THE NUMBER OF SOLUTIONS FOR THE DIOPHANTINE EQUATION $ax^2+by^2+cz^2=n$

PEI DINGYI (裴定一)
(Institute of Applied Mathematics, Academia Sinica, Beijing)
Received December 2, 1981.

(1) Let a, b, c, n be positive integers. Suppose the greatest common divisor of a, b, c is 1. Let $N(a, b, c, n)$ denote the number of solutions (x, y, z) of the diophantine equation

$$ax^2 + by^2 + cz^2 = n,$$

where x, y, z are integers. Put

$$\vartheta(z) = \sum_{n=-\infty}^{+\infty} e(n^2 z),$$

where $e(z) = e^{2\pi i z}$. Define

$$f(a, b, c, n) = \vartheta(az)\vartheta(bz)\vartheta(cz).$$

We have

$$f(a, b, c, n) = 1 + \sum_{n=1}^{\infty} N(a, b, c, n)e(nz).$$

For a positive integer N we define the group

$$\Gamma_0(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \text{ are integers, } ad - bc = 1, N \mid c\right\}.$$

For any element $r = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$, we know that

$$\vartheta\left(\frac{az + b}{cz + d}\right) = \left(\frac{c}{d}\right) \varepsilon_d^{-1}(cz + d)^{1/2}\vartheta(z),$$

where $\left(\frac{c}{d}\right)$ is the quadratic residue symbol, ε_d is defined for any odd integer d and

$$\varepsilon_d = \begin{cases} 1, & d \equiv 1 \pmod 4, \\ i, & d \equiv 3 \pmod 4. \end{cases}$$

We define $(cz + d)^{1/2}$ so that $-\pi/2 < \arg(cz + d) \leqslant \pi/2$. Put

$$j(r, z) = \left(\frac{c}{d}\right) \varepsilon_d^{-1}(cz + d)^{1/2}.$$

Suppose N is divided by 4. Let ω be an even character modulo N and k be a positive odd integer. We denote the linear space of the modular forms $f(z)$ which satisfy

$$f\left(\frac{az+b}{cz+d}\right)=\omega(d)j(r,\ z)^k f(z),\ \ \forall r=\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in\Gamma_0(N),$$

by $M_{k/2}(N,\omega)$. The reader is referred to the paper[4] by G. Shimura for the discussion of modular forms of half integral weight. Let χ_n be the primitive character satisfying

$$\chi_n(d)=\left(\frac{n}{d}\right).$$

It is easy to see that $\vartheta(nz)\in M_{1/2}(4n,\chi_n)$ and $f(a,\ b,\ c,\ z)\in M_{3/2}(4[a,\ b,\ c],\ \chi_{abc})$, where $[a,b,c]$ is the least common multiple of a,b,c.

Let $S_{k/2}(N,\omega)$ denote the subspace of cusp forms in $M_{k/2}(N,\omega)$, $\mathscr{E}_{k/2}(N,\omega)$ the orthogonal complement of $S_{k/2}\ (N,\ \omega)$ in $M_{k/2}(N,\ \omega)$ with respect to the Petersson inner product. We use $M(N,\ \omega)$, $S(N,\omega)$ and $\mathscr{E}(N,\omega)$ instead of $M_{3/2}(N,\omega)$, $S_{3/2}\ (N,\omega)$ and $\mathscr{E}_{3/2}(N,\omega)$ in this paper. A basis of $\mathscr{E}(N,\omega)$ is given in [2] when $N=4D$ or $8D$, where D is a square-free integer, $\omega=\chi_n(n|2D)$ or $N=2^e(e\geqslant 4)$, $\omega=\chi_1$. If for some special N and ω we have $S(N,\omega)=0$, then the basis is also one of $M(N,\omega)$. Using the theorem 2 of H. Cohen and J. Desterlé[1] and the result about the dimension of $M_{1/2}(N,\omega)$ in J. P. Serre and H. M. Stark[3], we can prove that

$$S(4,\chi_1)=0,\quad S(8,\chi_1)=0,\quad S(8,\chi_2)=0,\quad S(12,\chi_1)=0,$$
$$S(12,\chi_3)=0,\quad S(16,\chi_1)=0,\quad S(16,\chi_2)=0\quad S(20,\chi_1)=0,$$
$$S(20,\chi_5)=0,\quad S(24,\chi_1)=0,\quad S(24,\chi_2)=0,\quad S(24,\chi_3)=0,$$
$$S(24,\chi_6)=0,\quad S(32,\chi_1)=0,\quad S(32,\chi_2)=0,\quad S(64,\chi_2)=0.$$

If $f(a,b,c,z)$ belongs to the $M(N,\omega)$ corresponding to these N and ω and we can express $f(a,b,c,z)$ as a linear combination of the basis whose Fourier expansions are already given in [2], then we can find the expression for $N(a,b,c,n)$.

(2) When we express $f(a,b,c,z)$ as a linear combination of the basis, we should use the values at cusps of modular forms. All rational numbers and the infinite are cusps of the group $\Gamma_0(N)$. Let S_1 and S_2 be two cusps. If there exists an element $r\in\Gamma_0(N)$ such that $r(s_1)=s_2$, then we call s_1 and s_2 the $\Gamma_0(N)$-equivalence. Take a positive divisor c of N and put $g(c)=\phi((c,N/c))$, where ϕ is Euler's function. Let $d_1,d_2,\cdots,d_{g(c)}$ be a full set of representatives $(\boldsymbol{Z}/(c,N/c)\boldsymbol{Z})^*$. Then the set of cusps (suppose $(d_i,c)=1$)

$$S(N)=\{d_i/c\,|\,c\,|N,1\leqslant i\leqslant g(c)\}$$

is a full set of representatives of $\Gamma_0(N)$-equivalence classes of cusps. Suppose $f(z)\in M_{k/2}(N,\omega)$, and the value at the infinite of $f(z)$ is defined by $V(f,i\infty)=\lim\limits_{z\to\infty}f(z)$.

Now let $s=d/c\ (c>0,\ (c,\ d)=1)$ be a cusp. There exists an element $\rho=\begin{pmatrix} a & b \\ -c & d\end{pmatrix}$ $\in SL_2(\boldsymbol{Z})$ such that $\rho(s)=i\infty$, then the value at s of $f(z)$ is defined by

$$V(f,s)=\lim_{z\to i\infty} f\left(\frac{dz-b}{cz+a}\right)(cz+a)^{-k/2}$$

$$= \lim_{z\to i\infty} f\left(-\frac{1}{c(cz+a)}+\frac{d}{c}\right)(cz+a)^{-k/2}$$

$$= \lim_{\tau\to 0}(-c\tau)^{k/2}f(\tau+d/c). \qquad (*)$$

According to the definition of modular forms, these limitations are all finite.

(3) If the modular forms f and $f_i(1\leqslant i\leqslant m)$ belong to $M(N,\omega)$ and $f=\sum_{i=1}^{m}\alpha_i f_i$, then for any cusp s we have $V(f,s)=\sum_{i=1}^{m}\alpha_i V(f_i,s)$ by the formula (*). Conversely, if the last relation is true for any cusp s, then $f-\sum_{i=1}^{m}\alpha_i f_i$ is a cusp form. Furthermore, we have $f=\sum_{i=1}^{m}\alpha_i f_i$ when $S(N,\omega)=0$. Now we show how to find the expression $N(1,3,3,n)$ as an example. We know that $f(1,3,3,z)\in M(12,\chi_1)$ and the dimension $M(12,\chi_1)$ is 3. In [2], we have proved that the following three functions form a basis of $M(12,\chi_1)$:

$$g(\chi_1,3,12)=2\pi\sum_{n=1}^{\infty}\lambda(n,12)(A(3,n)-1/3)n^{1/2}e(nz),$$

$$g(\chi_1,4,12)=-4\pi(1+i)\sum_{n=1}^{\infty}\lambda(n,12)\left(A(2,n)-\frac{1-i}{4}\right)n^{1/2}e(nz),$$

$$g(\chi_1,12,12)=1-4\pi(1+i)\sum_{n=1}^{\infty}\lambda(n,12)\left(A(2,n)-\frac{1-i}{4}\right)(A(3,n)-1/3)n^{1/2}e(nz),$$

where the definitions of $\lambda(n,12)$ and $A(p,n)$ are given in [2]. Their values at the cusps 1/3, 1/4, and 1/12 are derived as follows:

	1/3	1/4	1/12
$g(\chi_1,3,12)$	$\frac{i-1}{4}$	0	0
$g(\chi_1,4,12)$	0	1	0
$g(\chi_1,12,12)$	$\frac{i-1}{4}$	$-1/3$	1.

On the other hand, we have

$$V(f(1,3,3,z),1/12)=V(\vartheta,1/12)V^2(\vartheta,1/4)=1,$$

$$V(f(1,3,3,z),1/4)=V(\vartheta,1/4)V^2(\vartheta,3/4)3^{-1}=-1/3,$$

$$V(f(1,3,3,z),1/3)=V(\vartheta,1/3)V^2(\vartheta,1)=\frac{1-i}{4}.$$

Here we have $V(\vartheta, 1/12) = V(\vartheta, 1/4) = 1$, $V(\vartheta, 1) = \frac{1-i}{2}$, $V(\vartheta, 3/4) - i$ and $V(\vartheta, 1/3) = \frac{1+i}{2}$. We should use Lemma 4.1 of [2], Prop. 2. of [4], the relation $\vartheta^3 = g(\chi_1, 4, 4)$ and $V(g(\chi_1, 4, 4), 1/2) = 0$ to calculate these ϑ' s values. Now we obtain

$$f(1, 3, 3, z) = g(\chi_1, 12, 12) - 2g(\chi_1, 3, 12).$$

Hence

$$N(1, 3, 3, n) = \pi n^{1/2}\lambda(n, 12)(1/3 - A(3, n))(4 - B(2, n)),$$

where $B(2, n) = 4(1 + i)(4^{-1}(1 - i) - A(2, n))$. Define

$$\delta(x) = \begin{cases} 1, & x \text{ is an integer,} \\ 0, & \text{otherwise.} \end{cases}$$

Now we list other results that we obtained as follows.

$$N(1, 1, 1, n) = \pi n^{1/2}\lambda(n, 4)B(2, n),$$

$$N(1, 2, 2, n) = \pi n^{1/2}\lambda(n, 4)\left(B(2, n) - 2\delta\left(\frac{n-1}{4}\right) - 2\delta\left(\frac{n-2}{4}\right)\right),$$

$$N(1, 5, 5, n) = \pi n^{1/2}\lambda(n, 20)B(2, n)(A(5, n) + 1/5),$$

$$N(1, 6, 6, n) = \pi n^{1/2}\lambda(n, 12)(1/3 - A(3, n))\left(2 + 2\delta\left(\frac{n-1}{4}\right) + 2\delta\left(\frac{n-2}{4}\right) - B(2, n)\right),$$

$$N(2, 3, 6, n) = \pi n^{1/2}\lambda(n, 12)(1/3 + A(3, n))\left(B(2, n) - 2\delta\left(\frac{n-1}{4}\right) - 2\delta\left(\frac{n-2}{4}\right)\right),$$

$$N(1, 1, 4, n) = \pi n^{1/2}\lambda(n, 4)\left(2\delta\left(\frac{n-1}{4}\right) + \delta\left(\frac{n-2}{4}\right) + \delta\left(\frac{n}{4}\right)B(2, n)\right),$$

$$N(1, 4, 4, n) = \pi n^{1/2}\lambda(n, 4)\left(\delta\left(\frac{n}{4}\right)B(2, n) + \delta\left(\frac{n-1}{4}\right)\right),$$

$$N(1, 2, 4, n) = \pi(2n)^{1/2}\lambda(2n, 4)\left(B(2, 2n) - \delta\left(\frac{n}{2}\right)\delta\left(\frac{n/2-1}{4}\right) - \delta\left(\frac{n}{4}\right)\delta\left(\frac{n/4-1}{2}\right) - 5/2\,\delta\left(\frac{n-1}{2}\right)\right),$$

$$N(1, 1, 8, n) = \pi n^{1/2}\lambda(2n, 4)\left(8^{-1/2}B(2, n/8)\,\delta\left(\frac{n}{8}\right) + 2^{1/2}\delta\left(\frac{n}{2}\right)\delta\left(\frac{n/2-1}{2}\right) + 2^{-1/2}\delta\left(\frac{n}{4}\right)\delta\left(\frac{n/4-1}{2}\right) + 2^{5/2}\delta\left(\frac{n-1}{4}\right)\right),$$

$$N(1, 4, 8, n) = \pi n^{1/2}\lambda(2n, 4)\left(8^{-1/2}B(2, n/8)\,\delta\left(\frac{n}{8}\right)\right.$$

$$+ 2^{-1/2}\delta\left(\frac{n}{4}\right)\delta\left(\frac{n/4-1}{2}\right) + 2^{-1/2}\delta\left(\frac{n-1}{4}\right)\Big);$$

and

$$N(1,1,2,n) = N(1,2,2,2n), \qquad N(1,1,3,n) = N(1,3,3,3n),$$
$$N(1,1,5,n) = N(1,5,5,5n), \qquad N(2,3,3,n) = N(1,6,6,2n),$$
$$N(1,3,6,n) = N(2,3,6,2n), \qquad N(2,2,3,n) = N(1,6,6,3n),$$
$$N(1,2,6,n) = N(2,3,6,3n), \qquad N(1,1,6,n) = N(1,6,6,6n),$$
$$N(1,2,3,n) = N(2,3,6,6n).$$

References

[1] Cohen, H. & Desterle, J., Dimensions des espaces de forms modulaires, Modular functions of one variable, *Lect. Notes in Math.* 627.

[2] Pei Dingyi, Eisenstein series of weight 3/2 (I), *Transactions of American Math. Soc.*, **274**(1982), 2:573—606.

[3] Serre, J. P. & Stark, H. M., Modular forms of weight 1/2, Modular functions of one variable, *Lect. Notes in Math.* 627.

[4] Shimura, G., On modular forms of half integral weight, *Ann. of Math.*, **97** (1973), 440—481.