TSUKUBA J. MATH.
Vol. 19 No. 1 (1995), 121–139

ON A FAMILY OF QUOTIENTS OF FERMAT CURVES

By

Susumu IROKAWA and Ryuji SASAKI

Introduction

Let F_N be the N-th Fermat curve defined by the equation:

$$u^N + v^N = 1 .$$

For a pair (r, s) of positive integers such that $r+s \leqq N-1$ and g.c.d. $(r, s, N) = 1$, we denote by $F(r, s)$ the quotient of F_N defined by the equation:

$$y^N = x^r(1-x)^s$$

where the projection $F_N \to F(r, s)$ is defined by

$$(x, y) \longmapsto (u^N, u^r v^s) .$$

We denote by $\sigma(r, s)$ the automorphism of $F(r, s)$ defined by $\sigma(r, s)^* : (x, y) \mapsto (x, \zeta_N y)$ where ζ_N is a primitive N-th root of unity. The order N of $\sigma(r, s)$ is quite large for the genus $g(r, s)$ of $F(r, s)$. Between them we have a relation:

$$(\sharp) \qquad N \geqq 2g(r, s)+1 .$$

Conversely the inequality $(\sharp)$ characterize the quotients $F(r, s)$. In fact we have the following (cf. Theorem 2.2):

THEOREM. *Let X be a complete non-singular curve of genus g over an algebraically closed field k of characteristic 0, and let σ be an automorphism of X of order N with $N \geqq 2g+1 \geqq 5$. Let H_λ be a hyperelliptic curve of genus g defined by the equation $y^2 = (x^{g+1}-1)(x^{g+1}-\lambda)$ with $\lambda \in k \setminus \{0, 1\}$, and let τ_λ be an automorphism of H_λ defined by $\tau_\lambda^* : (x, y) \mapsto (\zeta_{g+1}x, -y)$. Assume that the pair (X, σ) is not isomorphic to $(H_\lambda, \langle \tau_\lambda \rangle)$ for any λ with $N = 2g+2$ and g even. Then the pair (X, σ) is isomorphic to $(F(r, s), \sigma(r, s))$, for some (r, s).*

In this paper we are mainly concerned with the curves $F(r, s)$ in which the equality $N = 2g(r, s)+1$ holds in $(\sharp)$. In a family of these curves there are some interesting curves. For example we have a curve whose group of automor-

Received April 9, 1993. Revised November 9, 1993.

phisms is a cyclic group of maximal order and a Hurwitz curve (for the definition see the section 3.3). The main topics of this paper is to determine isomorphy classes of such curves and their groups of automorphisms completely.

When $N=2g(r, s)+1$ is a prime number, these results are obtained by Seyama [9]. In order to conquer difficulties which arise from the cause that N is not prime, we make use of a technique established by Koblitz-Rohrlich [6].

Let N is very large, then a curve with an automorphism of order N is uniquely determined. In his paper [8], Nakagawa determines curves of genus g with automorphisms of order $N\geqq 3g$.

1. Quotients of Fermat curves

Throughout this paper we fix an algebraically closed field k of characteristic 0. Let $F_N\subset \boldsymbol{P}^2$ denote the Fermat curve of degree N ($N\geqq 3$) defined by the equation

$$U^N+V^N+W^N=0\,.$$

Let u and v be the rational functions on F_N induced by U/W and V/W. For integers r, s such that $1\leqq r$, s we define the differential on F_N by

$$\omega_{r,s}=u^{r-1}v^{s-1}\frac{du}{v^{N-1}}\,.$$

Let

$$A_N=\{(r, s)\in \boldsymbol{Z}^2 \mid 1\leqq r,\ s \text{ and } r+s\leqq N-1\}\,.$$

Then the set $\{\omega_{r,s} \mid (r, s)\in A_N\}$ forms a basis for the space of differentials of the first kind of F_N.

From now on we assume that $(r, s)\in A_N$ satisfies g.c.d. $(r, s, N)=1$. We call such (r, s) a primitive pair. We put

$$x=u^N \quad\text{and}\quad y=u^r v^s\,.$$

Then the equation $u^N+v^N=1$ yields

$$y^N=x^r(1-x)^s\,. \tag{1.1}$$

Let $F(r, s)$ denote the "non-singular model" of the function field $k(x, y)$, so that we have the map $F_N\to F(r, s)$ induced by the inclusion $k(x, y)\subset k(u, v)$.

For $a\in \boldsymbol{Z}/N\boldsymbol{Z}$ or $\boldsymbol{Z}$, we let $\langle a\rangle$ be the integer such that

$$0\leqq\langle a\rangle\leqq N-1 \quad\text{and}\quad \langle a\rangle\equiv a \bmod N\,.$$

Let

$$A(r, s)=\{a\in \boldsymbol{Z}/N\boldsymbol{Z} \mid (\langle ar\rangle, \langle as\rangle)\in A_N\}\,.$$

If $a\in \boldsymbol{Z}/N\boldsymbol{Z}$, then we can regard $\omega_{\langle ar\rangle,\langle as\rangle}$ as a differential on $F(r, s)$ canonically. Then the set $\{\omega_{\langle ar\rangle,\langle as\rangle} \mid a\in A(r, s)\}$ forms a basis for the differentials of the first kind of $F(r, s)$. In particular the genus $g(r, s)$ of $F(r, s)$ is equal to the cardinality of $A(r, s)$. For details, we refer to [7].

Let $\sigma(r, s)$ denote the automorphism of $F(r, s)$ defined by

$$\sigma(r, s)^{*}x=x \quad \text{and} \quad \sigma(r, s)^{*}y=\zeta_{N}y\ . \tag{1.2}$$

We denote by

$$\pi=\pi(r, s): F(r, s) \longrightarrow \boldsymbol{P}^{1} \tag{1.3}$$

the morphism induced by $k(x)\subset k(x, y)$.

THEOREM 1.1. *If $(r, s)\in A_{N}$ is a primitive pair, then we have*

$$N\geqq 2g(r, s)+1\ .$$

Equality holds if and only if $(N, r)=(N, s)=(N, r+s)=1$.

PROOF. We put $e_{0}=N/(N, r)$, $e_{1}=N/(N, s)$ and $e_{\infty}=N/(N, r+s)$. Applying the Riemann-Hurwitz relation to the morphism (1.3), we get

$$\frac{2g(r, s)-2}{N}=1-\left(\frac{1}{e_{0}}+\frac{1}{e_{1}}+\frac{1}{e_{\infty}}\right).$$

Hence we have

$$N=2g(r, s)-2+\{(N, r)+(N, s)+(N, r+s)\}\geqq 2g(r, s)+1\ .$$

Q.E.D.

For later use we shall discuss gap sequences of points where the morphism $\pi: F_{(r,s)}\rightarrow \boldsymbol{P}^{1}$ ramifies. We fix three points P_{0}, P_{1} and P_{∞} such that $\pi(P_{0})=0$, $\pi(P_{1})=1$ and $\pi(P_{\infty})=\infty$. We denote by $\mathrm{Gap}(P_{i})$ the gap sequence of P_{i} $(i=0, 1, \infty)$, i.e., a positive integer n is contained in $\mathrm{Gap}(P_{i})$ means that there exists a differential ω of the first kind with $\mathrm{ord}_{P_{i}}\omega=n-1$.

If $a\in \boldsymbol{Z}/N\boldsymbol{Z}$, then we have

$$\mathrm{ord}_{P_{0}}\omega_{\langle ar\rangle,\langle as\rangle}=\langle ar\rangle-(N, r),$$

$$\mathrm{ord}_{P_{1}}\omega_{\langle ar\rangle,\langle as\rangle}=\langle as\rangle-(N, s)$$

and

$$\mathrm{ord}_{P_{\infty}}\omega_{\langle ar\rangle,\langle as\rangle}=\langle -a(r+s)\rangle-(N, r+s)\ .$$

PROPOSITION 1.2. *Let (r, s) be a pair in A_{N} with $(N, r)=1$ (resp. $(N, s)=1$). Then the map*

$$A(r, s) \longrightarrow \mathrm{Gap}(P_{0}) \quad (\textit{resp.}\ \mathrm{Gap}(P_{1}))$$

$$a \longmapsto \langle ar \rangle \quad (resp.\ \langle as \rangle)$$

is bijective.

PROOF. Since both of $A(r, s)$ and $\mathrm{Gap}(P_i)$ have the same cardinality, it suffices to show the injectiviły. It is easy to show it. Q.E.D.

2. A characterization of quotients of Fermat curves

Let X be a complete non-singular algebraic curve of genus $g \geqq 2$ defined over k. Such a curve is simply called a curve of genus g. Let σ be an automorphism of X of order N. We denote by $X/\langle\sigma\rangle$ the quotient of X by the cyclic group $\langle\sigma\rangle$ generated by σ and $\{\lambda_1, \lambda_2, \cdots, \lambda_n\}$ the set of points in $X/\langle\sigma\rangle$ over which the projection $\pi: X \to X/\langle\sigma\rangle$ ramifies. The automorphism said to be of type $(g_0; e_1, e_2, \cdots, e_n)$ if the genus of $X/\langle\sigma\rangle$ is g_0 and the ramification index at P_i is e_i, where P_i is any point in X such that $\pi(P_i)=\lambda_i$. Then we have the following fact which is proved by Harvey [3] using a topological method.

LEMMA 2.1. *Let M be the l.c.m. of $\{e_1, e_2, \cdots, e_n\}$. Then the following are satisfied:*

(1) *l.c.m. $\{e_1, \cdots, \hat{e}_i, \cdots, e_n\} = M$ for all i, where $\hat{e}_i$ denotes the omission of e_i;*

(2) *M divides N, and if $g_0=0$, $M=N$;*

(3) *$n \neq 1$, and if $g_0=0$, $n \geqq 3$;*

(4) *If $2^r \| M$, i.e., 2^r divides M and 2^{r+1} does not divide M, then the number of e_i's with $2^r \| e_i$ is even.*

PROOF. Suppose $n=1$. If p is a prime divisor of N, then the covering $X/\langle\sigma^p\rangle \to X/\langle\sigma\rangle$ has the only one ramification point. This contradicts a theorem of Lewittes (cf. [2]) which says that the number of the fixed points $\geqq 2$ for an automorphism of prime order. If $g_0=0$, then we have $n \geqq 3$ by the Riemann-Hurwitz formula. Thus we have (3). (2) follows immediately since all the e_i divide N. If $g_0=0$, we have an unramified covering $X/\langle\sigma^{N/M}\rangle \to X/\langle\sigma\rangle$, hence $N=M$.

We put l.c.m. $\{e_1, \cdots, \hat{e}_i, \cdots, e_n\} = M_i$. Consider the covering $\pi: X/\langle\tau\rangle \to X/\langle\sigma\rangle$ where $\tau = \sigma^{N/M_i}$. If $e_i \nmid M_i$, π_i ramifies only over λ_i. This contradicts (3). Thus we have $e_i | M_i$ and $M=M_i$.

For (4) we consider the covering $X/\langle\sigma^{N/2}\rangle \to X/\langle\sigma\rangle$ of degree 2. It ramifies only over λ_i's such that $2^r | e_i$. The number of ramification points of a covering of degree 2 is even. Q.E.D.

Let H_λ be a hyperelliptic curve of genus g defined by the equation

$$y^2=(x^{g+1}-1)(x^{g+1}-\lambda), \qquad \lambda\in k\setminus\{0, 1\}$$

and let τ_λ be an automorphism of H_λ defined by

$$\tau_\lambda^* : (x, y) \longmapsto (\zeta_{g+1}x, -y)$$

where ζ_{g+1} is primitive $(g+1)$-th root of unity.

Two pairs $(X, \langle\sigma\rangle)$ and $(Y, \langle\tau\rangle)$ of algebraic curves and cyclic groups generated by σ, τ are said to be isomorphic, if there exists an isomorphism $f: X\to Y$ such that $f^{-1}\cdot\langle\tau\rangle\cdot f=\langle\sigma\rangle$.

THEOREM 2.2. *Let $(X, \langle\sigma\rangle)$ be a pair of an algebraic curve X of genus $g\geqq 2$ and a cyclic group generated by an automorphism σ of X of order N. Assume $N\geqq 2g+1$. Then $(X, \langle\sigma\rangle)$ is isomorphic to either $(F(r, s), \langle\sigma(r, s)\rangle)$ for some primitive pair $(r, s)\in A_N$, or $(H_\lambda, \langle\tau_\lambda\rangle)$ for some $\lambda\in k\setminus\{0, 1\}$ with $N=2g+2$ and g even.*

PROOF. Let $(g_0; e_1, e_2, \cdots, e_n)$ denote the type of the automorphism σ, i.e., g_0 is the genus of $X/\langle\sigma\rangle$ and $\{e_1, e_2, \cdots, e_n\}$ is the set of ramification indices for the projection $X\to X/\langle\sigma\rangle$.

We may assume $e_1\leqq e_2\leqq\cdots\leqq e_n$. In this case the Riemann-Hurwitz formula asserts

$$\frac{2g-2}{N}=2g_0-2+\sum_{i=1}^{n}\left(1-\frac{1}{e_i}\right). \tag{2.1}$$

Then we have the following:

(i) $g_0=0$;

(ii) If N is odd, then $n=3$;

(iii) If N is even, then either $n=3$, or the type of σ is $(0; 2, 2, g+1, g+1)$ and g is even.

By the assumption the left hand side of the equation (2.1) is small than 1. Suppose $g_0\geqq 1$. Since $n\geqq 2$ by Lemma 2.1(3), it follows that the right hand side of (2.1)>1. This is a contradiction. Thus we have (i). Now we prove (ii). Obviously we have $n\geqq 3$ and that e_i is odd for any i. We consider the following four cases: (a) $n\geqq 5$, (b) $n=4$, $e_1\geqq 5$, (c) $n=4$, $e_1=3$, $e_2\geqq 5$, (d) $n=4$, $e_1=e_2=3$, $e_3\geqq 7$. Then the right hand side of (2.1)>1 for any case. If $n=4$, $e_1=e_2=e_3=3$, then $e_4=3$ and $N=3$ by Lemma 2.1(1, 2). If $n=4$, $e_1=e_2=3$, $e_3=5$, then $e_4=5$ or 15 and $N=15$ by Lemma 2.1 (1, 2). By (2.1), we have $g=8$ or 9; hence we have $N<2g+1$. Thus we have (ii). By arguments similar to these, we have (iii). It is easy and tiresome to pursue it, so we shall omit it.

If $n=3$, then $X\to X/\langle\sigma\rangle$ is a cyclic covering of degree N having three branch points. Therefore $(X, \langle\sigma\rangle)$ is isomorphic to $(F(r, s), \langle\sigma(r, s)\rangle)$ for some primitive $(r, s)\in A_N$.

Assume that $N=2g+2$ with g even and the type of σ is $(0; 2, 2, g+1, g+1)$. Then we may assume that the set of the branch points for $\pi: X\rightarrow X/\langle\sigma\rangle$ is α, 0, 1, ∞ with $\alpha\in k\backslash\{0, 1\}$ and that

$$\pi^{-1}(\alpha)=\{P, \sigma(P), \cdots, \sigma^{g}(P)\}, \qquad \pi^{-1}(1)=\{Q, \sigma(Q), \cdots, \sigma^{g}(Q)\},$$
$$\pi^{-1}(0)=\{P_0, \sigma(P_0)\}, \qquad \pi^{-1}(\infty)=\{P_\infty, \sigma(P_\infty)\}.$$

We put $\sigma^{g+1}=\tau$. Then the set of points invariant under τ is $\{P, \sigma(P), \cdots, \sigma^{g}(P), Q, \sigma(Q), \cdots, \sigma^{g}(Q)\}$. Applying the Riemann-Hurwitz formula for $X\rightarrow X/\langle\tau\rangle$, we have the genus of $X/\langle\tau\rangle=0$; hence X is a hyperelliptic curve. We denote by $\mathcal{L}=\mathcal{L}(P_\infty+\sigma(P_\infty))$ the vector space of rational functions f such that $\operatorname{div}(f)+P_\infty+\sigma(P_\infty)$ is a positive divisor. Then there is a function $x\in\mathcal{L}$ such that $\operatorname{div}(x)=P_0+\sigma(P_0)-P_\infty-\sigma(P_\infty)$. Moreover we have a function y such that

$$\operatorname{div}(y)=P+\cdots+\sigma^{g}(P)+Q+\cdots+\sigma^{g}(Q)-(g+1)(P_\infty+\sigma(P_\infty)).$$

Therefore we have $\operatorname{div}(y^2)=\operatorname{div}(\prod_{i=0}^{g}(x-a_i)(x-b_i))$ where $x(\sigma^{i-1}(P))=a_i$ and $x(\sigma^{i-1}(Q))=b_i$. Since $\sigma^*x\in\mathcal{L}$ and $(\sigma^{g+1})^*x=x$, it follows that $\sigma^*x=\zeta_{g+1}x$ for some primitive $(g+1)$-th root ζ_{g+1} of unity. Moreover we have $\operatorname{div}(\sigma^*(x-a_i))=\sigma(\operatorname{div}(x-a_i))=\operatorname{div}(x-a_{i+1})$. Arranging the constants we have

$$y^2=(x^{g+1}-1)(x^{g+1}-\lambda), \qquad \lambda\in k\backslash\{0, 1\}$$

and σ is induced by $\sigma^*: (x, y)\mapsto(\zeta_{g+1}x, -y)$. This completes the proof. Q.E.D.

REMARK 2.1. The exceptional curve H_λ has the following interesting proparty: Let σ_i $(i=1, 2)$ be the automorphism of H_λ defined by

$$\sigma_i^*(x, y)=(\mu^2x^{-1}, (-1)^i\mu^{g+1}x^{-(g+1)}y),$$

where μ satisfies $\mu^{2(g+1)}=\lambda$. Then we have

$$\operatorname{Jac}(H_\lambda)\cong\operatorname{Jac}(H_\lambda/\langle\sigma_1\rangle)\times\operatorname{Jac}(H_\lambda/\langle\sigma_2\rangle)$$

as abelian varieties (cf. [1]).

3. Algebraic curves of genus g with automorphisms of order $2g+1$

In this section we shall be concerned with a pair $(X, \langle\sigma\rangle)$ of an algebraic curve X of genus $g\geqq 2$ and a cyclic group generated by an automorphism σ of order $N=2g+1$. By Theorem 2.2 and Theorem 1.1, we know that it is isomorphic to a pair $(F(r, s), \langle\sigma(r, s\rangle)$:

$$F(r, s): y^{2g+1}=x^{r}(1-x)^{s},$$

$$\sigma(r, s)^{*}: (x, y)\longmapsto(x, \zeta_{N}y),$$

where $(r, s)\in A_{N}$ is primitive pair and $(N, r)=(N, s)=(N, r+s)=1$, and where ζ_{N} is a primitive N-th root of unity. If $r^{[-1]}$ is an integer such that $r\cdot r^{[-1]}\equiv 1$ mod N, then we have $1\leqq\langle s\cdot r^{[-1]}\rangle\leqq N-2$ and g. c. d. $(N, \langle s\cdot r^{[-1]}\rangle)=1$.

LEMMA 3.1. $(F(r, s), \langle\sigma(r, s)\rangle)\cong(F(1, \langle s\cdot r^{[-1]}\rangle), \langle\sigma(1, \langle s\cdot r^{[-1]}\rangle)\rangle)$.

PROOF. Define a and b by $r\cdot r^{[-1]}=1+Na$ and $s\cdot r^{[-1]}=\langle s\cdot r^{[-1]}\rangle+Nb$. We put

$$Y=\frac{y^{r[-1]}}{x^{a}(1-x)^{b}} \quad \text{and} \quad X=x .$$

Then we have $Y^{N}=X(1-X)^{\langle s\cdot r[-1]\rangle}$. Q.E.D.

Now we shall treat only pairs of the form $(F(1, \langle a\rangle), \langle\sigma(1, \langle a\rangle)\rangle)$ where $a\in(\boldsymbol{Z}/N\boldsymbol{Z})^{\times}$ (i.e., g. c. d. $(\langle a\rangle, N)=1$) and g. c. d. $(\langle a\rangle+1, N)=1$. For simplicity we put $F(1, \langle a\rangle)$, $\sigma(1, \langle a\rangle)$ and $A(1, \langle a\rangle)$ to $F(a)$, $\sigma(a)$ and $A(a)$, respectively. So we shall study the following set:

$$C(N)=\{a\in(\boldsymbol{Z}/N\boldsymbol{Z})^{\times}\mid \text{g. c. d.}(\langle a\rangle+1, N)=1\}.$$

Then $C(N)$ always contains 1, g and $2g-1=N-2$. In the following for a finite set S we denote by $|S|$ the cardinality of S.

LEMMA 3.2. *Let $N=p_{1}^{e_{1}}\cdots p_{n}^{e_{n}}$ be the decomposition into prime factors. Then we have*

$$|C(N)|=\prod_{i=1}^{n}p_{i}^{e_{i}-1}(p_{i}-2).$$

PROOF. If $N=N_{1}N_{2}$ and g. c. d. $(N_{1}, N_{2})=1$, then the map $(r \bmod N)\mapsto(r \bmod N_{1}, r \bmod N_{2})$ gives a bijection $C(N)\cong C(N_{1})\times C(N_{2})$. Since $|C(p^{e})|=p^{e-1}(p-2)$, we get the result. Q.E.D.

As in (1.3), let $\pi=\pi(a): F(a)\rightarrow F(a)/\langle\sigma(a)\rangle\cong\boldsymbol{P}^{1}$ denote the projection induced by the inclusion $k(x)\subset k(x, y)$. We denote by Fix $(\sigma(a))$ the set of points fixed under $\sigma(a)$, which consists of three points:

$$\pi^{-1}(0)=P_{0}^{(a)}, \qquad \pi^{-1}(1)=P_{1}^{(a)}, \qquad \pi^{-1}(\infty)=P_{\infty}^{(a)}.$$

Sometimes we omit the superscript (a) from the notation.

3.1. Automorphisms φ and ψ of $C(N)$.

We define φ and ψ by

$$\varphi(a)=-a(1+a)^{-1} \quad \text{and} \quad \psi(a)=a^{-1}, \qquad a\in C(N).$$

We denote by G the group of automorphisms of $C(N)$ generated by φ and ψ. Then we have

$$G=\{1, \varphi, \psi, \psi\varphi, \psi\varphi\psi, (\psi\varphi)^2\}$$

and an isomorphism ρ of G to the symmetric group of three letters $\{0, 1, \infty\}$ such that

$$\rho(\varphi)=\begin{pmatrix} 0 & 1 & \infty \\ \infty & 1 & 0 \end{pmatrix} \quad \text{and} \quad \rho(\psi)=\begin{pmatrix} 0 & 1 & \infty \\ 1 & 0 & \infty \end{pmatrix}.$$

Let G_a denote the stabilizer subgroup of G at $a\in C(N)$. Then we have the following:

(1) $|G_a|=1$, 2 or 3;

(2) $|G_a|=2$ if and only if $a\in\{1, g, 2g-1\}$;

(3) $|G_a|=3$ if and only it $a^2+a+1=0$.

LEMMA 3.3. *For any $\theta\in G$ and $a\in C(N)$, there is an isomorphism:*

$$\theta_a : (F(a), \langle\sigma(a)\rangle) \longrightarrow (F(\theta(a)), \langle\sigma(\theta(a))\rangle)$$

such that

$$\theta_a(P_i^{(a)})=P_{\rho(\theta)(i)}{}^{(\theta(a))}, \qquad i=0, 1, \infty.$$

PROOF. It suffices to prove the lemma for $\theta=\varphi$ and ψ. We denote by $k(x, y)$ (resp. $k(u, v)$) the rational function field of $F(a)$ (resp. $F(1, \theta(a))$) such that

$$y^N=x(1-x)^{\langle a\rangle} \quad (\text{resp. } v^N=u(1-u)^{\langle\theta(a)\rangle}).$$

For $\theta=\varphi$, let

$$(\varphi_a)^*(u)=x^{-1} \quad \text{and} \quad (\varphi_a)^*(v)=\frac{\zeta y^\alpha}{x(1-x)^{\alpha-\beta-1}}$$

where α, β and ζ are defined by the equations $\alpha=N-\langle\varphi(a)\rangle-1$, $\{N-(\langle a\rangle+1)\}\alpha=1+\beta N$ and $\zeta^N=(-1)^{\langle\varphi(a)\rangle}$. Then φ_a is a required one. On the other hand, for $\theta=\psi$, let

$$(\psi_a)^*(u)=1-x \quad \text{and} \quad (\psi_a)^*(v)=\frac{y^{\langle\psi(a)\rangle}}{(1-x)^\alpha}$$

where α is defined by $\langle a\rangle\cdot\langle\psi(a)\rangle=1+N\alpha$. Then ψ_a is a required one. Q.E.D.

3.2. Hyperelliptic curves.

The following gives a characterization of hyperelliptic curves of genus $g\geqq 2$ with an automorphism of order $N=2g+1$.

THEOREM 3.4. *$F(1)$, $F(g)$ and $F(2g-1)$ are hyperelliptic curves isomorphic to each ether and if $F(a)$, $a\in C(N)$, is a hyperelliptic curve then $a\in\{1, g, 2g-1\}$.*

PROOF. Obviously $F(1)$ is hyperelliptic. Since $\varphi(1)=g$ and $\psi(2g-1)=g$, it follows that the orbit of $1\in C(N)$ under the action of G is the set $\{1, g, 2g-1\}$. By Lemma 3.3, we have $F(1)\cong F(g)\cong F(2g-1)$.

Assume $F(a)$ is hyperelliptic. Since $(\psi\varphi\psi)(a)=-a-1$ and $\langle -a-1\rangle = N-\langle a\rangle -1$, we may assume $a\leqq g$, i.e., $a\leqq g-1$. The defining equation of $F(a)$ is $y^N=x(1-x)^a$. We put $\mathrm{Fix}(\sigma(a))=\{P_0, P_1, P_\infty\}$. Since the rational function y is contained in $\mathcal{L}((a+1)P_\infty)$, the gap sequence of P_∞ is not equal to $\{1, 2, \cdots, g\}$, that is, P_∞ is a Weierstrass point (cf. section 1). Since $F(a)$ is hyperelliptic, we have

$$\mathrm{Gap}(P_\infty)=\{1, 3, 5, \cdots, 2g-1\}.$$

Let $z\in\mathcal{L}(2P_\infty)$ be a rational function such that

$$\mathrm{div}(z)=P_0+P_0'-2P_\infty,$$

where "$'$" means the hyperelliptic involution. Then the set $\{1, z, \cdots, z^{(a+1)/2}\}$ forms a linear basis for $\mathcal{L}((a+1)P_\infty)$. Since $y(P_0)=z(P_0)=0$, we can put

$$y=zF(z), \tag{3.2}$$

where

$$F(z)=\alpha_1+\alpha_2 z+\cdots+\alpha_{(a+1)/2}z^{(a-1)/2}.$$

Comparing the divisors of both sides of (3.2), we have

$$P_0+aP_1-(a+1)P_\infty=P_0+P_0'-2P_\infty+\mathrm{div}(F(z)).$$

It follows that we have $P_0'=P_1$ and $\mathrm{div}(F(z))=(a-1)(P_1-P_\infty)$. If $a>1$, then $F(z)(P_1)=\alpha_1=0$. Hence we have $y=z^2(\alpha_2+\cdots)$. Then we have $P_0=P_1$. This is a contradiction. Q.E.D.

In general we have the following:

THEOREM 3.5. *Let (r, s) be a primitive pair in A_N for $N\geqq 5$. If $F(r, s)$ is a hyperelliptic curve, then the pair $(F(r, s), \langle\sigma(r, s)\rangle)$ is isomorphic to one of the following:*

(1) $N=2g+1$ *and* $(F(1, 1), \langle\sigma(1, 1)\rangle)$;

(2) $N=2g+2$ *with* g *even and* $(H_\lambda, \langle\tau_\lambda\rangle)$, $\lambda\in k\setminus\{0, 1\}$ (*cf. section* 2);

(3) $N=4g$ *and* $(H(4g), \langle\sigma)4g)\rangle)$ *which are defined by*

$$y^2=x(x^{2g}-1) \quad \text{and} \quad \sigma(4g)^*(x, y)=(\zeta_{4g}{}^2x, \zeta_{4g}y).$$

(4) $N=4g+2$ *and* $(H(4g+2), \langle\sigma(4g+2)\rangle)$ *which are defined by*

$$y^2=x^{2g+1}-1 \quad \text{and} \quad \sigma(4g+2)^*(x, y)=(\zeta_{2g+1}x, -y).$$

PROOF. We denote by "$'$" the hyperelliptic involution, which is contained in the center of the group of all automorphisms. For simplicity's sake we put $F(r, s)=F$ and $\sigma(r, s)=\sigma$. If P is a Weierstrass point of F, i.e., $P=P'$, then so is $\sigma(P)$. If there is a Weierstrass point which is not a ramification point for $\pi: F\rightarrow F/\langle\sigma\rangle\cong \boldsymbol{P}^1$, it follows that

$$\{P, \sigma(P), \cdots, \sigma^{N-1}(P)\}\subset \text{the set of Weierstrass points};$$

hence we have $N\leqq 2g+2$. Assume that any Weierstrass point is a ramification point. Then we have

$$\frac{N}{e_0}+\frac{N}{e_1}+\frac{N}{e_\infty}\geqq 2g+2,$$

where $e_0=N/(N, r)$, $e_1=N/(N, s)$ and $e_\infty=N/(N, r+s)$. By the Riemann-Hurwitz formula:

$$\frac{2g-2}{N}=1-\left(\frac{1}{e_0}+\frac{1}{e_1}+\frac{1}{e_\infty}\right), \tag{3.3}$$

we have $N\geqq 4g$.

The case $N\leqq 2g+2$ comes from Theorem 2.2 and Theorem 3.4. Now we assume $N\geqq 4g$. Then by (3.3) we have

$$\frac{1}{e_0}+\frac{1}{e_1}+\frac{1}{e_\infty}\geqq 1-\frac{2g-2}{4g}=\frac{2g+2}{4g}.$$

By Lemma 2.1, we have

$$(e_0, e_1, e_\infty)=\begin{cases}(2, 4g, 4g), & N=4g,\\ (2, 2g+1, 4g+2), & N=4g+2.\end{cases}$$

If $N=4g$, then we may assume that $F(r, s)$ is defined by

$$y^N=x^r(1-x)^{2g},$$

where $1\leqq r<2g$ and $(2g, r)=1$. We put $\pi^{-1}(0)=P_0$, $\pi^{-1}(\infty)=P_\infty$. Take a point P_1 such that $\pi(P_1)=1$. Then we have

$$\operatorname{div}(x)=N\cdot P_0-N\cdot P_\infty$$

and

$$\operatorname{div}(y)=P_1+\sigma(P_1)+\cdots+\sigma^{2g-1}(P_1)+rP_0-(2g+r)P_\infty .$$

Since the projection $F(r, 2g)\to F(r, 2g)/\langle\sigma^{2g}\rangle$ ramifies at P_0, P_∞ and $\sigma^i(P_1)$, $i=0, 1, \cdots, 2g-1$, it follows that the genus of $F(r, 2g)/\langle\sigma^{2g}\rangle$ is 0 (hence $F(r, 2g)$ is necessarily hyperelliptic). Take a function u on $F(r, 2g)$ such that

$$\operatorname{div}(u)=2P_0-2P_\infty, \qquad \operatorname{div}(u-1)=2P_1-2P_\infty .$$

Then we have

$$v^2=(u^{2g}-1)u$$

where $v=y\cdot u^{-(r-1)/2}$. By the same way as above we can prove the case $N=4g+2$, so we shall omit its proof. Q.E.D.

REMARK 3.1. In this proof, we have proved that if $N\geqq 4g$, then $(F(r, s), \sigma(r, s))$ is isomorphic to $(H(4g), \sigma(4g))$ or $(H(4g+2), \sigma(4g+2))$. This fact is, already, proved by Nakagawa ([8] Theorem 1, Theorem 2).

REMARK 3.2. We have $(F(1, 1), \langle\sigma(1, 1)\rangle)\cong(H(4g+2), \langle\sigma(4g+2)^2\rangle)$.

3.3. Hurwitz curves.

Let (a, b) be a pair of relatively prime positive integers. The Hurwitz curve, which we denote by $H(a, b)$, of index (a, b) is a non-singular model of the plane curve defined by the equation:

$$x^b y^{a+b}+y^b z^{a+b}+z^b x^{a+b}=0 .$$

In particular $H(2, 1)$ is the Klein curve, i.e., the algebraic curve of genus $g=3$ whose group of automorphisms has the order $168=84(g-1)$. Let

$$N=a^2+ab+b^2 .$$

Then we have $(N, a)=(N, b)=1$. If we regard a and b as elements of $(\boldsymbol{Z}/N\boldsymbol{Z})^\times$, then we have $ab^{-1}\in C(N)$, i.e., g.c.d. $(N, 1+\langle ab^{-1}\rangle)=1$ and $(ab^{-1})^2+(ab^{-1})+1\equiv 0 \bmod N$.

LEMMA 3.6. *Let N be a positive integer. Then the following are equivalent:*

(1) *There exists $r\in C(N)$ such that $r^2+r+1\equiv 0 \bmod N$;*

(2) *If $N=3^{e_0}p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$ is the decomposition into prime factors, then $e_0=0$ or 1 and $p_i\equiv 1 \bmod 3$ for all i.*

PROOF. (1)$\Rightarrow$(2) If the equation

(3.4) $$X^2+X+1=0$$

has a solution in $(\boldsymbol{Z}/N\boldsymbol{Z})^{\times}$, then it has a solution r in each $(\boldsymbol{Z}/p_i\boldsymbol{Z})^{\times}$ for $i=0, 1, \cdots, n$, where $p_0=3$. Since the subgroup $\langle r\rangle$ generated by r is of order 3 or 1, it follows that $p_i=3$ or 3 divides the order p_i-1 of $(\boldsymbol{Z}/p_i\boldsymbol{Z})^{\times}$. Thus we have $p_i\equiv 1 \bmod 3$. On the other hand the equation (3.3) has no solution in $(\boldsymbol{Z}/9\boldsymbol{Z})^{\times}$. Therefore we have $e_0=0$ or 1.

(2)⇒(1) For each i, we have a solution of (3.4) in $(\boldsymbol{Z}/P_i\boldsymbol{Z})^{\times}$ where $P_i=p_i^{e_i}$. By the isomorphism

$$(\boldsymbol{Z}/N\boldsymbol{Z})^{\times}\cong(\boldsymbol{Z}/P_0\boldsymbol{Z})^{\times}\times\cdots\times(\boldsymbol{Z}/P_n\boldsymbol{Z})^{\times} \tag{3.5}$$

we get a required solution. Q.E.D.

From now on we fix a positive integer

$$N=3^{e_0}p_1^{e_1}\cdots p_n^{e_n}$$

satisfying the condition (2) in Lemma 3.6. Then we have

LEMMA 3.7. *Let*

$$\Omega(N)=\{r\in C(N)\mid r^2+r+1=0\}$$

and

$$H(N)=\{(a, b)\in\boldsymbol{N}\times\boldsymbol{N}\mid N=a^2+ab+b^2,\ \text{g.c.d.}(N, a)=\text{g.c.d.}(N, b)=1\}.$$

Then the map of $H(N)$ to $\Omega(N)$ defined by $(a, b)\to ab^{[-1]}$ is bijective and $|\Omega(N)|=|H(N)|=2^n$, $b^{[-1]}$ is an integer such that $bb^{[-1]}\equiv 1 \bmod N$.

PROOF. We shall show that the injectivity of the map $(a, b)\to ab^{[-1]}$. There are two uniquely determined integers s and r satisfying

$$xs-yr=1$$

and the integer

$$l(x, y)=(2x+y)r+(x+2y)s$$

satisfies

$$l(x, y)^2\equiv -3 \bmod 4N, \qquad 0\leqq l(x, y)<2N. \tag{3.6}$$

(cf. [4] Chapter 11 Theorem 4.1). Then we have

$$\frac{(l(x, y)-1)}{2}=(x+y)r+ys$$

and

$$\frac{x\cdot(l(x, y)-1)}{2}=Nr+y,$$

hence we have

$$\frac{(l(x, y)-1)}{2} \equiv x^{[-1]}y \mod N.$$

If $ab^{[-1]} \equiv a'(b')^{[-1]}$, then we have

$$\frac{(l(a, b)-1)}{2} \equiv \frac{(l(a', b')-1)}{2} \mod N.$$

By (3.6), we have

$$l(a, b)=l(a', b').$$

It follows that there exists a unit u in the ring of the integers in $Q(\sqrt{-3})$ satisfying

$$a+b\omega=(a'+b'\omega)u$$

where $\omega=(1+\sqrt{-3})/2$ (cf. ibid, Chapter 11 Theorem 4.2). Since a, b, a' and b' are positive, we have $(a, b)=(a', b')$. This completes the proof. Q.E.D.

LEMMA 3.8. $H(a, b) \cong H(b, a) \cong F(a, b) \cong F(1, \langle ab^{[-1]}\rangle)$.

PROOF. The defining equation of the N-th Fermat curve is

$$U^N+V^N+W^N=0.$$

We put

$$X=U^{a+b}V^b, \qquad Y=V^{a+b}W^b, \qquad Z=W^{a+b}U^b.$$

Then we have the defining equatiin of the Hurwitz curve of index (a, b):

$$X^bY^{a+b}+Y^bZ^{a+b}+Z^bX^{a+b}=0.$$

Moreover we have $k(x, y)=k(x, u^N)$ where $x=X/Z$, $y=Y/Z$ and $u=U/W$. In fact we have $x=u^a v^b$, $y=v^{a+b}u^{-b}$, $u^N=x^{a+b}/y^b$ and $v^N=x^b y^a$ where $v=V/W$. Therefore y^a and $y^b \in k(x, u^N)$, because $v^N=-(u^N+1) \in k(x, u^N)$. Since $(a, b)=1$, $y \in k(x, u^N)$.

Now let $r=-u^N$ and $s=\xi x$ where $\xi^N=(-1)^{a+b}$. Then we have

$$s^N=r^a(1-r)^b;$$

hence we have $H(a, b) \cong F(a, b)$. Q.E.D.

Combining Lemma 3.7 and 3.8, we get

LEMMA 3.9. *Let $c \in C(N)$. Then $F(c)$ is a Hurwitz curve, i.e., there exists a pair (a, b) of relatively prime integers such that $N=a^2+ab+b^2$ and $ab^{[-1]} \equiv c$* mod N *if and only if $c^2+c+1=0$.*

Let $a \in \Omega(N)$, i.e., $a^2+a+1=0$. Then we have $\phi\varphi(a)=a$, hence we have the automorphism $(\psi\varphi)_a : F(a) \to F(a)$, which we denote $\tau(a)$. By an easy calculatiin (cf. Lemma 3.3), we have

LEMMA 3.10. *$\tau(a) \cdot \sigma(a) = \sigma(a)^\alpha \cdot \tau(a)$, where $\alpha = N - \langle a^{-1} \rangle - 1 \geqq 2$.*

EXAMPLE 3.1. Let $N=39$. Then we have

$$C(N) = \{1, 4, 7, 10, 16, 19, 22, 28, 31, 34, 37\}.$$

We have three orbits of the action of G:

(i) $\{1, 19, 37\}$, $F(1, 1)$ is a hyperelliptic curve;

(ii) $\{4, 7, 10, 28, 31, 34\}$;

(iii) $\{16, 22\} = \Omega(N)$, $F(1, 16)$ is a Hurwitz curve of index $(2, 5)$.

3.4. Isomorphism theorem.

Now we shall prove the main theorem in this paper.

THEOREM 3.11. *Let a and b be elements in $C(N)$. Then $F(a)$ and $F(b)$ are isomorphic if and only if there exists an element θ in the group G (cf. the section 3.1) such that $\theta(a) = b$.*

PROOF. "if"-part comes from Lemma 3.3. When $F(a)$ is the Klein curve, then the proof is obvious. So we shall exclude this case. Assume there is an isomorphism

$$f : F(a) \longrightarrow F(b).$$

Then we have $\langle f^{-1}\sigma(b) f \rangle = \langle \sigma(a) \rangle$ and $f(\mathrm{Fix}\,(\sigma(a))) = \mathrm{Fix}\,(\sigma(b))$ by Lemma 3.13 in the section 3.5. Now, put $f(P_i^{(a)}) = P_{f_i}^{(b)}$ $(i=0, 1, \infty)$, so we can take the element in G corresponding to the permutation $(f_0, f_1, f_\infty) \mapsto (0, 1, \infty)$. It means we may assume

$$f(P_i^{(a)}) = P_i^{(b)}, \qquad i=0, 1, \infty.$$

by Lemma 3.3 And we have $\mathrm{Gap}\,(P_0^{(a)}) = \mathrm{Gap}\,(P_0^{(b)})$; hence we have $A(a) = A(b)$ by Proposition 1.2. We put

$$A(c)^\times = A(c) \cap (\boldsymbol{Z}/N\boldsymbol{Z})^\times \qquad \text{for } c = a, b.$$

Then the theorem comes from the following:

LEMMA 3.12. *$A(a)^\times = A(b)^\times$ if and only if $a=b$ or $-b-1$.*

PROOF OF LEMMA. Since we have $A(-b-1) = A(b)$, it follows the proof of "if"-part. We shall now follow a technique of the proof of Theorem 1 in [6] to prove "only if"-part. For any $r\in(\boldsymbol{Z}/N\boldsymbol{Z})^{\times}$, we define an element $G(r)$ in the group algebra $\boldsymbol{Q}[\mathrm{Gal}(\boldsymbol{Q}(\zeta_N)/\boldsymbol{Q})]$, (where $\zeta_N=e^{2\pi i/N}$):

$$G(r)=\sum_{h\in(\boldsymbol{Z}/N\boldsymbol{Z})^{\times}} B_1(hr)\sigma_h$$

where $B_1(s)=\langle s\rangle/N-1/2$ and σ_h is the automorphism of $\boldsymbol{Q}(\zeta_N)$ over $\boldsymbol{Q}$ defined by $\zeta_N\to\zeta_N^h$. If $h\in A(a)^{\times}$ (resp. $h\notin A(a)^{\times}$), then $\langle h\rangle+\langle ha\rangle+\langle h(-a-1)\rangle=N$ (resp. $\langle h\rangle+\langle ha\rangle+\langle h(-a-1)\rangle=2N$). Hence we have

$$G(1)+G(a)+G(-a-1)\sum_{h\notin A(a)^{\times}}\frac{1}{2}\sigma_h-\sum_{h\in A(a)^{\times}}\frac{1}{2}\sigma_h\,.$$

It follows that

$$G(a)+G(-a-1)=G(b)+G(-b-1)\,. \tag{3.7}$$

Applying a character

$$\chi:\mathrm{Gal}(\boldsymbol{Q}(\zeta_N)/\boldsymbol{Q})\longrightarrow\boldsymbol{C}^{\times}$$

to both sides of (2.7), we get

$$B_{1,\chi}\bar{\chi}(a)+B_{1,\chi}\bar{\chi}(-a-1)=B_{1,\chi}\bar{\chi}(b)+B_{1,\chi}\bar{\chi}(-b-1)$$

where $B_{1,\chi}$ is the generalized Bernoulli number

$$B_{1,\chi}=\sum_h B_1(h)\chi(h)\,.$$

We fix an odd character χ_0. Then we have

$$\bar{\chi}_0(a)\bar{\psi}(a)+\bar{\chi}_0(-a-1)\bar{\psi}(-a-1)=\bar{\chi}_0(b)\bar{\psi}(b)+\bar{\chi}_0(-b-1)\bar{\psi}(-b-1) \tag{3.8}$$

for all even character ψ with $B_{1,\chi_0\psi}\neq 0$. Now we shall use the following results proved by Koblitz-Rohrlich (cf. ibid. section 2 Proposition, Remark 2 and Lemma):

SUBLEMMA A. *Suppose N is odd. Let $S(N)$ be the set of odd characters of $(\boldsymbol{Z}/N\boldsymbol{Z})^{\times}$, and let*

$$S_0(N)=\{\chi\in S(N)\mid B_{1,\chi}=0\}\,.$$

Then $|S_0(N)|\leqq(1/4)|S(N)|$ and equality holds if and only if $N=39$.

SUBLEMMA B. *Let A be a finite abelian group, S a subset of the group $\hat{A}$ of characters, T a subset of A. If*

$$|S|>\frac{|T|-1}{|T|}|A|$$

then the rows of the matrix

$$(\psi(g))_{(g,\psi)\in T\times S}$$

are linearly independent.

Suppose $N\neq 39$. Let $A=(\boldsymbol{Z}/N\boldsymbol{Z})^{\times}/\{+1,-1\}$. Then $\hat{A}$ can be naturally identified with the set of even characters of $(\boldsymbol{Z}/N\boldsymbol{Z})^{\times}$. We put

$$S=\{\psi\in\hat{A}\mid B_{1,\chi_0\psi}\neq 0\}$$

and

$$T=\{(a),(-a-1),(b),(-b-1)\}$$

where (c) denotes the element of A determined by c. By sublemma A, we have

$$\frac{|S|}{|A|}>\frac{3}{4}.$$

Considering the relations (3.8), we have $a=b$ or $-b-1$ by sublemma B.

When $N=39$, $A(1)$, $A(4)$ and $A(16)$ are distinct from each other (cf. Example 3.1.). This completes the proof of Lemma. Q.E.D.

3.5. The group $\mathrm{Aut}(F(a))$ of automorphisms.

As usual let X be a curve of genus $g\geqq 2$ and let σ be an automorphism of order $N=2g+1$. We denote by $\mathrm{Aut}(X)$ the group of automorphisms of X.

LEMMA 3.13. *Let X be a non-hyperelliptic curve of genus $g\geqq 3$ and let H be a cyclic subgroup of $\mathrm{Aut}(X)$ of order $2g+1$. Assume X is not isomorphic to the Klein curve: $H(1, 2)$. Then H is a normal subgroup of $\mathrm{Aut}(X)$ of index $\leqq 3$.*

PROOF. Let $\pi: X\to X/\mathrm{Aut}(X)$ be the projection. The genus of X/H is zero, so is $X/\mathrm{Aut}(X)$. Let $\{\lambda_1, \lambda_2, \cdots, \lambda_n\}$ be the set of branch points. Take a point P_i such that $\pi(P_i)=\lambda_i$ and put

$$G_i=\{\sigma\in\mathrm{Aut}(X)\mid\sigma(P_i)=P_i\},$$

which is a cyclic subgroup of $\mathrm{Aut}(X)$. We denote by e_i the order of G_i and assume $2\leqq e_1\leqq e_2\leqq\cdots$. H is a subgroup of some G_i. Then $e_i=m(2g+1)$ for some positive integer m. Moreover we have $m=1$ or 2 by Theorem 3.5. If $m=2$, then $X\cong F(1)$ which is a hyperelliptic curve. By the Riemann-Hurwitz formula for π:

$$\frac{2g-2}{|\mathrm{Aut}(X)|}=-2+\sum_{i=1}^{n}\left(1-\frac{1}{e_i}\right), \tag{3.9}$$

we easily have $n=3$. Then we have

$$\frac{2g-2}{|\mathrm{Aut}(X)|}=1-\left(\frac{1}{e_1}+\frac{1}{e_2}+\frac{1}{2g+1}\right). \tag{3.10}$$

By this relation we have $|\mathrm{Aut}(X):H|\leqq 3$ except $(e_1, e_2)=(2, 3)$. In the exceptional case (3.10) becomes

$$\frac{2g-1}{2g-5}=\frac{|\mathrm{Aut}(X):H|}{6}>1;$$

hence we have $|\mathrm{Aut}(X):H|\leqq 12$ and $\equiv 0 \bmod 4$ for $g\geqq 4$. If $|\mathrm{Aut}(X):H|=8$ then $g=7$ and $2g+1=15$. If $|\mathrm{Aut}(X):H|=12$, then $g=4$ and $2g+1=9$. Since $|C(15)|=|C(9)|=3$ by Lemma 3.2, such curves are hyperelliptic. When $g=3$, we have $|\mathrm{Aut}(X):H|=24$. Then X is the Klein curve. Thus we have shown that $|\mathrm{Aut}(X):H|\leqq 3$. Since the order of H is odd, H is a normal subgroup of $\mathrm{Aut}(X)$. Q.E.D.

As we saw in the section 3.2, the hyperelliptic curve $F(1)$ is defined by the equation:

$$x^2=y^{2g+1}-1.$$

The automorphism $\tilde{\sigma}$ of $F(1)$ defined by $\tilde{\sigma}^*(x, y)=(-x, \zeta_{2g+1}y)$ has the order $4g+2$ and $\tilde{\sigma}^2=\sigma(1)$. Then the following fact is well-known and it is proved by arguments similar to the proof of the preceding lemma, so we shall omit its proof.

LEMMA 3.14. $\mathrm{Aut}(F(1))=\langle\tilde{\sigma}\rangle$.

LEMMA 3.15. *Let a and b be elements in $C(N)$. Assume $F(a)$ is not the Klein curve. If*

$$f: F(a) \longrightarrow F(b)$$

is an isomorphism, then $\langle\sigma(a)\rangle=\langle f^{-1}\sigma(b)f\rangle$. In particular we have

$$f(\mathrm{Fix}(\sigma(a)))=\mathrm{Fix}(\sigma(b)).$$

PROOF. We put $H=\langle\sigma(a)\rangle$ and $H'=\langle f^{-1}\sigma(b)f\rangle$. By Lemma 3.13 and 3.14, we have $|HH':H|\leqq 3$ unless $F(a)$ is the Klein curve. Since the order of H is $N=2g+1\geqq 5$, we have $|HH':H|=1$ or 3. If $F(a)$ is hyperelliptic then $|HH':H|=1$ and $H=H'$. Otherwise $(f^{-1}\sigma(b)f)^3\in H$. Therefore we have $\mathrm{Fix}(\sigma(a))=\mathrm{Fix}(f^{-1}\sigma(b)f)$. Since the stabilizer group at $F_0^{(a)}$ is H, we have $H=H'$. Q.E.D.

Let $a\in C(N)$. By the preceding lemma, we see that each automorphism of $F(a)$ induces a permutation of the three points in $\mathrm{Fix}(\sigma(a))=\{P_0, P_1, P_\infty\}$. Therefore we get a homomorphism:

$$p(a): \mathrm{Aut}(F(a)) \longrightarrow \mathrm{Per}(\mathrm{Fix}(\sigma(a))),$$

where $\mathrm{Per}(\mathrm{Fix}(\sigma(a)))$ is the group of permutations.

THEOREM 3.16. *Assume $F(a)$ is not the Klein curve. Then we have an exact sequence:*

$$1 \longrightarrow \langle\sigma(a)\rangle \longrightarrow \mathrm{Aut}(F(a)) \longrightarrow G_a .$$

where G_a is the stabilizer subgroup of G at a.

PROOF. Since the kernel of $p(a)$ is $\langle\sigma(a)\rangle$ (cf. Lemma 3.1 in [9]), it is enough to show $\mathrm{Im}(p(a))\cong G_a$. If $|G_a|=2$, i.e., $F(a)$ is hyperelliptic, then there is only one Weierstrass point in $\mathrm{Fix}(\sigma(a))$. Hence we have $|\mathrm{Im}(p(a))|=2$. If $|G_a|=3$, i.e., $F(a)$ is a Hurwitz curve, then the automorphism $\tau(a)$ induces a permutation of order 3. Assume $|G_a|=1$. Let

$$f: F(a) \longrightarrow F(a)$$

be an automorphism. Then by Lemma 3.3 we have an element $\theta\in G$ such that

$$(f\cdot\theta_a)(P_i^{(a)})=P_i^{(\theta(a))} \qquad \text{for } i=0, 1, \infty .$$

Then by Lemma 3.12 we have $\theta(a)=a$ or $-a-1$. If $\sigma(a)=a$, we have $\theta=1$ by $G_a=\{1\}$; hence $f\in\langle\sigma(a)\rangle$. Suppose $\theta(a)=-a-1$. Then the composite morphism

$$f'=(\phi\cdot\varphi\cdot\phi)_a^{-1}\cdot\theta_a\cdot f: F(a) \longrightarrow F(-a-1) \longrightarrow F(a)$$

satisfies

$$f'(P_0^{(a)})=P_0^{(a)}, \qquad f'(P_1^{(a)})=P_\infty^{(a)} .$$

Therefore $(f')^2\in\langle\sigma(a)\rangle$, i.e., the order of f' is $2N=2(2g+1)$. Then $F(a)$ is hyperelliptic by Theorem 3.5; hence $|G_a|=2$. This is a contradiction. Q.E.D.

REMARK 3.3. If $F(a)$ is a Hurwitz curve then the exact sequence in the theorem does not split (cf. Lemma 3.11).

References

[1] C, Earle, Some Jacobians which split, Lecture Notes in Math. **747** (1979), 101-107.
[2] H. M. Farkas and I. Kra, Riemann surfaces, G. T. M. Springer-Verlag, 1980.
[3] W. J. Harvey, Cyclic groups of automorphisms of a compact Riemann surfaces, Quart. J. Math. Oxford(2) 17 (1977), 86-97.
[4] L. K. Hua, Introduction to Number Theory, Springer-Verlag, 1982.
[5] A. Hurwitz, Über die diophantische Gleichung $x^3y+y^3z+z^3x=0$, Math. Ann. **41** (1908), 428-430.
[6] N. Koblitz and D. Rohrlich, Simple factors in the Jacobian of a Fermat curve, Can. J. Math. **30** (1978), 1183-1205.
[7] S. Lang, Complex multiplication, Springer-Verlag, 1983.
[8] K. Nakagawa, On the orders of automorphisms of a closed Riemann surface, Pacific J. Math. **115** (1984), 435-443.

[9] A. Seyama, On the curves of genus g with automorphisms of prime order $2g+1$, Tsukuba J. Math. **6** (1982), 62–77.

Susumu Irokawa
Department of Mathematics,
Faculty of Science and Technology
Science University of Tokyo
Noda, Chiba 278
Japan

Ryuji Sasaki
Department of Mathematics
College of Science and Technology
Nihon University
Kanda, Tokyo 101
Japan