ACTA ARITHMETICA
LVI (1990)

On numbers of type x^2+Ny^2

by

TOYOKAZU HIRAMATSU (Göttingen) and YOSHIO MIMURA (Kobe)

1. Introduction. Let N be a positive integer and consider the problem when a natural number n can be represented in the form $n = x^2+Ny^2$ with $x, y \in \mathbf{Z}$. This problem is of interest from the point of view of history. For $N = 1$, the answer is the two-square theorem of Fermat. Fermat and Euler considered the cases $N = 2, 3$ (Weil [8]). In Section 2, we shall treat the case of single class in each genus. Section 3 is devoted to the study of class number 2 case through some examples.

Remark 1. For $N < 100\,000$, there are 65 values of N such that the class number of x^2+Ny^2 is equal to 1 (Dickson [2]). Such numbers are called *idoneal*. In general, it is conjecturable that there are exactly 65 idoneal numbers.

2. The case of one class per genus.

THEOREM. *Let N be a positive integer and suppose that the class number of the genus of quadratic forms in which x^2+Ny^2 lies, is equal to 1. Let n be a natural number which is coprime with N and satisfies the following conditions:*

(1) *n is a quadratic residue* $\bmod N$;

(2) *$-N$ is a quadratic residue* $\bmod n$;

(3) *If $N \equiv 7 \bmod 8$, then n is odd.*

Then, n has a primitive representation as $n = x^2+Ny^2$ with $x, y \in \mathbf{Z}$.

Proof. By the condition (2), there exist integers b and c (> 0) such that $-N = b^2-nc$. We put

$$Q(x, y) = [1, 0, N] = x^2+Ny^2,$$

$$Q'(x, y) = [n, b, c] = nx^2+2bxy+cy^2.$$

Then, as shown below, these two positive definite quadratic forms Q and Q' are in the same genus. This means that Q and Q' are in the same class by the assumption:

$$Q'(x, y) = Q(\alpha x+\beta y, \gamma x+\delta y)$$

for some

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{GL}(2, \boldsymbol{Z}).$$

In particular,

$$n = Q'(1, 0) = Q(\alpha, \gamma) = \alpha^2 + N\gamma^2, \quad (\alpha, \gamma) = 1,$$

as contended in the theorem.

In the following, we shall confirm that Q and Q' are in the same genus, i.e. that

$$(*) \qquad Q \underset{p}{\cong} Q' \quad \text{for all primes } p.$$

It is clear that Q' is primitive and its discriminant is equal to $-N$. The proof of $(*)$ is divided into the following three cases.

(i) $p > 2$ and $p \nmid N$. In general, it is known that

$$Q' \underset{p}{\cong} [1, 0, N] = Q.$$

(ii) $p > 2$ and $p \mid N$. By (1), there exists a unit ε in the p-adic integers $\boldsymbol{Z}_p$ such that $n = \varepsilon^2$. Therefore

$$Q'(x, y) = \left(\varepsilon x + \frac{b}{\varepsilon} y\right)^2 + N\left(\frac{1}{\varepsilon} y\right)^2 = Q\left(\varepsilon x + \frac{b}{\varepsilon} y, \frac{1}{\varepsilon} y\right)$$

and

$$\begin{bmatrix} \varepsilon & b/\varepsilon \\ 0 & 1/\varepsilon \end{bmatrix} \in \mathrm{GL}(2, \boldsymbol{Z}_p).$$

Hence we have $Q \underset{p}{\cong} Q'$.

(iii) $p = 2$. This case is an essential part of the proof. Let Q'' be a quadratic form of discriminant $-N$ and put $Q'' = [A, B, C]$. Let p be any prime and define a symbol S_p by

$$S_p(Q'') = \left(\frac{N, -1}{p}\right)\left(\frac{A, -N}{p}\right),$$

where $\left(\frac{\ ,\ }{p}\right)$ denotes the Hilbert norm-residue symbol. The symbol S_p is independent of the choice of A and has the following fundamental properties:

1. If $Q'' \underset{p}{\cong} Q'''$, then $S_p(Q'') = S_p(Q''')$;

2. $\prod_{\text{all } p} S_p(Q'') = 1$.

Applying the above results to Q and Q', we have

$$(2.1) \qquad S_2(Q') = S_2(Q) = \left(\frac{N, -1}{2}\right).$$

If $8 \mid N$, then we have $Q \underset{2}{\cong} Q'$ in the same way as in the proof of Case (ii). If 4 divides exactly N, then $n \equiv 1, 5 \bmod 8$; hence $n = \varepsilon^2$ or $5\varepsilon^2$ ($\varepsilon \in \boldsymbol{Z}_2^\times$). The proof of the case $n = \varepsilon^2$ is the same as in (ii). If $n = 5\varepsilon^2$, then

$$Q'(x, y) = 5\left(\varepsilon x + \frac{b}{5\varepsilon} y\right)^2 + \frac{N}{5}\left(\frac{1}{\varepsilon} y\right)^2 \underset{2}{\cong} [5, 0, N/5].$$

Denote by $Q''(x, y)$ the right-hand side of the above. Then

$$Q''(x, x+y) = [5 + N/5, N/5, N/5]$$

and $5 + N/5 \equiv 1 \bmod 8$ in $\boldsymbol{Z}_2$, i.e. $5 + N/5 = \eta^2$ ($\eta \in \boldsymbol{Z}_2^\times$). Next we consider the case that 2 divides exactly N. In this case,

$$Q'(x, y) = n\left(x + \frac{b}{n} y\right)^2 + \frac{N}{n} y^2 \underset{2}{\cong} [n, 0, N/n]$$

with n odd. For $n \equiv 1 \bmod 8$ or $n \equiv 7 \bmod 8$, $Q \underset{2}{\cong} Q'$ is trivial. If $n \equiv 3 \bmod 8$, then we have

$$\left(\frac{N, -1}{2}\right)\left(\frac{3, -N}{2}\right) = \left(\frac{N, -1}{2}\right);$$

hence $\left(\frac{3, -N}{2}\right) = 1$, i.e. $N \equiv 2 \bmod 8$. Therefore, $3 + N/3 \equiv 1 \bmod 8$ in $\boldsymbol{Z}_2$. If $n \equiv 5 \bmod 8$, then

$$\left(\frac{N, -1}{2}\right)\left(\frac{5, -N}{2}\right) = -\left(\frac{N, -1}{2}\right) \neq \left(\frac{N, -1}{2}\right),$$

which contradicts the relation (2.1). Finally, we treat the case $2 \nmid N$. The quadratic forms of discriminant $-N$ over $\boldsymbol{Z}_2$ can be classified to one of the following types: $[1, 0, N]$, $[3, 0, N/3]$, $[5, 0, N/5]$, $[7, 0, N/7]$, $[2, 1, 2]$ and $[0, 1, 0]$.

1° $Q' \underset{2}{\cong} [3, 0, N/3]$. In this case

$$\left(\frac{N, -1}{2}\right)\left(\frac{3, -N}{2}\right) = \left(\frac{N, -1}{2}\right);$$

hence $\left(\frac{3, -N}{2}\right) = 1$. Therefore, $N \equiv 3 \bmod 4$. If $N \equiv 3 \bmod 8$, then $N/3 \equiv 1 \bmod 8$, i.e.

$$Q' \underset{2}{\cong} [N/3, 0, 3] \underset{2}{\cong} Q.$$

If $N \equiv 7 \bmod 8$, then $N/3 \equiv 5 \bmod 8$:

$$Q' \underset{2}{\cong} [N/3, 0, 3] \underset{2}{\cong} [N/3 + 12, 6, 3] \underset{2}{\cong} Q.$$

2° $Q' \underset{2}{\cong} [5, 0, N/5]$. We have

$$Q' \underset{2}{\cong} [5+\tfrac{4}{5}N, \tfrac{2}{5}N, N/5];$$

and $5+\frac{4}{5}N \equiv 1 \bmod 8$.

3° $Q' \underset{2}{\cong} [7, 0, N/7]$. This case is similar to 1°.

4° $Q' \underset{2}{\cong} [2, 1, 2]$. In this case, $N \equiv 3 \bmod 8$. Therefore

$$\left(\frac{N, -1}{2}\right)\left(\frac{2, -N}{2}\right) = -\left(\frac{N, -1}{2}\right) \neq \left(\frac{N, -1}{2}\right),$$

which is a contradiction.

5° $Q' \underset{2}{\cong} [0, 1, 0]$. In this case, $N \equiv 7 \bmod 8$. Thus, by the condition (3), n is odd, namely Q' is odd. But, $[0, 1, 0]$ is even. ∎

3. Examples of $h = 2$. For an example, we put $N = 41$. Then, the class number of x^2+41y^2 is equal to 3 and its representative elements are given by

$$x^2+41y^2, \quad 2x^2+2xy+21y^2 \quad \text{and} \quad 5x^2+4xy+9y^2.$$

Then, $n = 1$, 5, 21, 42 and 105 satisfy the conditions (1), (2) and (3), and are represented by the following:

$$\begin{aligned} 1 &= x^2+41y^2, \\ 5 &= 5x^2+4xy+9y^2, \\ 21 &= 2x^2+2xy+21y^2 = 5X^2+4XY+9Y^2, \\ 42 &= x^2+41y^2 = 5X^2+4XY+9Y^2, \\ 105 &= x^2+41y^2 = 2X^2+2XY+21Y^2 = 5t^2+4ts+9s^2. \end{aligned}$$

Denote by h the class number of x^2+Ny^2 and suppose $h \geqslant 2$. Then, as shown in the above example, we do not have enough information to judge whether n can be represented in the form $n = x^2+Ny^2$ $(x, y \in \boldsymbol{Z})$. Let $F_d(x, y)$ be a principal form of discriminant d (<0):

$$F_d(x, y) = \begin{cases} x^2-\dfrac{d}{4}y^2, & d \equiv 0 \bmod 4, \\ x^2+xy-\dfrac{d-1}{4}y^2, & d \equiv 1 \bmod 4, \end{cases}$$

where $d = d_0 f^2$ for d_0 the discriminant of the imaginary quadratic field $\boldsymbol{Q}(\sqrt{d_0})$. Let K denote the so-called ring class field over $\boldsymbol{Q}$. Then, for a prime $p \nmid 2d$,

$$p = F_d(x, y) \Leftrightarrow p \text{ splits in } K.$$

This means that the ideal (p) factors into as many distinct ideal factors as $[K:\boldsymbol{Q}]$, or all monic defining polynomials for K factor completely into distinct linear factors mod p (Weber).

In the following, we shall consider the case $h = 2$ through some examples. Let $Q \in \{1, 2, 3, 4\}$. The Hecke group $G(\sqrt{Q})$ is the subgroup of $\mathrm{SL}_2(\boldsymbol{R})$ which is generated by the matrices

$$\begin{bmatrix} 1 & \sqrt{Q} \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Put

$$\eta_Q(z) = \eta\left(\frac{z}{\sqrt{Q}}\right)\eta(\sqrt{Q}\,z),$$

where $\eta(z)$ denotes the Dedekind eta function. Then, $\eta_Q(z)$ is a cusp form of weight 1 on $G(\sqrt{Q})$ whose multiplier v_Q is determined by

$$v_Q\left(\begin{bmatrix} 1 & \sqrt{Q} \\ 0 & 1 \end{bmatrix}\right) = e^{2\pi i(Q+1)/24}, \quad v_Q\left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right) = -i.$$

Also we denote by $a_Q(n)$ the nth Fourier coefficient of $\eta_Q(z)$.

Example 1 (Köhler [6]). $N = 3^3$. The class number of $x^2+3^3y^2$ equals 2 and its representatives are given by $x^2+3^3y^2$ and $4x^2+2xy+7y^2$. For each prime p such that $p \equiv 1 \bmod 6$, we have

$$p = x^2+27y^2 \Leftrightarrow a_3(p) = 2.$$

Example 2 ([6]). $N = 2^2 \cdot 3^2$. $h = 2$ and representatives: $x^2+2^2 \cdot 3^2 y$ and $4x^2+9y^2$. For prime p such that $p \equiv 1 \bmod 12$, we have

$$p = x^2+36y^2 \Leftrightarrow a_1(p) = 2.$$

Example 3 ([6]). $N = 2^5$. In this case, $h = 2$ and we may choose for the representatives: $x^2+2^5y^2$, $4x^2+4xy+9y^2$. Let p be any prime such that $p \equiv 1 \bmod 8$. Then,

$$p = x^2+32y^2 \Leftrightarrow a_2(p) = 2 \Leftrightarrow p = \mathrm{Norm}(\pi), \quad \pi \equiv 1 \bmod 4(1+i).$$

Example 4 ([4], [5]). $N = 2^2 \cdot 3^3$. $h = 2$ and representatives: $x^2+2^2 \cdot 3^3 y^2$ and $9x^2+6xy+13y^2$. We have

$$p = x^2+108y^2 \Leftrightarrow b(p) = 2,$$

where $b(p)$ denotes the pth Fourier coefficient of $\eta(18z)\eta(6z)$.

Example 5 ([3]). $N = 2^6$. $h = 2$ and representatives: $x^2+2^6y^2$, $4x^2+4xy+17y^2$. For each prime p such that $p \equiv 1 \bmod 8$, we have

$$p = x^2+64y^2 \Leftrightarrow c(p) = 2 \Leftrightarrow \left(\frac{2}{p}\right)_4 = 1.$$

The notations used here are defined as follows:

$$\vartheta_0(z)=\sum_{m\in\boldsymbol{Z}}(-1)^m e^{\pi i m^2 z},\qquad \vartheta_2(z)=\sum_{m\equiv 1 \bmod 2} e^{\pi i m^2 z/4};$$

$c(p)$: the pth Fourier coefficient of $\vartheta_0(32z)\vartheta_2(8z)$;

$\left(\frac{r}{p}\right)_4$: 1 or -1 according as r is or is not a fourth-power residue mod p.

Remark 2. $N=2^8$. In this case, $h=3$ and Cohn ([1]) obtained the following:

$$p=x^2+256y^2 \Leftrightarrow p \text{ splits in } \boldsymbol{Q}(i, \sqrt{1+\sqrt{2}}\sqrt[8]{2}).$$

We may ask the following question: Can one obtain a modular criterion for the problem when p can be written as $p=x^2+256y^2$ with $x,\ y\in\boldsymbol{Z}$?

Remark 3 (Petersson [7]). Let N be a natural number and define

$$\Gamma_{\vartheta,0}(N)=\Gamma_\vartheta\cap\Gamma_0(N),$$

where

$$\Gamma_\vartheta=\left\{L\in \mathrm{SL}(2,\boldsymbol{Z}):\ L\equiv\begin{bmatrix}1&0\\0&1\end{bmatrix} \text{ or } \begin{bmatrix}0&-1\\1&0\end{bmatrix} \bmod 2\right\}.$$

Also we define the function $\vartheta_3(z)$ by

$$\vartheta_3(z)=\sum_{m\in\boldsymbol{Z}} e^{\pi i m^2 z}.$$

Then, the function $\vartheta_3(z)\vartheta_3(Nz)$ is a cusp form of weight 1 on $\Gamma_{\vartheta,0}(N)$ whose multiplier v_N is determined by

$$v_N(L)=\begin{cases}\left(\frac{d}{N}\right)\xi_4^{(N+1)(d-1)}, & L=\begin{bmatrix}a&b\\c&d\end{bmatrix}\equiv\begin{bmatrix}1&0\\0&1\end{bmatrix}\bmod 2,\\[2ex] \left(\frac{d}{N}\right)\xi_4^{-(N+1)c}, & L=\begin{bmatrix}a&b\\c&d\end{bmatrix}\equiv\begin{bmatrix}0&-1\\1&0\end{bmatrix}\bmod 2\end{cases}$$

for $N\equiv 1 \bmod 2$, where $\xi_4=e^{\pi i/4}$. Let $a(n)$ denote the nth Fourier coefficient of $\vartheta_3(z)\vartheta_3(Nz)$. Then $a(n)$ is the number of integral representations of n by the quadratic form x^2+Ny^2. Therefore, our problem is to find a condition ensuring that $a(n)\neq 0$.

References

[1] H. Cohn, *Some examples of Weber–Hecke ring class field theory*, Math. Ann. 265 (1983), 83–100.
[2] L. E. Dickson, *Introduction to the Theory of Numbers*, Chelsea, 1929.

[3] T. Hiramatsu, *Higher reciprocity law and modular forms of weight one*, Comment. Math. Univ. St. Pauli 31 (1982), 75–85.
[4] T. Hiramatsu, N. Ishii and Y. Mimura, *On indefinite modular forms of weight one*, J. Math. Soc. Japan 38 (1986), 67–83.
[5] T. Hiramatsu, *Theory of automorphic forms of weight* 1, Adv. Studies in Pure Math. 13, Investigations in Number Theory, 1988, 503–584.
[6] G. Köhler, *Theta series on the Hecke groups $G(\sqrt{2})$ and $G(\sqrt{3})$*, Math. Z. 197 (1988), 69–96.
[7] H. Petersson, *Modulfunktionen und quadratische Formen*, Springer-Verlag, 1982.
[8] A. Weil, *Number Theory*, Birkhäuser, 1983.

SONDERFORSCHUNGSBEREICH 170
MATHEMATISCHES INSTITUT
Bunsenstrasse 3-5 D-3400 Göttingen
Federal Republic of Germany
Current address:
DEPARTMENT OF MATHEMATICS
KOBE UNIVERSITY
Kobe 657, Japan

Received on 30.5.1989 (1940)