufficient to evaluate rotation numbers at only elements of S_q.

Lemma 3.1. *Let n be a divisor of $q\geq 5$ and $p=\frac{q}{n}$. We describe by $\frac{x}{z}$ a representative of $\kappa\in S_q$, where x and z are coprime integers. We take integers y and w such that $xw-yz=1$. Furthermore, let k be the remainder of w^2 divided by $\gcd(p,z)$. Then the rotation number at κ of τ_n is*

$$\mathcal{R}_{\tau_n}(\kappa) = \mathcal{R}\left(\frac{p}{\gcd(p,z)},k\right).$$

Proof. The width of Γ_q is always q since Γ_q is a normal subgroup of $SL(2,\mathbb{Z})$. By Lemma 2.6, the smallest number m such that $\tau_n^m(\kappa) = \kappa$ satisfied with $p \cdot \mathcal{W}_{\Gamma_q^n}(\kappa) = m \cdot q$. By Step 1 of Proposition 2.9, we have $m = \frac{p}{\gcd(p,z)}$.

We recall that elements of $SL(2,\mathbb{Z})$ acts continuously on $\hat{\mathbb{H}}$ and it is easy to be calculated the rotation number of parallel displacement at infinity points. If $\mathcal{W}_\Gamma(\infty) = R$ for a subgroup $\Gamma \subset SL(2,\mathbb{Z})$,

$$\varphi_{[\infty]}(t) = \begin{cases} \exp\left(\frac{2\pi i t}{R}\right) & (\operatorname{Im} t > C) \\ 0 & (t = \infty) \end{cases}$$

is a chart around the infinity point $[\infty] \in \hat{\mathbb{H}}/\Gamma$. We take $\left(\begin{smallmatrix} w & -y \\ -z & x \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$ which maps $\frac{x}{z}$ to ∞. By easy computation, we have

$$\begin{pmatrix} w & -y \\ -z & x \end{pmatrix} \left(\frac{x}{z} + \varepsilon \right) = \frac{1 + \varepsilon z w}{-\varepsilon z^2}$$

$$\begin{pmatrix} w & -y \\ -z & x \end{pmatrix} \left(\frac{x}{z} + \varepsilon + mn \right) = \frac{1 + \varepsilon z w + mnzw}{-\varepsilon z^2 - mnz^2}$$

and

$$\begin{pmatrix} mnzw + 1 & mnw^2 \\ -mnz^2 & -mnzw + 1 \end{pmatrix} \left(\frac{1 + \varepsilon z w}{-\varepsilon z^2} \right) = \frac{1 + \varepsilon z w + mnzw}{-\varepsilon z^2 - mnz^2}. \tag{3.1}$$

Since $mnz = \frac{qz}{\gcd(p,z)}$ is a multiple of q, the matrix of (3.1) is equal to

$$\begin{pmatrix} 1 & mnw^2 \\ 0 & 1 \end{pmatrix}$$

in modular q. Then the rotation number is given by the remainder of $mnw^2 \div mn = w^2$ divided by $p \div m = \gcd(p,z)$. □

For $q \leq 10$ or $q = 12$, everything to find an equation of X_q except for values of constant numbers is ready now. We first consider X_8.

Since the denominators of the representatives of the branched points of the natural projection $X_8 \to X_8^1$ is not coprime to 8, the branched points of it are $[\infty]$, $\left[\frac{3}{8}\right]$, $\left[\frac{1}{4}\right]$, $\left[\frac{3}{4}\right]$, $\left[\frac{1}{2}\right]$, $\left[\frac{3}{2}\right]$, $\left[\frac{5}{2}\right]$ and $\left[\frac{7}{2}\right]$. Here $\left[\frac{1}{4}\right]$, $\left[\frac{3}{4}\right]$ are τ_1 equivalent. $\left[\frac{1}{2}\right]$, $\left[\frac{3}{2}\right]$, $\left[\frac{5}{2}\right]$, $\left[\frac{7}{2}\right]$ are also τ_1 equivalent. By Theorem 1.6 and Lemma 3.1, we get table 2 and

$$y^8 = (x - a_1)(x - a_2)(x - a_3)^2(x - a_4)^4$$

which gives an equation of X_8. Here, n, k are rotation numbers, and m is an exponent of an equation about X_8. By normalizing, we have

$$y^8 = x^2(x - 1)(x - a). \tag{3.2}$$

Theorem 3.2. *An equation of X_8 is given by*

$$y^8 = x^2(x - 1)(x + 1). \tag{3.3}$$

$\frac{x}{z}$	n	$xw-yz=1$	example of w^2	$\gcd(8,z)$	k	conditions of m	m
$\frac{1}{0}$	1	$w=1$	1	8	1	$1=\gcd(8,m)$ and $m\equiv 1 \bmod 8$	1
$\frac{3}{8}$	1	$3w-8z=1$	9	8	1	$1=\gcd(8,m)$ and $m\equiv 1 \bmod 8$	1
$\frac{1}{4}$	2	$w-4z=1$	1	4	1	$2=\gcd(8,m)$ and $\frac{m}{2}\equiv 1 \bmod 4$	2
$\frac{1}{2}$	4	$w-2y=1$	1	2	1	$4=\gcd(8,m)$ and $\frac{m}{4}\equiv 1 \bmod 2$	4

Table 2: Rotation numbers and exponents about X_8

We give the proof of Theorem 3.2 in §4.

Remark 3.3. *The compact Riemann surface defined by*

$$y^4 = x(x-1)(x+1)(x^2+1)^2 \tag{3.4}$$

is isomorphic to the compact Riemann surface defined by (3.3)*. An isomorphism is given by*

$$\begin{array}{ccc} \{y^8 = x^2(x-1)(x+1)\} & \longrightarrow & \{y^4 = x(x-1)(x+1)(x^2+1)^2\} \\ (x,y) & \longmapsto & \left(\dfrac{\zeta^4 y^4}{x(x+1)}, \dfrac{\sqrt[4]{8}y}{\zeta(x+1)}\right) \\ \left(-\dfrac{x^2-1}{x^2+1}, \dfrac{\sqrt[4]{2}\zeta y}{x^2+1}\right) & \longmapsto & (x,y) \quad , \end{array}$$

where $\zeta = \zeta_{16}$*. Therefore, the equation* (3.4) *also gives* X_8*. The form* $y^4 = f(x)$ *corresponds to* $g_8^2 = 0$*.*

Remark 3.4. *By table 3, table 4 and table 5, we also have equations of* X_9*,* X_{10} *and* X_{12}*. They are given by*

$$\begin{aligned} y^9 &= x(x-1)^3(x-p_1)^3(x-p_2)^4 \\ y^{10} &= x(x-1)^2(x-q_1)^5(x-q_2)^5(x-q_3)^8 \\ y^{12} &= x(x-1)^2(x-r_1)^3(x-r_2)^3(x-r_3)^4(x-r_4)^4(x-r_5)^6. \end{aligned}$$

[Ya] gives these equations completely. We see that his equation of X_9 *is different from our one. These equations are given by*

$$\begin{aligned} y^6 &= x(x^3+1)y^3 + x^5(x^3+1)^2 \\ y^{10} &= x(x+1)^2(x-1)^8(x^2+x-1)^5 \\ y^{12} &= x(x-1)^2(x+1)^6(x^2+1)^4(x^2-x+1)^3. \end{aligned}$$

Of course, the sums of the column of m in these tables are multiple of each q since the infinity points are non-branched points before normalization. We also obtain an equation of X_q for $q \leq 7$ by the same way. In particular, it means that it gives other way to get the classical equation $y^7 = x(x-1)^2$ of the Klein's quartic X_7.

$\frac{x}{z}$	n	$xw-yz=1$	example of w^2	$\gcd(9,z)$	k	conditions of m	m
$\frac{1}{0}$	1	$w=1$	1	9	1	$1=\gcd(9,m)$ and $m\equiv 1 \bmod 9$	1
$\frac{2}{9}$	1	$2w-9z=1$	25	9	7	$1=\gcd(9,m)$ and $7m\equiv 1 \bmod 9$	4
$\frac{4}{9}$	1	$4w-9z=1$	4	9	4	$1=\gcd(9,m)$ and $4m\equiv 1 \bmod 9$	7
$\frac{1}{3}$	3	$w-3y=1$	1	3	1	$3=\gcd(9,m)$ and $\frac{m}{3}\equiv 1 \bmod 3$	3
$\frac{2}{3}$	3	$2w-3y=1$	1	3	1	$3=\gcd(9,m)$ and $\frac{m}{3}\equiv 1 \bmod 3$	3

Table 3: Rotation numbers and exponents about X_9

$\frac{x}{z}$	n	$xw-yz=1$	example of w^2	$\gcd(10,z)$	k	conditions of m	m
$\frac{1}{0}$	1	$w=1$	1	10	1	$1=\gcd(10,m)$ and $m\equiv 1 \bmod 10$	1
$\frac{3}{10}$	1	$3w-10z=1$	9	10	9	$1=\gcd(10,m)$ and $9m\equiv 1 \bmod 10$	9
$\frac{1}{5}$	2	$w-5y=1$	1	5	1	$2=\gcd(10,m)$ and $\frac{m}{2}\equiv 1 \bmod 5$	2
$\frac{2}{5}$	2	$2w-5y=1$	4	5	4	$2=\gcd(10,m)$ and $4\frac{m}{2}\equiv 1 \bmod 5$	8
$\frac{1}{2}$	5	$w-2y=1$	1	2	1	$5=\gcd(10,m)$ and $\frac{m}{5}\equiv 1 \bmod 2$	5
$\frac{1}{4}$	5	$w-4y=1$	1	2	1	$5=\gcd(10,m)$ and $\frac{m}{5}\equiv 1 \bmod 2$	5

Table 4: Rotation numbers and exponents about X_{10}

$\frac{x}{z}$	n	$xw-yz=1$	example of w^2	$\gcd(12,z)$	k	conditions of m	m
$\frac{1}{0}$	1	$w=1$	1	12	1	$1=\gcd(12,m)$ and $m\equiv 1 \bmod 12$	1
$\frac{5}{12}$	1	$5w-12z=1$	25	12	1	$1=\gcd(12,m)$ and $m\equiv 1 \bmod 12$	1
$\frac{1}{6}$	2	$w-6z=1$	1	6	1	$2=\gcd(12,m)$ and $\frac{m}{2}\equiv 1 \bmod 6$	2
$\frac{1}{4}$	3	$w-4y=1$	1	4	1	$3=\gcd(12,m)$ and $\frac{m}{3}\equiv 1 \bmod 4$	3
$\frac{3}{4}$	3	$3w-4y=1$	1	4	1	$3=\gcd(12,m)$ and $\frac{m}{3}\equiv 1 \bmod 4$	3
$\frac{1}{3}$	4	$w-3y=1$	1	3	1	$4=\gcd(12,m)$ and $\frac{m}{4}\equiv 1 \bmod 3$	4
$\frac{2}{3}$	4	$2w-3y=1$	1	3	1	$4=\gcd(12,m)$ and $\frac{m}{4}\equiv 1 \bmod 3$	4
$\frac{1}{2}$	6	$w-2y=1$	1	2	1	$6=\gcd(12,m)$ and $\frac{m}{6}\equiv 1 \bmod 2$	6

Table 5: Rotation numbers and exponents about X_{12}

4 A canonical model of X_8 in the projective space

As we announced, in this section, we prove Theorem 3.2. Namely, we determine a constant number a of (3.2). Two points $(1,0)$ and $(a,0)$ on this algebraic curve are corresponding to $[\infty]$ and $\left[\frac{3}{8}\right]$ on $X_8=\hat{\mathbb{H}}/\Gamma_8$, respectively. Since there is an automorphism which $[\infty]$ maps $\left[\frac{3}{8}\right]$, for example $\left(\begin{smallmatrix}3 & 1\\ 8 & 3\end{smallmatrix}\right)$, we take an automorphism σ which satisfies $\sigma\left((1,0)\right)=(a,0)$. However, depending the value of a, the compact Riemann surface defined by (3.2) dosen't always have such automorphisms. We see that there is such σ if and only if $a=-1$ and thus, we determine a as -1.

To find automorphisms of (3.2), we consider a canonical model in the projective space because it is difficult to find automorphisms remains of two variables irreducible polynomials. The next lemma is fundamental and useful to look for the automorphisms (cf. [KK]).

Lemma 4.1. *Let X be a non-hyperelliptic compact Riemann surface of genus $g \geq 3$ and X' be a canonical model of X in the projective space $\mathbb{P}^{g-1}$. Then an automorphism σ of X is obtained as projective transformation of $\mathbb{P}^{g-1}$ restricted to X'.*

We see that X_8 is a non-hyperelliptic curve. If X_8 is a hyperelliptic curve, there is an automorphism with order 2 which lies in the center of $\mathrm{Aut}(X_8)$. By appendix, $\mathrm{Aut}(X_8)$ is isomorphic to $PSL\,(2, \mathbb{Z}/8\mathbb{Z})$. However, the center of $PSL\,(2, \mathbb{Z}/8\mathbb{Z})$ is trivial. It is a contradiction.

Since $g_8 = 5$, the projective space is $\mathbb{P}^4$. We should find a basis of holomorphic differentials of X_8 to get a canonical model. We set projections $\mathbf{x} : (x, y) \mapsto x$ and $\mathbf{y} : (x, y) \mapsto y$. By §1, we get table 6, here $l = 1, 2$ and $l' = 1, 2, 3, 4$, and a basis as

$$\left\langle \frac{1}{\mathbf{y}^3}d\mathbf{x}, \frac{\mathbf{x}}{\mathbf{y}^5}d\mathbf{x}, \frac{\mathbf{x}}{\mathbf{y}^6}d\mathbf{x}, \frac{\mathbf{x}(\mathbf{x}-1)}{\mathbf{y}^7}d\mathbf{x}, \frac{\mathbf{x}}{\mathbf{y}^7}d\mathbf{x} \right\rangle.$$

	$\mathbf{x}$	$\mathbf{x}-1$	$\mathbf{y}$	$d\mathbf{x}$	$\frac{1}{\mathbf{y}^3}d\mathbf{x}$	$\frac{\mathbf{x}}{\mathbf{y}^5}d\mathbf{x}$	$\frac{\mathbf{x}}{\mathbf{y}^6}d\mathbf{x}$	$\frac{\mathbf{x}(\mathbf{x}-1)}{\mathbf{y}^7}d\mathbf{x}$	$\frac{\mathbf{x}}{\mathbf{y}^7}d\mathbf{x}$
0_l	4	0	1	3	0	2	1	0	0
$(1,0)$	0	8	1	7	4	2	1	8	0
$(a,0)$	0	0	1	7	4	2	1	0	0
$\infty_{l'}$	-2	-2	-1	-3	0	0	1	0	2

Table 6: Orders of meromorphic functions and differentials

By three equations

$$\begin{aligned}
\left(\frac{x}{y^6}\right)^2 &= \frac{x}{y^5}\cdot\frac{x}{y^7} \\
\left(\frac{x}{y^5}\right)^2 &= \frac{1}{y^3}\left(\frac{x(x-1)}{y^7} + \frac{x}{y^7}\right) \\
\left(\frac{1}{y^3}\right)^2 &= \frac{x(x-1)}{y^7}\left(\frac{x(x-1)}{y^7} - (a-1)\cdot\frac{x}{y^7}\right),
\end{aligned}$$

we get a canonical model

$$\left\{[z_1, z_2, z_3, z_4, z_5] \in \mathbb{P}^4 \,|\, z_3^2 = z_2z_5, z_2^2 = z_1(z_4+z_5), z_1^2 = z_4\left(z_4 - (a-1)z_5\right)\right\}. \tag{4.1}$$

An isomorphism from the algebraic curve (3.2) is

$$\begin{aligned}
(x, y) &\mapsto \left[\frac{1}{y^3}, \frac{x}{y^5}, \frac{x}{y^6}, \frac{x(x-1)}{y^7}, \frac{x}{y^7}\right] \\
0_l &\mapsto [\pm\sqrt{a}, 0, 0, -1, 1] \\
(1,0) &\mapsto [0, 0, 0, 0, 1] \\
(a,0) &\mapsto [0, 0, 0, a-1, 1] \\
\infty_{l'} &\mapsto [1, \pm 1, 0, 1, 0], [1, \pm\sqrt{-1}, 0, -1, 0].
\end{aligned}$$

We define an automorphism $\sigma : [z_1, \cdots, z_5] \mapsto [z'_1, \cdots, z'_5]$ of (4.1) by

$$\begin{pmatrix} z'_1 \\ \vdots \\ z'_5 \end{pmatrix} = \begin{pmatrix} c_{1,1} & \cdots & c_{1,5} \\ \vdots & \ddots & \vdots \\ c_{5,1} & \cdots & c_{5,5} \end{pmatrix} \begin{pmatrix} z_1 \\ \vdots \\ z_5 \end{pmatrix}$$

and then we must have

$$z'^2_3 = z'_2 z'_5 \tag{4.2}$$
$$z'^2_2 = z'_1(z'_4 + z'_5) \tag{4.3}$$
$$z'^2_1 = z'_4\left(z'_4 - (a-1)z'_5\right). \tag{4.4}$$

We should consider the case of an automorphism σ maps $[0,0,0,0,1]$ to $[0,0,0,a-1,1]$ and so

$$\lambda \begin{pmatrix} 0 \\ 0 \\ 0 \\ a-1 \\ 1 \end{pmatrix} = \begin{pmatrix} c_{1,1} & \cdots & c_{1,5} \\ \vdots & \ddots & \vdots \\ c_{5,1} & \cdots & c_{5,5} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Here, λ is a non-zero constant. We may assume $\lambda = 1$ and then we have

$$c_{1,5} = c_{2,5} = c_{3,5} = 0, \quad c_{4,5} = a-1, \quad c_{5,5} = 1.$$

Lemma 4.2. *If an automorphism τ of X_8 satisfies $\tau([\infty]) = \left[\frac{3}{8}\right]$, we have*

$$\tau\left(\left[\frac{3}{8}\right]\right) = [\infty],$$
$$\tau\left(\left\{\left[\frac{1}{4}\right], \left[\frac{3}{4}\right]\right\}\right) = \left\{\left[\frac{1}{4}\right], \left[\frac{3}{4}\right]\right\},$$
$$\tau\left(\left\{\left[\frac{1}{2}\right], \left[\frac{3}{2}\right], \left[\frac{5}{2}\right], \left[\frac{7}{2}\right]\right\}\right) = \left\{\left[\frac{1}{2}\right], \left[\frac{3}{2}\right], \left[\frac{5}{2}\right], \left[\frac{7}{2}\right]\right\}.$$

Proof. We regard τ as a element of $PSL(2, \mathbb{Z}/8\mathbb{Z})$. Since $\tau([\infty]) = \left[\frac{3}{8}\right]$, τ is the form $\pm\left(\begin{smallmatrix} 3 & * \\ 0 & 3 \end{smallmatrix}\right)$ in modular 8. Then we have this claim by direct calculation. □

Since σ maps $[0,0,0,a-1,1]$ to $[0,0,0,0,1]$ and $a \neq 1$, we have

$$c_{1,4} = c_{2,4} = c_{3,4} = 0, \quad c_{4,4} = -1.$$

Since $\left[\frac{1}{2}\right]$ corresponding to $\infty_{l'}$ and so $[1, \pm 1, 0, 1, 0]$ or $[1, \pm\sqrt{-1}, 0, -1, 0]$, we get

$$c_{3,1} \pm c_{3,2} = 0$$
$$c_{5,1} \pm c_{5,2} + c_{5,4} = c_{5,1} \pm \sqrt{-1}c_{5,2} - c_{5,4} = 0.$$

and therefore, we have

$$c_{3,1} = c_{3,2} = c_{5,1} = c_{5,2} = c_{5,4} = 0.$$

By the behavior of the automorphism at $\left[\frac{1}{4}\right]$ corresponding to 0_l, we also have $c_{2,1} = 0$. Then (4.2) become to

$$\begin{aligned} & c_{3,3}^2 z_3^2 = (c_{2,2}z_2 + c_{2,3}z_3)(c_{5,3}z_3 + z_5) \\ \Leftrightarrow\ & (c_{3,3}^2 - c_{2,2} - c_{2,3}c_{5,3})z_3^2 = c_{2,2}c_{5,3}z_2z_3 + c_{2,3}z_3z_5 \end{aligned}$$

and thus, we have

$$c_{2,3} = 0, \quad c_{3,3}^2 = c_{2,2} \neq 0, \quad c_{5,3} = 0.$$

(4.3) become to

$$c_{2,2}^2 z_2^2 = (c_{1,1}z_1 + c_{1,2}z_2 + c_{1,3}z_3)\,(c_{4,1}z_1 + c_{4,2}z_2 + c_{4,3}z_3 - z_4 + az_5)\,.$$

By the coefficient of z_3z_5 and $a \neq 0$, we have $c_{1,3} = 0$ and then, by the coefficient of z_2z_5, we have $c_{1,2} = 0$. Thus, $c_{1,1} \neq 0$ and (4.3) is

$$(c_{1,1} + c_{2,2}^2)z_1z_4 = c_{1,1}c_{4,1}z_1^2 + c_{1,1}c_{4,2}z_1z_2 + c_{1,1}c_{4,3}z_1z_3 + (ac_{1,1} - c_{2,2}^2)z_1z_5.$$

We have

$$c_{4,1} = c_{4,2} = c_{4,3} = 0, \quad c_{1,1} = -c_{2,2}^2, \quad a = -1.$$

Therefore, the proof of Theorem 3.2 is completed.

We see the form of σ. Since we get $c_{1,1}^2 = 1$ by (4.4), the form of σ is

$$\begin{pmatrix} -\eta_1 & & & & & \\ & \eta_2 & & & & \\ & & \eta_3 & & & \\ & & & -1 & -2 & \\ & & & & 1 & \end{pmatrix}.$$

Here, $\eta_1^2 = 1, \eta_2^2 = \eta_1$ and $\eta_3^2 = \eta_2$. We remark that the number of such σ is 8 and it is equal to the number of the automorphisms of X_8 which maps $[\infty]$ to $\left[\frac{3}{8}\right]$. σ corresponding to $(x, y) \mapsto (-x, \eta_3 y)$ on the semi-hyperelliptic curve $y^8 = x^2(x-1)(x+1)$. We hope that we get equations of X_9, X_{10} and X_{12} completely by like way as X_8.

A Appendix

We note that $PSL(q)$ is $PSL\,(2, \mathbb{Z}/q\mathbb{Z})$. In this appendix, we see some properties of $\mathrm{Aut}(X_q)$, especially their orders. We first show $\mathrm{Aut}(X_q)$ is isomorphic to $PSL(q)$ for $q \geq 7$. Of course, the condition $q \geq 7$ is because of $g_q > 1$. The number of $PSL(q)$ is $R_q < \infty$. Since elements of $PSL(q)$ are regarded as elements of $\mathrm{Aut}(X_q)$, we may show $\#\mathrm{Aut}(X_q) \leq R_q$. We use Hurwitz theorem.

Theorem A.1. *Let X be a compact Riemann surface with genus $g > 1$ and $\{p_1, \cdots, p_n\}$ be a maximal set of fixed points of $\mathrm{Aut}(X)$ inequivalent under the action of $\mathrm{Aut}(X)$. We denote the number of the stabilizer of p_i in $\mathrm{Aut}(X)$ by m_i. Then we get*

$$2g - 2 = N\left(2\overline{g} - 2 + \sum_{i=1}^{n}\left(1 - \frac{1}{m_i}\right)\right) \tag{A.1}$$

where we have denoted $N = \#\mathrm{Aut}(X)$ and $\overline{g}$ is the genus of $X/\mathrm{Aut}(X)$.

In our case, by Theorem 2.3, we have $g = g_q = 1 + \frac{(q-6)q^2}{24}\prod_{l\in\mathcal{P}(q)}\left(1-\frac{1}{l^2}\right)$ and $\overline{g} = 0$. Since the number of the stabilizer of the infinity point in $\mathrm{Aut}(X_q)$ is at least q, we can assume $m_1 \geq q$. We also have $n = 3$. Indeed, if $n \leq 2$, we have $2g_q - 2 < N(-2+1+1) \Leftrightarrow g_q < 1$ by (A.1). On the other hand, if $n \geq 4$, (A.1) gives

$$\begin{aligned} 2g_q - 2 &\geq N\left(-2 + (n-1)\cdot\frac{1}{2} + 1 - \frac{1}{q}\right) > N\left(\frac{1}{6} - \frac{1}{q}\right) \\ \Rightarrow N &< \frac{q^3}{2}\prod_{l\in\mathcal{P}(q)}\left(1-\frac{1}{l^2}\right) = R_q\,. \end{aligned}$$

Then (A.1) is equivalent to

$$2g_q - 2 = N\left(1 - \frac{1}{m_1} - \frac{1}{m_2} - \frac{1}{m_3}\right) \tag{A.2}$$

in our case. We can assume $m_2 \geq 3$ since if $m_2 = m_3 = 2$, we get $g_q < 1$ by (A.2). Then (A.2) become to

$$2g_q - 2 \geq N\left(1 - \frac{1}{q} - \frac{1}{3} - \frac{1}{2}\right) \Leftrightarrow N \leq R_q$$

and so $N = R_q$. Therefore, $\mathrm{Aut}(X_q)$ is isomorphic to $PSL(q)$ for $q \geq 7$.

Next, we consider the largest order of elements of $\mathrm{Aut}(X_q)$. If the remainder of q divided by 4 is 2 and isn't divided by 3, we call q type I. Otherwise, we call q type II. For example, $q = 2, 10, 14, 20, \cdots$ are type I.

Lemma A.2. *If q is type I, the largest order of elements of $PSL(q)$ is $\frac{3}{2}q$. If q is type II, the largest order is q.*

Proof. Since the order of $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \in PSL(q)$ is q and the order of $\left(\begin{smallmatrix}p+1 & 1\\ p & 1\end{smallmatrix}\right) \in PSL(2p)$ is $3p$ for type I $q = 2p$, the existence is shown. We take $A \in PSL(q)$ and see that its order is at most $\frac{3}{2}q$ or q. We prove for each case of q.

Case 1: $q = p$ is prime.
For $p = 2$, since $PSL(2)$ is the dihedral group D_3, the largest order is 3. We set p be an odd prime. $\mathbb{Z}/p\mathbb{Z}$ is a finite field $\mathbb{F}_p$. Let $\alpha \in \overline{\mathbb{F}}_p$ be an eigenvalue of A, where $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$. α is a solution of

$$x^2 - \mathrm{tr}(A)x + 1 = 0. \tag{A.3}$$

If A is a diagonalization impossible, α is a multiple root of (A.3) and thus, Jordan normal form of A is $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ whose order is q. We assume A is a diagonalizable matrix. By Frobenius endomorphism, we realize that α^p is also a solution of (A.3). If $\alpha \neq \alpha^p$, $\left(\begin{smallmatrix}\alpha & 0\\ 0 & \alpha^p\end{smallmatrix}\right)$ is a diagonal matrix of A and $\alpha\cdot\alpha^p = 1$. We have its order is at most $\frac{p+1}{2}$. If $\alpha = \alpha^p$, the other eigenvalue of A is α^{-1}. Thus, the order of A is at most $\frac{p-1}{2}$.

Case 2: $q = 4$.
By (A.3), we have

$$\begin{aligned} A^3 &= \left(t^2-1\right)A - tI \\ A^4 &= t\left(t^2-2\right)A - \left(t^2-1\right)I \end{aligned}$$

where $t = \mathrm{tr}(A)$ and I is the unit matrix. By considering each case of t in modular 4, we see that the order of A is at most 4.

Case 3: $q = p^r$ is a prime power.
We use a induction on r. Let assume that the claim is held for $r-1$. We regard $A \in PSL(p^r)$ as an element of $PSL(p^{r-1})$. By assumption, we take n such that A^n is a unit matrix in $PSL(p^{r-1})$ with $1 \leq n \leq p^{r-1}$. It means $A^n = I + p^{r-1}B$ in $PSL(p^r)$ with some $B \in PSL(p^r)$. Then by

$$A^{np} = \left(I + p^{r-1}B\right)^p = I,$$

we get the order of A is at most $np\,(\leq p^r)$.

Case 4: For general q.
By Chinese remainder theorem, we may prove it for only $q = 2 \cdot 3^r$, which is type II. If the order of

$$A = B \otimes C \in PSL(2) \otimes PSL(3^r)$$

is larger than q, the order of B is 3 and the order of C is larger than $2 \cdot 3^{r-1}$. By proof of Case 3, we have that the order of C is 3^r. However, then the order of $A = B \otimes C$ is 3^r. It is a contradiction. □

From above results, we have

Proposition A.3. *For $q \geq 7$, the order of elements of $\mathrm{Aut}(X_q)$ is at most $\frac{3}{2}q$ if q is type I. If q is type II, the order is at most q.*

In Theorem 2.12, we have the genus of $X_q^1 = X_q/\langle z \mapsto z+1 \rangle$. For type I $q = 2p$, we shall consider the genus of

$$X_q' := X_q/\left\langle z \mapsto Mz \right\rangle,$$

where

$$M = \begin{pmatrix} p+1 & 1 \\ p & 1 \end{pmatrix},$$

which is an order $3p$ automorphism of X_q. An odd number p isn't divided by 3. We denote the genus of X_q' by g_q'.

Proposition A.4. *Let $q = 2p$ be type I. For $q \geq 10$, thus for $p \geq 5$, we have*

$$g_q' = g_{2p}' = 1 + \frac{(p - 3\mathcal{N}(p))\,p}{12} \prod_{l \in \mathcal{P}(p)} \left(1 - \frac{1}{l^2}\right).$$

Proof. By

$$\begin{pmatrix} p+1 & 1 \\ p & 1 \end{pmatrix}^3 \equiv \begin{pmatrix} 1 & p+3 \\ 0 & 1 \end{pmatrix} \pmod{2p},$$

X_q' is isomorphic to

$$X_q^2/\left\langle z \mapsto Mz \right\rangle$$

and the order of M is 3 in X_q^2. We see that $X_q^2 \to X_q'$ is the unbranched natural projection. The subgroup of $SL(2,\mathbb{Z})$ generated by Γ_q^2 and A acts freely on $\mathbb{H}$ since diagonal components of its

elements are 1 in modular p. Then we may consider whether only points of S_q^2 are branched points or not. If $\left[\frac{x}{z}\right] \in S_q^2$ with $\gcd(x,z)=1$ is a branched point of the natural projection, we have

$$\left[\frac{(p+1)x+z}{px+z}\right]_{\Gamma_q^2} = \left[\frac{x}{z}\right]_{\Gamma_q^2}.$$

We remark that $\gcd\left((p+1)x+z, px+z\right) = \gcd(x,z) = 1$. Then we have $px+z \equiv z$ or $px+z \equiv -z$ in modular $2p$. In either case, x is an even number and thus, z is an odd number. We have

$$\left[\frac{(p+1)x+z}{px+z}\right]_{\Gamma_q^2} = \left[\frac{x+z}{z}\right]_{\Gamma_q^2}$$

and there is $n \in \mathbb{Z}$ such that $x+z \equiv x+2nz$ in modular $2p$. However, it is a contradiction with z is odd.

Since the natural projection $X_q^2 \to X_q'$ is unbranched, we have

$$2g_q^2 - 2 = 3\left(2g_q' - 2\right)$$

by Hurwitz Theorem A.1. The proof is completed by Theorem 2.12 and a direct computation. □

By table 7, we notice that g_q' isn't always smaller than g_q^1 even though the order of the corresponding automorphism of X_q' is larger than one of X_q^1. Moreover, unfortunately $g_q' \neq 0$ except for $q=2$. Therefore, considering g_q' is of no use to get a semi-hyperelliptic curve after all and we naturally think that X_q is a semi-hyperelliptic curve if and only if $q \leq 10$ or $q = 12$.

q	2	10	14	22	26	34	38	$\cdots$
g_q	0	13	49	241	421	1009	1441	$\cdots$
g_q^1	0	0	1	6	10	21	28	$\cdots$
g_q'	0	1	2	6	9	17	22	$\cdots$

Table 7: Genera for type I q

References

[Fr] E. Freitag, *Complex Analysis 2*, Springer, 2010

[GG] E. Girodo and G. Gonzâlez-Diez, *Introduction to Compact Riemann Surfaces and Dessins d'Enfants*, CAMBRIDGE, 2012, 126-143

[II] N. Ishida and N. Ishii, *The equations for modular function fields of principal congruence subgroups of prime level*, Manuscripta Math. 90, 1996, 271-285

[Is] N. Ishida, *Generators and equations for modular function fields of principal congruence subgroups*, Acta Arith. 85, 1998, 197-207

[KK] A. Kuribayashi and K. Komiya, *On Weierstrass points and automorphisms of curves of genus three*, volume 732 of Lecture Notes in Math., Springer-Verlag, Berlin, 1979, 253-299

[Kl] F. Klein, *Ueber die Transformation siebenter Ordnung der elliptischen Functionen*, Math. Ann., 1878, 253-299

[Ku] A. Kuribayashi, *On analytic families of compact Riemann surfaces with non-trivial automorphisms*, Nagoya Math. J. 28, 1966, 119-165

[Si] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton University Press, 1971

[Ya] Y. Yang, *Defining equations of modular curves*, Volume 204 of Advances in Mathematics, 2006, 481-508