On certain cohomology sets attached to Riemann surfaces

By Takashi ONO

Department of Mathematics, Johns Hopkins University, Baltimore, Maryland, 21218-2689, U.S.A.

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 2000)

Abstract: Let G be the principal congruence subgroup of level $N \geq 3$ and g be the group generated by the involution $z \mapsto -1/z$ of the upper half plane. We shall determine the cardinality of the (first) cohomology set $H(g,G)$ in terms of the binary form $x^2+y^2 \mod N$.

Key words: The principal congruence subgroup of level N; the involution; cohomology sets; binary quadratic forms; orthogonal groups.

1. Introduction. Let X be a Riemann surface and $\widetilde{X}$ be its universal covering space. Then X is the quotient of $\widetilde{X}$ by a group G of automorphisms of $\widetilde{X}$ acting discretely and without fixed points: $X = G \setminus \widetilde{X}$, $G = \pi_1(X)$. Consider a subgroup g of $\mathrm{Aut}(\widetilde{X})$ which normalizes G. Thus we can speak of the (first) cohomology set $H(g, \pi_1(X))$. In this paper, we shall determine the cardinality of the set for the very special case where $\widetilde{X} = \mathcal{H}$, the upper half plane, $G = \Gamma(N)$, $N \geq 3$, and $g =$ the group generated by the involution $z \mapsto -1/z$ of $\mathcal{H}$. It turns out that

$$(1.1) \qquad \sharp H(g, \Gamma(N)) = \frac{1}{2} \sharp\, \mathrm{SO}_2(\mathbf{Z}/N\mathbf{Z}),$$

where $\mathrm{SO}_2(\mathbf{Z}/N\mathbf{Z})$ = the special orthogonal group for x^2+y^2 over $\mathbf{Z}/N\mathbf{Z}$. If, in particular, $N = p$, an odd prime, then we have

$$(1.2) \qquad \sharp H(g, \Gamma(p)) = \frac{1}{2}\left(p - (-1)^{(p-1)/2}\right).$$

2. Generality. In general, let g, G be subgroups of a group such that g normalizes G. We shall write the action of g on G by $a^s = sas^{-1}$, $s \in g$, $a \in G$. Denote by $Z(g,G)$ the set of all cocycles of g in G:

$$(2.1) \quad Z(g,G) = \{f : g \to G \text{ (maps)}; f(st) = f(s)f(t)^s,\ s,t \in g\}.$$

The equivalence $f \sim f'$, $f, f' \in Z(g,G)$ is defined by

$$(2.2) \quad f \sim f' \Longleftrightarrow f'(s) = a^{-1} f(s) a^s,\ a \in G,\ s \in g.$$

The cohomology set is then defined by

$$(2.3) \qquad H(g,G) = Z(g,G)/\sim.$$

2000 Mathematics Subject Classification. 11F75.

Now suppose that $g = \langle s \rangle$ with $s^2 = 1$. Then a cocycle f is entirely determined by the value $a = f(s)$ with $aa^s = 1$, we may set

$$(2.4) \quad Z(g,G) = \{a \in G; aa^s = 1\},$$

$$(2.5) \quad H(g,G) = Z(g,G)/\sim \quad \text{where} \quad a \sim a' \Longleftrightarrow a' = c^{-1}ac^s,\ c \in G.$$

3. $\Gamma(N)$. For an integer $N \geq 3$, put

$$(3.1) \qquad \Gamma(N) = \{A \in \mathrm{SL}_2(\mathbf{Z}); A \equiv I \mod N\}.$$

Let S be the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$. Note that S is of order four, whereas its image s in $\mathrm{PSL}_2(\mathbf{R}) = \mathrm{Aut}(\mathcal{H})$ is of order two. On the other hand, since $N \geq 3$, the group (3.1) is identified with its image in $\mathrm{Aut}(\mathcal{H})$. In accordance with notation in **2**, we set

$$(3.2) \qquad g = \langle s \rangle, \quad G = \Gamma(N).$$

Clearly g, G are subgroups of $\mathrm{Aut}(\mathcal{H})$, $s^2 = 1$, g normalizes G and $g \cap G = 1$. For a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$, we put

$$(3.3) \qquad A^s = SAS^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = {}^tA^{-1}.$$

Then, from (2.4), (2.5), (3.2) and (3.3), it follows that

$$(3.4) \quad Z(g,G) = \{A \in \Gamma(N),\ {}^tA = A\},$$

$$(3.5) \quad H(g,G) = Z(g,G)/\sim \quad \text{where} \quad A \sim A' \Longleftrightarrow A' = {}^tTAT,\ T \in G.$$

In other words, the set (3.4) of cocycles is nothing else than the set of symmetric matrices in $\Gamma(N)$ and the equivalence in (3.5) is a refinement of the ordinary congruence of integral quadratic forms. Having these in mind, we shall modify our notation as follows:

$$(3.6)\quad Z(N) = Z(g,G) = \left\{ A = \begin{pmatrix} a & b \\ b & c \end{pmatrix},\ a \equiv c \equiv 1, \right.$$
$$\left. b \equiv 0 \mod N,\ (2b)^2 - 4ac = -4 \right\},$$

$$(3.7)\quad A \sim A',\ A, A' \in Z(N) \iff A' = {}^tTAT,\ T \in \Gamma(N).$$

Furthermore, in view of theory of integral quadratic forms, we shall split $Z(N)$ into two parts $Z^+(N)$ and $Z^-(N)$:

$$(3.8)\quad Z^+(N) = \left\{ A = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in Z(N),\ a > 0 \right\},$$

$$(3.9)\quad Z^-(N) = \left\{ A = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in Z(N),\ a < 0 \right\}.$$

Since a matrix in $Z^+(N)$ is not equivalent to one in $Z^-(N)$ in the sense of (3.5), we have the following splitting of cohomology set:

$$(3.10)\quad \begin{aligned} H(g,G) &= Z(N)/\sim \\ &= H(N) = H^+(N) + H^-(N) \\ H^+(N) &= Z^+(N)/\sim, \\ H^-(N) &= Z^-(N)/\sim . \end{aligned}$$

Hence our problem of counting $\sharp H(g,G)$ is reduced to that for $\sharp H^+(N)$ and $\sharp H^-(N)$ respectively. We shall use the symbol $\approx$ for ordinary congruence of integral matrices:

$$(3.11)\quad A \approx A' \iff A' = {}^tUAU,\ U \in \mathrm{SL}_2(\mathbf{Z}).$$

Let $\mathcal{R}$ be a complete set of representatives of $\mathrm{SL}_2(\mathbf{Z})$ modulo $\Gamma(N)$: $\mathcal{R} = \mathrm{SL}_2(\mathbf{Z})/\Gamma(N) = \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. Now take a matrix $A \in Z^+(N)$. Since the binary form corresponding to A is primitive positive definite with discriminant -4, we have $A \approx I$ and so there is a matrix $U \in \mathrm{SL}_2(\mathbf{Z})$ such that $A = {}^tUU$ by (3.11). If we write $U = RT$, $T \in \Gamma(N)$, $R \in \mathcal{R}$, we have $A = {}^tT({}^tRR)T \sim {}^tRR$. Note that ${}^tRR$ is symmetric, positive and $\equiv I \mod N$, i.e., an element of $Z^+(N)$. Next, take a matrix $A \in Z^-(N)$. Then $-A$ is positive with discriminant -4, and so $-A \approx I$, hence $-A = {}^tUU = {}^tT({}^tRR)T$ as above, and we have $A \sim -{}^tRR$, $R \in \mathcal{R}$. Summarizing, we get, for $\varepsilon = \pm$,

$$(3.12)\quad A \sim \varepsilon {}^tRR, \text{ for some } R \in \mathcal{R}, \text{ for } A \in Z^\varepsilon(N).$$

To complete the proof of (1.1), in view of (3.12), it remains to clarify the relation between R and R' when ${}^tRR \sim {}^tR'R'$. First of all, one verifies easily the following

$$(3.13)\quad \text{For } W \in \mathrm{SL}_2(\mathbf{Z}),\ {}^tWW = I \iff W = \langle S \rangle, S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Next, we have

$$(3.14)\quad \begin{aligned} {}^tRR \sim {}^tR'R' &\iff {}^tR'R' = {}^tT{}^tRRT,\ T \in \Gamma(N) \\ &\iff {}^t(RTR'^{-1})(RTR'^{-1}) = I \\ &\overset{(3.13)}{\iff} RTR'^{-1} = S^i \\ &\iff R' = S^jRT \\ &\iff R' = S^jT'R,\ T' \in \Gamma(N). \end{aligned}$$

If we set $\Gamma^*(N) = \langle S \rangle \Gamma(N)$, then (3.14) means that

$$(3.15)\quad {}^tRR \sim {}^tR'R' \iff R \equiv R' \mod \Gamma^*(N).$$

Since $N \geq 3$, one sees at once that $[\Gamma^*(N) : \Gamma(N)] = 4$. From (3.10), (3.12) and (3.15) we obtain

$$\sharp H^\varepsilon(N) = \sharp(\mathrm{SO}_2(\mathbf{Z}/N\mathbf{Z}))/4,\ \varepsilon = \pm$$

and hence

$$(1.1)\quad \sharp H(N) = \frac{1}{2}\sharp(\mathrm{SO}_2(\mathbf{Z}/N\mathbf{Z})).$$

Added in proof. As Prof. H. Wada pointed out the argument after line 6, p. 117 is invalid when $N \equiv 0$, mod 4, because the set $Z^-(N)$ is empty. It is easy to check that

$${}^tXX \equiv -I \mod N \text{ is solvable} \iff N \not\equiv 0 \mod 4.$$

Hence, in case $N \equiv 0 \mod 4$, the number in (1.1) should be reduced to its half.