Canad. Math. Bull. Vol. **28** (4), 1985

A MULTIPLE EXPONENTIAL SUM TO MODULUS p^2

BY

D. R. HEATH-BROWN*

Dedicated to the memory of Robert Arnold Smith

ABSTRACT. For suitable polynomials $f(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ in n variables, of total degree d, it is shown that

$$\left| \sum_{\boldsymbol{x} \pmod{p^2}} e_{p^2}(f(\boldsymbol{x})) \right| \leq (d-1)^n p^n.$$

This is, formally, a precise analogue of a theorem of Deligne [1] on exponential sums (mod p). However the proof uses no more than elementary algebraic geometry.

It is well known that the estimation of exponential sums over finite fields is intimately related to the Weil Conjectures for the corresponding zeta-function. We shall be concerned with the following situation. Let p be a prime, and let K be the field with p elements. Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ and let $F(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ be a form of degree d, with $p \nmid d$. Suppose $F(\boldsymbol{x}) = 0$ defines a non-singular absolutely irreducible projective variety over $\bar{K}$, the algebraic closure of K. (Here, by abuse of notation, we do not distinguish between F and its image in K.) Let $E(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ be a polynomial of total degree $<d$. We shall write $e_d(y) = \exp(2\pi i y/d)$. Then according to Deligne ([1], Theorem 8.4) we have

$$\left| \sum_{\boldsymbol{x} \pmod{p}} e_p(F(\boldsymbol{x}) + E(\boldsymbol{x})) \right| \leq (d-1)^n p^{n/2},$$

where the summation condition means that each variable x_i runs (mod p).

For many purposes one wants analogous results for sums (mod p^e), with a bound $O(p^{en/2})$. This however is not possible in general. If $n = 3$, $d = 3$ and $F = x_1^3 + x_2^3 + x_3^3$, and $E = 0$, then

$$\sum_{\boldsymbol{x} \pmod{p^3}} e_{p^3}(F(\boldsymbol{x}) + E(\boldsymbol{x})) = p^6, \qquad (p \neq 3).$$

However it turns out that a suitable bound is indeed possible for sums (mod p^2).

Received by the editors April 12, 1984.

*Written while the author was enjoying a visiting professorship at Oklahoma State University, Stillwater.

AMS Subject Classification (1980): 10G10.

THEOREM. *Let p, F, E and d be as above. Then*

$$\left| \sum_{\boldsymbol{x} \,(\mathrm{mod}\, p^2)} e_{p^2}(F(\boldsymbol{x}) + E(\boldsymbol{x})) \right| \leq (d-1)^n p^n.$$

It is noteworthy that both the conditions of this result and the shape of the upper bound should be exactly the same as in Deligne's theorem. When this result was described to Professor Smith, he replied that "he thought he could prove something similar"; so it seems appropriate that the proof should be published in this volume.

For the proof we denote the sum occuring in the theorem by S. We replace the vector $\boldsymbol{x}$ by $\boldsymbol{y} + p\boldsymbol{z}$, where $\boldsymbol{y}, \boldsymbol{z}$ run (mod p). Then

$$F(\boldsymbol{x}) + E(\boldsymbol{x}) \equiv F(\boldsymbol{y}) + E(\boldsymbol{y}) + p\boldsymbol{z}.(\nabla F(\boldsymbol{y}) + \nabla E(\boldsymbol{y})) \,(\mathrm{mod}\, p^2).$$

Moreover

$$\sum_{\boldsymbol{z} \,(\mathrm{mod}\, p)} e_p(\boldsymbol{z}.(\nabla F(\boldsymbol{y}) + \nabla E(\boldsymbol{y}))) = \begin{cases} p^n, & p \mid \nabla F(\boldsymbol{y}) + \nabla E(\boldsymbol{y}), \\ 0, & \text{otherwise.} \end{cases}$$

Consequently

$$|S| \leq p^n \,\#\{\boldsymbol{y} \,(\mathrm{mod}\, p);\ p \mid \nabla F(\boldsymbol{y}) + \nabla E(\boldsymbol{y})\}.$$

Now let $\boldsymbol{x} = (x_0, x_1, \ldots, x_n)$ and let $G(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ be the form given by

$$G(\boldsymbol{x}) = F(\boldsymbol{x}) + x_0{}^d E(x_0^{-1}\boldsymbol{x}).$$

We define $G_0(\boldsymbol{x}) = x_0$ and $G_i(\boldsymbol{x}) = \partial G / \partial x_i$ for $1 \leq i \leq n$. Then

$$\{\boldsymbol{x} \in \bar{K}^{n+1};\ G_i(\boldsymbol{x}) = 0,\ 0 \leq i \leq n\} = \{\boldsymbol{x} = (0, x_1, \ldots, x_n) \in \bar{K}^{n+1};\ \nabla F(\boldsymbol{x}) = \boldsymbol{0}\}$$

By the non-singularity condition on F, the latter set contains only the origin, so that the intersection of the projective hypersurfaces $G_i = 0$, $(0 \leq i \leq n)$ is empty. Now let V denote the intersection of the hypersurfaces $G_i = 0$ for $1 \leq i \leq n$. If any irreducible component of V were to have positive dimension, its intersection with the hyperplane $G_0 = 0$ would be non-empty. Consequently V consists of finitely many points. Each form $G_i (1 \leq i \leq n)$ has degree $d - 1$. Thus, by Bezout's Theorem (Shafarevich ([2], p. 198) we have $\#V \leq (d-1)^n$. It follows that

$$\#\{\boldsymbol{x} \in K^{n+1} - \{\boldsymbol{0}\};\ G_i(\boldsymbol{x}) = 0,\ 1 \leq i \leq n\} \leq (p-1)\,\#V \leq (p-1)(d-1)^n.$$

Finally we observe that

$$\#\{\boldsymbol{x} \in K^n;\ \nabla F(\boldsymbol{x}) + \nabla E(\boldsymbol{x}) = \boldsymbol{0}\} = \#\{\boldsymbol{x} \in K^n;\ G_i(1, x_1, x_2, \ldots, x_n) = 0, 1 \leq i \leq n\} \leq \frac{1}{p-1} \#\{\boldsymbol{x} \in K^{n+1};\ G_i(\boldsymbol{x}) = 0,\ 1 \leq i \leq n\} \leq (d-1)^n,$$

and the theorem follows.

https://doi.org/10.4153/CMB-1985-046-2 Published online by Cambridge University Press

References

1. P. Deligne, *La conjecture de Weil*. I. Publications Mathématiques 43, Institue des Hautes Études Scientifiques, Paris, 1974, pp. 273–307.

2. I. R. Shafarevich, *Basic algebraic geometry*, Grundlehren der mathematischen Wissenchaften 213, Springer, New York, 1974.

Magdalen College
Oxford OX1 4AU
England