Tôhoku Math. J.
41 (1989), 283–290

ON SOME ARITHMETIC PROPERTIES OF CERTAIN QUADRATIC FIBRATIONS

Dedicated to Professor Ichiro Satake on his sixtieth birthday

TAKASHI ONO

(Received January 25, 1988)

Introduction. For a natural number n, consider the following two sets:

$$A(n)=\{(x, y, t, u)\in \boldsymbol{Z}^4;\ \text{g.c.d.}(x, y, t, u)=1,\ x^2+y^2=tu,\ t+u=n\}\,,$$

$$B(n)=\{(x, y, t, u)\in \boldsymbol{Z}^4;\ \text{g.c.d.}(x, y, t, u)=1,\ x^2+y^2=tu=n,\ t, u\geqq 1\}\,.$$

Denote by $a(n)$, $b(n)$ the cardinality of $A(n)$, $B(n)$, respectively. In this paper the reader will find a proof of the following formulas:

$$(0.1)\qquad \vartheta_3{}^4(\tau)=1+\sum_{n=1}^{\infty} a(n)(\vartheta_3{}^2(n\tau)-1)\,,\qquad \text{where}\quad \vartheta_3(\tau)=\sum_{k\in\boldsymbol{Z}} e^{\pi i\tau k^2}\,,$$

$$(0.2)\qquad \frac{4\zeta_{\boldsymbol{Q}(i)}(s)^2}{\zeta_{\boldsymbol{Q}(i)}(2s)}=\sum_{n=1}^{\infty}\frac{b(n)}{n^s}\,,\qquad \text{where}\quad \zeta_{\boldsymbol{Q}(i)}(s)=\frac{1}{4}\sum_{(a,b)\in\boldsymbol{Z}^2}\frac{1}{(a^2+b^2)^s}\,,\ (a, b)\neq(0, 0)\,.$$

As the reader will also find in this paper, these formulas are special cases of more general formulas ((5.1), (6.7)) and are proved by looking at a quadratic map f whose fibres are circles. We shall arrange the matter so that the final results ((3.7), (4.11)) can be stated at least for any imaginary quadratic field of class number one. This paper has some points in common with my earlier paper (Hopf maps and quadratic forms over $\boldsymbol{Z}$, Contributions to Algebra, A Collection of Papers dedicated to Ellis Kolchin, Academic Press, (1977), 295–304) but is independent of it logically.

Notation and conventions. The symbols $\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ denote the set of natural numbers ($0\notin \boldsymbol{N}$), integers, rational numbers, real numbers and complex numbers. For a complex number $c\in\boldsymbol{C}$, $\bar{c}$ is its conjugate, $Nc=\bar{c}c=|c|^2$ and $Tc=\bar{c}+c$. For a commutative associative ring R with unit, we denote by $R^\times$ the group of invertible elements of R, by R^n the product of n copies of R and by R_n the ring of matrices of degree n over R. For $a\in R_n$, $\operatorname{tr} a$ is the trace of a. When $a=(a_{ij})\in R_n$, we often write a_i for a_{ii}. For a set $*$, we denote by $[*]$ the cardinality of $*$. Given functions $a, b\colon \boldsymbol{N}\to\boldsymbol{C}$, we define functions $a\circ b$ and $a*b$ by $(a\circ b)(n)=\sum_{x+y=n} a(x)b(y)$ (Cauchy product), $(a*b)(n)=\sum_{xy=n} a(x)b(y)$ (Dirichlet product).

1. The map f. Let $X=\boldsymbol{C}^n$, $n\in\boldsymbol{N}$, be the complex vector space of dimension n and $Y=\boldsymbol{C}_n$ be the set of complex matrices of degree n. Call f the map $X\to Y$ defined by

$$(1.1)\qquad y=f(x)={}^t\bar{x}x=(\bar{x}_ix_j)\,,\qquad x=(x_1,\cdots,x_n)\in X\,.$$

If we put $e_k=(0,\cdots,1,\cdots,0)$ where 1 is the kth component, $1\leqq k\leqq n$, then $E_k={}^te_ke_k=f(e_k)$. The matrix y is hermitian and $y_i=y_{ii}\in\boldsymbol{R}$. Furthermore, $y=(y_{ij})$ satisfies the following conditions:

$$(1.2)\qquad y_i\geqq 0\,,\qquad y_{ik}y_{kj}=y_ky_{ij}\,,\qquad 1\leqq i,j,k\leqq n\,.$$

We shall denote by V the set of all hermitian matrices $y\in\boldsymbol{C}_n$ satisfying (1.2). Hence, $\operatorname{Im}f\subset V$. We shall use the letter v for matrices in V. For $\alpha\in\boldsymbol{N}$, $1\leqq\alpha\leqq n$, we put

$$(1.3)\qquad V_\alpha=\{v\in V;\ v_k=0,\ 1\leqq k\leqq\alpha-1,\ v_\alpha>0\}\,.$$

For each α, V_α is not empty because E_α is in it. Since $|v_{ij}|^2=v_{ij}\bar{v}_{ij}=v_iv_j$ by (1.2), there is an α such that $v_\alpha>0$ when $v\neq 0$. Therefore, we get the disjoint union of non-empty sets:

$$(1.4)\qquad V=\{0\}\cup V_1\cup\cdots\cup V_n\,.$$

From (1.2) one sees that

$$(1.5)\qquad v\in V_\alpha\Rightarrow v_{ij}=0\qquad\text{unless}\quad i,j\geqq\alpha\,.$$

For $t\in\boldsymbol{R}$, $t\geqq 0$, we put

$$(1.6)\qquad S(t)=\{c\in\boldsymbol{C};\ |c|^2=t\}\qquad\text{(circle of radius } t^{1/2})\,.$$

(1.7) PROPOSITION. *Let $v\in V_\alpha$, $1\leqq\alpha\leqq n$. There is a bijection*

$$\varphi_v: f^{-1}(v)\approx S(v_\alpha)$$

given by $\varphi_v(x)=x_\alpha$, $x=(x_1,\cdots,x_n)\in f^{-1}(v)$.

PROOF. (i) *φ_v is well-defined.* Since $v=f(x)={}^t\bar{x}x$, we have $v_\alpha=\bar{x}_\alpha x_\alpha=|x_\alpha|^2$, i.e. $x_\alpha=\varphi_v(x)\in S(v_\alpha)$. (ii) *$\varphi_v$ is injective.* Since $0=v_k=|x_k|^2$, $1\leqq k\leqq\alpha-1$, we have $x_k=0$ for $k\leqq\alpha-1$. Assume next that $k\geqq\alpha$. Since $v_\alpha=|x_\alpha|^2$, we have $x_\alpha\neq 0$ and so $x_k=\bar{x}_\alpha^{-1}v_{\alpha k}$ by (1.1). Hence x is completely determined by x_α, i.e. φ_v is injective. (iii) *φ_v is surjective.* Take any $c\in S(v_\alpha)$. Put $x_1=\cdots=x_{\alpha-1}=0$, $x_\alpha=c$ and $x_k=\bar{x}_\alpha^{-1}v_{\alpha k}$ for $k>\alpha$. We must show that $x\in f^{-1}(v)$, i.e. $v_{ij}=\bar{x}_ix_j$, $1\leqq i,j\leqq n$. In view of (1.5), we may assume that $i,j\geqq\alpha$. Then, we have

$$\bar{x}_ix_j=\overline{\bar{x}_\alpha^{-1}v_{\alpha i}}\bar{x}_\alpha^{-1}v_{\alpha j}=\frac{1}{|x_\alpha|^2}v_{i\alpha}v_{\alpha j}=\frac{1}{v_\alpha}v_\alpha v_{ij}=v_{ij}\,,$$

which proves that φ_v is surjective. q.e.d.

2. The map f_L. Let K be an imaginary quadratic field, $\mathfrak{o}_K$ be the ring of integers of K and

(2.1) $$L=\mathfrak{o}_K{}^n\subset X=\boldsymbol{C}^n .$$

We shall denote by f_L the restriction on L of the map f in (1.1). Clearly, we have $\mathrm{Im}\, f_L\subset V(\mathfrak{o}_K)=V\cap(\mathfrak{o}_K)_n$. For α, $1\leqq\alpha\leqq n$, we put

(2.2) $$V_\alpha(\mathfrak{o}_K)=V_\alpha\cap(\mathfrak{o}_K)_n .$$

Since $E_\alpha\in V_\alpha(\mathfrak{o}_K)$, $V_\alpha(\mathfrak{o}_K)$ is still not empty and we get the disjoint union of non-empty sets:

(2.3) $$V(\mathfrak{o}_K)=\{0\}\cup V_1(\mathfrak{o}_K)\cup\cdots\cup V_n(\mathfrak{o}_K) .$$

For $t\in\boldsymbol{R}$, $t\geqq 0$, and a lattice $\mathfrak{a}$ in $\boldsymbol{C}$, put

(2.4) $$S_{\mathfrak{a}}(t)=\mathfrak{a}\cap S(t) .$$

For $v\in V_\alpha(\mathfrak{o}_K)$, put

(2.5) $$\mathfrak{a}_v=\{c\in\mathfrak{o}_K;\ cv_{\alpha j}\equiv 0\ (\mathrm{mod}\, v_\alpha),\ \alpha\leqq j\leqq n\} .$$

Obviously, $\mathfrak{a}_v$ is an ideal of $\mathfrak{o}_K$.

(2.6) PROPOSITION. *Let v be in $V_\alpha(\mathfrak{o}_K)$, $1\leqq\alpha\leqq n$. Then, the bijection φ in* (1.7) *induces the bijection*

$$\varphi_{v,L}: f_L^{-1}(v)\approx S_{\mathfrak{a}_v}(v_\alpha) .$$

PROOF. (i) $\varphi_{v,L}$ *is well-defined.* In view of (1.7), it is enough to check that $x_\alpha\in\mathfrak{a}_v$. In fact, multiplying x_α on both sides of $\bar{x}_\alpha x_j=v_{\alpha j}$, we have $x_\alpha v_{\alpha j}=|x_\alpha|^2 x_j=v_\alpha x_j\equiv 0$ $(\mathrm{mod}\, v_\alpha)$ which proves our assertion. (ii) $\varphi_{v,L}$ *is injective.* This is obvious from (ii) of (1.7). (iii) $\varphi_{v,L}$ *is surjective.* Take any $c\in S_{\mathfrak{a}_v}(v_\alpha)$ and define $x=(x_1,\cdots,x_n)$ as in (iii) of (1.7). It remains to check that $x\in L$, i.e. all $x_j\in\mathfrak{o}_K$. For j, $1\leqq j\leqq\alpha-1$, this is trivial because $x_j=0$. For $j=\alpha$, we have $x_\alpha=c\in\mathfrak{a}_v$. Finally, for j, $j>\alpha$, we have

$$x_j=\bar{x}_\alpha{}^{-1}v_{\alpha j}=\frac{1}{|x_\alpha|^2}x_\alpha v_{\alpha j}=\frac{1}{v_\alpha}x_\alpha v_{\alpha j}=\frac{1}{v_\alpha}cv_{\alpha j}\in\mathfrak{o}_K ,$$

which proves that $\varphi_{v,L}$ is surjective. q.e.d.

For $v=(v_{ij})\in V(\mathfrak{o}_K)$, we put

(2.7) $$n(v)=\mathrm{g.c.d.}(v_i,\ Tv_{ij})\qquad (i\neq j) .$$

Since v is hermitian, we have $Tv_{ij}=v_{ij}+v_{ji}$. For α, $1\leqq\alpha\leqq n$, we define

(2.8) $$V_\alpha^*(\mathfrak{o}_K)=\{v\in V_\alpha(\mathfrak{o}_K);\ n(v)=1\} ,$$

(2.9) $$V^*(\mathfrak{o}_K)=\{0\}\cup V_1^*(\mathfrak{o}_K)\cup\cdots\cup V_n^*(\mathfrak{o}_K) .$$

As E_α is still in $V_\alpha^*(\mathfrak{o}_K)$, (2.9) is the disjoint union of non-empty sets.

(2.10) PROPOSITION. *For* $v \in V_\alpha(\mathfrak{o}_K)$ *define a matrix* v^* *by* $v = n(v)v^*$. *Then* $v^* \in V_\alpha^*(\mathfrak{o}_K)$ *and* $\mathfrak{a}_v = \mathfrak{a}_{v^*}$.

PROOF. Assume that $v^* = (v_{ij}^*)$. Since $v_i = n(v)v_i^*$ and $n(v)$ divides v_i, we have $v_i^* \in \boldsymbol{Z}$. Next, we must verify that $v_{ij}^* \in \mathfrak{o}_K$ for $i \neq j$, or, equivalently, that Nv_{ij}^* and Tv_{ij}^* are in $\boldsymbol{Z}$. Since $v_{ij}v_{ji} = v_i v_j$, we have $Nv_{ij}^* = v_{ij}^* v_{ji}^* = v_i^* v_j^* \in \boldsymbol{Z}$. On the other hand, we have $Tv_{ij}^* = (1/n(v))Tv_{ij} \in \boldsymbol{Z}$ and so $v^* \in V_\alpha^*(\mathfrak{o}_K)$. The last statement is obvious. q.e.d.

From (2.10), it follows that

$$S_{\mathfrak{a}_v}(v_\alpha) = S_{\mathfrak{a}_{v^*}}(n(v)v_\alpha^*)\,, \qquad v \in V_\alpha(\mathfrak{o}_K)\,. \tag{2.11}$$

(2.12) PROPOSITION. *If* $v = (v_{ij}) \in V_\alpha^*(\mathfrak{o}_K)$, *then* $N\mathfrak{a}_v = v_\alpha$.*)

PROOF. (i) $N\mathfrak{a}_v$ *divides* v_α. Clearly $v_\alpha \in \mathfrak{a}_v$ and so $v_\alpha \in \bar{\mathfrak{a}}_v$. Since $v_{i\alpha}v_{\alpha j} = v_\alpha v_{ij} \equiv 0 \pmod{v_\alpha}$, we have $v_{i\alpha} \in \mathfrak{a}_v$ and hence $v_{\alpha i} = \bar{v}_{i\alpha} \in \bar{\mathfrak{a}}_v$. Therefore $(N\mathfrak{a}_v) = \mathfrak{a}_v \bar{\mathfrak{a}}_v$ contains v_α^2, $v_\alpha v_{\alpha i}$, $v_\alpha v_{i\alpha}$, $v_{i\alpha}v_{\alpha i} = v_i v_\alpha$ and $v_{i\alpha}v_{\alpha j} = v_\alpha v_{ij}$, $1 \leqq i, j \leqq n$. We have $(N\mathfrak{a}_v) \supset v_\alpha(v_i, v_{ij} + v_{ji}) \ni v_\alpha$ because $n(v) = \text{g.c.d.}(v_i, Tv_{ij}) = 1$, which shows that $N\mathfrak{a}_v$ divides v_α. (ii) v_α *divides* $N\mathfrak{a}_v$. Let c be any number in $\mathfrak{a}_v$. Since $n(v) = 1$ by the assumption, there are a_k, b_{ij} in $\boldsymbol{Z}$ such that

$$1 = \sum_{k=\alpha}^{n} a_k v_k + \sum_{\alpha \leqq i < j \leqq n} b_{ij} T v_{ij}\,. \tag{2.13}$$

Multiplying $Nc = |c|^2$ on both sides of (2.13), we get

$$|c|^2 = a_\alpha v_\alpha |c|^2 + \sum_{k=\alpha+1}^{n} a_k v_k |c|^2 + \sum_{\alpha < j \leqq n} b_{\alpha j} T v_{\alpha j} |c|^2 + \sum_{\alpha < i < j \leqq n} b_{ij} T v_{ij} |c|^2\,. \tag{2.14}$$

We shall show that all four terms in (2.14) are divisible by v_α. There is no problem on the first term because v_α is already there. Next, since $c \in \mathfrak{a}_v$, we have

$$c v_{\alpha j} = v_\alpha d_j\,, \qquad d_j \in \mathfrak{o}_K\,. \tag{2.15}$$

Taking the norm of both sides of (2.15), we get

$$\begin{array}{c} |c|^2 |v_{\alpha j}|^2 = v_\alpha^2 |d_j|^2 \\ \| \\ |c|^2 v_{\alpha j} v_{j\alpha} = |c|^2 v_\alpha v_j \end{array}$$

and so $|c|^2 v_j = v_\alpha |d_j|^2 \equiv 0 \pmod{v_\alpha}$, which shows that the second term is divisible by v_α. As for the third term, because of (2.15) we have $|c|^2 v_{\alpha j} = v_\alpha \bar{c} d_j$. Taking the trace of this, we get $|c|^2 T v_{\alpha j} = v_\alpha T(\bar{c} d_j) \equiv 0 \pmod{v_\alpha}$, which shows that the third term is divisible by v_α. Finally, again by (2.15), we have

$$|c|^2 v_{\alpha i} = v_\alpha \bar{c} d_i \quad \text{and} \quad |c|^2 v_{j\alpha} = v_\alpha c \bar{d}_j\,.$$

---

*) I thank Ming-Guang Leu for his valuable advice on the proof of (2.10).

Multiplying these equalities, we get $|c|^2 v_{\alpha i} v_{j\alpha} = v_\alpha^2 |c|^2 d_i \bar{d}_j$. Taking the trace of the last equality, we have

$$\begin{gathered} |c|^2(v_{\alpha i}v_{j\alpha} + v_{i\alpha}v_{\alpha j}) = v_\alpha^2 T(d_i\bar{d}_j) \\ \| \\ |c|^2(v_\alpha v_{ji} + v_\alpha v_{ij}) . \end{gathered}$$

Hence we have $|c|^2 T v_{ij} = v_\alpha T(d_i \bar{d}_j) \equiv 0 \pmod{v_\alpha}$, which shows that the fourth term is divisible by v_α. The above argument implies that v_α divides $|c|^2 = Nc$ for all $c \in \mathfrak{a}_v$. Now, since $\mathfrak{a}_v$ is the g.c.d. of (c)'s, $c \in \mathfrak{a}_v$, $N\mathfrak{a}_v$ is the g.c.d. of (Nc)'s, $c \in \mathfrak{a}_v$, and so v_α must divide $N\mathfrak{a}_v$. q.e.d.

3. Case $h_K = 1$. From now on, we assume that the class number h_K of the imaginary quadratic field K is one. As is well known, such a field is one of the nine fields $\boldsymbol{Q}(\sqrt{m})$ with $-m = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

As in §2, take a matrix $v = (v_{ij}) \in V_\alpha(\mathfrak{o}_K)$. By (2.10), one can write

$$v = n(v) v^* , \qquad v^* \in V_\alpha^*(\mathfrak{o}_K) . \tag{3.1}$$

Since $h_K = 1$, we have

$$\mathfrak{a}_v = \mathfrak{a}_{V^*} = (a) , \qquad a \in \mathfrak{o}_K . \tag{3.2}$$

From (2.12), it follows that

$$|a|^2 = Na = N\mathfrak{a}_{v^*} = v_\alpha^* . \tag{3.3}$$

Since we have

$$c \in \mathfrak{a}_{v^*} \Leftrightarrow c = ab , \qquad b \in \mathfrak{o}_K ,$$

we obtain the following chain of equivalences:

$$\begin{aligned} c \in S_{\mathfrak{a}_{v^*}}(n(v)v_\alpha^*) &\Leftrightarrow c \in \mathfrak{a}_{v^*} \text{ and } |c|^2 = n(v)v_\alpha^* \\ &\Leftrightarrow b = a^{-1}c \in \mathfrak{o}_K \text{ and } |a|^2|b|^2 = n(v)v_\alpha^* \\ &\Leftrightarrow b \in \mathfrak{o}_K \text{ and } |b|^2 = n(v) \text{ (by (3.3))} \\ &\Leftrightarrow b \in S_{\mathfrak{o}_K}(n(v)) . \end{aligned} \tag{3.4}$$

By (2.6), (2.11), (3.4), we get the equalities of cardinalities:

$$[f_L^{-1}(v)] = [S_{\mathfrak{a}_v}(v_\alpha)] = [S_{\mathfrak{a}_{v^*}}(n(v)v_\alpha^*)] = [S_{\mathfrak{o}_K}(n(v))] . \tag{3.5}$$

For an integer $t \geqq 1$, we denote by $r_K(t)$ the number of $a \in \mathfrak{o}_K$ such that $Na = t$. Hence we have

$$r_K(t) = [S_{\mathfrak{o}_K}(t)] = [\mathfrak{o}_K^\times](1 * \chi_K)(t) \tag{3.6}$$

where χ_K is the Kronecker character belonging to K.

To sum up, we proved the following:

(3.7) THEOREM. *Let K be an imaginary quadratic field of class number one. Let f_L be the map from $L=\mathfrak{o}_K{}^n$ to $(\mathfrak{o}_K)_n$ defined by $f_L(x)={}^t\bar{x}x$. Let $V(\mathfrak{o}_K)$ be the set of all hermitian matrices $v=(v_{ij})\in(\mathfrak{o}_K)_n$ such that $v_i=v_{ii}\geqq 0$, $v_{ik}v_{kj}=v_kv_{ij}$, $1\leqq i,j,k\leqq n$, and let $V_\alpha(\mathfrak{o}_K)$ be the subset of $V(\mathfrak{o}_K)$ consisting of v's such that $v_k=0$, $1\leqq k\leqq\alpha-1$ and $v_\alpha>0$. Then f_L maps L into $V(\mathfrak{o}_K)=\{0\}\cup V_1(\mathfrak{o}_K)\cup\cdots\cup V_n(\mathfrak{o}_K)$, where the latter is the disjoint union of non-empty sets. Furthermore, for each $v\in V_\alpha(\mathfrak{o}_K)$, the cardinality of the fibre $f_L^{-1}(v)$ is equal to $r_K(n(v))$ where $n(v)=$g.c.d.(v_i, Tv_{ij}) and $r_K(t)$ is the number of $a\in\mathfrak{o}_K$ such that $Na=|a|^2=t$.*

4. Use of the series ψ_K. Let K be, as in § 3, an imaginary quadratic field of class number one. Consider the formal power series in variable q:

$$\psi_K(q)=\sum_{c\in\mathfrak{o}_K} q^{|c|^2}. \tag{4.1}$$

Since $|x_i|^2=v_i$ when $f(x)=v$, we have, by (3.7), (2.10),

$$\begin{aligned}\psi_K(q)^n&=\sum_{x\in L} q^{|x_1|^2+\cdots+|x_n|^2}=\sum_{v\in V(\mathfrak{o}_K)}[f_L^{-1}(v)]q^{\operatorname{tr} v}=1+\sum_{\alpha=1}^{n}\sum_{v\in V_\alpha(\mathfrak{o}_K)} r_K(n(v))q^{\operatorname{tr} v}\\&=1+\sum_{\alpha=1}^{n}\sum_{m=1}^{\infty} r_K(m)\sum_{\substack{v\in V_\alpha(\mathfrak{o}_K)\\ n(v)=m}} q^{\operatorname{tr} v}=1+\sum_{\alpha=1}^{n}\sum_{m=1}^{\infty} r_K(m)\sum_{v^*\in V_\alpha^*(\mathfrak{o}_K)} q^{m(\operatorname{tr} v^*)}.\end{aligned} \tag{4.2}$$

Now, for $t\in\boldsymbol{N}$, consider the set

$$V_{\alpha,t}^*(\mathfrak{o}_K)=\{v\in V_\alpha^*(\mathfrak{o}_K);\ \operatorname{tr} v=t\}. \tag{4.3}$$

If we put

$$a_\alpha(t)=[V_{\alpha,t}^*(\mathfrak{o}_K)], \tag{4.4}$$

we get from (4.2) that

$$\psi_K(q)^n=1+\sum_{\alpha=1}^{n}\sum_{m=1}^{\infty} r_K(m)\sum_{t=1}^{\infty} a_\alpha(t)q^{mt}=1+\sum_{\alpha=1}^{n}\sum_{t=1}^{\infty} a_\alpha(t)\sum_{m=1}^{\infty} r_K(m)q^{mt}. \tag{4.5}$$

Since $\psi_K(q)=\sum_{c\in\mathfrak{o}_K} q^{|c|^2}=\sum_{\nu=0}^{\infty} r_K(\nu)q^\nu$, we have, by (4.5),

$$\psi_K(q)^n=\sum_{\nu=0}^{\infty}(\overbrace{r_K\circ\cdots\circ r_K}^{n\text{-times}})(\nu)q^\nu=1+\sum_{\alpha=1}^{n}\sum_{t=1}^{\infty} a_\alpha(t)(\psi_K(q^t)-1). \tag{4.6}$$

If we put

$$a(t)=\sum_{\alpha=1}^{n} a_\alpha(t), \tag{4.7}$$

then, (4.6) implies that

(4.8)
$$\psi_K(q)^n = 1 + \sum_{t=1}^{\infty} a(t)(\psi_K(q^t) - 1)^{\sharp)} .$$

On the other hand, we have

(4.9)
$$\sum_{t=1}^{\infty} a_\alpha(t) \sum_{m=1}^{\infty} r_K(m) q^{mt} = \sum_{v=1}^{\infty} (a_\alpha * r_K)(v) q^v ,$$

and so, by (4.7), (4.8), (4.9), we have

(4.10)
$$\sum_{v=1}^{\infty} \overbrace{(r_K \circ \cdots \circ r_K)}^{n\text{-times}}(v) q^v = \sum_{v=1}^{\infty} (a * r_K)(v) q^v ,$$

where $a(t)$ is the cardinality of the set

$$V_t^*(\mathfrak{o}_K) = \{v \in V(\mathfrak{o}_K);\ n(v) = 1,\ \mathrm{tr}\, v = t\} .$$

To sum up, we have proved the following:

(4.11) THEOREM. *Let K be an imaginary quadratic field of class number one and $V(\mathfrak{o}_K)$ be the set of all hermitian matrices $v = (v_{ij})$ such that $v_i \geqq 0$ and $v_{ik} v_{kj} = v_k v_{ij}$, $1 \leqq i, j, k \leqq n$. Then the cardinality $a(t)$ of the set $V_t^*(\mathfrak{o}_K) = \{v \in V(\mathfrak{o}_K);\ n(v) = 1,\ \mathrm{tr}\, v = t\}$, $t \in \boldsymbol{N}$, satisfies the relation*

(4.12)
$$\overbrace{r_K \circ \cdots \circ r_K}^{n\text{-times}} = a * r_K .$$

5. The cse $K = \boldsymbol{Q}(i)$. In this case, $\mathfrak{o}_K = \boldsymbol{Z}[i]$ and, for $t \in \boldsymbol{N}$, $a(t)$ is the cardinality of hermitian matrices $v = (v_{ij}) \in \boldsymbol{Z}[i]_n$ such that $v_i \geqq 0$, $v_{ik} v_{kj} = v_k v_{ij}$, $n(v) = 1$ and $\mathrm{tr}\, v = t$. Let $q = e^{\pi i \tau}$, $\tau \in \boldsymbol{C}$, $\mathrm{Im}\, \tau > 0$. Then, we have

$$\psi_K(q) = \sum_{c \in \mathfrak{o}_K} q^{|c|^2} = \sum_{(a,b) \in \boldsymbol{Z}^2} q^{a^2 + b^2} = \left(\sum_{a \in \boldsymbol{Z}} q^{a^2} \right)^2 = \vartheta_3{}^2(\tau) \qquad \text{where} \quad \vartheta_3(\tau) = \sum_{a \in \boldsymbol{Z}} q^{a^2} .$$

Therefore (4.8) can be written

(5.1)
$$\vartheta_3{}^{2n}(\tau) = 1 + \sum_{t=1}^{\infty} a(t)(\vartheta_3{}^2(t\tau) - 1)$$

or, by the footnote ♯),

(5.2)
$$\vartheta_3{}^{2n}(\tau) - n\vartheta_3{}^2(\tau) + (n-1) = \sum_{t=2}^{\infty} a(t)(\vartheta_3{}^2(t\tau) - 1) .$$

If, in particular, $n = 2$, then, since g.c.d.$(t, u, 2x) = 1$ if and only if g.c.d.$(x, y, t, u) = 1$ for $(x, y, t, u) \in \boldsymbol{Z}^4$, (5.1) boils down to the formula (0.1) in the introduction.

♯) One verifies easily that $a(1) = n$. Hence (4.8) can also be written as $\psi_K(q)^n - n\psi_K(q) + (n-1) = \sum_{t=2}^{\infty} a(t)(\psi_K(q^t) - 1)$.

6. $\zeta_K(s)$. The field K being as in § 3, we shall consider the subsets $U(\mathfrak{o}_K)$, $U^*(\mathfrak{o}_K)$ of $V(\mathfrak{o}_K)$ defined by

$$U(\mathfrak{o}_K)=\{u\in V(\mathfrak{o}_K);\ u_i\geqq 1,\ 1\leqq i\leqq n\}\,, \tag{6.1}$$

$$U^*(\mathfrak{o}_K)=\{u\in U(\mathfrak{o}_K);\ n(u)=1\}\,. \tag{6.2}$$

Call $b(t)$, $t\in \boldsymbol{N}$, the cardinality of the set

$$U_t^*(\mathfrak{o}_K)=\{u\in U(\mathfrak{o}_K);\ n(v)=1,\ v_1\cdots v_n=t\}\,. \tag{6.3}$$

Consider the Dedekind zeta function $\zeta_K(s)$. Since $h_K=1$, we have

$$[\mathfrak{o}_K^\times]\zeta_K(s)=\sum_{c\neq 0\in\mathfrak{o}_K}\frac{1}{(Nc)^s}=\sum_{v=1}^{\infty}\frac{r_K(v)}{v^s}\,. \tag{6.4}$$

By (3.7), (6.1), (6.2), (6.3), (6.4), we have

$$\begin{aligned}[\mathfrak{o}_K^\times]^n\zeta_K(s)^n&=\sum_{\substack{x\in L\\ \text{all } x_i\neq 0}}\frac{1}{N(x_1\cdots x_n)^s}=\sum_{u\in U(\mathfrak{o}_K)}[f_L^{-1}(u)]\frac{1}{(u_1\cdots u_n)^s}\\ &=\sum_{u\in U(\mathfrak{o}_K)}\frac{r_K(n(v))}{(u_1\cdots u_n)^s}=\sum_{m=1}^{\infty}r_K(m)\sum_{\substack{u\in U(\mathfrak{o}_K)\\ n(u)=m}}\frac{1}{(u_1\cdots u_n)^s}\\ &=\sum_{m=1}^{\infty}\frac{r_K(m)}{m^{ns}}\sum_{t=1}^{\infty}\sum_{u^*\in U_t^*(\mathfrak{o}_K)}\frac{1}{t^s}=\sum_{m=1}^{\infty}\frac{r_K(m)}{m^{ns}}\sum_{t=1}^{\infty}\frac{b(t)}{t^s}=[\mathfrak{o}_K^\times]\zeta_K(ns)\sum_{t=1}^{\infty}\frac{b(t)}{t^s}\,.\end{aligned} \tag{6.5}$$

To sum up, we proved the following:

(6.6) THEOREM. *Let K be an imaginary quadratic field of class number one and $U(\mathfrak{o}_K)$ be the set of all hermitian matrices $u=(u_{ij})\in(\mathfrak{o}_K)_n$ such that $u_i\geqq 1$, $u_{ik}u_{kj}=u_ku_{ij}$, $1\leqq i,j,k\leqq n$, and $b(t)$ be the cardinality of the set*

$$U_t^*(\mathfrak{o}_K)=\{u\in U(\mathfrak{o}_K);\ n(u)=1,\ u_1\cdots u_n=t\}\,,\qquad t\in\boldsymbol{N}\,.$$

Then, we have

$$[\mathfrak{o}_K^\times]^{n-1}\frac{\zeta_K(s)^n}{\zeta_K(ns)}=\sum_{t=1}^{\infty}\frac{b(t)}{t^s}\,. \tag{6.7}$$

If, in particular, $K=\boldsymbol{Q}(i)$ and $n=2$, then (6.7) boils down to the formula (0.2) in the introduction.

DEPARTMENT OF MATHEMATICS
THE JOHNS HOPKINS UNIVERSITY
BALTIMORE, MD 21218
U.S.A.