ACTA ARITHMETICA
XCVI.4 (2001)

A note on Waring's problem in finite fields

by

ARNE WINTERHOF (Wien)

In memory of Karl Mathiak

1. Introduction. Let $g(k,p^n)$ be the smallest s such that every element of $\mathbb{F}_{p^n}$ is a sum of s kth powers in $\mathbb{F}_{p^n}$.

It is sufficient to restrict ourselves to the case $1\neq k\,|\,p^n-1$, and it is well known (see [1, Theorem G]) that

$$(1)\qquad g(k,p^n) \text{ exists}\quad \text{if and only if}\quad \frac{p^n-1}{p^d-1}\nmid k \text{ for all } d\,|\,n,\ d\neq n.$$

We shall suppose from now on that $g(k,p^n)$ exists.

Several bounds for $g(k,p^n)$ are known. For surveys see [7] and [13]. Recent results can be found in [5]–[9] and [13].

In the case $n=1$ it was proved in [4, Theorem 1] that

$$(2)\qquad g(k,p)<68k^{1/2}(\ln k)^2 \quad \text{for } k<(p-1)/2.$$

Whether (2) holds true for $n>1$ has not been known yet.

In this note we prove

$$g(k,p^n)<6.2n(2k)^{1/n}\ln k,$$

which yields an extension of (2) to arbitrary n. Moreover, we show

$$g(k,p^n)>\tfrac{1}{2}(((n+1)k)^{1/n}-1)$$

if $n+1$ is a prime such that p is a primitive root modulo $n+1$ and $k=(p^n-1)/(n+1)$.

2. Preliminary results. The following result can be found in [2] for $n=1$. For arbitrary n but p odd it is a simple deduction from [10, Theorem 1]. For arbitrary n and $p=2$ the result was shown in [13, Theorem 3].

2000 *Mathematics Subject Classification*: 11P05, 11T24.

Lemma 1. *For $k < (p^n - 1)/2$ we have*

$$g(k, p^n) \le \lfloor k/2 \rfloor + 1.$$

The next lemma was proved in [3, Section 1] for $n = 1$ and in [13, Theorem 1] for arbitrary n.

Lemma 2. *For $p^n > k^2$ we have*

$$g(k, p^n) \le \lfloor 32 \ln k \rfloor + 1.$$

3. Extension of the Dodson–Tietäväinen bound. Let

$$A_s = \{x_1^k + \ldots + x_s^k \mid x_1, \ldots, x_s \in \mathbb{F}_{p^n}\}, \qquad \psi(x) = e^{2\pi i \mathrm{Tr}(x)/p},$$
$$S_s(u) = \sum_{y \in A_s} \psi(uy) \quad \text{and} \quad M_s = \max\{|S_s(u)| \mid u \in \mathbb{F}_{p^n}^*\}.$$

Lemma 3 (cf. [11, Lemma 1]).

$$M_s < (|A_s| k)^{1/2}.$$

Proof. We have

$$\sum_{u \in \mathbb{F}_{p^n}^*} |S_s(u)|^2 = \sum_{u \in \mathbb{F}_{p^n}} |S_s(u)|^2 - |A_s|^2$$
$$= \sum_{y,z \in A_s} \sum_{u \in \mathbb{F}_{p^n}} \psi(u(y - z)) - |A_s|^2 = (p^n - |A_s|)|A_s|.$$

Since $S_s(uv) = S_s(u)$ for every $0 \ne v \in A_1$ we get

$$\sum_{u \in \mathbb{F}_{p^n}^*} |S_s(u)|^2 \ge \frac{p^n - 1}{k} M_s^2.$$

Hence,

$$M_s^2 \le (p^n - |A_s|)|A_s| k/(p^n - 1) < |A_s| k. \ \blacksquare$$

Lemma 4 (cf. [12, Lemma 2]). *If $|A_s| \ge 2k$ then*

$$g(k, p^n) \le s(1 + \lfloor (2 \ln p^n)/\ln 2 \rfloor).$$

Proof. Let $r = 1 + \lfloor (2 \ln p^n)/\ln 2 \rfloor$, $a \in \mathbb{F}_{p^n}$ and let $N = N(a)$ be the number of solutions of

$$y_1 + \ldots + y_r = a \in \mathbb{F}_{p^n}, \qquad y_i \in A_s.$$

Then

$$p^n N = \sum_{y_1, \ldots, y_r \in A_s} \sum_{u \in \mathbb{F}_{p^n}} \psi(u(y_1 + \ldots + y_r - a))$$
$$= \sum_{u \in \mathbb{F}_{p^n}} (S_s(u))^r \psi(-ua) \ge |A_s|^r - (p^n - 1) M_s^r.$$

Hence, by Lemma 3, $|A_s|/k \geq 2$ and $r/2 > (\ln p^n)/\ln 2$, we get

$$N > p^{-n}(|A_s|k)^{r/2}((|A_s|/k)^{r/2} - p^n + 1) \geq p^{-n}(|A_s|k)^{r/2}(2^{r/2} - p^n + 1) > 0. \ \blacksquare$$

THEOREM 1. *If* $g(k, p^n)$ *exists then for* $1 < k < (p^n - 1)/2$ *we have*

$$g(k, p^n) < 6.2n(2k)^{1/n} \ln k.$$

Proof. For $2 \leq k \leq 11$ we get the result by Lemma 1. For $12 \leq k < p^{n/2}$ the theorem follows by Lemma 2 since

$$\frac{32 \ln k + 1}{nk^{1/n} \ln k} \leq \frac{32 \ln 12 + 1}{n12^{1/n} \ln 12} < 6.$$

Hence, we may restrict ourselves to the case $k \geq \max(12, p^{n/2})$. If $g(k, p^n)$ exists, then there exists a basis $\{b_1, \ldots, b_n\} \subset A_1$ of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Since $k < p^n/2$ the expression

$$m_1 b_1 + \ldots + m_n b_n, \qquad 0 \leq m_i \leq \lfloor (2k)^{1/n} \rfloor < p,$$

which is a sum of at most $n\lfloor (2k)^{1/n} \rfloor$ kth powers, represents at least

$$(\lfloor (2k)^{1/n} \rfloor + 1)^n \geq 2k$$

distinct elements of $\mathbb{F}_{p^n}$. Hence by Lemma 4,

$$\begin{aligned} g(k, p^n) &\leq n\lfloor (2k)^{1/n} \rfloor (1 + (2 \ln p^n)/\ln 2) \\ &\leq 2^{1/n}\left(\frac{1}{\ln k} + \frac{4}{\ln 2}\right) nk^{1/n} \ln k < 6.2n(2k)^{1/n} \ln k. \ \blacksquare \end{aligned}$$

COROLLARY 1. *If* $g(k, p^n)$ *exists then for* $1 < k < (p^n - 1)/2$ *we have*

$$g(k, p^n) < 68k^{1/2}(\ln k)^2.$$

Proof. By (2) and Lemma 2 we may suppose that $n \geq 2$ and $k \geq p^{n/2}$. Then

$$6.2n(2k)^{1/n} \ln k < 34 \ln p^n k^{1/n} \ln k \leq 68k^{1/2}(\ln k)^2$$

and the assertion is covered by the previous theorem. $\blacksquare$

4. A lower bound. Now we prove a lower bound, that is, an existence theorem.

THEOREM 2. *Let* r *and* p *be primes such that* p *is a primitive root modulo* r. *Let* $n = r - 1$ *and* $k = (p^n - 1)/(n + 1)$. *Then* $g(k, p^n)$ *exists and we have*

$$g(k, p^n) > \tfrac{1}{2}(((n + 1)k)^{1/n} - 1).$$

Proof. Since $p^d \not\equiv 1 \bmod (n+1)$ for $1 \leq d < n$ we have $(p^n - 1)/(p^d - 1) \nmid k$ and $g(k, p^n)$ exists by (1).

We have $A_1 = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^n\}$, where ζ denotes a primitive rth root of unity. Then

$$\begin{aligned}A_s &= \{\nu_0 + \nu_1\zeta + \nu_2\zeta^2 + \ldots + \nu_n\zeta^n \mid 0 \le \nu_0 + \nu_1 + \nu_2 + \ldots + \nu_n \le s\}\\ &= \{(\nu_0 - \nu_n) + (\nu_1 - \nu_n)\zeta\\ &\qquad + \ldots + (\nu_{n-1} - \nu_n)\zeta^{n-1} \mid 0 \le \nu_0 + \ldots + \nu_n \le s\}\\ &\subset \{\mu_0 + \mu_1\zeta + \ldots + \mu_{n-1}\zeta^{n-1} \mid -s \le \mu_0, \mu_1, \ldots, \mu_{n-1} \le s\}.\end{aligned}$$

The cardinality of the latter set is at most $(2s+1)^n$, whence

$$A_s \ne \mathbb{F}_{p^n} \quad \text{if } s \le \tfrac{1}{2}(((n+1)k)^{1/n} - 1),$$

which implies the theorem. ■

References

[1] M. Bhaskaran, *Sums of mth powers in algebraic and abelian number fields*, Arch. Math. (Basel) 17 (1966), 497–504; Correction, ibid. 22 (1971), 370–371.

[2] S. Chowla, H. B. Mann and E. G. Straus, *Some applications of the Cauchy–Davenport theorem*, Norske Vid. Selsk. Forh. Trondheim 32 (1959), 74–80.

[3] M. M. Dodson, *On Waring's problem in* GF[p], Acta Arith. 19 (1971), 147–173.

[4] M. M. Dodson and A. Tietäväinen, *A note on Waring's problem in* GF[p], ibid. 30 (1976), 159–167.

[5] C. Garcia and P. Solé, *Diameter lower bounds for Waring graphs and multiloop networks*, Discrete Math. 111 (1993), 257–261.

[6] D. R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from kth powers and for Heilbronn's exponential sum*, Quart. J. Math. 51 (2000), 221–235.

[7] S. V. Konyagin, *On estimates of Gaussian sums and Waring's problem for a prime modulus*, Trudy Mat. Inst. Steklov. 198 (1992), 111–124 (in Russian); English transl.: Proc. Steklov Inst. Math. 1994, no. 1, 105–117.

[8] I. Shparlinskiĭ, *On bounds of Gaussian sums*, Mat. Zametki 50 (1991), 122–130 (in Russian); English transl.: Math. Notes 50 (1991), 740–746.

[9] —, *On exponential sums with sparse polynomials and rational functions*, J. Number Theory 60 (1996), 233–244.

[10] A. Tietäväinen, *On diagonal forms over finite fields*, Ann. Univ. Turku Ser. A I 118 (1968), 10 pp.

[11] —, *Proof of a conjecture of S. Chowla*, J. Number Theory 7 (1975), 353–356.

[12] —, *Note on Waring's problem* (*mod* p), Ann. Acad. Sci. Fenn. A I 554 (1973), 7 pp.

[13] A. Winterhof, *On Waring's problem in finite fields*, Acta Arith. 87 (1998), 171–177.

Institute of Discrete Mathematics
Austrian Academy of Sciences
Sonnenfelsgasse 19
A-1010 Wien, Austria
E-mail: Arne.Winterhof@oeaw.ac.at

Received on 17.12.1999
and in revised form 25.2.2000 (3731)