ACTA ARITHMETICA
107.3 (2003)

Some applications of Bombieri's estimate for exponential sums

by

Wenpeng Zhang and Yuan Yi (Xi'an)

1. Introduction. Let $p \geq 3$ be a prime, k be any fixed positive integer, and let $F_p[x,y]$ denote the set of all polynomials with coefficients in the residue system modulo p. For any $f \in F_p[x,y]$ and $0 < \sigma \leq 1$, we define

$$\mathcal{A} = \mathcal{A}(f,k,\sigma) = \left\{(a,b) : f(a,b) \equiv 0 \ (\mathrm{mod}\, p), \ \left|\left\{\frac{a^k}{p}\right\} - \left\{\frac{b^k}{p}\right\}\right| < \sigma\right\}$$

and

$$M(p,\mathcal{A},k) = \sum_{a=1}^{p} \sum_{\substack{b=1 \\ (a,b)\in\mathcal{A}}}^{p} 1, \tag{1}$$

where $[x]$ denotes the greatest integer not exceeding x and $\{x\} = x - [x]$. The main purpose of this paper is to study the asymptotic properties of (1). Some special cases of this problem have been studied before. For example, the first author [4] obtained an asymptotic formula

$$M(p,\mathcal{A},k) = \sigma(2-\sigma)p + O(p^{1/2}\ln^2 p) \quad \text{if } f(x,y) = xy - 1.$$

Zheng Zhiyong [5] proved that

$$M(p,\mathcal{A},1) = \sigma(2-\sigma)p + O(p^{1/2}\ln^2 p)$$

if $f(x,y)$ is absolutely irreducible in $F_p[x,y]$.

This problem is interesting, because it can help us to find new distribution properties in finite fields. In this paper, we use J. H. H. Chalk and R. A. Smith's deep result [2], which is based on E. Bombieri's work on exponential sums [1], and the estimates for trigonometric sums to obtain a general conclusion for (1). The constants implied by the O-symbols and the symbols $\ll$ used in this paper do not depend on any parameter, unless otherwise indicated. Under the notations above, we shall prove the following:

2000 *Mathematics Subject Classification*: 11N69, 11L05.

Key words and phrases: exponential sum, Bombieri's estimates, asymptotic formula.

Theorem. *Let k be any fixed positive integer, f be a given polynomial in $F_p[x,y]$ and suppose that:*

(a) *$f(x,y)$ is absolutely irreducible in $F_p[x,y]$,*

(b) *$rx^k + sy^k \not\equiv c \pmod{f(x,y)}$ in $F_p[x,y]$ for any integers c, r and s with $\{r/p\} + \{s/p\} \neq 0$.*

Then

$$M(p,\mathcal{A},k) = \sigma(2-\sigma) + O(p^{1/2}\ln^2 p),$$

where the O-constants depend only on k and the degrees of f.

From this theorem we may immediately deduce the following

Corollary. *Let k be a fixed positive integer and let f be a polynomial with integer coefficients such that for any large enough prime number p, the image of f in $F_p[x,y]$ satisfies the conditions:*

(a) *$f(x,y)$ is absolutely irreducible in $F_p[x,y]$,*

(b) *$rx^k + sy^k \not\equiv c \pmod{f(x,y)}$ in $F_p[x,y]$ for any integers c, r and s with $\{r/p\} + \{s/p\} \neq 0$.*

Then for any fixed real number $0 < \sigma \le 1$, we have the limit distribution formula

$$\lim_{p\to\infty} \frac{1}{p} \sum_{\substack{a=1 \\ f(a,b)\equiv 0 \pmod p \\ |\{a^k/p\}-\{b^k/p\}|<\sigma}}^{p} \sum_{b=1}^{p} 1 = \sigma(2-\sigma).$$

Let F_p^* denote the multiplicative group of nonzero residue classes mod p. It is clear that the k-powers of nonzero residue classes mod p form a multiplicative subgroup, say U_k, of F_p^*. If k and $p-1$ are relatively prime, then U_k is the full group F_p^* and the result of our theorem reduces exactly to the case $k=1$, which was investigated in [5]. The new feature in this paper is when $(k,p-1) = d > 1$ in which case $U_k = U_d$ is a proper subgroup of F_p^*. Thus the results of the present paper can be interpreted as results on the distribution of the solutions of $f(x,y) \equiv 0 \pmod p$ inside a subgroup of small index in F_p^*.

2. Several lemmas.

In this section, we give some lemmas which are necessary in the proof of the theorem. First we have

Lemma 1 ([3, Corollary 2c]). *Let $f(x,y)$ be a polynomial with rational integer coefficients which is absolutely irreducible. If $N(p)$ denotes the number of solutions of the congruence*

$$f(x,y) \equiv 0 \pmod p, \qquad 1 \le x,y \le p,$$

then for large primes p,

$$N(p) = p + O(p^{1/2}).$$

LEMMA 2 ([2, Theorem 2]). *Let* $f, g \in F_p[x, y]$ *and suppose that*:

(a) $f(x, y)$ *is absolutely irreducible in* $F_p[x, y]$,

(b) $g(x, y) \not\equiv c \pmod{f(x, y)}$ *in* $F_p[x, y]$ *for any integer* c.

Then

$$S_2(f, g) = \sum_{\substack{a=1 \\ f(a,b)\equiv 0 \pmod p}}^{p} \sum_{b=1}^{p} e\left(\frac{g(a, b)}{p}\right)$$
$$\ll (d_1^2 - 3d_1 + 2d_1 d_2)p^{1/2} + d_1^2$$

for all primes p, *where* $d_1 = d(f)$ *and* $d_2 = d(g)$ *are the degrees of* f *and* g *in* $F_p[x, y]$, *and* $e(y) = e^{2\pi i y}$.

LEMMA 3. *Let* p *be an odd prime. Then for any real number* $0 < \sigma \le 1$,

$$\text{(I)} \qquad \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \Bigg| \sum_{\substack{a=1 \\ |a-b|<\sigma p}}^{p} \sum_{b=1}^{p} e\left(\frac{ra + sb}{p}\right) \Bigg| \ll p^2 \ln^2 p;$$

$$\text{(II)} \qquad \sum_{r=1}^{p-1} \Bigg| \sum_{\substack{a=1 \\ |a-b|<\sigma p}}^{p} \sum_{b=1}^{p} e\left(\frac{ra}{p}\right) \Bigg| \ll p \ln p.$$

Proof. We only prove (I); the proof of (II) is similar. For any real number $\alpha \ge 0$ and integer u with $p \nmid u$,

$$\sum_{1 \le n \le N} n^{\alpha} e\left(\frac{nu}{p}\right) \ll \frac{N^{\alpha}}{\left|\sin \frac{\pi u}{p}\right|} \ll \frac{N^{\alpha}}{\left\|\frac{u}{p}\right\|},$$

where $\|x\| = \min(x - [x], 1 + [x] - \{x\})$. We immediately get

$$\sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \Bigg| \sum_{\substack{a=1 \\ |a-b|<\sigma p}}^{p} \sum_{b=1}^{p} e\left(\frac{ra + sb}{p}\right) \Bigg| \le 2 \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \Bigg| \sum_{m=0}^{[\sigma p]} \sum_{\substack{a=1 \\ a=b+m}}^{p} \sum_{b=1}^{p} e\left(\frac{ra + sb}{p}\right) \Bigg|$$

$$\ll \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \Bigg| \sum_{m=0}^{[\sigma p]} \sum_{b=1}^{p-m} e\left(\frac{rm + (s + r)b}{p}\right) \Bigg|$$

$$\begin{aligned}
&\ll \sum_{r=1}^{p-1}\Bigg|\sum_{m=0}^{[\sigma p]}(p-m)e\bigg(\frac{rm}{p}\bigg)\Bigg| \\
&\quad+\sum_{\substack{r=1\\ r+s\neq p}}^{p-1}\sum_{s=1}^{p-1}\Bigg|\sum_{m=0}^{[\sigma p]}e\bigg(\frac{rm+r+s}{p}\bigg)\frac{e\big(\frac{(r+s)(p-m)}{p}\big)-1}{e\big(\frac{r+s}{p}\big)-1}\Bigg| \\
&\ll \sum_{r=1}^{p-1}\frac{p}{\big|\sin\frac{\pi r}{p}\big|}+\sum_{\substack{r=1\\ r+s\neq p}}^{p-1}\sum_{s=1}^{p-1}\frac{1}{\big|\sin\frac{\pi(r+s)}{p}\big|}\bigg(\frac{1}{\big|\sin\frac{\pi r}{p}\big|}+\frac{1}{\big|\sin\frac{\pi s}{p}\big|}\bigg) \\
&\ll p^2\sum_{r=1}^{p-1}\frac{1}{r}+p\sum_{\substack{r=1\\ r+s\neq p}}^{p-1}\sum_{s=1}^{p-1}\frac{1}{\big\|\frac{r+s}{p}\big\|}\bigg(\frac{1}{r}+\frac{1}{s}\bigg) \\
&\ll p^2\ln^2 p.
\end{aligned}$$

This proves (I).

3. Proof of the Theorem. In this section, we shall complete the proof of the Theorem. First from the definition of $M(p,\mathcal{A},k)$ and the trigonometric identity

$$\sum_{a=1}^{n}e\bigg(\frac{au}{n}\bigg)=\begin{cases} n & \text{if } n\mid u,\\ 0 & \text{if } n\nmid u,\end{cases}$$

we have the identity

$$M(p,\mathcal{A},k)=\sum_{\substack{a=1\\ f(a,b)\equiv 0\ (\mathrm{mod}\ p)\\ |p\{a^k/p\}-p\{b^k/p\}|<\sigma p}}^{p}\sum_{b=1}^{p}1 \tag{2}$$

$$\begin{aligned}
&=\frac{1}{p^2}\sum_{\substack{a=1\\ f(a,b)\equiv 0\ (\mathrm{mod}\ p)}}^{p}\sum_{b=1}^{p}\ \sum_{r=1}^{p}\sum_{s=1}^{p}\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p}e\bigg(\frac{r(c-p\{a^k/p\})}{p}\bigg)e\bigg(\frac{s(d-p\{b^k/p\})}{p}\bigg) \\
&=\frac{1}{p^2}\sum_{\substack{a=1\\ f(a,b)\equiv 0\ (\mathrm{mod}\ p)}}^{p}\sum_{b=1}^{p}\ \sum_{r=1}^{p}\sum_{s=1}^{p}\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p}e\bigg(\frac{r(c-a^k)}{p}\bigg)e\bigg(\frac{s(d-b^k)}{p}\bigg) \\
&=\frac{1}{p^2}\sum_{r=1}^{p}\sum_{s=1}^{p}\Bigg(\sum_{\substack{a=1\\ f(a,b)\equiv 0\ (\mathrm{mod}\ p)}}^{p}\sum_{b=1}^{p}e\bigg(\frac{-ra^k-sb^k}{p}\bigg)\Bigg)\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p}e\bigg(\frac{rc+sd}{p}\bigg)
\end{aligned}$$

$$= \frac{1}{p^2}\Big(\sum_{\substack{a=1\\ f(a,b)\equiv 0 \,(\mathrm{mod}\, p)}}^{p}\sum_{b=1}^{p} 1\Big)\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p} 1$$

$$+ \frac{1}{p^2}\sum_{r=1}^{p-1}\Big(\sum_{\substack{a=1\\ f(a,b)\equiv 0 \,(\mathrm{mod}\, p)}}^{p}\sum_{b=1}^{p} e\Big(\frac{-ra^k}{p}\Big)\Big)\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p} e\Big(\frac{rc}{p}\Big)$$

$$+ \frac{1}{p^2}\sum_{s=1}^{p-1}\Big(\sum_{\substack{a=1\\ f(a,b)\equiv 0 \,(\mathrm{mod}\, p)}}^{p}\sum_{b=1}^{p} e\Big(\frac{-sb^k}{p}\Big)\Big)\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p} e\Big(\frac{sd}{p}\Big)$$

$$+ \frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\Big(\sum_{\substack{a=1\\ f(a,b)\equiv 0 \,(\mathrm{mod}\, p)}}^{p}\sum_{b=1}^{p} e\Big(\frac{-ra^k - sb^k}{p}\Big)\Big)\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p} e\Big(\frac{rc+sd}{p}\Big)$$

$$\equiv M_1 + M_2 + M_3 + M_4.$$

Now we estimate each term in (2) separately. From Lemma 1 and the asymptotic formula

$$\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p} 1 = 2\sum_{m=0}^{[\sigma p]}\sum_{\substack{c=1\\ c=d+m}}^{p}\sum_{d=1}^{p} 1 + O(p) = 2\sum_{m=0}^{[\sigma p]}(p-m) + O(p)$$

$$= 2p[\sigma p] - [\sigma p]([\sigma p]+1) + O(p) = \sigma(2-\sigma)p^2 + O(p)$$

we immediately get

$$\text{(3)} \qquad M_1 = \frac{1}{p^2}\,(p + O(p^{1/2}))(\sigma(2-\sigma)p^2 + O(p)) = \sigma(2-\sigma)p + O(p^{1/2}).$$

Applying Lemmas 2 and 3 we have

$$\text{(4)} \quad M_4 = \frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\Big(\sum_{\substack{a=1\\ f(a,b)\equiv 0 \,(\mathrm{mod}\, p)}}^{p}\sum_{b=1}^{p} e\Big(\frac{-ra^k - sb^k}{p}\Big)\Big)\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p} e\Big(\frac{rc+sd}{p}\Big)$$

$$\le \frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\Big|\sum_{\substack{a=1\\ f(a,b)\equiv 0 \,(\mathrm{mod}\, p)}}^{p}\sum_{b=1}^{p} e\Big(\frac{-ra^k - sb^k}{p}\Big)\Big|\Big|\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p} e\Big(\frac{rc+sd}{p}\Big)\Big|$$

$$\ll \frac{\sqrt{p}}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\Big|\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p} e\Big(\frac{rc+sd}{p}\Big)\Big| \ll \sqrt{p}\ln^2 p.$$

Similarly, we can also deduce the estimates

$$(5)\quad M_2=\frac{1}{p^2}\sum_{r=1}^{p-1}\Bigg(\sum_{\substack{a=1\\ f(a,b)\equiv 0\,(\mathrm{mod}\,p)}}^{p}\sum_{b=1}^{p} e\bigg(\frac{-ra^k}{p}\bigg)\Bigg)\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p} e\bigg(\frac{rc}{p}\bigg)\ll\sqrt{p}\ln^2 p$$

and

$$(6)\quad M_3=\frac{1}{p^2}\sum_{s=1}^{p-1}\Bigg(\sum_{\substack{a=1\\ f(a,b)\equiv 0\,(\mathrm{mod}\,p)}}^{p}\sum_{b=1}^{p} e\bigg(\frac{-sb^k}{p}\bigg)\Bigg)\sum_{\substack{c=1\\ |c-d|<\sigma p}}^{p}\sum_{d=1}^{p} e\bigg(\frac{sd}{p}\bigg)\ll\sqrt{p}\ln^2 p.$$

Combining (2)–(6) we obtain the asymptotic formula

$$M(p,\mathcal{A},k)=\sigma(2-\sigma)+O(p^{1/2}\ln^2 p).$$

This completes the proof of the Theorem.

Acknowledgements. The authors express their gratitude to the referee for his helpful and detailed comments.

References

[1] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. 88 (1966), 71–105.

[2] J. H. H. Chalk and R. A. Smith, *On Bombieri's estimate for exponential sums*, Acta Arith. 18 (1971), 191–212.

[3] W. M. Schmidt, *Equations over Finite Fields*, Lecture Notes in Math. 536, Springer, Berlin, 1976.

[4] W. P. Zhang, *On the distribution of inverses modulo p (II)*, Acta Arith. 100 (2001), 189–194.

[5] Z. Y. Zheng, *Distribution of zeros of an irreducible curve over a finite field*, J. Number Theory 59 (1996), 106–118.

Research Center for Basic Science
Xi'an Jiaotong University
Xi'an Shaanxi, People's Republic of China
E-mail: wpzhang@nwu.edu.cn
yiyuan74@163.com

Received on 27.11.2001
and in revised form on 20.5.2002 (4157)