ON THE EXPRESSION OF A NUMBER AS THE SUM OF TWO SQUARES IN TOTALLY REAL ALGEBRAIC NUMBER FIELDS[1]

WERNER SCHAAL

Introduction. Let K be a totally real algebraic number field of degree n and with discriminant d. Let $\mathfrak{a}$ be an ideal of K which may be integral or fractional. The number of solutions of the equation

$$\xi = \mu^2 + \nu^2 \qquad (\xi \in \mathfrak{a})$$

in numbers $\mu, \nu \in \mathfrak{a}$ is denoted by $f(\xi, \mathfrak{a})$. For $x_1, \cdots, x_n$ being positive real numbers the following theorem will be proved:

THEOREM.

$$\sum_{0<\xi^{(h)}<x_h;\,\mathfrak{a}\mid\xi} f(\xi, \mathfrak{a}) = \frac{\pi^n}{dN\mathfrak{a}^2}(x_1 \cdots x_n) + R(x_1, \cdots, x_n).$$

(*The index h always takes on the values* $1, \cdots, n$ *if not otherwise indicated.*) *For any* $\delta > 0$, $x_1 \cdots x_n \to \infty$, *then*

$$R(x_1, \cdots, x_n) = O((x_1 \cdots x_n)^{n/(n+1)+\delta})$$

holds.

This result has been already proved in [4] for the case $n=2$, $\mathfrak{a}=(1)$. There was also shown that

$$\limsup_{x_1x_2\to\infty} \frac{R(x_1, x_2)}{(x_1x_2)^{1/4}} > 0.$$

For the proof of the theorem an identity given by Siegel in [5] for real quadratic number fields is generalized to totally real algebraic number fields. This identity will be applied to the problem in a similar way as it was done in [4].

1. In what follows the real numbers $c_1, \cdots, c_5$ are constants greater than 1 which only depend on the field K and the ideal $\mathfrak{a}$ if not otherwise indicated. We define $S(\alpha) = \alpha^{(1)} + \cdots + \alpha^{(n)}$, $N(\alpha) = \alpha^{(1)} \cdots \alpha^{(n)}$ for numbers $\alpha \in K$. Let $r = n-1$, and let

Presented to the Society, November 23, 1963, received by the editors January 7, 1964.

[1] Research was partially supported by contract DSR 7700 AF 49-638-42.

[2] We introduce Hecke's characters for a number $\alpha \in K$ with respect to these unit $\eta_1, \cdots, \eta_r$.

$$m = 2\pi i \begin{pmatrix} m_1 \\ \cdot \\ \cdot \\ \cdot \\ m_r \end{pmatrix}$$

where $m_1, \cdots, m_r$ are rational integers.

The set of squares of all units of K forms a group G which may be generated by the r independent units $\eta_1, \cdots, \eta_r$.[2] For this purpose let E be the $r \times n$ matrix $(e_p^{(q)})$, $q = 1, \cdots, r$; $p = 1, \cdots, n$ (see [2]), and let

$$a = \begin{pmatrix} \log |\alpha^{(1)}| \\ \cdot \\ \cdot \\ \cdot \\ \log |\alpha^{(n)}| \end{pmatrix}.$$

Then following Hecke's definition we set

$$\lambda_m(\alpha) = \exp\{m^T E a\}. \tag{1}$$

If $\eta \in G$ it follows from the definition of the numbers $e_p^{(q)}$ that

$$\lambda_m(\alpha\eta) = \lambda_m(\alpha).$$

Two numbers $\alpha, \beta \neq 0$, 0 of K are called "associated" if their quotient is an element of the group G. Otherwise α, β are called "not associated."

LEMMA 1. *If x is a positive real number then*

$$\sum_{N(\xi) \leq x}{}' f(\xi, \mathfrak{a}) = O(x)$$

where the dash at the sign of summation indicates that the sum is to be taken over a set of not associated numbers $\xi \in \mathfrak{a}$.

PROOF. For every number α of K there exists a number c_1 and a unit $\eta \in G$ which only depends on α such that the following n inequalities hold:

$$c_1^{-1} |N(\alpha)|^{1/n} \leq |\alpha^{(h)} \eta^{(h)}| \leq c_1 |N(\alpha)|^{1/n}, \qquad h = 1, \cdots, n,$$

(see [6, Hilfssatz 6]). Because of

$$f(\eta\xi, \mathfrak{a}) = f(\xi, \mathfrak{a}), \qquad \eta \in G \tag{2}$$

we may choose the set of not associated numbers ξ such that the following inequalities are satisfied:

$$c_1^{-1}(N\xi)^{1/n} \leqq \xi^{(h)} \leqq c_1(N\xi)^{1/n}, \qquad h = 1, \cdots, n.$$

Whence we have

$$\sum_{N(\xi)\leq x}' f(\xi, \mathfrak{a}) \leqq \sum_{0<\xi^{(h)}<c_1x^{1/n};\, \mathfrak{a}|\xi} f(\xi, \mathfrak{a}).$$

Since $f(\xi, \mathfrak{a})$ is the number of distinct pairs (μ, ν), $\mu, \nu \in \mathfrak{a}$ with $\xi = \mu^2 + \nu^2$ it is sufficient to estimate the number of elements $\mu \in \mathfrak{a}$ which satisfy the inequalities $|\mu^{(h)}| < c_2 x^{1/2n}$, $h = 1, \cdots, n$. Let $\alpha_1, \cdots, \alpha_n$ be a basis of the ideal $\mathfrak{a}$. We have to estimate the number of distinct n-tuples of rational integers $(k_1, \cdots, k_n)$ for which the inequalities

$$-c_2 x^{1/2n} < \sum_{p=1}^{n} k_p \alpha_p^{(h)} < c_2 x^{1/2n}, \qquad h = 1, \cdots, n$$

hold. Since $|\det(\alpha_p^{(h)})| = N\mathfrak{a}\sqrt{d} \neq 0$ we obtain that there are at most $c_3\sqrt{x}$ of such n-tuples. This proves the lemma.

For each character (1) we define the function

$$\Phi_m(s, \mathfrak{a}) = \sum_{\xi}' \frac{f(\xi, \mathfrak{a})\lambda_m(\xi)}{N(\xi)^s},$$

where by $s = \sigma + it$ a complex variable is denoted. Applying the method of partial summation it is an easy consequence of Lemma 1 that the functions $\Phi_m(s, \mathfrak{a})$ converge absolutely and uniformly for $\sigma > 1$.

Let R be the determinant

$$\begin{vmatrix} 1 & \log \eta_1^{(1)} & \cdots & \log \eta_r^{(1)} \\ \vdots & \vdots & & \vdots \\ 1 & \log \eta_1^{(n)} & \cdots & \log \eta_r^{(n)} \end{vmatrix};$$

moreover, we introduce the abbreviation

$$E_p(m) = 2\pi \sum_{q=1}^{r} m_q e_p^{(q)}, \qquad p = 1, \cdots, n.$$

Then the following lemma holds:

LEMMA 2. *Let $x_1, \cdots, x_n$ be positive real numbers and let*

$$g(x_1, \cdots, x_n) = \sum_{0<\xi^{(h)}x_h<1;\, \mathfrak{a}|\xi} f(\xi, \mathfrak{a}) \prod_{p=1}^{n} (1 - \xi^{(p)}x_p).$$

Then we have for $\sigma > 1$:

$$g(x_1, \cdots x_n) = \frac{n}{2\pi i |R|} \sum_{m_1, \cdots, m_r; =-\infty}^{+\infty} \int_{\sigma-i\infty}^{\sigma+i\infty} \Phi_m(s, \mathfrak{a})$$

$$\cdot \prod_{p=1}^{n} \frac{x_p^{-s+iE_p(m)}}{(s - iE_p(m))(s + 1 - iE_p(m))} ds.$$

PROOF. The proof of the given identity proceeds on the same lines as the proof in the case $n=2$ given in [5]. We define the column vectors

$$k = \begin{pmatrix} k_1 \\ \cdot \\ \cdot \\ \cdot \\ k_r \end{pmatrix}, \quad v = \begin{pmatrix} v_1 \\ \cdot \\ \cdot \\ \cdot \\ v_r \end{pmatrix}, \quad y^{(p)} = \begin{pmatrix} \log \eta_1^{(p)} \\ \cdot \\ \cdot \\ \cdot \\ \log \eta_r^{(p)} \end{pmatrix} \qquad (p = 1, \cdots, n),$$

where $k_1, \cdots, k_r$ are rational integers and $v_1, \cdots, v_r$ are real variables. Making the substitution

$$x_p = u \exp\{v^T y^{(p)}\}, \qquad p = 1, \cdots, n \tag{3}$$

we observe that the function $g(x_1, \cdots, x_n)$ becomes a periodic function with respect to $v_1, \cdots, v_r$ because of property (2). The period is 1 with respect to each of the variables. Furthermore, $g(x_1, \cdots, x_n)$ is a continuous function and has piecewise continuous partial derivatives with respect to $v_1, \cdots, v_r$. Whence $g(x_1, \cdots, x_n)$ furnishes an absolutely convergent Fourier series. Denoting the right-hand side of (3) by $t^{(p)}(v)$ its coefficient is given by:

$$a_m(u) = \int_0^1 \cdots \int_0^1 \exp\{-v^T m\} \sum_{0<\xi^{(h)}t^{(h)}(v)<1;\, \mathfrak{a}|\xi} f(\xi, \mathfrak{a})$$

$$\cdot \prod_{p=1}^{n} (1 - \xi^{(p)} t^{(p)}(v)) dv_1 \cdots dv_r$$

$$= \int_0^1 \cdots \int_0^1 \exp\{-v^T m\} \sum_{0<N(\xi)<u^{-n}}' f(\xi, \mathfrak{a})$$

$$\cdot \sum_{k_1, \cdots, k_r=-\infty}^{\infty} \sum_{0<\xi^{(h)}t^{(h)}(v+k)<1} \prod_{p=1}^{n} (1 - \xi^{(p)} t^{(p)}(v+k)) dv_1 \cdots dv_r$$

$$= \int_0^1 \cdots \int_0^1 \exp\{-v^T m\} \sum_{k_1, \cdots, k_r=-\infty}^{\infty} \sum_{0<N(\xi)<u^{-n}}' f(\xi, \mathfrak{a})$$

$$\cdot \sum_{0<\xi^{(h)}t^{(h)}(v+k)<1} \prod_{p=1}^{n} (\cdots) dv_1 \cdots dv_r.$$

We are allowed to interchange the integration and the summation with respect to $k_1, \cdots, k_r$ because the sum is finite. Making the change of variables $v_q+k_q \to v_q$, $q=1, \cdots, r$, we obtain:

$$a_m(u) = \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} \exp\{-v^T m\} \sum_{0<\xi^{(h)}t^{(h)}(v)<1}' f(\xi, \mathfrak{a}) \cdot \prod_{p=1}^{n} (1 - \xi^{(p)}t^{(p)}(v))dv_1 \cdots dv_r.$$

Now we form the integral $\int_0^\infty u^{ns-1}a_m(u)du$ for $\sigma>1$. Making the change of variables (3) we get:

$$\begin{aligned}\int_0^\infty & u^{ns-1}a_m(u)du \\ &= \frac{1}{|R|}\int_0^\infty \cdots \int_0^\infty \prod_{p=1}^{n} x_p^{s-1-iE_p(m)} \sum_{0<\xi^{(h)}x_h<1}' f(\xi, \mathfrak{a}) \cdot \prod_{p=1}^{n} (1 - \xi^{(p)}x_p)dx_1 \cdots dx_n \\ &= \frac{1}{|R|} \sum_{\xi}' f(\xi, \mathfrak{a}) \prod_{p=1}^{n} \int_0^{(\xi^{(p)})^{-1}} x_p^{s-1-iE_p(m)}(1 - \xi^{(p)}x_p)dx_p \\ &= \frac{1}{|R|} \Phi_m(s, \mathfrak{a}) \prod_{p=1}^{n} [(s - iE_p(m))(s + 1 - iE_p(m))]^{-1}.\end{aligned}$$

The application of Mellin's inversion formula yields for $\sigma>1$:

$$a_m(u) = \frac{n}{2\pi i|R|}\int_{\sigma-i\infty}^{\sigma+i\infty} u^{-ns}\Phi_m(s, \mathfrak{a}) \prod_{p=1}^{n} [(s-iE_p(m))(s+1-iE_p(m))]^{-1}ds.$$

Since

$$g(x_1, \cdots, x_n) = \sum_{m_1, \cdots, m_r=-\infty}^{\infty} a_m(u) \exp\{v^T m\},$$

this proves the lemma.

Let

$$F(v_1, \cdots, v_n) = \sum_{0<\xi^{(h)}<v_h} f(\xi, \mathfrak{a}).$$

Then we have

$$(x_1 \cdots x_n) g\left(\frac{1}{x_1}, \cdots, \frac{1}{x_n}\right)$$

$$= \sum_{0<\xi^{(h)}<x_h;\, \mathfrak{a}|\xi} f(\xi, \mathfrak{a}) \prod_{p=1}^{n} (x_p - \xi^{(p)})$$

$$= \sum_{0<\xi^{(h)}<x_h;\, \mathfrak{a}|\xi} \int_{\xi^{(1)}}^{x_1} \cdots \int_{\xi^n}^{x_n} f(\xi, \mathfrak{a}) dv_1 \cdots dv_n$$

$$= \int_0^{x_1} \cdots \int_0^{x_n} F(v_1, \cdots, v_n) dv_1 \cdots dv_n.$$

An elementary calculation furnishes the result:

$$\int_0^{y_1} \cdots \int_0^{y_n} F(x_1 + v_1, \cdots, x_n + v_n) dv_1 \cdots dv_n$$

$$= \frac{n}{2\pi i \,|\, R\,|} \sum_{m_1, \cdots, m_r = -\infty}^{+\infty} \int_{\sigma - i\infty;\, \sigma > 1}^{\sigma + i\infty} \tag{4}$$

$$\cdot \prod_{p=1}^{n} \frac{(y_p + x_p)^{s+1-iE_p(m)} - x_p^{s+1-iE_p(m)}}{(s - iE_p(m))(s + 1 - iE_p(m))} \Phi_m(s, \mathfrak{a}) ds.$$

2. The left-hand side of (4) may be abbreviated by J. Since $f(\xi, \mathfrak{a}) \geqq 0$ we obtain the inequality:

$$F(x_1, \cdots, x_n) \leqq (y_1 \cdots y_n)^{-1} J \leqq F(x_1 + y_1, \cdots, x_n + y_n).$$

We observe from this inequality that the asymptotic behaviours of $F(x_1, \cdots, x_n)$ and $(y_1 \cdots y_n)^{-1} J$ are the same. Therefore we shall try to find an approximation of J. For this purpose the functions $\Phi_m(s, \mathfrak{a})$ are analytically continued over the whole s-plane. Let:

$$\Theta(z_1, \cdots, z_n; \mathfrak{a}) = \sum_{\mathfrak{a}|\mu} \exp\left\{-\frac{\pi}{\sqrt[n]{(dN\mathfrak{a}^2)}} \sum_{p=1}^{n} \mu^{(p)2} z_p\right\},$$

$z_1, \cdots, z_n$ being complex variables with $\operatorname{Re} z_h > 0$, $h = 1, \cdots, n$; then Hecke proved in [3]:

$$\Theta(z_1, \cdots, z_n; \mathfrak{a}) = (z_1 \cdots z_n)^{-1/2} \Theta\left(\frac{1}{z_1}, \cdots, \frac{1}{z_n}; \frac{1}{\mathfrak{a}\mathfrak{d}}\right), \tag{5}$$

where $\mathfrak{d}$ is the ramification ideal of the field K. Well known calculations and the application of (5) lead to the equation:

$$\left(\frac{dN\mathfrak{a}^2}{\pi^n}\right)^s \frac{1}{|R|} \Phi_m(s, \mathfrak{a}) \prod_{p=1}^{n} \Gamma(s - iE_p(m))$$

$$= \frac{b_m}{s(s-1)} + \int_{u=1}^{u=\infty} \int_{-1/2}^{1/2} \cdots \int_{-1/2}^{1/2} [\Theta^2(u\eta_1^{(1)v_1} \cdots \eta_r^{(1)v_r}, \cdots,$$

(6)
$$\cdot u\eta_1^{(n)v_1} \cdots \eta_r^{(n)v_r}; \mathfrak{a}) - 1]u^{ns} \exp\{-v^T m\} dv_1 \cdots dv_r \frac{du}{u}$$

$$+ \int_{u=1}^{u=\infty} \int_{-1/2}^{1/2} \cdots \int_{-1/2}^{1/2} \left[\Theta^2\left(u\eta_1^{(1)v_1} \cdots \eta_r^{(1)v_r}, \cdots,\right.\right.$$

$$\left.\left. u\eta_1^{(n)v_1} \cdots \eta_r^{(n)v_r}; \frac{1}{\mathfrak{a}\mathfrak{d}}\right) - 1\right] u^{n(1-s)} \exp\{v^T m\} dv_1 \cdots dv_r \frac{du}{u}$$

with

$$b_m = \begin{cases} 1/n & \text{if } m_1 = \cdots = m_r = 0, \\ 0 & \text{otherwise.} \end{cases}$$

If $m_1^2 + \cdots + m_r^2 > 0$ the right-hand side of (6) is an integral function of s; if $m_1 = \cdots = m_r = 0$ there are two simple poles at $s = 0$ and $s = 1$. So we recognize that $\Phi_m(s, \mathfrak{a})$ is an integral function of s except in the case $m_1 = \cdots = m_r = 0$; $\Phi_0(s, \mathfrak{a})$ has a simple pole at $s = 1$. Another immediate consequence of equation (6) is the functional equation

(7) $$\Phi_m(s, \mathfrak{a}) = \left(\frac{dN\mathfrak{a}^2}{\pi^n}\right)^{1-2s} \prod_{p=1}^{n} \frac{\Gamma(1 - s + iE_p(m))}{\Gamma(s - iE_p(m))} \Phi_{-m}\left(1 - s, \frac{1}{\mathfrak{a}\mathfrak{d}}\right),$$

which holds for all $m_1, \cdots, m_r$.

By equations (6) and (7) we can estimate the functions $\Phi_m(s, \mathfrak{a})$ uniformly in $m_1, \cdots, m_r$ in the infinite strip $-\epsilon \leqq \sigma \leqq 1 + \epsilon$, $\epsilon > 0$. If we apply Phragmén-Lindelöf's extension of the maximum-modulus theorem to the functions $\Phi_m(s, \mathfrak{a})$ we obtain the inequalities:

(8)
$$|\Phi_m(\sigma + it, \mathfrak{a})| \leqq c_4(\epsilon) \prod_{p=1}^{n} (1 + |t - E_p(m)|)^{1-\sigma+\epsilon},$$
$$-\epsilon \leqq \sigma \leqq 1 + \epsilon, m_1^2 + \cdots + m_r^2 > 0.$$

Inequality (8) also holds for $\Phi_0(s, \mathfrak{a})$ if $|t| \geqq c_5$. (The calculations which lead to (8) are given very explicitly for a similar case in [1].)

3. Now it is easy to investigate the asymptotic behaviour of the right-hand side of (4) for $(x_1 \cdots x_n) \to \infty$. The path of integration in (4) is replaced by a straight line in the critical strip whose point of

intersection with the real axis may be $\sigma=\delta$, $0<\delta<1$. Considering the pole of $\Phi_0(s, \mathfrak{a})$ at $s=1$ we find:

$$
\begin{aligned}
J = {} & \frac{1}{2^n}\frac{\pi^n}{dN\mathfrak{a}^2}\prod_{p=1}^{n}\left[(y_p+x_p)^2-x_p^2\right] \\
(9) \qquad & + \frac{n}{2\pi i\,|R|}\sum_{m_1,\cdots,m_r=-\infty}^{+\infty}\int_{\delta-i\infty}^{\delta+i\infty}\Phi_m(s,\mathfrak{a}) \\
& \cdot\prod_{p=1}^{n}\frac{(y_p+x_p)^{s+1-iE_p(m)}-x_p^{s+1-iE_p(m)}}{(s-iE_p(m))(s+1-iE_p(m))}\,ds, \\
& s=\delta+it,\ 0<\delta<1.
\end{aligned}
$$

The infinite sum in (9) can be easily estimated if one considers that the following determinant does not vanish for $1\leqq k\leqq n$:

$$
\begin{vmatrix}
e_k^{(1)}-e_1^{(1)} & \cdots & e_k^{(1)}-e_{k-1}^{(1)} & e_k^{(1)}-e_{k+1}^{(1)} & \cdots & e_k^{(1)}-e_n^{(1)} \\
\vdots & & \vdots & \vdots & & \vdots \\
e_k^{(r)}-e_1^{(r)} & \cdots & e_k^{(r)}-e_{k-1}^{(r)} & e_k^{(r)}-e_{k+1}^{(r)} & \cdots & e_k^{(r)}-e_n^{(r)}
\end{vmatrix}.
$$

Then we obtain from (9)

$$
(10)\quad J=\frac{1}{2^n}\frac{\pi^n}{dN\mathfrak{a}^2}\prod_{p=1}^{n}\left[(y_p+x_p)^2-x_p^2\right]+O\left(\prod_{p=1}^{n}(y_p+x_p)^{\delta+1}\right).
$$

If we choose

$$
y_p=x_p(x_1\cdots x_n)^{-1/(n+1)},\qquad p=1,\cdots,n
$$

and divide J by the product $y_1\cdots y_n$ equation (10) yields for $x_1\cdots x_n\to\infty$ and any $\delta>0$

$$
(11)\quad \frac{J}{y_1\cdots y_n}=\left(\frac{\pi^n}{dN\mathfrak{a}^2}\right)(x_1\cdots x_n)+O((x_1\cdots x_n)^{n/(n+1)+\delta}).
$$

Recalling the remark in the beginning of §2 we observe that (11) also gives the asymptotic behaviour of $F(x_1,\cdots,x_n)$ for $x_1\cdots x_n\to\infty$ and any $\delta>0$:

$$
F(x_1,\cdots,x_n)=\left(\frac{\pi^n}{dN\mathfrak{a}^2}\right)(x_1\cdots x_n)+O((x_1\cdots x_n)^{n/(n+1)+\delta}).
$$

This proves the theorem formulated in the introduction.

References

1. Heinrich Behnke, *Analytische Funktionen und algebraische Zahlen*, Abh. Math. Sem. Univ. Hamburg, **2** (1923), 81–111.

2. E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen*, Math. Z., **1** (1918), 357–376.

3. ———, *Über die Zetafunktionen beliebiger algebraischer Zahlkörper*, Nachr. König. Ges. Wiss. Göttingen Math.-Phys. Kl. (1917), 77–89.

4. W. Schaal, *Übertragung des Kreisproblems auf reell-quadratische Zahlkörper*, Math. Ann., **145** (1962), 273–284.

5. C. L. Siegel, *Mittelwerte arithmetischer Funktionen in Zahlkörpern*, Trans. Amer. Math. Soc. **39** (1936), 219–224.

6. ———, *Additive Theorie der Zahlkörper*. II, Math. Ann. **88** (1923), 184–210.

Massachusetts Institute of Technology