PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 116, Number 3, November 1992

ON THE POINCARÉ SERIES FOR DIAGONAL FORMS

JUN WANG

(Communicated by William W. Adams)

ABSTRACT. Let p be a fixed prime, $f(x_1, \ldots, x_s)$ a polynomial over $\mathbf{Z}_p$, the p-adic integers, c_n the number of solutions of $f = 0$ over $\mathbf{Z}/p^n\mathbf{Z}$, and $P_f(t) = \sum_{n=0}^{\infty} c_n t^n$ the Poincaré series. Explicit formulas for $P_f(t)$ are derived for diagonal forms.

1. INTRODUCTION

Let p be a fixed prime and $f(x_1, \ldots, x_s)$ a polynomial with coefficients in $\mathbf{Z}_p$, the p-adic integers. Let c_n denote the number of solutions of $f = 0$ over the ring $\mathbf{Z}/p^n\mathbf{Z}$, 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 [2, 3]. Since the proof is nonconstructive, deriving explicit formulas for $P_f(t)$ is an interesting problem. In this direction Goldman [4, 5] 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 Stevenson [6], using Jacobi sums.

In this paper we discuss, by means of exponential sums, the general diagonal form as

$$f(x) = a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s} , \tag{1}$$

where s, $d_1, \ldots, d_s$, and n are positive integers and $a_1, \ldots, a_s$ are the units in $\mathbf{Z}_p$.

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

Throughout this paper, we set $d = \operatorname{lcm}\{d_1, \ldots, d_s\}$, $f_i = d/d_i$, $r = f_1 + \cdots + f_s$, and $\bar{c}_n = p^{-n(s-1)} c_n$.

Received by the editors January 2, 1990 and, in revised form, November 21, 1990.
1991 *Mathematics Subject Classification.* Primary 11T99, 11E76; Secondary 11L03.

2. Exponential sums

Let $m \geq 0$ and define

$$e_m(u) = e^{2\pi i u/p^m}, \qquad u \in \mathbf{Z}_p .$$

The function $e_m(u)$ defines an additive character mod p^m and has the following simple properties:

$$e_0(u) = 1, \quad e_m(u) = e_m(u') \quad \text{if } u \equiv u' \mod p^m, \tag{2}$$

$$e_m(up^j) = e_{m-j}(u) \qquad (0 \leq j \leq m), \tag{3}$$

$$\sum_{z \bmod p^m} e_m(uz) = \begin{cases} p^m & \text{if } u \equiv 0 \mod p^m, \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

For $k \geq 1$, we define

$$S_m(u, k) = \sum_{z \bmod p^m} e_m(uz^k), \qquad S_0(u, k) = 1 .$$

It is clear that if $m \geq j \geq 0$ then

$$S_m(up^j, k) = p^j S_{m-j}(u, k). \tag{5}$$

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

Lemma 1. *Let* $(u, p) = 1$, $m \geq k \geq 1$, *and* $(p, m, k) \neq (2, 2, 2), (2, 3, 2),$ *and* $(2, 4, 4)$. *Then*

$$S_m(u, k) = p^{k-1} S_{m-k}(u, k).$$

Proof. Suppose $\operatorname{ord}_p k = l \geq 0$. From $m \geq l + 1$ and $(p, m, k) \neq (2, 2, 2)$ it follows that $m > l + 1$ and $\{z \bmod p^m\} = \{y + xp^{m-l-1} | y \bmod p^{m-l-1}, x \bmod p^{l+1}\}$. Using the Binomial theorem, we have

$$(y + xp^{m-l-1})^k = \sum_{i=0}^{k} \binom{k}{i} y^{k-i} x^i p^{i(m-l-1)} .$$

If $l \geq 3$ then $p^l \geq 2(l + 1)$. From this it follows that $m \geq k \geq p^l \geq 2(l + 1)$, $i(m - l - 1) \geq 2(m - l - 1) \geq m$, and

$$\operatorname{ord}_p \binom{k}{i} + i(m - l - 1) \geq m, \qquad 1 < i \leq k . \tag{6}$$

For $l = 0, 1,$ and 2, it is not difficult to show that (6) is true except for $p = 2$, $m = 3$, $k = 2$ and $p = 2$, $m = k = 4$. Hence, under the conditions of the lemma, we have

$$(y + xp^{m-l-1})^k \equiv y^k + ky^{k-1} xp^{m-l-1} \mod p^m$$

and

$$S_m(u, k) = \sum_{y \bmod p^{m-l-1}} e_m(uy^k) \sum_{x \bmod p^{l+1}} e_{l+1}(uky^{k-1} x).$$

Since $\operatorname{ord}_p k = l$, by (4), the inner sum $= 0$ unless $y \equiv 0 \bmod p$, in which case

it has the value p^{l+1}. Hence, we have, by setting $y = y_1 p$, $y_1 \bmod p^{m-l-2}$, that

$$S_m(u, k) = p^{l+1} \sum_{y_1 \bmod p^{m-l-2}} e_{m-k}(uy_1^k).$$

From this it is easy to see that $S_m(u, k) = p^{k-1} S_{m-k}(u, k)$ when $m - k \leq m - l - 2$. If $m - k > m - l - 2$ then $k = l + 1$, it follows that $k = p = 2$. In this case, from $m \geq 4$ it can be seen that if $y_1 \equiv y_2 \bmod 2^{m-3}$ then $y_1^2 \equiv y_2^2 \bmod 2^{m-2}$, in which case

$$S_m(u, 2) = 2^2 \sum_{y_1 \bmod 2^{m-3}} e_{m-2}(uy_1^2) = 2 \sum_{y_1 \bmod 2^{m-2}} e_{m-2}(uy_1^2) = 2S_{m-2}(u, 2).$$

The proof is complete. □

From Lemma 1, we distinguish two cases.

Case A. p is an odd prime or $d_i \neq 2, 4$ for each i, $1 \leq i \leq s$.

Case B. $p = 2$ and $d_i = 2$ or 4 for some i, $1 \leq i \leq s$.

From $m \geq 0$, put $T_m = p^{-ms} \sum_{(v, p^m)=1} S_m(va_1, d_1) \cdots S_m(va_s, d_s)$.

Lemma 2. *$T_{d+j} = p^{d-r} T_j$, for $j > 0$ in Case* A *and for $j > 1$ in Case* B. *$T_d = p^{d-r} - p^{d-r-1}$ in Case* A.

Proof. For $j > 1$, if $d_i = 2$ then $d_i + j \geq 4$ and if $d_i = 4$ then $d_i + j \geq 6$, and Lemma 1 gives

$$S_{d+j}(u, d_i) = p^{f_i(d_i-1)} S_j(u, d_i), \qquad i = 1, 2, \ldots, s.$$

Evidently, this is true for $j = 1$ in Case A. Therefore,

$$T_{d+j} = p^{-(d+j)s} \sum_{(v, p^{d+j})=1} S_{d+j}(va_1, d_1) \cdots S_{d+j}(va_s, d_s)$$

$$= p^{-(d+j)s} \sum_{(v, p^{d+j})=1} \prod_{i=1}^{s} p^{f_i(d_i-1)} s_j(va_i, d_i) = p^{d-r} T_j.$$

In Case A, we have

$$T_d = p^{-ds} \sum_{(v, p^d)=1} \prod_{i=1}^{s} S_d(va_i, d_i)$$

$$= p^{-ds} \sum_{(v, p^d)=1} \prod_{i=1}^{s} p^{f_i(d_i-1)} S_0(va_i, d_i) = p^{d-r} - p^{d-r-1}. \quad \square$$

3. Main results

Theorem 1. *For any prime p and $f(x)$ as in* (1), *we have*

(i) *recursion: For $n \geq 2$, $\bar{c}_{n+d} = c + p^{d-r} \bar{c}_n$;*

(ii) *the Poincaré series is given by*

$$P(t) = \frac{(1 - p^{s-1}t)(\sum_{i=0}^{d+1} c_i t^i) + cp^{(d+2)(s-1)} t^{d+2} - p^{ds-r} t^d (1 - p^{s-1}t)(1 + c_1 t)}{(1 - p^{s-1}t)(1 - p^{ds-r} t^d)},$$

where $c = \bar{c}_{d+1} - p^{d-r} \bar{c}_1$ is a constant depending only upon the polynomial $f(x)$.

Proof. (i) From (4), we have

$$c_n = p^{-n} \sum_{x_1, \dots, x_s \bmod p^n} \sum_{u \bmod p^n} e_n(u(a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s}))$$
$$= p^{-n} \sum_{u \bmod p^n} S_n(ua_1, d_1) \cdots S_n(ua_s, d_s).$$

In the summation $u \bmod p^n$, we may set $u = vp^{n-m}$, $0 \le m \le n$, $v \bmod p^m$, and $(v, p) = 1$. From (5) one has

$$c_n = p^{n(s-1)} \sum_{m=0}^{n} p^{-ms} \sum_{(v, p^m)=1} S_m(va_1, d_1) \cdots S_m(va_s, d_s)$$
$$= p^{n(s-1)} \sum_{m=0}^{n} T_m.$$

For $n \ge 2$, by Lemma 2, we have

$$\bar{c}_{n+d} = \sum_{m=0}^{n+d} T_m = \sum_{m=0}^{d+1} T_m + \sum_{m=2}^{n} T_{d+m}$$
$$= \bar{c}_{d+1} + \sum_{m=2}^{n} p^{d-r} T_m = \bar{c}_{d+1} + p^{d-r}(\bar{c}_n - \bar{c}_1) = c + p^{d-r}\bar{c}_n.$$

(ii) Put $p^{s-1}t = t_1$, then

$$P(t) = \sum_{n=0}^{\infty} c_n t^n = \sum_{i=0}^{d+1} c_i t^i + \sum_{n=2}^{\infty} c_{n+d} t^{n+d}$$
$$= \sum_{i=0}^{d+1} c_i t^i + \sum_{n=2}^{\infty} \bar{c}_{n+d} t_1^{n+d} = \sum_{i=0}^{d+1} c_i t^i + \sum_{n=2}^{\infty} (c + p^{d-r}\bar{c}_n) t_1^{n+d}$$
$$= \sum_{i=0}^{d+1} c_i t^i + c t_1^{d+2}(1 - t_1)^{-1} + p^{d-r} t_1^d (P(t) - 1 - c_1 t).$$

This gives the result of the theorem. □

In Case A, by Lemma 2, we have

$$\bar{c}_d = \sum_{m=0}^{d} T_m = \bar{c}_{d-1} + T_d = \bar{c}_{d-1} - p^{d-r-1} + p^{d-r},$$
$$\bar{c}_{d+1} = \sum_{m=0}^{d+1} T_m = \bar{c}_d + T_{d+1} = \bar{c}_d + p^{d-r} T_1$$
$$= \bar{c}_{d-1} - p^{d-r-1} + p^{d-r} + p^{d-r}(\bar{c}_1 - 1) = \bar{c}_{d-1} - p^{d-r-1} + p^{d-r}\bar{c}_1.$$

Set $c' = \bar{c}_{d-1} - p^{d-r-1}$; then $c' = c$. The preceding discussion suggests that we may take $\bar{c}_0, \bar{c}_1, \dots, \bar{c}_{d-1}$ as the original values of the recursion relation of $\bar{c}_n$, and we have

Theorem 2. *Suppose that* p *is an odd prime or* $p = 2$, $d_i \neq 2, 4$ *for each* i, $1 \leq i \leq s$. *Then we have*

(i) *recursion: For* $n \geq 0$, $\bar{c}_{n+d} = c' + p^{d-r}\bar{c}_n$;

(ii) *the Poincaré series is given by*

$$P(t) = \frac{(1 - p^{s-1}t)(\sum_{i=0}^{d-1} c_i t^i) + c' p^{d(s-1)} t^d}{(1 - p^{s-1}t)(1 - p^{ds-r}t^d)},$$

where $c' = \bar{c}_{d-1} - p^{d-r-1}$ *is a constant depending only upon the polynomial* $f(x)$.

ACKNOWLEDGMENTS

The author is deeply indebted to the referee for valuable suggestions.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York, 1966.
2. J. Igusa, *Complex powers and asymptotic expansions*. II, J. Reine Angew. Math. **278/279** (1979), 307–321.
3. ____, *Some observations on higher degree character*, Amer. J. Math. **99** (1977), 393–471.
4. J. R. Goldman, *Numbers of solutions of congruences: Poincaré series for strongly nondegenerate forms*, Proc Amer. Math. Soc. **87** (1983), 586–590.
5. ____, *Numbers of solutions of congruences: Poincaré series for algebraic curves*, Adv. in Math. **62** (1986), 68–83.
6. E. Stevenson, *The rationality of the Poincaré series of a diagonal form*, Thesis, Princeton Univ., 1978.

INSTITUTE OF APPLIED MATHEMATICS, DALIAN UNIVERSITY OF TECHNOLOGY, DALIAN 116024, PEOPLE'S REPUBLIC OF CHINA