On certain cohomology set for $\Gamma_0(N)$

By Takashi Ono

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

(Communicated by Shokichi Iyanaga, M. J. A., March 12, 2001)

Abstract: Let $G = \Gamma_0(N)$, $N \not\equiv 3 \pmod 4$ and g be the group generated by the involution $z \mapsto -1/Nz$ of the upper half plane. We determine the cohomology set $H^1(g, G)$ in terms of the class number of quadratic forms of discriminant $-4N$.

Key words: Congruence subgroups of level N; the involution; cohomology sets; binary quadratic forms; class number of orders.

1. Introduction. Let g, G be groups where g acts on G to the left and $H(g, G)$ be the (first) cohomology set of (g, G). When $g = \langle s \rangle$, $s^2 = 1$, let us put $a^* = a^{-s}$. Then $(ab)^* = b^* a^*$, $a^{**} = a$ for $a, b \in G$ and so we can make the identification:

$$\begin{aligned} &H(g, G) \\ (1.1) \quad &= \{a \in G;\ a^* = a, \text{symmetric elements}\}/\sim \\ &\text{where } a \sim b \text{ (congruence)} \iff b = c^* a c, c \in G \end{aligned}$$

In [2], we treated the case where $G = \Gamma(N)$ with $s = (z \mapsto -1/z)$. This time, as the second step, we take the case where $G = \Gamma_0(N)$ with $s = (z \mapsto -1/Nz)$. Unlike in [2] where $a^* = {}^t a$ (transpose), we shall meet various binary positive quadratic forms and hence imaginary quadratic fields $K = \mathbf{Q}(\sqrt{-N})$. We shall show that there is a bijection between the set $H^+(g, \Gamma_0(N))$, the positive part of $H(g, \Gamma_0(N))$, and the form class group $C(-4N)$ whenever $N \not\equiv 3 \pmod 4$.

2. $\boldsymbol{F^+(N)}$. For a positive integer N, put

$$(2.1) \qquad S = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}.$$

For $g = \langle s \rangle$, $s^2 = 1$ and $A \in G = \Gamma_0(N)$, put

$$(2.2) \qquad A^s = SAS^{-1} = U\,{}^t A^{-1} U^{-1}.$$

One checks that g acts on G. We also put

$$(2.3) \qquad A^* = A^{-s} = U\,{}^t A U^{-1}.$$

Denoting by $Z(g, G)$ the set of all cocycles in (g, G), we have, from (2.2), (2.3),

$$(2.4) \qquad Z(g, G) = \{A \in G;\ A^* = A\}.$$

2000 Mathematics Subject Classification. 11F75.

Dedicated to Professor S. Iyanaga, M.J.A., on his 95th birthday.

Now put

$$(2.5) \qquad F = \varphi(A) = AU, \quad A \in Z(g, G).$$

Then, we find that

$$(2.6) \qquad A^* = A \iff {}^t F = F.$$

From (2.4), (2.5), (2.6) we see that the map φ identifies the set $Z(g, G)$ of cocycles with the following set $\mathcal{F}(N)$ of symmetric matrices:

$$(2.7)\ \mathcal{F}(N) = \left\{ F = \begin{pmatrix} a & Nb \\ Nb & Nc \end{pmatrix};\ ac - Nb^2 = 1 \right\}.$$

Furthermore, note that the (right) action $A \mapsto T^* A T$ of $T \in \Gamma_0(N)$ on $Z(g, G)$ corresponds to the (right) action $F \mapsto {}^t T_1 F T_1$ of $T_1 = U^{-1} T U \in \Gamma^0(N)$ on $\mathcal{F}(N)$ under the identification of $Z(g, G)$ and $\mathcal{F}(N)$ by the map φ. In other words, we have, via φ,

$$(2.8) \qquad H(g, \Gamma_0(N)) = \mathcal{F}(N)/\Gamma^0(N).$$

As usual, for a negative integer D, we denote by $\Phi(D)$ the set of all integral primitive positive definite binary quadratic forms of discriminant D:

$$\begin{aligned} (2.9) \quad \Phi(D) = \{&f = ax^2 + bxy + cy^2; (a, b, c) = 1, \\ &a > 0,\ b^2 - 4ac = D < 0\}. \end{aligned}$$

We identify $f \in \Phi(D)$ with the half-integral matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$, as usual.

From now on we assume that

$$N \not\equiv 3 \pmod 4, \text{ i.e., } N \equiv 0, 1 \text{ or } 2 \pmod 4.$$

Back to the set $\mathcal{F}(N)$ of (2.7), we set

$$(2.10) \qquad \begin{cases} \mathcal{F}^+(N) = \{F \in \mathcal{F}(N);\ a > 0\} \\ \mathcal{F}^-(N) = \{F \in \mathcal{F}(N);\ a < 0\} \\ \qquad\qquad = \{-F; F \in \mathcal{F}^+(N)\}. \end{cases}$$

Then $\mathcal{F}(N)$ is a disjoint sum of $\mathcal{F}^+(N)$ and $\mathcal{F}^-(N)$, and each summand is stable under the the action of $\Gamma^0(N)$. Hence the following definition makes sense:

$$(2.11)\qquad H^e(g, \Gamma_0(N)) = \mathcal{F}^e(N)/\Gamma^0(N),\ e = \pm,$$

and we have

$$(2.12)\qquad \sharp H(g, \Gamma_0(N)) = 2\sharp(\mathcal{F}^+(N)/\Gamma^0(N)).$$

In view of (2.7), (2.9), (2.10), the set $\mathcal{F}^+(N)$ may be considered as

$$(2.13)\qquad \begin{aligned}\mathcal{F}^+(N) = \{f = ax^2 + 2Nbxy + Ncy^2;\\ a > 0, D_f = -4N\},\end{aligned}$$

and so, by (2.9), (2.13), we have

$$(2.14)\qquad \mathcal{F}^+(N) \subset \Phi(-4N).^{*)}$$

Consequently, from (2.8), (2.11), we see that the embedding (2.14) induces naturally a map

$$(2.15)\qquad \begin{aligned}\pi : H^+(g, \Gamma_0(N)) = \mathcal{F}^+(N)/\Gamma^0(N)\\ \to \Phi(-4N)/SL_2(\mathbf{Z}).\end{aligned}$$

3. π is injective. We shall prove that the map π in (2.15) is injective. So, for a matrix (or a quadratic form) $F \in \mathcal{F}^+(N)$, we denote by $[F]$, $[F]^0$, the class of F modulo $SL_2(\mathbf{Z})$, $\Gamma^0(N)$, respectively. We must then show that $[F] = [G]$, $F, G \in \mathcal{F}^+(N)$, $\Rightarrow [F]^0 = [G]^0$. Now the assumption says that

$$(3.1)\qquad G = {}^tTFT \text{ for some } T \in SL_2(\mathbf{Z}).$$

If we put

$$(3.2)\qquad \begin{aligned}T = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ F = \begin{pmatrix} p & Nq \\ Nq & Nr \end{pmatrix},\ G = \begin{pmatrix} u & Nv \\ Nv & Nw \end{pmatrix},\\ ad - bc = 1,\ pr - Nq^2 = 1,\ uw - Nv^2 = 1,\end{aligned}$$

then, (3.1) means that

$$(3.3)\ \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} p & Nq \\ Nq & Nr \end{pmatrix} = \begin{pmatrix} u & Nv \\ Nv & Nw \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

On taking (3.3) modulo N we have

$$\begin{pmatrix} ap & 0 \\ bp & 0 \end{pmatrix} \equiv \begin{pmatrix} du & -bu \\ 0 & 0 \end{pmatrix} \pmod N$$

and hence $bp \equiv 0 \pmod N$. As $pr \equiv 1 \pmod N$ by (3.2), we have $b \equiv 0 \pmod N$, i.e., $T \in \Gamma^0(N)$, or $[F]^0 = [F]^0$. □

*) It is easy to verify that every form in $\mathcal{F}^+(N)$ is primitive whenever $N \not\equiv 3 (\mathrm{mod}\ 4)$. For $N \equiv 3 (\mathrm{mod}\ 4)$, this is not true: e.g., $N = 3$, $a = c = 2$, $b = 1$, $f = 2x^2 + 6xy + 6y^2$. One finds similar nonprimitive forms for any $N \equiv 3 (\mathrm{mod}\ 4)$.

**) As for basic facts on orders see [2, §7, §8].

4. π is surjective. Let $F = F(x, y) = ax^2 + 2Nbxy + Ncy^2$ be a quadratic form in $\mathcal{F}^+(N)$ for $N \not\equiv 3 \pmod 4$. The discriminant of F is $D = -4N$. Call τ the root of $F(x, 1) = ax^2 + 2Nbx + Nc = 0$ in the upper half plane. Then $a\tau = -bN + \sqrt{-N}$ is an algebraic integer in $\mathcal{O}_K$ with $K = \mathbf{Q}(\sqrt{-N})$. We put

$$(4.1)\qquad \mathcal{O}(N) = [1, a\tau] = \mathbf{Z} + a\tau\mathbf{Z},$$

which is an order of the ring $\mathcal{O}_K$. The index $f = [\mathcal{O}_K : \mathcal{O}(N)]$ is the conductor of $\mathcal{O}(N)$. The discriminant of $\mathcal{O}(N)$ becomes $D = -4N$ above. We have the equality: $D = -4N = f^2 d_K$ where d_K is the discriminant of K. If we put

$$(4.2)\qquad \omega_K = \frac{d_K + \sqrt{d_K}}{2},$$

then we have

$$(4.3)\qquad \mathcal{O}_K = [1, \omega_K],\quad \mathcal{O}(N) = [1, f\omega_K].$$

In what follows, let $\mathcal{O} = \mathcal{O}(N) \subset \mathcal{O}_K$ with conductor f.**) We denote by $I(\mathcal{O})$ the group of proper fractional $\mathcal{O}$-ideals, by $P(\mathcal{O})$ the subgroup of principal $\mathcal{O}$-ideals and put $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$, the ideal class group of the order $\mathcal{O}$. On the other hand, we set $C(D) = \Phi(D)/SL_2(\mathbf{Z})$, the form class group for the discriminant $D = -4N$. There is an isomorphism

$$(4.4)\qquad C(D) \xrightarrow{\sim} C(\mathcal{O})$$

which is induced by sending the quadratic form $ax^2 + bxy + cy^2$ in $\Phi(D)$ to the proper ideal $[a, h + \sqrt{-N}] \subset \mathcal{O}$, with $b = 2h$.

Next, let $I(\mathcal{O}, f)$ be the subgroup of $I(\mathcal{O})$ generated by ideals prime to f, $P(\mathcal{O}, f)$ be the subgroup of $I(\mathcal{O}, f)$ generated by principal ideals $\alpha\mathcal{O}$ where $\alpha \in \mathcal{O}$ has the norm prime to f.

Finally, let $I_K(f)$ be the subgroup of the group of fractional $\mathcal{O}_K$-ideals I_K generated by ideals prime to f, $P_{K,\mathbf{Z}}(f)$ be the subgroup of $I_K(f)$ generated by principal ideals of the form $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for some integer a relatively prime to f. Then there are natural isomorphisms

$$(4.5)\qquad \begin{aligned}C(\mathcal{O}) &\xrightarrow{\sim} I(\mathcal{O}, f)/P(\mathcal{O}, f)\\ &\xrightarrow{\sim} I_K(f)/P_{K,\mathbf{Z}}(f),\end{aligned}$$

where the second isomorphism is the inverse one induced by the map:

$$(4.6)\qquad [a, b + \omega_K] \mapsto [a, f(b + \omega_K)]$$

from $I_K(f)$ to $I(\mathcal{O}, f)$.

Consequently we end up with the isomorphism

$$C(-4N) \xrightarrow{\sim} I_K(f)/P_{K,\mathbf{Z}}(f) \tag{4.7}$$

induced by $F = ax^2 + bxy + cy^2 \mapsto [a, -h + \sqrt{-N}]$, $b = 2h$.

We are now ready to prove that π is surjective. So take any form $F = ax^2 + bxy + cy^2 \in \Phi(-4N)$. By (4.7), an ideal $\mathfrak{a}_F = [a, -h + \sqrt{-N}]$ in $I_K(f)$ corresponds to F. Let $\mathfrak{p} = [p, r + \sqrt{-N}]$ be a prime ideal in $I_K(f)$ which is congruent to $\mathfrak{a}_F$ modulo $P_{K,\mathbf{Z}}(f)$. The existence of such a $\mathfrak{p}$ is guaranteed by the Čebotarev density theorem. Since $\mathfrak{p}$ is an ideal, we have

$$p \mid \mathrm{Norm}(r + \sqrt{-N}) = r^2 + N. \tag{4.8}$$

Choose u such that $-r \equiv Nu \pmod p$. In view of (4.8), we have $N^2u^2 \equiv r^2 \equiv -N \pmod p$, hence $p \mid 1 + Nu^2$ as $p \nmid N$. Consequently

$$\mathfrak{p} = [p, r + \sqrt{-N}] = [p, -Nu + \sqrt{-N}]. \tag{4.9}$$

Using v such that $pv = 1 + Nu^2$, put $G = px^2 + 2Nuxy + Nvy^2$. Then $D_G = (2Nu)^2 - 4pNv = 4N^2u^2 - 4N(1 + Nu^2) = -4N$, hence $G \in \mathcal{F}^+(N)$ and $G \sim F$. Since $\pi([G]) = [\mathfrak{p}]$, we see from (4.7), (4.9) that π is surjective. □

Summarizing arguments in 3 and 4 up to here, we obtain

(4.10) **Theorem.** *Let N be a positive integer $\equiv 3 \pmod 4$, π be the map $H^+(g, \Gamma_0(N)) = \mathcal{F}^+(N)/\Gamma^0(N) \to C(-4N) = \Phi(-4N)/SL_2(\mathbf{Z})$ given in (2.15). Then π is a bijection. In particular, the cohomology set $H^+(g, \Gamma_0(N))$ acquires a structure of a finite abelian group isomorphic to the form class group of discriminant $-4N$.*

From (2.12), (4.10), we have

(4.11) **Theorem.** *Notation being as before, $\sharp H(g, \Gamma_0(N)) = 2h(-4N)$ where $h(-4N)$ means the class number of the order $\mathcal{O}(N)$ ((4.1)).*

5. Examples. (5.1) Assume that the positive integer $N \not\equiv 3 \pmod 4$ is square free. Hence $N \equiv 1, 2 \pmod 4$. Since $-N \equiv 2, 3 \pmod 4$, $d_K = -4N$, $K = \mathbf{Q}(\sqrt{-N})$. Let $\mathcal{O}(N)$ be the order of $\mathcal{O}_K$ in (4.1). As the discriminant D of $\mathcal{O}(N)$ is $-4N$, we see that $\mathcal{O}(N) = \mathcal{O}_K$ and hence $h(-4N) = h_K$, the ordinary class number of K.

(5.2) Let p be a prime number $\equiv 1 \pmod 4$ and $N = p^{2K+1}$, $k \geq 0$. Then $K = \mathbf{Q}(\sqrt{-N}) = \mathbf{Q}(\sqrt{-p})$, $d_K = -4p$. Let D be as before the discriminant of the order $\mathcal{O}(N)$. Then $D = -4N = f^2 d_K$. Hence we find $f = p^k$. We have $\mathcal{O}_K^\times = \mathcal{O}(N)^\times = \{\pm 1\}$. By a well-known formula on class numbers of orders, we have

$$h(-4N) = h_K f\left(1 - \left(\frac{d_K}{p}\right) p^{-1}\right) = p^k h_K$$

and we find

$$\frac{\sharp H(g_K, \Gamma_0(p^{2k+1}))}{p^k} = 2h_K \text{ for all } k \geq 0,$$

where g_K shows the dependence of the group g on k.

References

[1] Cox, D.: Primes of the Form $x^2 + ny^2$. John Wiley, New York (1989).

[2] Ono, T.: On certain cohomology sets attached to Riemann surfaces. Proc. Japan Acad., **76A**, 116–117 (2000).