Explicit representations of classes of some binary quadratic forms of discriminants $4q^2+1$

By Ryūta HASHIMOTO

Graduate school of Human Informatics, Nagoya University, Furou-cho, Chikusa-ku, Nagoya 464–8601

(Communicated by Shokichi IYANAGA, M.J.A., Jan. 12, 1999)

Let K be the quadratic field over $\mathbf{Q}$ of a given discriminant D. We denote the ideal class group of K by $H(D)$ and the class number of K by $h(D)$. In this paper, we give explicit representations of some reduced binary quadratic forms of discriminant $4q^2+1$, which will be applied to obtain some informations on $H(4q^2+1)$ and $h(4q^2+1)$.

1. Notations and preliminaries. For details on this section, see [3] and [4, Chap. 5].

To investigate $H(D)$, we consider the binary quadratic forms $aX^2+bXY+cY^2 \in \mathbf{Z}[X,Y]$ of discriminant $D=b^2-4ac$. Let $F(D)$ be the set of such forms. We denote $f(X,Y) = aX^2+bXY+cY^2$ simply by $f=[a,b,c]$, or $[a,b,*]$ since $*$ is easily calculated from a, b, and D. We say that two forms $f=[a,b,c]$ and $f'=[a',b',c']$ in $F(D)$ are *equivalent* (denoted by $f \sim f'$) if there exists $A \in \mathrm{SL}_2(\mathbf{Z})$ such that $f(X,Y)=f'(X',Y')$, where $\begin{pmatrix} X \\ Y \end{pmatrix} = A \begin{pmatrix} X' \\ Y' \end{pmatrix}$.

We define the binary operation $\circ$ of two forms $f_1=[a_1,b_1,c_1]$ and $f_2=[a_2,b_2,c_2]$ in $F(D)$ as follows:

$$\begin{aligned} f_1 \circ f_2 &= [a_3,b_3,c_3], \\ a_3 &= \frac{a_1a_2}{e^2}, \\ b_3 &= b_2 + \frac{2a_2}{e}(v(s-b_2)-wc_2), \\ c_3 &= \frac{{b_3}^2-D}{4a_3}, \end{aligned}$$

where $s=(b_1+b_2)/2$, $e=\gcd(a_1,a_2,s)$, and u, v, $w \in \mathbf{Z}$ satisfy $a_1u+a_2v+sw=e$. The operation $\circ$ is well-defined as that on $F(D)/\sim$. And we have the following Proposition:

Proposition 1. (1) *$F(D)/\sim$, with $\circ$, is isomorphic to the ideal class group of $\mathbf{Q}(\sqrt{D})$ in the narrow sense. In particular, if $D=4q^2+1$ and D is square-free, then $F(D)/\sim$ is isomorphic to $H(D)$.*

(2) *The forms of type $[1,*,*]$ and $[*,*,1]$ belong to the unit class in $F(D)/\sim$.*

(3) $[a_1,b,a_2c] \circ [a_2,b,a_1c] \sim [a_1a_2,b,c]$.

$[a,b,c]$ of discriminant D is called reduced if $0<b<\sqrt{D}$ and $\sqrt{D}-b<2|a|<\sqrt{D}+b$. Every class has at least one reduced form, and all the reduced forms in a class make exactly one "cycle" (For details on cycle, see [3, §3.1]).

2. Explicit representations of reduced binary quadratic forms. We have

$$4q^2+1=(2q-(2l-1))^2+4((2l-1)q-l(l-1))$$

for any positive integers l. So, for a positive divisor λ of $(2l-1)q-l(l-1)$, let $C_{(2l-1)}(\lambda)$ be an equivalence class in $F(4q^2+1)$ including the form $[\lambda, 2q-(2l-1), -\mu]$, where $\mu=((2l-1)q-l(l-1))/\lambda$.

Using these notations throughout this paper, we can get the cycles of reduced forms in $C_{(2l-1)}(\lambda)$ where $l=1$ or 2 as follows.

Theorem 1. *In case $l=1$, put $\mu=q/\lambda$.*

$C_1(\lambda)$ has the following cycle of reduced forms of period 6 :

$$\begin{aligned} &[\lambda,2q-1,-\mu] \sim [-\mu,b_1,c_1] \\ &\sim [c_1,b_2,-\lambda] \sim [-\lambda,2q-1,\mu] \\ &\sim [\mu,b_1,-c_1] \sim [-c_1,b_2,\lambda], \end{aligned}$$

where

$$\begin{aligned} b_1 &= 2q+1-2\mu, \\ c_1 &= 2q+1-\lambda-\mu, \\ b_2 &= 2q+1-2\lambda. \end{aligned}$$

Theorem 2. *In case $l=2$, put $\mu=(3q-2)/\lambda$.*

(1) *When $\lambda \equiv 1 \pmod 3$ and $1<\lambda<3q-2$, $C_3(\lambda)$ has the following cycle of reduced forms of period* 10 :

$$\begin{aligned} &[\lambda,2q-3,-\mu] \sim [-\mu,b_1,c_1] \\ &\sim [c_1,b_2,-c_2] \sim [-c_2,b_3,c_3] \\ &\sim [c_3,b_4,-\lambda] \sim [-\lambda,2q-3,\mu] \\ &\sim [\mu,b_1,-c_1] \sim [-c_1,b_2,c_2] \end{aligned}$$

$$\sim [c_2, b_3, -c_3] \sim [-c_3, b_4, \lambda],$$

where

$$\begin{aligned} b_1 &= 2q - (4\mu - 1)/3, \\ c_1 &= 1 + (\lambda - 1)(4\mu - 1)/9, \\ b_2 &= 2q - 1 - 2(\lambda - 1)(2\mu + 1)/9, \\ c_2 &= q - (\lambda - 1)(\mu - 1)/9, \\ b_3 &= 2q - 1 - 2(2\lambda + 1)(\mu - 1)/9, \\ c_3 &= 1 + (4\lambda - 1)(\mu - 1)/9, \\ b_4 &= 2q - (4\lambda - 1)/3. \end{aligned}$$

(2) *When* $\lambda \equiv 2 \pmod 3$ *and* $2 < \lambda < (3q-2)/2$, $C_3(\lambda)$ *has the following cycle of reduced forms of period* 6 :

$$\begin{aligned} &[\lambda, 2q-3, -\mu] \sim [-\mu, b_1, c_1] \\ &\sim [c_1, b_2, -\lambda] \sim [-\lambda, 2q-3, \mu] \\ &\sim [\mu, b_1, -c_1] \sim [-c_1, b_2, \lambda], \end{aligned}$$

where

$$\begin{aligned} b_1 &= 2q - (2\mu - 1)/3, \\ c_1 &= q - (\lambda + 1)(\mu + 1)/9, \\ b_2 &= 2q - (2\lambda - 1)/3. \end{aligned}$$

(3) *When* $\lambda \in \{1, 2, (3q-2)/2, 3q-2\}$, $C_3(\lambda)$ *coincides with* $C_1(*)$ *as follows*:

$$\begin{gathered} C_3(1) = C_3(3q-2) = C_1(1), \\ C_3(2) = C_1(q/2), \\ C_3((3q-2)/2) = C_1(2). \end{gathered}$$

We can also get the cycle in case $l = 3$, i.e. in $C_5(\lambda)$, as follows.

Theorem 3. *Put* $\mu = (5q-6)/\lambda$.

(1) *When* $\lambda \equiv 1 \pmod 5$ *and* $1 < \lambda < (5q-6)/4$, $C_5(\lambda)$ *has the following cycle of period* 10 :

$$\begin{aligned} &[\lambda, 2q-5, -\mu] \sim [-\mu, b_1, c_1] \\ &\sim [c_1, b_2, -c_2] \sim [-c_2, b_3, c_3] \\ &\sim [c_3, b_4, -\lambda] \sim [-\lambda, 2q-5, \mu] \\ &\sim [\mu, b_1, -c_1] \sim [-c_1, b_2, c_2] \\ &\sim [c_2, b_3, -c_3] \sim [-c_3, b_4, \lambda], \end{aligned}$$

where

$$\begin{aligned} b_1 &= 2q - (4\mu - 1)/5, \\ c_1 &= 1 + (\lambda - 1)(4\mu - 1)/25, \\ b_2 &= 2q - 1 - 4(\lambda - 1)(\mu + 1)/25, \\ c_2 &= 1 + (4\lambda + 1)(\mu + 1)/25, \\ b_3 &= 2q - 2 - (4\lambda + 1)(2\mu - 3)/25, \\ c_3 &= q + (\lambda - 1)(\mu - 9)/25, \\ b_4 &= 2q - (6\lambda - 1)/5. \end{aligned}$$

(2) *When* $\lambda \equiv 2 \pmod 5$ *and* $2 < \lambda < (5q-6)/2$, $C_5(\lambda)$ *has the following cycle of period* 10 :

$$\begin{aligned} &[\lambda, 2q-5, -\mu] \sim [-\mu, b_1, c_1] \\ &\sim [c_1, b_2, -c_2] \sim [-c_2, b_3, c_3] \\ &\sim [c_3, b_4, -\lambda] \sim [-\lambda, 2q-5, \mu] \\ &\sim [\mu, b_1, -c_1] \sim [-c_1, b_2, c_2] \\ &\sim [c_2, b_3, -c_3] \sim [-c_3, b_4, \lambda], \end{aligned}$$

where

$$\begin{aligned} b_1 &= 2q + (1 - 8\mu)/5, \\ c_1 &= 2 + (\lambda - 2)(8\mu - 1)/25, \\ b_2 &= 2q - 1 - 2(\lambda - 2)(2\mu + 1)/25, \\ c_2 &= (2\lambda\mu + \lambda + \mu + 13)/25, \\ b_3 &= 2q - 1 - 2(2\lambda + 1)(\mu - 2)/25, \\ c_3 &= 2 + (8\lambda - 1)(\mu - 2)/25, \\ b_4 &= 2q + (1 - 8\lambda)/5. \end{aligned}$$

(3) *When* $\lambda \equiv 3 \pmod 5$, $C_5(\lambda)$ *has the following cycle of period* 6 :

$$\begin{aligned} &[\lambda, 2q-5, -\mu] \sim [-\mu, b_1, c_1] \\ &\sim [c_1, b_2, -\lambda] \sim [-\lambda, 2q-5, \mu] \\ &\sim [\mu, b_1, -c_1] \sim [-c_1, b_2, \lambda], \end{aligned}$$

where

$$\begin{aligned} b_1 &= 2q + (1 - 2\mu)/5, \\ c_1 &= (2\lambda\mu - \lambda - \mu + 13)/25, \\ b_2 &= 2q + (1 - 2\lambda)/5. \end{aligned}$$

(4) *When* $\lambda \equiv 4 \pmod 5$, $C_5(\lambda)$ *has the following cycle of period* 10 :

$$\begin{aligned} &[\lambda, 2q-5, -\mu] \sim [-\mu, b_1, c_1] \\ &\sim [c_1, b_2, -c_2] \sim [-c_2, b_3, c_3] \\ &\sim [c_3, b_4, -\lambda] \sim [-\lambda, 2q-5, \mu] \\ &\sim [\mu, b_1, -c_1] \sim [-c_1, b_2, c_2] \\ &\sim [c_2, b_3, -c_3] \sim [-c_3, b_4, \lambda], \end{aligned}$$

where

$$\begin{aligned} b_1 &= 2q - (6\mu - 1)/5, \\ c_1 &= q + (\lambda - 9)(\mu - 1)/25, \\ b_2 &= 2q - 2 - (2\lambda - 3)(4\mu + 1)/25, \end{aligned}$$

$$c_2 = 1 + (\lambda+1)(4\mu+1)/25,$$
$$b_3 = 2q - 1 - 4(\lambda+1)(\mu-1)/25,$$
$$c_3 = 1 + (4\lambda-1)(\mu-1)/25,$$
$$b_4 = 2q - (4\lambda-1)/5.$$

(5) *When* $\lambda \in \{1, 2, 4, (5q-6)/4, (5q-6)/2, 5q-6\}$, $C_5(\lambda)$ *coincides with* $C_1(*)$ *or* $C_3(*)$ *as follows*:

$$C_5(1) = C_5(5q-6) = C_1(1),$$
$$C_5(2) = C_1(2),$$
$$C_5((5q-6)/2) = C_1(q/2),$$
$$C_5(4) = C_3((3q-2)/4),$$
$$C_5((5q-6)/4) = C_3(4).$$

In comparing these reduced forms, we obtain the following results.

Theorem 4. (1) $C_1(\lambda) \neq C_1(\lambda')$ *for* $\lambda \neq \lambda'$, *except that* $C_1(1) = C_1(q)$.

(2) $C_3(\lambda) \neq C_3(\lambda')$ *for* $\lambda \neq \lambda'$, *except for* $C_3(1) = C_3(3q-2)$ *and* $C_3(5) = C_3((3q-2)/5)$.

(3) $C_5(\lambda) \neq C_5(\lambda')$ *for* $\lambda \neq \lambda'$, *except for* $C_5(1) = C_5(5q-6)$ *and* $C_5(13) = C_5((5q-6)/13)$.

Theorem 5. (1) $C_3(*)$ *does not coincide with* $C_1(*)$, *except for*

$$C_3(1) = C_3(3q-2) = C_1(1),$$
$$C_3(2) = C_1(q/2),$$
$$C_3((3q-2)/2) = C_1(2).$$

(2) $C_5(*)$ *coincides with neither* $C_1(*)$ *nor* $C_3(*)$, *except for*

$$C_5(1) = C_5(5q-6) = C_1(1),$$
$$C_5(2) = C_1(2),$$
$$C_5((5q-6)/2) = C_1(q/2),$$
$$C_5(3) = C_1(q/3),$$
$$C_5((5q-6)/3) = C_1(3),$$
$$C_5(4) = C_3((3q-2)/4),$$
$$C_5((5q-6)/4) = C_3(4),$$
$$C_5(8) = C_3((3q-2)/8),$$
$$C_5((5q-6)/8) = C_3(8).$$

3. Subgroups of $H(4q^2+1)$. The foregoing results have the following corollaries:

Corollary 1. *Let* q *be a positive integer. Assume that* $4q^2+1$ *is square-free.*

(1) *Assume that* $q > 1$. *If* q *is an* n*-th power of some integer* ($n \geq 2$), *then* $H(4q^2+1)$ *has a cyclic subgroup of order* n.

(2) *Assume that* $q > 2$. *If* $3q-2$ *is an* n*-th power of some integer* ($n \geq 2$), *then* $H(4q^2+1)$ *has a cyclic subgroup of order* n.

(3) *Assume that* $q > 3$. *If* $5q-6$ *is an* n*-th power of some integer* ($n \geq 2$), *then* $H(4q^2+1)$ *has a cyclic subgroup of order* n.

To prove Corollary 1 (1), put $q = m^n$. $C_1(m^i) = C_1(m)^i$ holds by Proposition 1 (3). And $C_1(m)^n = C_1(q)$ is a unit in $F(4q^2+1)/\sim$ by Proposition 1 (2). Moreover, $C_1(m^i) \neq C_1(m^j)$ for $0 \leq i < j < n$ by Theorem 4 (1). From Proposition 1 (1), Corollary 1 (1) is proved. Corollaries 1 (2) and 1 (3) are proved likewise.

Note: Corollary 1 (1) is a special case of the fact in [6], which says that $H(a^{2n}+4b^{2n})$ has a cyclic subgroup of order n, where $a^{2n}+4b^{2n}$ is a square-free positive integer.

4. Lower bounds of $h(4q^2+1)$.

Corollary 2. *Let* q *be a positive integer such that* $4q^2+1$ *is square-free. Assume that* q *is big enough* (*say*, $q \geq 30$). *Then we have*

$$h(4q^2+1) \geq (\tau(q)-1) + (\tau(3q-2)-c_3) + (\tau(5q-6)-c_5),$$

where

$$c_3 = 2 + 2\delta_2(3q-2) + \delta_5(3q-2),$$
$$c_5 = 2 + 2\delta_2(5q-6) + 2\delta_4(5q-6) + 2\delta_8(5q-6) + 2\delta_3(5q-6) + \delta_{13}(5q-6),$$

$\tau(q)$ *is the divisor function of* q, *and*

$$\delta_n(Q) = 1 \text{ if } n \mid Q;\ 0 \text{ if } n \nmid Q.$$

Corollary 2 follows easily from Theorems 4 and 5.

Corollary 2 is concerned with Chowla's conjecture, which says that there exist exactly 6 q's such that $h(4q^2+1) = 1$. In particular, the last inequality gives a better lower bound than the formulas given in [5] and [2].

5. Remark. One can obtain the same results as in this paper also using Amara's method in [1].

References

[1] H. Amara: Cycles canoniques d'idéaux reduits et nombre des classes de certains corps quadratique

reels. Nagoya Math. J., **103**, 127–132 (1986).
[2] H. Amara: Lower bounds for the class number and the caliber of certain real quadratic fields. Tokyo J. Math., **18** no.2, 437–441 (1995).
[3] D.A. Buell: Binary Quadratic Forms: Classical Theory and Modern Computations. Springer-Verlag, New York (1990).
[4] H. Cohen: A Course in Computational Algebraic Number Theory. **GTM 138**, Springer-Verlag, New York (1993).
[5] R.A. Mollin: On the divisor function and class numbers of real quadratic fields I. Proc. Japan Acad., **66A**, 109–111 (1990).
[6] T. Nakahara: On real quadratic fields whose ideal class group have a cyclic p-subgroup. Rep. Fac. Sci. Engin. Saga Univ., **6**, 15–26 (1978).