ON BRANCHED COVERING OF COMPACT RIEmann SURFACES WITH AUTOMORPHISMS*

Gustavo Labbé Morales
Universidad de La Serena, La Serena - Chile

Abstract

In this work, we give an algorithm to count the different conformal equivalence classes of compact Riemann surfaces that admit a group of automorphisms isomorphic to \( \mathbb{Z}/n\mathbb{Z} \), \( n \in \mathbb{N} \), and that are branched coverings of the Riemann sphere, with signature \( (n,0); m_1, m_2, m_3 \), \( m_1, m_2, m_3 \in \mathbb{N} \).

By using the previous result, we count the different conformal equivalence classes of compact Riemann surfaces in the cases of coverings with signature \( (p,0); p, p, p \), \( p \geq 5 \) and prime, and signature \( (p^2,0); p^2, p^2, p \), \( p \geq 3 \) and prime.

--

*Partially supported by grant 130-2-18, DIULS, U. de La Serena and by CIMAT, Guanajuato-México.
1. Introduction.

Let $\mathcal{M}_g$ be the moduli space of equivalence classes of compact Riemann surfaces of genus $g$. In this space, the surfaces with a cyclic group of automorphisms are of special significance and were studied by Scorza, Lefschetz and Weil among others.

Lefschetz [3] consider the Riemann surfaces of genus $g = (p - 1)/2$ given by algebraic equations of the form $y^p = x^\alpha(x - 1)$ where $\alpha$ is an integer and where $p$ is a prime, and asked whether for different values of $\alpha$ these surfaces were conformally distinct.

On the other hand, Lloyd [4] study the number of inequivalent Riemann surface transformation groups $(G, S)$ which have to $(\Gamma, D)$ as universal covering group, where $G$ is a finite group, $\Gamma$ is a Fuchsian group and $D$ is the upper half plane.

Finally, Harvey [2] study the equivalence classes of subloci under the action of the modular group and compute the number of conjugacy classes of elements of prime order in the mapping class group of compact surfaces.

2. Branched Coverings of the Sphere with Signature $\langle (n, 0); m_1, m_2, m_3 \rangle$.

In this section, we give an algorithm to count the different conformal equivalence classes of compact Riemann surfaces that admit a group of automorphisms isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and that are branched coverings of the Riemann sphere with signature $\langle (n, 0); m_1, m_2, m_3 \rangle$ where $m_1 \geq m_2 \geq m_3$, $n, m_i \in \mathbb{N}, i = 1, 2, 3$.

By Harvey [2], such coverings exist if and only if:

1. $m_i | n, i = 1, 2, 3$

2. $\mcm(m_1, m_2, m_3) = \mcm(m_1, m_2) = \mcm(m_1, m_3) = \mcm(m_2, m_3) = \frac{n}{n}$

By the Riemann-Hurwitz relation, the genus $g$ of $S$ is given by

$$g = -n + 1 + \frac{n}{2} [3 - (\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3})].$$

Also by Harvey [2], these Riemann surfaces are characterized by the algebraic curves:

$$y^n = (x - x_1)^\alpha(x - x_2)^\beta(x - x_3)^\tau,$$
\( x_i \neq x_j, \ i, j \in \{1, 2, 3\}, \ i \neq j \) where 

(i) \( 1 \leq \alpha, \beta, \tau < n \)

(ii) \( n|\alpha + \beta + \tau \)

(iii) \( \gcd(\alpha, n) = \frac{n}{m_1}, \ \gcd(\beta, n) = \frac{n}{m_2}, \ \gcd(\tau, n) = \frac{n}{m_3}. \)

We denote by \( S_{(\alpha, \beta, \tau)} \) the Riemann surface characterized by the algebraic curve \((*)\).

By using the notations of \([6]\), this surface is obtained by taking \(n\)-copies of the Riemann sphere, cutting along the curves \(\sigma_1, \sigma_2\) and \(\sigma_3\) as it is shown in the Figure 1, and identifying using the exponents \(\alpha, \beta\) and \(\tau\) around the branch points \(x_1, x_2\) and \(x_3\).

Around \(x_1\), the exponent \(\alpha\) gives the identifications of copies (or sheets):

\[
\begin{align*}
(1) & \ 1 + \alpha & 1 + 2\alpha & \ldots & 1 + (m_1 - 1)\alpha \pmod{n} \\
(2) & \ 2 + \alpha & 2 + 2\alpha & \ldots & 2 + (m_1 - 1)\alpha \pmod{n} \\
\vdots & \ \vdots & \ \vdots & \ \vdots & \ \vdots \\
(\frac{n}{m_1}) & \ \frac{n}{m_1} + \alpha & \frac{n}{m_1} + 2\alpha & \ldots & \frac{n}{m_1} + (m_1 - 1)\alpha \pmod{n};
\end{align*}
\]

there are \(\frac{n}{m_1}\) cycles of length \(m_1\).

Around \(x_2\), the exponent \(\beta\) gives the identifications:

\[
\begin{align*}
(1) & \ 1 + \beta & 1 + 2\beta & \ldots & 1 + (m_2 - 1)\beta \pmod{n} \\
(2) & \ 2 + \beta & 2 + 2\beta & \ldots & 2 + (m_2 - 1)\beta \pmod{n} \\
\vdots & \ \vdots & \ \vdots & \ \vdots & \ \vdots \\
(\frac{n}{m_2}) & \ \frac{n}{m_2} + \beta & \frac{n}{m_2} + 2\beta & \ldots & \frac{n}{m_2} + (m_2 - 1)\beta \pmod{n};
\end{align*}
\]

there are \(\frac{n}{m_2}\) cycles of length \(m_2\), and around \(x_3\), the exponent \(\tau\) gives the identifications:

\[
\begin{align*}
(1) & \ 1 + \tau & 1 + 2\tau & \ldots & 1 + (m_3 - 1)\tau \pmod{n} \\
(2) & \ 2 + \tau & 2 + 2\tau & \ldots & 2 + (m_3 - 1)\tau \pmod{n} \\
\vdots & \ \vdots & \ \vdots & \ \vdots & \ \vdots \\
(\frac{n}{m_3}) & \ \frac{n}{m_3} + \tau & \frac{n}{m_3} + 2\tau & \ldots & \frac{n}{m_3} + (m_3 - 1)\tau \pmod{n};
\end{align*}
\]

there are \(\frac{n}{m_3}\) cycles of length \(m_3\).
Let $\alpha = \frac{n}{m_1}$, then by using a conformal automorphism of the surface, we may reenumerate the sheets according to the rule:

\[
\begin{align*}
1 & \rightarrow 1 \\
(1 + \alpha) \pmod{n} & \rightarrow 1 + \frac{n}{m_1} \\
\vdots & \vdots \vdots \\
\{1 + (m_1 - 1)\alpha\} \pmod{n} & \rightarrow 1 + (m_1 - 1) \frac{n}{m_1} \\
2 & \rightarrow 2 \\
(2 + \alpha) \pmod{n} & \rightarrow 2 + \frac{n}{m_1} \\
\vdots & \vdots \vdots \\
\{2 + (m_1 - 1)\alpha\} \pmod{n} & \rightarrow 2 + (m_1 - 1) \frac{n}{m_1} \\
\vdots & \vdots \vdots \\
\frac{n}{m_1} & \rightarrow \frac{n}{m_1} \\
\left(\frac{n}{m_1} + \alpha\right) \pmod{n} & \rightarrow \frac{2n}{m_1} \\
\vdots & \vdots \vdots
\end{align*}
\]
\[ \left\{ \frac{n}{m_1} + (m_1 - 1)\alpha \right\} \pmod{n} \rightarrow n, \]

with which we may assume that the identifications associated to \( x_1 \) are the \( \frac{n}{m_1} \) cycles of length \( m_1 \):

\[
\left\{ \begin{array}{cccc}
1 & 1 + \frac{n}{m_1} & 1 + 2\frac{n}{m_1} & \ldots \quad 1 + (m_1 - 1)\frac{n}{m_1} \\
2 & 2 + \frac{n}{m_1} & 2 + 2\frac{n}{m_1} & \ldots \quad 2 + (m_1 - 1)\frac{n}{m_1} \\
\vdots & \vdots & \vdots & \ddots \\
\frac{n}{m_1} & 2\frac{n}{m_1} & 3\frac{n}{m_1} & \ldots \quad n.
\end{array} \right.
\]

Thus, the algebraic curves that characterize the Riemann surfaces \( S \) which are branched coverings of the Riemann sphere with signature \( (n, 0); m_1, m_2, m_3 \) and admit a group of automorphisms isomorphic to \( \mathbb{Z}/n\mathbb{Z} \) are given by the family:

\[
(\circ) \quad y^n = (x - x_1)^{\frac{n}{m_1}}(x - x_2)^{\beta}(x - x_3)^{\tau}
\]

with \( 0 < \beta, \tau < n, \frac{n}{m_1} + \beta + \tau, \gcd(\beta, n) = \frac{n}{m_2}, \gcd(\tau, n) = \frac{n}{m_3} \).

**Definition 1.** For \( n, m_1, m_2, m_3 \in \mathbb{N} \) such that

1. \( m_i | n, \ i = 1, 2, 3 \).
2. \( \operatorname{mcm}(m_1, m_2, m_3) = \operatorname{mcm}(m_1, m_2) = \operatorname{mcm}(m_1, m_3) = \operatorname{mcm}(m_2, m_3) = n \),

we define

\[
A^n = A^n(m_1, m_2, m_3) = \{ (\frac{n}{m_1}, \beta, \tau) / 0 < \beta, \tau < n, n| (\frac{n}{m_1} + \beta + \tau),
\]

\[\gcd(\beta, n) = \frac{n}{m_2}, \gcd(\tau, n) = \frac{n}{m_3} \}.
\]

Hence, there exists a bijection between the elements of \( A^n \) and the algebraic curves given by \( (\circ) \). This bijection is given by:

\[
\left( \frac{n}{m_1}, \beta, \tau \right) \leftrightarrow y^n = (x - x_1)^{\frac{n}{m_1}}(x - x_2)^{\beta}(x - x_3)^{\tau} \leftrightarrow S_{(\frac{n}{m_1}, \beta, \tau)}.
\]
Remark 1.

(1) If \( m_1 = m_2 = m_3 \) and \((\alpha, \beta, \tau) \in A^n\), then
\[
S_{(\alpha, \beta, \tau)} \simeq S_{(\beta, \tau, \alpha)} \simeq S_{(\tau, \alpha, \beta)} \simeq S_{(\alpha, \tau, \beta)} \simeq S_{(\beta, \alpha, \tau)},
\]

since a permutation of \((\alpha, \beta, \tau)\) is equivalent to a conformal automorphism of \(S_{(\alpha, \beta, \tau)}\) that exchanges the branch points.

(2) If \( m_1 = m_2 \neq m_3 \) (or \( m_1 \neq m_2 = m_3 \)) and \((\alpha, \beta, \tau) \in A^n\), then
\[
S_{(\alpha, \beta, \tau)} \simeq S_{(\beta, \alpha, \tau)} \quad \text{(or } S_{(\alpha, \beta, \tau)} \simeq S_{(\alpha, \tau, \beta)}\text{)},
\]

since they differ by an automorphism that exchanges \(x_1\) and \(x_2\), and fixes \(x_3\) (or exchanges \(x_2\) and \(x_3\), and fixes \(x_1\)).

(3) We denote by \((Z/nZ)^* = \{ k \in (Z/nZ) | \gcd(k, n) = 1 \}\), that is, \((Z/nZ)^*\) are the elements invertibles of \(Z/nZ\).

Definition 2. For \((\frac{n}{m_1}, \beta, \tau), (\frac{n}{m_1}, \beta', \tau') \in A^n\) we define:

\[
(\frac{n}{m_1}, \beta, \tau) \simeq (\frac{n}{m_1}, \beta', \tau') \Longleftrightarrow \text{there exist } k \in (Z/nZ)^* \text{ such that}
\]

(1) \((\frac{n}{m_1}, \beta', \tau') \equiv (\frac{kn}{m_1}, k\beta, k\tau) \pmod{n} \pmod{\text{Per}}\) if \(m_1 = m_2 = m_3\).

(2) \((\frac{n}{m_1}, \beta') \equiv (\frac{kn}{m_1}, k\beta) \pmod{n} \pmod{\text{Per}}\) and \(\tau' \equiv k\tau \pmod{n}\) if \(m_1 = m_2 \neq m_3\).

(3) \(\frac{n}{m_1} \equiv \frac{kn}{m_1} \pmod{n}\) and \((\beta', \tau') \equiv (k\beta, k\tau) \pmod{n} \pmod{\text{Per}}\) if \(m_1 \neq m_2 = m_3\).

(4) \((\frac{n}{m_1}, \beta', \tau') \equiv (\frac{kn}{m_1}, k\beta, k\tau) \pmod{n}\) if \(m_i \neq m_j, \ i, j = 1, 2, 3, \ i \neq j\).

It is clear that this relation is an equivalence relation on \(A^n\).

Proposition 1. Let \((\frac{n}{m_1}, \beta, \tau), (\frac{n}{m_1}, \beta', \tau') \in A^n\) be, such that \((\frac{n}{m_1}, \beta, \tau) \simeq (\frac{n}{m_1}, \beta', \tau')\). Then
\[
S_{(\frac{n}{m_1}, \beta, \tau)} \simeq S_{(\frac{n}{m_1}, \beta', \tau')},
\]

Proof. It is sufficient to show that for \(k \in (Z/nZ)^*\)
\[
S_{(\frac{kn}{m_1}, k\beta, k\tau)} \pmod{n} \simeq S_{(\frac{n}{m_1}, \beta, \tau)}.
\]
In fact, we have that \((\frac{kn}{m_1}, k\beta, k\tau) \pmod{n}\) gives the identifications of the sheets around the branch points \(x_1, x_2\) and \(x_3\) as follows:

\[
\begin{align*}
\{ (1 + \frac{kn}{m_1}) & \pmod{n} & \rightarrow & 1 + \frac{n}{m_1} \\
\{ 1 + (m_1 - 1)\frac{kn}{m_1} & \pmod{n} & \rightarrow & 1 + (m_1 - 1)\frac{n}{m_1} \\
\{ 2 + \frac{kn}{m_1} & \pmod{n} & \rightarrow & 2 + \frac{n}{m_1} \\
\{ 2 + (m_1 - 1)\alpha & \pmod{n} & \rightarrow & 2 + (m_1 - 1)\frac{n}{m_1} \\
\{ \frac{n}{m_1} + \frac{kn}{m_1} & \pmod{n} & \rightarrow & \frac{2n}{m_1} \\
\{ \frac{n}{m_1} + (m_1 - 1)\frac{kn}{m_1} & \pmod{n} & \rightarrow & n, \\
\end{align*}
\]

Now by using a conformal automorphism that reenumerates the sheets according to the rule:
we obtain \( k = 1 \) and the permutations given above correspond to the permutations associated to \( \left( \frac{n}{m_1}, \beta, \tau \right) \). Hence

\[
S\left( \frac{kn}{m_1}, k\beta, k\tau \right) \pmod{n} \cong S\left( \frac{n}{m_1}, \beta, \tau \right).
\]

**Case 1:** \( m_1 = m_2 = m_3 = n \). We have that there exists \( k \in (\mathbb{Z}/n\mathbb{Z})^* \) such that

\[
\left( \frac{n}{m}, \beta', \tau' \right) \equiv \left( \frac{kn}{m}, k\beta, k\tau \right) \pmod{n} \pmod{\text{Per}}.
\]

By remark 1:

\[
S\left( \frac{kn}{m}, k\beta, k\tau \right) \pmod{n} \cong S(\theta_1, \theta_2, \theta_3)
\]

where \((\theta_1, \theta_2, \theta_3)\) is any permutation of \( \left( \frac{kn}{m}, \beta, k\tau \right) \pmod{n} \), in particular \((\theta_1, \theta_2, \theta_3) = \left( \frac{n}{m}, \beta', \tau' \right)\) and so

\[
S\left( \frac{n}{m}, \beta, \tau \right) \cong S\left( \frac{kn}{m}, k\beta, k\tau \right) \pmod{n} \cong S\left( \frac{kn}{m}, \beta', \tau' \right).
\]

**Case 2:** \( m_1 = m_2 \neq m_3 \) (or \( m_1 \neq m_2 = m_3 \)). In this case, there exists \( k \in (\mathbb{Z}/n\mathbb{Z})^* \) such that

\[
\left( \frac{kn}{m_1}, \beta, k\tau \right) \equiv \left\{ \begin{array}{l}
\left( \frac{kn}{m_1}, \beta, k\tau \right) \pmod{n} \\
\left( k\beta, \frac{kn}{m_1}, k\tau \right) \pmod{n}
\end{array} \right.
\]

Hence:

\[
(**) \quad S\left( \frac{n}{m_1}, \beta, \tau \right) \cong S\left( \frac{kn}{m_1}, k\beta, k\tau \right) \pmod{n} \cong S\left( \frac{kn}{m_1}, \beta', \tau' \right)
\]

or

\[
S\left( \frac{n}{m_1}, \beta, \tau \right) \cong S\left( k\beta, \frac{kn}{m_1}, k\tau \right) \pmod{n} \cong S\left( \frac{n}{m_1}, \beta', \tau' \right).
\]

**Case 3:** \( m_i \neq m_j, i, j = 1, 2, 3, i \neq j \). Then there exists \( k \in (\mathbb{Z}/n\mathbb{Z})^* \) such that

\[
\left( \frac{n}{m_1}, \beta', \tau' \right) \equiv \left( \frac{kn}{m_1}, k\beta, k\tau \right) \pmod{n}.
\]

Hence we have (**). 

\[\text{Remark 2.}\] Thus, to calculate the number of different conformal equivalence classes of compact Riemann surfaces which are branched coverings of the sphere with signature \( \langle (n, 0); m_1, m_2, m_3 \rangle \) and which admit a group of automorphisms isomorphic to \( \mathbb{Z}/n\mathbb{Z} \) we have to determine the cardinality to \( A^n/\sim \).
3. Branched Coverings with Signature  
\((p,0);p,p,p)\) and with Signature  
\((p^2,0);p^2,p^2,p)\).

In this section, by using the result of the section 1, we count the different conformal equivalence classes of compact Riemann surfaces \(S\) which are branched coverings of degree \(p\) of the Riemann sphere with signature  
\((p,0);p,p,p)\), with \(p \geq 5\) and prime, which admit a group of automorphisms isomorphic to \(\mathbb{Z}/p\mathbb{Z}\).

Also we count the different conformal equivalence classes of compact Riemann surfaces \(S\) which are branched coverings of degree \(p^2\) of the Riemann sphere with signature  
\((p^2,0);p^2,p^2,p)\), \(p \geq 3\) and prime, which admit a group of automorphisms isomorphic to \(\mathbb{Z}/p^2\mathbb{Z}\).

3.1. Branched Coverings with Signature  
\((p,0);p,p,p)\).

Let \(S\) be the compact Riemann surfaces which are branched coverings of the Riemann sphere with signature  
\((p,0);p,p,p)\), \(p \geq 5\) and prime, which admit a group of automorphisms isomorphic to \(\mathbb{Z}/p\mathbb{Z}\).

In this case, the genus \(g\) of \(S\) is \(g = \frac{p-1}{2}\).

By section 1, these Riemann surfaces are characterized by the algebraic curves:

\[y^p = x(x - 1)^\beta(x - i)^\tau\]

where \(1 \leq \beta \leq \tau < p\) and \(1 + \beta + \tau = p\).

Hence, we consider the set:

\[A^p = A^p(p,p,p) = \{(1,\beta,\tau)/\beta,\tau \in \mathbb{N}, 1 \leq \beta \leq \tau < p, 1 + \beta + \tau = p\}\.

The equivalence relation on \(A^p\) is given by:

\[(1,\beta,\tau) \sim (1,\beta',\tau') \iff\] there exists \(k \in \{1,2,\ldots,p-1\}\) such that \((1,\beta',\tau') \equiv (k,k\beta,k\tau) \pmod{p} \pmod{Per}\).

**Lemma 1.** Let \(p \geq 5\) be and prime. Then

(i) \(3 \mid (p-1) \implies \frac{p-5}{2} \equiv 0 \pmod{3}\)

(ii) \(3
\mid(p-1) \implies \frac{p-5}{2} \equiv 1 \pmod{3}\)
The following proposition was proven by I. Barradas.

**Proposition 2.** Let $p \geq 5$ be and prime. Then, there exists $eta \in \mathbb{Z}/p\mathbb{Z}$ such that $\beta^2 \equiv p - 3 \pmod{3} \iff 3 \mid (p - 1)$.

**Proof.** It is known that $p - 3$ is a quadratic residue in $\mathbb{Z}/p\mathbb{Z}$ if and only if 

$$ (p - 3)^{\frac{p-1}{2}} \equiv 1 \pmod{p}. $$

Now, if $p$ and $q$ are primes $> 2$, then by the quadratic reciprocity theorem (see [1]):

$$ (\Delta) \quad [p^{\frac{q-1}{2}} \pmod{q}][q^{\frac{p-1}{2}} \pmod{p}] = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}; $$

that is, the quadratic character of the prime $p$ with respect to the $q$ is the same or opposite to the quadratic character of $q$ with respect to $p$, according to at least one or none of these primes is of the form $4n + 1$.

**Case 1:** $p \equiv 1 \pmod{4} \iff p - 1 \equiv 0 \pmod{4}$.

Thus

$$ (p - 3)^{\frac{p-1}{2}} \equiv (-3)^{\frac{p-1}{2}} \pmod{p} $$

$$ \equiv [(-3)^2]^{\frac{p-1}{4}} \pmod{p} $$

$$ \equiv 3^{\frac{p-1}{2}} \pmod{p}. $$

Now we apply $(\Delta)$ to the primes 3 and $p$ to obtain:

$$ [3^{\frac{p-1}{2}} \pmod{p}][p \pmod{3}] = (-1)^{\frac{p-1}{2}} = 1. $$

Hence:
\( p - 3 \) is a quadratic residue in \( \mathbb{Z}/p\mathbb{Z} \) if and only if

\[(p - 3)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \iff 3^{\frac{p-1}{2}} \equiv 1 \pmod{p} \iff p \equiv 1 \pmod{3} \iff 3 \mid (p - 1).\]

**Case 2:** \( p \equiv 3 \pmod{4} \iff p = 4n + 3 \) for some \( n \in \mathbb{N} \iff \frac{p-1}{2} = 2n + 1. \)

Now:

\[ (p - 3)^{\frac{p-1}{2}} \equiv (-3)^{2n+1} \pmod{p} \equiv -3^{2n+1} \pmod{p}. \]

We apply again (\( \Delta \)) to the primes 3 and \( p \) to obtain:

\[ [3^{\frac{p-1}{2}} \pmod{p}][p \pmod{3}] = (-1)^{2n+1} = -1 \iff \]

\[ [-3^{\frac{p-1}{2}} \pmod{p}][p \pmod{3}] = 1. \]

Thus:

\[ (p - 3)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \iff -3^{\frac{p-1}{2}} \equiv 1 \pmod{p} \iff \]

\[ p \equiv 1 \pmod{3} \iff 3 \mid (p - 1). \]

\[ \Box \]

**Corollary 1.** \( \alpha^2 + \alpha + 1 \equiv 0 \pmod{p} \) has a solution if and only if \( 3 \mid (p - 1) \). Moreover, if \( \beta \) is a root, then so is \( [p - (\beta + 1)] \pmod{p} \).

**Proof:** \( \alpha^2 + \alpha + 1 \equiv 0 \pmod{p} \) has solution \( \iff p - 3 \) is quadratic residues in \( \mathbb{Z}/p\mathbb{Z} \iff 3 \mid (p - 1) \).

Now, if \( \beta \) is a root, then:

\[ [p - (\beta + 1)]^2 + p - (\beta + 1) + 1 \equiv [(\beta + 1)^2 - \beta] \pmod{p} \equiv \beta^2 + \beta + 1 \pmod{p} \equiv 0 \pmod{p}. \]

\[ \Box \]

**Corollary 2.** Let \( p \geq 7 \) be a prime.

(i) If \( 3 \nmid (p - 1) \) and \( 2 \leq \beta \leq \frac{p-3}{2} \), then there exists a unique \( k, k' \in \{2, \ldots, p - 1\} \setminus \{\beta, p - (\beta + 1)\}, k \neq k' \) such that \( k\beta \equiv 1 \pmod{p} \) and \( k'[p - (\beta + 1)] \equiv 1 \pmod{p} \).
(ii) If \(3|(p-1)\), then there exists a unique \(\beta''\), \(2 \leq \beta'' \leq \frac{p-3}{2}\) such that 
\[\beta''[p-(\beta'' + 1)] \equiv 1 \pmod{p}\] and any \(\beta \neq \beta''\), \(2 \leq \beta \leq \frac{p-3}{2}\) satisfies part (i) of the corollary.

**Proof:**

(i) If \(2 \leq \beta \leq \frac{p-3}{2}\), as \(p\) is prime, there exists a unique \(k \in \{2, \ldots, p-1\}\) such that \(k \beta \equiv 1 \pmod{p}\).

(a) \(k \neq \beta\). In fact:

\[
k = \beta \implies \beta^2 \equiv 1 \pmod{p} \implies \]
\[(\beta - 1)(\beta + 1) \equiv 0 \pmod{p} \implies \]
\[p|(\beta - 1)(\beta + 1) \implies \]
\[p|(\beta - 1) \lor p|(\beta + 1) \implies \]
\[\beta \equiv 1 \pmod{p} \lor \beta \equiv p-1 \pmod{p},\]

which is a contradiction because \(2 \leq \beta \leq \frac{p-3}{2}\).

(b) \(k \neq p-(\beta + 1)\). In fact:

\[
k = p-(\beta + 1) \implies \]
\[\beta[p-(\beta + 1)] \equiv 1 \pmod{p} \implies \]
\[\beta^2 + \beta + 1 \equiv 0 \pmod{p} \implies \]
\[3|(p-1)\]

which is a contradiction.

Thus, \(k \in \{2, \ldots, p-1\} - \{\beta, p-(\beta + 1)\}\).

Now, because of the symmetry of the equations, there exists a unique \(k' \in \{2, \ldots, p-1\} - \{\beta, p-(\beta + 1)\}, k \neq k'\) such that

\[k'[p-(\beta + 1)] \equiv 1 \pmod{p} .\]

(ii) If \(3|(p-1)\), there exist \(\beta^0, p-(\beta^0 + 1) \in \mathbb{Z}/p\mathbb{Z}\) such that they are roots of the equation \(\alpha^2 + \alpha + 1 \equiv 0 \pmod{p}\), or equivalently 
\[\beta^0[p-(\beta^0 + 1)] \equiv 1 \pmod{p}.\]

For \(\beta \neq \beta^0, 2 \leq \beta \leq \frac{p-3}{2}\), \(\beta\) is not a solution of the quadratic equation, hence satisfies the part (i) of the corollary.
Theorem 1. Let $p \geq 5$ be and prime. Then:

$$\#(A^p/\sim) = \begin{cases} \frac{p+1}{6} & \text{if } 3 \nmid (p-1) \\ \frac{p+5}{6} & \text{if } 3|(p-1). \end{cases}$$

Proof: The number of elements of $A^p$ is $\frac{p-1}{2}$ and they are given in the following list:

$$\frac{p-1}{2} \left\{ \begin{array}{c} (1, 2, p-3) \\ : \\ (1, \frac{p-3}{2}, \frac{p+1}{2}) \\ (1, \frac{p-1}{2}, \frac{p-1}{2}) \end{array} \right\}$$

Here $(1, 1, p-2) \sim (1, \frac{p-1}{2}, \frac{p-1}{2})$ and they are not equivalent to any other (this class corresponds to the unique hyperelliptic Riemann surface of genus $g = \frac{p-1}{2}$ which is a branched covering of the Riemann sphere with signature $((p,0);p,p,p)$).

Thus we have to classify the elements of

$$A^p - \{(1,1,p-2), (1,\frac{p-1}{2},\frac{p-1}{2})\}.$$ 

We assume that $p \geq 11$. Then:

(a) $3 \nmid (p-1) \implies 3|\left(\frac{p-5}{2}\right)$ and by corollary 2, the classes consist of three elements.

Hence:

$$\#(A^p/\sim) = \frac{p-5}{2} + 1 = \frac{p+1}{6}.$$

(b) $3|(p-1) \implies \frac{p-5}{2} \equiv 1 \pmod{3}$. By corollary 2, there exists a unique class which consists of one element, and any other class consists of three elements.

Hence:

$$\#(A^p/\sim) = \left\lceil \frac{p-5}{2} - 1 \right\rceil / 3 + 2 = \frac{p+5}{6}.$$ 

Now if $p = 7$, $A^7 = \{(1,1,5), (1,2,4), (1,3,3)\}$ and $(1,1,5) \sim (1,3,3)$, thus $\#(A^7/\sim) = 2$.

If $p = 5$, $A^5 = \{(1,1,3), (1,2,2)\}$, where $(1,1,3) \sim (1,2,2)$ and hence $\#(A^5/\sim) = 1$. 
Thus, for $p \geq 5$:
\[
\#(A^p/\simeq) = \begin{cases} 
\frac{p+1}{6} & \text{if } 3 \nmid (p-1) \\
\frac{p+5}{6} & \text{if } 3|(p-1).
\end{cases}
\]

3.2. Branched covering with signature $<(p^2,0);p^2,p^2,p>$. 

Now we consider the compact Riemann surfaces $S$ which are branched coverings of the Riemann sphere with signature $<(p^2,0);p^2,p^2,p>$, $p \geq 3$ and prime, which admit a group of automorphisms isomorphic to $Z/p^2Z$. In this case, the genus $g$ of $S$ is $g = \frac{p(p-1)}{2}$.

These Riemann surfaces are characterized by the algebraic curves:
\[
y^{p^2} = x(x-1)^\beta(x-i)^\tau
\]
with $1 \leq \beta, \tau < p^2$, $\beta + \tau = p^2 - 1$, $\gcd(\beta,p^2) = 1$, $\gcd(\tau,p^2) = p$.

Hence, we consider the set:
\[
A^{p^2} = A^{p^2}(p^2, p^2, p) = \{(1, \beta, \tau)/\beta, \tau \in \mathbb{N}, 0 < \beta, \tau < p^2,
\]
\[
\quad \gcd(\beta,p^2) = 1, \gcd(\tau,p^2) = p\}.
\]

The equivalence relation on $A^{p^2}$ is given by: $(1, \beta, \tau) \simeq (1, \beta', \tau') \iff$

(i) $\beta = \beta'$ and $\tau = \tau'$ or

(ii) there exists $k \in \mathbb{Z}/p^2\mathbb{Z}$, such that
\[
(1, \beta', \tau') \equiv (k\beta, k, k\tau) \pmod{p^2}
\]

**Lemma 2.** Given $\beta = kp - 1 \in \mathbb{Z}/p^2\mathbb{Z}$, $k \in \{1, \ldots, p-1\}$ and $k' \in \mathbb{N}$ such that $k + k' = p$, then $\beta^{-1} = k'p - 1 \in \mathbb{Z}/p^2\mathbb{Z}$.

**Proof:**
\[
(kp - 1)(k'p - 1) = kk'p^2 - (k + k')p + 1 
\equiv 1 \pmod{p^2}.
\]

**Theorem 2.** Let $p \geq 3$ be and prime. Then:
\[
\#(A^{p^2}/\simeq) = \frac{p-1}{2}.
\]
Proof: The number of elements of $A^p^2$ is $p - 1$ and they are given by the following list:

\[
\begin{align*}
(1, &\quad p - 1, \quad (p - 1)p) \\
(1, &\quad 2p - 1, \quad (p - 2)p) \\
&\quad \vdots \\
(1, &\quad (p - 1)p - 1, \quad p).
\end{align*}
\]

By lemma 2:

\[
(1, kp - 1, (p - k)p) = \{(1, kp - 1, (p - k)p), (1, k'p - 1, (p - k')p)\}
\]

where $k + k' = p$.

Hence

\[
\#(A^p^2 / \simeq) = \frac{p - 1}{2}.
\]

References


Received: June 24, 1997.

Gustavo Labbé Morales
Departamento de Matemáticas
Universidad de La Serena
Casilla 559
La Serena
Chile