On the Poincaré series for diagonal forms over algebraic number fields

by

JUN WANG (Dalian)

1. Introduction. Let $p$ be a fixed prime and $f(x_1, \ldots, x_s)$ a polynomial with coefficients in $\mathbb{Z}_p$, the $p$-adic integers. Let $c_n$ denote the number of solutions of $f = 0$ over the ring $\mathbb{Z}/p^n\mathbb{Z}$, with $c_0 = 1$. Then the Poincaré series $P_f(t)$ is the generating function

$$P_f(t) = \sum_{n=0}^{\infty} c_n t^n.$$

This series was introduced by Borevich and Shafarevich [1, p. 47], who conjectured that $P_f(t)$ is a rational function of $t$ for all polynomials. This was proved by Igusa in 1975 in a more general setting, by using a mixture of analytic and algebraic methods [5, 6]. Since the proof is nonconstructive, deriving explicit formulas for $P_f(t)$ is an interesting problem. In this direction Goldman [2, 3] treated strongly nondegenerate forms and algebraic curves all of whose singularities are “locally” of the form $\alpha x^a = \beta y^b$, while polynomials of form $\sum x_i^{d_i}$ with $p \nmid d_i$ were investigated earlier by E. Steven-son [7], using Jacobi sums. In [8] explicit formulas for $P_f(t)$ were derived for diagonal forms. This paper generalizes the results of [8] to algebraic number fields.

Let $F$ be a finite extension of the rational field, and $P$ a prime ideal of $F$ with norm $N(P) = q$ which is a rational prime power. Using the previous notations, we let $c_n$ denote the number of solutions of the congruence

$$a_1 x_1^{d_1} + \ldots + a_s x_s^{d_s} \equiv 0 \pmod{P^n},$$

where $d_1, \ldots, d_s$ are positive integers, $a_1, \ldots, a_s$ are integers of $F$ prime to $P$, and write $P(t) = \sum_{n=0}^{\infty} c_n t^n$.

It is clear that $c_n = q^{n(s-1)}$ if $d_i = 1$, for some $i, 1 \leq i \leq s$. Therefore we assume that $d_1, \ldots, d_s$ are all integers greater than 1.

Research supported by the National Natural Science Foundation of China.
Throughout this paper, we set \( d = \text{lcm}\{d_1, \ldots, d_s\} \), \( f_i = d/d_i, r = f_1 + \ldots + f_s \) and \( c_n = q^{-n(s-1)}c_n \).

2. Exponential sums. For the prime ideal \( P \) of \( F \), choose an ideal \( C \) of \( F \) such that \( (P, C) = 1 \) and \( PC = (\theta) \) is principal. Then we may assume that any integer \( u \) in \( F \) is of the form 
\[ u = \theta^j \xi \quad (j \geq 0, \ (\xi, P) = 1). \]

In this case we write \( \text{ord}_P u = j \). Let \( D \) represent the different of \( F \) (see [4, Ch. 36]), and choose \( B, (B, P) = 1 \) such that \( (\zeta) = B/P^m D \) is principal.

We set \( \zeta_m = \zeta\theta^{n-m}, 0 \leq m \leq n \), such that \( \zeta = \zeta_n \), and define further 
\[ e_m(u) = e^{2\pi i \text{tr}(u\zeta_m)}, \]
where the symbol \( \text{tr}(\gamma) \) denotes the trace in \( F \). The function \( e_m(u) \) defines an additive character (mod \( P^m \)) and has the following simple properties:
\[ e_0(u) = 1, \quad e_m(u) = e_m(u') \quad \text{if} \ u \equiv u' \pmod{P^m}, \]
\[ e_m(u^j) = e_{m-j}(u) \quad (0 \leq j \leq m), \]
\[ \sum_{z \pmod{P^m}} e_m(uz) = \begin{cases} q^m & \text{if} \ u \equiv 0 \pmod{P^m}, \\ 0 & \text{otherwise}. \end{cases} \]

For \( k \geq 1 \), we define
\[ S_m(u, k) = \sum_{z \pmod{P^m}} e_m(uz^k), \quad S_0(u, k) = 1. \]

It is clear that if \( m \geq j \geq 0 \), then
\[ S_m(u^j, k) = q^j S_{m-j}(u, k). \]

The following lemmas are useful in the proof of the main theorem.

**Lemma 1.** For any positive integer \( k \), there is an integer \( a \geq k \) such that whenever \( m \geq a \), then
\[ S_m(u, k) = q^{k-1}S_{m-k}(u, k), \quad (u, P) = 1. \]

**Proof.** Suppose \( \text{ord}_P k = l \). Then take \( a \) to be a positive integer which is greater than \( k \) and all of \( i(l+1)/(i-1), i = 2, \ldots, k \). Thus, when \( m \geq a \) we have
\[ i(m - 1) \geq m, \quad i = 2, \ldots, k. \]

From this it follows that \( m \geq l + 1 \) and
\[ \{z \pmod{P^m}\} = \{y + x\theta^{m-l-1} | y \pmod{P^{m-l-1}}, x \pmod{P^{l+1}}\}. \]

Using the binomial theorem and (7) we have
\[ (y + x\theta^{m-l-1})^k \equiv y^k + ky^{k-1}x\theta^{m-l-1} \pmod{P^m}, \]
and
\[ S_m(u, k) = \sum_{y \text{ (mod } P^{m-1-1})} e_m(uy^k) \sum_{x \text{ (mod } P^{l+1})} e_{l+1}(uky^{-1}x). \]

Since \( \text{ord} Pk = l \), by (4), the inner sum is 0 unless \( y \equiv 0 \) (mod \( P \)), in which case it has the value \( q^{l+1} \). Hence we have, by setting \( y = y_1 \theta \),
\[ S_m(u, k) = q^{l+1} \sum_{y_1 \text{ (mod } P^{m-1-2})} e_{m-k}(uy_1^k) = q^{k-1}S_{m-k}(u, k). \]

Let \( a(k) \) be the least positive integer such that (6) holds when \( m \geq a(k) \), and write
\[ \varrho = \max\{a(d_1), \ldots, a(d_s)\}. \]

**Lemma 2.** Put \( T_m = q^{-ms} \sum_{(v, P^m) = 1} S_m(va_1, d_1) \ldots S_m(va_s, d_s) \). Then \( T_{d+j} = q^{d-r}T_j \) for \( j \geq \varrho - 1 \).

**Proof.** Since \( j \geq \varrho - 1 \) and \( d_i \geq 2 \), we have \( d_i + j \geq a(d_i) \). By Lemma 1 one gets
\[ S_{d+j}(u, d_i) = q^{f_i(d_i-1)}S_j(u, d_i), \quad i = 1, 2, \ldots, s. \]
Therefore,
\[ T_{d+j} = q^{-(d+j)s} \sum_{(v, P^d+j) = 1} S_{d+j}(va_1, d_1) \ldots S_{d+j}(va_s, d_s) \]
\[ = q^{-(d+j)s} \sum_{(v, P^d+r) = 1} \prod_{i=1}^s q^{f_i(d_i-1)}S_j(va_i, d_i) = q^{d-r}T_j. \]

**3. Main results**

**Theorem.** Let \( \varrho \) be as in (8). We have
(i) recursion: for \( n \geq \varrho \),
\[ \varpi_{n+d} = c + q^{d-r}\varpi_n, \]
(ii) the Poincaré series is given by
\[ P(t) = \frac{1 - q^{s-1}t}{(1 - q^{s-1}t)(1 - q^{d-s}t^{d+d})}, \]
\[ = \frac{1 - q^{s-1}t}{(1 - q^{s-1}t)(1 - q^{d-s}t^{d+d})} \]
where \( c = \varpi_{d+1} - q^{d-r}\varpi_{d-1} \) is a constant depending only upon the diagonal form as in (1).
Proof. (i) From (4) we have
\[ c_n = q^{-n} \sum_{x_1, \ldots, x_s \pmod{P^n}} e_n(u(a_1x_1^{d_1} + \ldots + a_sx_s^{d_s})) \]
\[ = q^{-n} \sum_{u \pmod{P^n}} S_n(ua_1, d_1) \ldots S_n(ua_s, d_s). \]

In the summation over \( u \pmod{P^n} \), we may set \( u = v\theta^{n-m}, 0 \leq m \leq n \), \( v \pmod{P^m} \) and \( (v, P^m) = 1 \). From (5) one has
\[ c_n = q^{-n} \sum_{m=0}^{n} q^{-ms} \sum_{(v, P^m) = 1} S_m(va_1, d_1) \ldots S_m(va_s, d_s) \]
\[ = q^{-n} \sum_{m=0}^{n} T_m. \]

Set \( n = \varrho + l, l \geq 0 \). By Lemma 2, we have
\[ \tau_{n+d} = \sum_{m=0}^{n+d-1} T_m = \sum_{m=0}^{\varrho+d-1} T_m + \sum_{m=0}^{l} T_{\varrho+d+m} = \tau_{\varrho+d-1} + \sum_{m=0}^{l} q^{d-r} T_{\varrho+m} \]
\[ = \tau_{\varrho+d-1} + q^{d-r}(\tau_n - \tau_{\varrho-1}) = c + q^{d-r} \tau_n. \]

(ii) Put \( q^{s-1}t = t_1 \). Then
\[ P(t) = \sum_{n=0}^{\infty} c_n t^n = \sum_{n=\varrho}^{\varrho+d-1} c_i t^i + \sum_{n=\varrho}^{n+d} c_{n+d} t^{n+d} \]
\[ = \sum_{i=0}^{\varrho+d-1} c_i t^i + \sum_{n=\varrho}^{\varrho+d} \tau_{n+d} t^{n+d} = \sum_{i=0}^{\varrho+d-1} c_i t^i + \sum_{n=\varrho}^{\varrho+d} (c + q^{d-r} \tau_n) t^{n+d} \]
\[ = \sum_{i=0}^{\varrho+d-1} c_i t^i + ct_1^{\varrho+d}(1 - t_1)^{-1} + q^{d-r} t_1^{\varrho-1} \left( P(t) - \sum_{i=0}^{\varrho-1} c_i t^i \right). \]

This gives the result of the theorem. \( \blacksquare \)

References


INSTITUTE OF MATHEMATICAL SCIENCES
DALIAN UNIVERSITY OF TECHNOLOGY
DALIAN 116024, PEOPLE’S REPUBLIC OF CHINA

Received on 4.7.1991