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

WERNER SCHAAL

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

$$\xi = \mu^2 + \nu^2 \quad (\xi \in a)$$

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

**Theorem.**

$$\sum_{0 < \xi < \delta \leq a} f(\xi, a) = \frac{n^n}{dN^2} (x_1 \cdots x_n) + R(x_1, \ldots, x_n).$$

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

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

holds.

This result has been already proved in [4] for the case $n = 2$, $a = (1)$. 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 $c_1, \ldots, c_8$ are constants greater than 1 which only depend on the field $K$ and the ideal $a$ 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

---

1 Research was partially supported by contract DSR 7700 AF 49-638-42.
2 We introduce Hecke's characters for a number $a \in K$ with respect to these unit $\eta_1, \ldots, \eta_r$.
\[ m = 2\pi i \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} \]

where \( m_1, \ldots, m_r \) 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 \( \eta_1, \ldots, \eta_r \). For this purpose let \( E \) be the \( r \times n \) matrix \((a_p^q)\), \( q = 1, \ldots, r; p = 1, \ldots, n \) (see [2]), and let

\[
a = \begin{pmatrix} \log |a^{(1)}| \\ \vdots \\ \log |a^{(n)}| \end{pmatrix}.
\]

Then following Hecke's definition we set

\[(1) \quad \lambda_m(a) = \exp \{ mT Ea \}.\]

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 \( \alpha, \beta \) are called "not associated."

**Lemma 1.** If \( x \) is a positive real number then

\[ \sum' f(\xi, a) = O(x) \]

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

**Proof.** For every number \( \alpha \) of \( K \) there exists a number \( c_1 \) and a unit \( \eta \in G \) which only depends on \( \alpha \) such that the following \( n \) inequalities hold:

\[ c_1^{-1} | N(\alpha) |^{1/n} \leq | (\alpha^{(h)} \eta) |^{(h)} \leq c_1 | N(\alpha) |^{1/n}, \quad h = 1, \ldots, n, \]

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

\[(2) \quad f(\eta \xi, a) = f(\xi, a), \quad \eta \in G \]

we may choose the set of not associated numbers \( \xi \) such that the following inequalities are satisfied:
1965

A NUMBER AS THE SUM OF TWO SQUARES

\[ c_1 (N \xi)^{1/n} \leq \xi^{(h)} \leq c_1 (N \xi)^{1/n}, \quad h = 1, \ldots, n. \]

Whence we have

\[ \sum' f(\xi, a) \leq \sum_{0 < \xi^{(h)} < c_2 x^{1/2n}; a | \xi} f(\xi, a). \]

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

\[ -c_2 x^{1/2n} < \sum_{p=1}^n k_p \alpha_p^{(h)} < c_2 x^{1/2n}, \quad h = 1, \ldots, n \]

hold. Since \( |\det(\alpha_p^{(h)})| = N\alpha \sqrt{d} \neq 0 \) 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

\[ \Phi_m(s, a) = \sum \frac{f(\xi, a)\lambda_m(\xi)}{N(\xi)^s}, \]

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 \( \Phi_m(s, a) \) converge absolutely and uniformly for \( \sigma > 1 \).

Let \( R \) be the determinant

\[ \begin{vmatrix}
1 & \log \eta_1^{(1)} & \cdots & \log \eta_r^{(1)} \\
& \ddots & \ddots & \ddots \\
& & 1 & \log \eta_1^{(n)} \\
& & & \ddots & \log \eta_r^{(n)}
\end{vmatrix} ; \]

moreover, we introduce the abbreviation

\[ E_p(m) = 2\pi \sum_{q=1}^r m_q c_p^{(q)}, \quad p = 1, \ldots, n. \]

Then the following lemma holds:

**Lemma 2.** Let \( x_1, \ldots, x_n \) be positive real numbers and let

\[ g(x_1, \ldots, x_n) = \sum_{0 < \xi^{(h)} x_1 < 1; a | \xi} f(\xi, a) \prod_{p=1}^n (1 - \xi^{(h)p} x_p). \]

Then we have for \( \sigma > 1 \):
g(x_1, \ldots, x_n) = \frac{n}{2\pi i} \lim_{m_i \to \pm\infty} \int_{x_i - i\infty}^{x_i + i\infty} \Phi_m(s, a) \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

\[
k = \begin{pmatrix} k_1 \\ \vdots \\ k_r \end{pmatrix}, \quad \phi = \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_r \end{pmatrix}, \quad \eta^{(p)} = \begin{pmatrix} \log \eta_1^{(p)} \\ \vdots \\ \log \eta_r^{(p)} \end{pmatrix} \quad (p = 1, \ldots, n),
\]

where \( k_1, \ldots, k_r \) are rational integers and \( \phi_1, \ldots, \phi_r \) are real variables. Making the substitution

\[
x_p = u \exp\{v^T \phi^{(p)}\}, \quad p = 1, \ldots, n
\]

we observe that the function \( g(x_1, \ldots, x_n) \) becomes a periodic function with respect to \( \phi_1, \ldots, \phi_r \) because of property (2). The period is 1 with respect to each of the variables. Furthermore, \( g(x_1, \ldots, x_n) \) is a continuous function and has piecewise continuous partial derivatives with respect to \( \phi_1, \ldots, \phi_r \). Whence \( g(x_1, \ldots, x_n) \) furnishes an absolutely convergent Fourier series. Denoting the right-hand side of (3) by \( t^{(p)}(u) \) its coefficient is given by:

\[
a_m(u) = \int_0^1 \cdots \int_0^1 \exp\{-v^T m\} \sum_{0 < \xi(t) \eta(t) \in a_1} f(\xi, a) \prod_{p=1}^n (1 - \xi^{(p)} \eta^{(p)}(u)) dv_1 \cdots dv_r
\]

\[
= \int_0^1 \cdots \int_0^1 \exp\{-v^T m\} \sum_{0 < N(\xi) < u - n} f(\xi, a) \prod_{p=1}^n (1 - \xi^{(p)} \eta^{(p)}(u + k)) dv_1 \cdots dv_r
\]

\[
= \int_0^1 \cdots \int_0^1 \exp\{-v^T m\} \sum_{k_1, \ldots, k_r = -\infty}^{\infty} \sum_{0 < N(\xi) < u - n} f(\xi, a) \prod_{p=1}^n (\cdots) dv_1 \cdots dv_r.
\]
We are allowed to interchange the integration and the summation with respect to \( k_1, \ldots, k_r \) because the sum is finite. Making the change of variables \( v_q + k_q \rightarrow v_q, \ q = 1, \ldots, r, \) we obtain:

\[
a_m(u) = \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} \exp\left\{-v^Tm\right\} \sum'_{0 < l^{(b)}(x^{(a)}) < 1} f(\xi, a) \cdot \prod_{p=1}^{n} (1 - \xi^{(p)}(v)) dv_1 \cdots dv_r.
\]

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

\[
\int_0^\infty u^{n-1} a_m(u) du = \frac{1}{|R|} \int_0^\infty \cdots \int_0^\infty \prod_{p=1}^{n} x_p^{s-1-E_p(m)} \sum'_{0 < l^{(b)}(x^{(a)}) < 1} f(\xi, a) \cdot \prod_{p=1}^{n} (1 - \xi^{(p)}(x)) dx_1 \cdots dx_n
\]

\[
= \frac{1}{|R|} \sum'_{i} f(\xi, a) \prod_{p=1}^{n} \int_0^{(\xi^{(p)})^{-1}} x_p^{s-1-E_p(m)} (1 - \xi^{(p)}(x)) dx_p
\]

\[
= \frac{1}{|R|} \Phi_m(s, a) \prod_{p=1}^{n} [(s - iE_p(m))(s + 1 - iE_p(m))]^{-1}.
\]

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

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

Since

\[
g(x_1, \ldots, x_n) = \sum_{m_1, \ldots, m_n = -\infty}^{\infty} a_m(u) \exp\{v^Tm\},
\]

this proves the lemma.

Let

\[
F(v_1, \ldots, v_n) = \sum_{0 < l^{(b)}(x^{(a)}) < 1} f(\xi, a).
\]

Then we have
\[(x_1 \cdots x_n)g\left(\frac{1}{x_1}, \cdots, \frac{1}{x_n}\right)\]
\[= \sum_{0<\xi^{(1)}<\xi^{(2)}<\xi} f(\xi, a) \prod_{p=1}^{n} (x_p - \xi^{(p)})\]
\[= \sum_{0<\xi^{(1)}<\xi^{(2)}<\xi} \int_{\xi^{(1)}}^{\xi} \cdots \int_{\xi^{(n)}}^{\xi} f(\xi, a) dv_1 \cdots dv_n\]
\[= \int_{0}^{\xi} \cdots \int_{0}^{\xi} F(v_1, \cdots, v_n) dv_1 \cdots dv_n.\]

An elementary calculation furnishes the result:
\[
\int_{0}^{\xi_1} \cdots \int_{0}^{\xi_n} F(x_1 + v_1, \cdots, x_n + v_n) dv_1 \cdots dv_n
\]
\[= \frac{n}{2\pi i} \left| R \right| \sum_{m_1, \cdots, m_r = -\infty}^{\infty} \int_{\sigma - i\infty}^{\sigma + i\infty}
\cdot \prod_{p=1}^{n} \frac{(y_p + x_p)^{s+1-iE_p(m)} - x_p^{s+1-iE_p(m)}}{(s - iE_p(m))(s + 1 - iE_p(m))} \Phi_m(s, a) ds.\]

2. The left-hand side of (4) may be abbreviated by \(J\). Since \(f(\xi, a) \geq 0\) we obtain the inequality:
\[F(x_1, \cdots, x_n) \leq (y_1 \cdots y_n)^{-1}J \leq F(x_1 + y_1, \cdots, x_n + y_n).\]

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 \(\Phi_m(s, a)\) are analytically continued over the whole \(s\)-plane. Let:
\[\Theta(z_1, \cdots, z_n; a) = \sum_{a|\mu} \exp \left\{ -\frac{\pi}{\bar{\nu}(dN a^2)} \sum_{p=1}^{n} \mu^{(p)} z_p \right\},\]
\[z_1, \cdots, z_n\] being complex variables with \(\text{Re } z_h > 0, h = 1, \cdots, n;\) then Hecke proved in [3]:
\[\Theta(z_1, \cdots, z_n; a) = (z_1 \cdots z_n)^{-1/2} \Theta\left(\frac{1}{z_1}, \cdots, \frac{1}{z_n}; \frac{1}{ab}\right),\]
where \(b\) is the ramification ideal of the field \(K\). Well known calculations and the application of (5) lead to the equation:
(\frac{dN\alpha^2}{\pi^n})^s \frac{1}{|R|} \Phi_m(s, 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} \left[ \Theta^2(w_{\eta_1}^{(1)} \cdots w_{\eta_r}^{(1)}), \cdots, \right]

\cdot \frac{1}{u^{1/2}} u^{(1-\varepsilon)} u^{n-1} \exp\{\mu r m\} dv_1 \cdots dv_r \frac{du}{u}

\text{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 \( \Phi_m(s, a) \) is an integral function of \( s \) except in the case \( m_1 = \cdots = m_r = 0; \Phi_0(s, a) \) has a simple pole at \( s = 1 \). Another immediate consequence of equation (6) is the functional equation

(7) \Phi_m(s, a) = (\frac{dN\alpha^2}{\pi^n})^{1-2s} \prod_{p=1}^{n} \frac{\Gamma(1 - s + iE_p(m))}{\Gamma(s - iE_p(m))} \Phi_{m_1} \left( 1 - \frac{1}{ab} \right),

which holds for all \( m_1, \cdots, m_r \).

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

(8) \left| \Phi_m(\sigma + it, a) \right| \leq c_4(\varepsilon) \prod_{p=1}^{n} (1 + |t - E_p(m)|)^{1-\sigma+\varepsilon},

\quad -\varepsilon \leq \sigma \leq 1 + \varepsilon, \quad m_1^2 + \cdots + m_r^2 > 0.

Inequality (8) also holds for \( \Phi_0(s, a) \) if \( |t| \geq c_6 \). (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 \( (x_1, \cdots, x_n) \rightarrow \infty \). 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 $\Phi_v(s, a)$ at $s = 1$ we find:

$$J = \frac{1}{2^n} \frac{\pi^n}{dNa^2} \prod_{p=1}^{n} [(y_p + x_p)^2 - x_p^2]$$

$$+ \frac{n}{2\pi i} \sum_{m_1, \ldots, m_n = -\infty}^{+\infty} \int_{e-i\infty}^{e+i\infty} \Phi_v(s, a)$$

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

$$s = \delta + it, \ 0 < \delta < 1.$$  

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

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

Then we obtain from (9)

$$J = \frac{1}{2^n} \frac{\pi^n}{dNa^2} \prod_{p=1}^{n} [(y_p + x_p)^2 - x_p^2] + O\left(\prod_{p=1}^{n} (y_p + x_p)^{s+1}\right).$$

If we choose

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

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

$$J = \left(\frac{\pi^n}{dNa^2}\right) (x_1 \cdots x_n) + O((x_1 \cdots x_n)^{n/(n+1)+\delta}).$$

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 $\delta > 0$:

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

This proves the theorem formulated in the introduction.
REFERENCES


Massachusetts Institute of Technology