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

By Takashi Ono

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

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

Abstract: Let $G = \Gamma_0(N)$ 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 numbers $h(-N)$ and $h(-4N)$ of quadratic forms.

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

1. Introduction. This is a continuation (and a completion) of my preceding paper [3] which will be referred to as (I) in this paper.

For any positive integer N, let $G = \Gamma_0(N)$ and $S = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Using this S we can let $g = \langle s \rangle$, $s^2 = 1$, act on G by $A^s = SAS^{-1}$ and speak of the first cohomology set $H^1(g, G)$. In (I), we determined this set when $N \not\equiv 3 \pmod 4$. In this paper, we shall remove this restriction on N. As usual, for a negative integer D, $D \equiv 0$ or $1 \pmod 4$, we denote by $h(D)$ the number of classes of primitive positive integral binary quadratic forms of discriminant D. Then we have the following

(1.1) **Theorem.**

$$\sharp H^1(g, \Gamma_0(N)) = \begin{cases} 2h(-4N), & N \not\equiv 3 \pmod 4, \\ 2(h(-4N) + h(-N)), & N \equiv 3 \pmod 4. \end{cases}$$

2. $\mathcal{F}^+(N)$. As in (I), the proof of (1.1) is based on the equality

$$(2.1) \quad H^1(g, \Gamma_0(N)) = \mathcal{F}(N)/\Gamma^0(N), \quad \text{(I, (2.8))},$$

where

$$(2.2) \quad \mathcal{F}(N) = \left\{ F = \begin{pmatrix} a & Nb \\ Nb & Nc \end{pmatrix}; ac - Nb^2 = 1 \right\}.$$

On the right side of (2.1), we consider the right action of $\Gamma^0(N)$ on the set (2.2) defined by $F \mapsto {}^tTFT$, $T \in \Gamma^0(N)$.

As usual, for a negative integer D, $D \equiv 0$, or $1 \pmod 4$, we denote by $\Phi(D)$ the set of all primitive positive integral binary quadratic forms of discriminant D:

$$(2.3) \quad \Phi(D) = \left\{ \begin{array}{l} f = ax^2 + bxy + cy^2;\ (a, b, c) = 1, \\ a > 0,\ b^2 - 4ac = D < 0 \end{array} \right\}.$$

We often identify $f \in \Phi(D)$ with the half-integral matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. The right action of the group $\mathrm{SL}_2(\mathbf{Z})$ on $\Phi(D)$ is given by $f \mapsto {}^tUfU$, $U \in \mathrm{SL}_2(\mathbf{Z})$. We denote by $C(D)$ the orbit space $\Phi(D)/\mathrm{SL}_2(\mathbf{Z})$ and by $h(D)$ the cardinality of $C(D)$, i.e., the class number of forms of discriminant D.

Back to the set $\mathcal{F}(N)$ in (2.2), we set

$$(2.4) \quad \begin{array}{l} \mathcal{F}^+(N) = \{F \in \mathcal{F}(N);\ a > 0\}, \\ \mathcal{F}^-(N) = \{F \in \mathcal{F}(N);\ a < 0\}. \end{array}$$

Since $\mathcal{F}(N)$ is a disjoint sum of $\mathcal{F}^+(N)$ and $\mathcal{F}^-(N)$, and each summand is stable under the action of $\Gamma^0(N)$, we have

$$(2.5) \quad \sharp H^1(g, \Gamma_0(N)) = 2\sharp(\mathcal{F}^+(N)/\Gamma^0(N)).$$

In view of (2.2), (2.3), (2.4), the set $\mathcal{F}^+(N)$ may be written as

$$(2.6) \quad \mathcal{F}^+(N) = \left\{ \begin{array}{l} f = ax^2 + 2Nbxy + Ncy^2; \\ a > 0,\ D_f = -4N \end{array} \right\}.$$

For an integral form $f = ax^2 + bxy + cy^2$, we put

$$(2.7) \quad i(f) = (a, b, c) = \text{the g.c.d. of coefficients}.$$

It is easy to see that $i(f) = i(g)$ if $f \sim g$, i.e., if $g = {}^tTfT$, $T \in \mathrm{SL}_2(\mathbf{Z})$. Needless to say $i(f) = 1$ means f is primitive. Since forms in $\mathcal{F}^+(N)$ are not necessary primitive for general N, we are forced to reclassify $\mathcal{F}^+(N)$ according to the invariant $i(f)$ when we compare it with the set $\Phi(D)$ where $i(f) = 1$ always. Thus, we set, for an integer $k > 0$,

2000 Mathematics Subject Classification. 11F75.

(2.8) $\mathcal{F}_k(N)$
$= \{f = ax^2 + 2Nbxy + Ncy^2 \in \mathcal{F}^+(N);\ i(f) = k\}.$

Actually, there are not many choices for the values $i(f)$, $f \in \mathcal{F}^+(N)$. In fact the condition $ac - Nb^2 = 1$ in (2.2) implies that

(2.9) $\mathcal{F}_k(N) = \phi$ for all N and $k > 2$,

and

(2.10) $\mathcal{F}_2(N) \neq \phi \iff N \equiv 3 \pmod 4$.

Hence we have the decomposition

(2.11) $\mathcal{F}^+(N) = \mathcal{F}_1(N) \cup \mathcal{F}_2(N)$ for all N

and

(2.12) $\mathcal{F}^+(N) = \mathcal{F}_1(N)$ when $N \not\equiv 3 \pmod 4$.

A typical element in $\mathcal{F}_2(N)$ for $N \equiv 3 \pmod 4$ is $f = 2x^2 + 2Nxy + (1/2)N(N+1)$.

From now on let $k = 1$ or 2. Clearly $\mathcal{F}_k(N)$ is stable under the action of $\Gamma^0(N)$. For a form $f \in \mathcal{F}_k(N)$ the form $k^{-1}f$ is primitive of discriminant $-4k^{-2}N$ and hence a form in $\Phi(-4k^{-2}N)$. Consequently the map $f \mapsto k^{-1}f$ induces naturally a map:

(2.13) $\pi_k : \mathcal{F}_k(N)/\Gamma^0(N) \to \Phi(-4k^{-2}N)/\operatorname{SL}_2(\mathbf{Z})$.

We shall prove that π_k is bijective.

3. $\boldsymbol{\pi_k}$ is injective. To prove that π_k is injective, take $F, G \in \mathcal{F}_k(N)$ such that $k^{-1}F \sim k^{-1}G$ (mod $\operatorname{SL}_2(\mathbf{Z})$). We must then show that $F \sim G$ (mod $\Gamma^0(N)$). The assumption, however, implies that $F \sim G$ (mod $\operatorname{SL}_2(\mathbf{Z})$) and hence the same argument as in (I, 3) works to conclude $F \sim G$ (mod $\Gamma^0(N)$). □

4. $\boldsymbol{\pi_k}$ is surjective. For $k = 1$ or 2, put

(4.1) $D = -4k^{-2}N < 0.$

Since $k = 2$ only if $N \equiv 3 \pmod 4$, we have $D \equiv 0, 1 \pmod 4$. Let K be the quadratic field $\mathbf{Q}(\sqrt{D}) = \mathbf{Q}(\sqrt{-N})$ with the discriminant d_K and

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

Then $\mathcal{O}_K = [1, \omega_K]$ is the ring of integers of K. Any order $\mathcal{O}$ of K is given as $\mathcal{O} = [1, f\omega_K]$ with the conductor f such that $D = f^2 d_K$ and $[\mathcal{O}_K : \mathcal{O}] = f$. Any ideal in $\mathcal{O}$ is of the form

(4.3) $\mathfrak{a} = [a, b + f\omega_K]$, $a, b \in \mathbf{Z}$, $a = (\mathcal{O} : \mathfrak{a})$,

(4.4) $a \big| N(b + f\omega_K)$, N being the norm in $K/\mathbf{Q}$.

Notice that there is an integer h so that

(4.5) $$b + f\omega_K = \frac{h + \sqrt{D}}{2}.$$

To prove that π_k is surjective, for any form $F = ax^2 + bxy + cy^2$ in $\Phi(D)$ we must find a form G in $\mathcal{F}_k(N)$ such that the form class of $k^{-1}G$ is mapped on the class of F. By the well-known isomorphism

(4.6) $C(D) \approx C(\mathcal{O}) \approx I_K(f)/P_{K,\mathbf{Z}}(f)$
(see [1, Prop. 7.22])

we may assume that the coefficient a of x^2 in F is prime to f, $(a, f) = 1$. In view of (4.5), the ideal corresponding to F is of the form

(4.7) $$\mathfrak{a} = \left[a, \frac{b + \sqrt{D}}{2}\right].$$

Since we are dealing with ideal classes in the last term of (4.6), by the Cěbotarev theorem applied to the ideal class group in (4.6), we can replace $\mathfrak{a}$ by a prime ideal $\mathfrak{p} = [p, (r + \sqrt{D})/2]$ such that $(p, N) = 1$.

Now we have

(4.8) $$D = \begin{cases} -4N, & \text{if } k = 1, \\ -N, & \text{if } k = 2 \\ & \text{(the case } N \equiv 3 \pmod 4 \text{ only).} \end{cases}$$

Since the argument in (I, 4) works for $k = 1$ without any change, from now on we shall consider exclusively the case $k = 2$, and so $N \equiv 3 \pmod 4$. First note that, by (4.4),

(4.9) $4p \big| N + r^2.$

Next choose u so that $Nu \equiv -r \pmod{4p}$. In view of (4.9), we have $N^2u^2 \equiv r^2 \equiv -N \pmod{4p}$, hence $4p \big| N(1 + Nu^2)$ and so $4p \big| 1 + Nu^2$.
Consequently, we find

(4.10) $$\mathfrak{p} = \left[p, \frac{r + \sqrt{-N}}{2}\right] = \left[p, \frac{-Nu + \sqrt{-N}}{2}\right].$$

Using v such that $4pv = 1 + Nu^2$, put $G = 2px^2 + 2Nuxy + 2Nvy^2$. Then, one verifies that $D_G = -4N$ and $i(G) = 2$, i.e., $G \in \mathcal{F}_2(N)$. Since the ideal $\mathfrak{p}$ corresponds to $2^{-1}G$, the form class of $2^{-1}G$ is mapped to the class of F since $\mathfrak{p}$, $\mathfrak{a}$ are in the same ideal class.

Having verified that the map π_k is bijective, our proof of (1.1) Theorem is a consequence of materials in 2, especially of (2.9)–(2.12). □

5. $\boldsymbol{\Gamma_0(p^{2n+1})}$. Let p be a prime and n be a nonnegative integer. As an application of (1.1) Theorem we shall determine the cardinality of the set $H^1(g, \Gamma_0(p^{2n+1}))$ where the action of g on $\Gamma_0(p^{2n+1})$

Table

Case 1. $D = -4p^{2n+1}$.

	$p \equiv 1, 2 \pmod 4$	$p = 3$	$p \equiv 3 \pmod 4$, $(p \neq 3)$
d_K	$-4p$	-3	$-p$
f	p^n	$2 \cdot 3^n$	$-2p^n$
$[\mathcal{O}_K^\times : \mathcal{O}_f^\times]$	1	3	1
$\prod_{p\,\mid\, f}$	1	$3/2$	$3/2,\ p \equiv 3 \pmod 8$ $1/2,\ p \equiv 7 \pmod 8$
$h(D)$	$h_K p^n$	$h_K 3^n$	$3h_K p^n,\ p \equiv 3 \pmod 8$ $h_K p^n,\ p \equiv 7 \pmod 8$

Case 2. $D = -p^{2n+1}$, $p \equiv 3 \pmod 4$.

	$p = 3$	$p \equiv 3 \pmod 4$, $(p \neq 3)$
d_K	-3	$-p$
f	3^n	p^n
$[\mathcal{O}_K^\times : \mathcal{O}_f^\times]$	$1,\ n = 0$ $3,\ n \geq 1$	1
$\prod_{p\,\mid\, f}$	1	1
$h(D)$	$h_K,\ n = 0$ $h_K 3^{n-1},\ n \geq 1$	$h_K p^n$

is the one described in 1. For simplicity we denote this cardinality by $h^1(\Gamma_0(p^{2n+1}))$. Hence (1.1) Theorem implies that

$$(5.1)\quad h^1(\Gamma_0(p^{2n+1})) = \begin{cases} 2h(-4p^{2n+1}), & p \not\equiv 3 \pmod 4, \\ 2(h(-4p^{2n+1}) + h(-p^{2n+1})), & p \equiv 3 \pmod 4. \end{cases}$$

Since

$$K = \mathbf{Q}(\sqrt{-4p^{2n+1}}) = \mathbf{Q}(\sqrt{-p^{2n+1}}) = \mathbf{Q}(\sqrt{-p}),$$

the class numbers on the right side of (5.1) can be expressed in terms of $h(-p) = h_K$, the class number of K. This is based on the well-known formula:

$$(5.2)\ h(D) = \frac{h_K f}{[\mathcal{O}_K^\times : \mathcal{O}_f^\times]} \prod_{p\,\mid\, f} \left(1 - \left(\frac{d_K}{p}\right) p^{-1}\right)$$

where D is a negative integer, $\equiv 0, 1 \pmod 4$, $K = \mathbf{Q}(\sqrt{D})$, d_K the discriminant of K, $\mathcal{O}_f$ the order of conductor f in $\mathcal{O}_K$ and (d_K/p) is the Kronecker symbol. Note that $D = d_K f^2$. The above tables exhibit values of ingredients of (5.2) for $D = -4p^{2n+1}$ and $-p^{2n+1}$.

Substituting these data in (5.1), we obtain

$$(5.3)\ h^1(\Gamma_0(p^{2n+1})) = \begin{cases} 2h_K p^n, & p \not\equiv 3 \pmod 4) \\ 8h_K p^n, & p \equiv 3 \pmod 8),\ (p \neq 3) \\ 4h_K p^n, & p \equiv 7 \pmod 8) \\ 4, & p = 3,\ n = 0, \\ 8h_K 3^{n-1}, & p = 3,\ n \geq 1. \end{cases}$$

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).

[3] Ono, T.: On certain cohomology set for $\Gamma_0(N)$. Proc. Japan Acad., **77A**, 39–41 (2001).