ACTA ARITHMETICA
LXXXVII.2 (1998)

On Waring's problem in finite fields

by

ARNE WINTERHOF (Braunschweig)

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 $\mathbb{F}_{p^n}$.

In Section 2 we summarize the basic results on $g(k,p^n)$. In Section 3 we generalize Dodson's upper bound for small k ([5], Lemma 2.5.4):

$$g(k,p) < \lfloor 8\ln p\rfloor + 1; \qquad k \mid p-1,\ p/2 < k^2 < p,$$

and deduce

$$g(k,p^n) \le \lfloor 32\ln k\rfloor + 1 \qquad \text{for } p^n > k^2.$$

The object of Section 4 is to investigate to what extent Waring's problem for $\mathbb{F}_{p^n}$ can be reduced to the problem for $\mathbb{F}_p$. It is proven that if $g(k,p^n)$ exists, then

$$g(k,p^n) \le ng(d,p); \qquad d = \frac{k}{(k,(p^n-1)/(p-1))},\ k \mid p^n-1.$$

It is well known (see [3]) that

$$g(k,p) \le \lfloor k/2\rfloor + 1; \qquad k < (p-1)/2.$$

[15], Theorem 1, implies that if $g(k,p^n)$ exists and p is odd, then $g(k,p^n) \le \lfloor k/2\rfloor + 1$ for $k < (p^n-1)/2$. Whether p has to be odd has not been known yet. In Section 5 we show that p need not be odd.

2. Basic results on $g(k,p^n)$. Every (k,p^n-1)th power is at the same time a kth power. Hence,

$$g(k,p^n) = g((k,p^n-1),p^n). \tag{1}$$

It is sufficient to restrict ourselves to the case

$$k \mid p^n-1. \tag{2}$$

Remember that the multiplicative group $\mathbb{F}_{p^n}^*$ is cyclic. Hence

$$g(k,p^n) = 1 \Leftrightarrow k = 1. \tag{3}$$

1991 *Mathematics Subject Classification*: 11P05, 11T99.

Since $L := \{x_1^k + \ldots + x_s^k \mid x_1, \ldots, x_s \in \mathbb{F}_{p^n},\ s \in \mathbb{N}\}$ is a field ([16], Lemma 1), $g(k, p^n)$ exists if and only if L is not a proper subfield of $\mathbb{F}_{p^n}$, and thus

$$g(k,p^n) \text{ exists if and only if } \frac{p^n-1}{p^d-1} \nmid k \text{ for all } n \neq d \mid n. \tag{4}$$

This result is essentially that of [1], Theorem G.

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

Let $A_i = \{z_1^k + \ldots + z_i^k \mid z_1, \ldots, z_i \in \mathbb{F}_{p^n}\}$. If $A_i \subsetneq A_{i+1}$ then $y \in A_{i+1} \backslash A_i$ implies $xy \in A_{i+1} \backslash A_i$ for each $0 \neq x \in A_1$, so that

$$|A_{i+1}| \geq |A_i| + |A_1| - 1 = |A_i| + \frac{p^n - 1}{k}.$$

Hence in the chain $A_1 \subset A_2 \subset \ldots \subset A_s = \mathbb{F}_{p^n}$ there are at most $k-1$ strict inclusions and therefore

$$g(k, p^n) \leq k, \tag{5}$$

which is a specialization of [10], Théorème 7.14.

Equality holds for the following examples:

$$g(1,p^n) = 1, \quad g(2,p^n) = 2, \quad g\left(\frac{p-1}{2}, p\right) = \frac{p-1}{2}, \quad g(p-1,p) = p-1.$$

Since $|A_s| \leq \left(\frac{p^n-1}{k} + 1\right)^s$, we get a trivial lower bound for $g(k, p^n)$:

$$g(k,p^n) \geq \left\lceil \frac{\ln p^n}{\ln\left(\frac{p^n-1}{k}+1\right)} \right\rceil. \tag{6}$$

For $n = 1$ the following results are well known:

(7) $g(k,p) \leq \max(3, \lfloor 32 \ln k \rfloor + 1)$; $p > k^2$ [6],

(8) $g(k,p) \leq 68 (\ln k)^2 k^{1/2}$; $p > 2k+1$ [7],

(9) $g(k,p) \leq \lfloor k/2 \rfloor + 1$; $p > 2k+1$ [3],

(10) $g(k,p) \leq \left(1 + \frac{2k^2}{p-1}\right)(1 + \lfloor 2 \log_2 p \rfloor)$; $p > k^{3/2}$ [2],

(11) $g(k,p) \leq 170 \frac{k^{7/3}}{(p-1)^{4/3}} \ln p$; $p \leq k^{7/4} + 1$ [8],

(12) $g(k,p) \leq c_\varepsilon (\ln k)^{2+\varepsilon}$; $k \geq 2,\ p \geq \frac{k \ln k}{(\ln(\ln k + 1))^{1-\varepsilon}}$, $\varepsilon > 0$ [11],

(13) $g(k,p) \leq c_\varepsilon$; $k < p^{2/3-\varepsilon}$, $\varepsilon > 0$ [9].

3. Extension of Dodson's bound for small k. Now we consider the case $0 < (k-1)^2 < p^n$. In this case $g(k, p^n)$ exists.

The number $N_s(b)$; $b \in \mathbb{F}_{p^n}^*$, of solutions of the equation

$$x_1^k + \ldots + x_s^k = b; \qquad x_1, \ldots, x_s \in \mathbb{F}_{p^n},$$

can be expressed in terms of Jacobi sums ([12], Theorem 6.34)

$$N_s(b) = p^{n(s-1)} + \sum_{j_1,\ldots,j_s=1}^{k-1} \lambda^{j_1+\ldots+j_s}(b) J(\lambda^{j_1}, \ldots, \lambda^{j_s}),$$

where λ is a multiplicative character of $\mathbb{F}_{p^n}$ of order k.

Using the fact that

$$|J(\lambda^{j_1}, \ldots, \lambda^{j_s})| = \begin{cases} p^{n(s-1)/2} & \text{if } \lambda^{j_1+\ldots+j_s} \text{ is non-trivial,} \\ p^{n(s-2)/2} & \text{if } \lambda^{j_1+\ldots+j_s} \text{ is trivial} \end{cases}$$

([12], Theorem 5.22), we obtain

$$|N_s(b) - p^{n(s-1)}| \le (k-1)^s p^{n(s-1)/2}$$

and in particular

$$N_s(b) \ge p^{n(s-1)} - (k-1)^s p^{n(s-1)/2}.$$

Hence,

$$g(k, p^n) \le s \qquad \text{for } p^{n(s-1)} > (k-1)^{2s}. \tag{14}$$

For $s = 2$ this is Small's [14] result.

If $0 < \theta(k-1)^2 \le p^n$ for $\theta > 1$, then

$$s > \frac{\ln \theta(k-1)^2}{\ln \theta} \ge \frac{\ln p^n}{\ln(p^n/(k-1)^2)} \quad \text{implies} \quad p^{n(s-1)} > (k-1)^{2s},$$

and thus

$$g(k, p^n) \le \left\lfloor \frac{\ln \theta(k-1)^2}{\ln \theta} \right\rfloor + 1 \qquad \text{for } 0 < \theta(k-1)^2 \le p^n;\ \theta > 1. \tag{15}$$

We define

$$S(b) = \sum_{x \in \mathbb{F}_{p^n}} \psi(bx^k),$$

where $\psi(x) = e^{\frac{2\pi i}{p}\mathrm{Tr}(x)}$ denotes the additive canonical character. We denote by $\sum_b^*$ a summation in which $b \ne 0$ runs through a set of representatives, one from each of the $k-1$ non-power classes and one from the kth power class.

Lemma 1.

$$\sum_b{}^* |S(b)|^2 = k(k-1)p^n.$$

Proof. The deduction is the same as for Dodson's Lemma 2.5.1. We have

$$\sum_{b\in\mathbb{F}_{p^n}} |S(b)|^2 = \sum_{x,y\in\mathbb{F}_{p^n}} \sum_{b\in\mathbb{F}_{p^n}} \psi(b(x^k-y^k)) = p^n M,$$

where M denotes the number of solutions of $x^k = y^k$ in $\mathbb{F}_{p^n}$. Since $M = 1+(p^n-1)k$ and $S(0)=p^n$ we obtain

$$\sum_{b\in\mathbb{F}^*_{p^n}} |S(b)|^2 = (k-1)p^n(p^n-1).$$

The lemma follows since $S(b)$ has the same value for each element of the same class. ■

Lemma 2. *Suppose that* $x_1^k+\ldots+x_s^k$ *does not represent every element of* $\mathbb{F}_{p^n}$. *Then there exist some* $c\in\mathbb{F}^*_{p^n}$ *such that*

$$|S(mc)| > p^n\left(1-m^2\frac{\ln p^n}{s}\right); \qquad m=1,\ldots,p-1.$$

Proof. The proof is a direct extension of Dodson's proof for Lemma 2.5.2. Verify that

$$N_s(b) = p^{-n}\sum_{x_1,\ldots,x_s\in\mathbb{F}_{p^n}}\sum_{t\in\mathbb{F}_{p^n}}\psi(t(x_1^k+\ldots+x_s^k-b)) = p^{-n}\sum_{t\in\mathbb{F}_{p^n}} S(t)^s\psi(-tb)$$

and suppose that there exists a $b\in\mathbb{F}_{p^n}$ such that $N_s(b)=0$. Hence we get

$$\sum_{t\in\mathbb{F}^*_{p^n}} S(t)^s\psi(-tb) = -p^{ns}.$$

It follows that there exists an element $c\in\mathbb{F}^*_{p^n}$ such that

$$|S(c)|^s \ge \frac{p^{ns}}{p^n-1} > p^{n(s-1)},$$

whence

$$|S(c)| > p^n\exp\left(-\frac{\ln p^n}{s}\right) > p^n\left(1-\frac{\ln p^n}{s}\right),$$

which is the result for $m=1$.

For some real ϑ we have

$$|S(c)| = \sum_{x\in\mathbb{F}_{p^n}}\exp\left(\frac{2\pi i}{p}(\mathrm{Tr}(cx^k)-\vartheta)\right)$$

and thus

$$\sum_{x\in\mathbb{F}_{p^n}}\cos\left(\frac{2\pi}{p}(\mathrm{Tr}(cx^k)-\vartheta)\right) > p^n\left(1-\frac{\ln p^n}{s}\right),$$

whence

$$\sum_{x\in\mathbb{F}_{p^n}} \sin^2\left(\frac{\pi}{p}(\mathrm{Tr}(cx^k)-\vartheta)\right) < \frac{p^n \ln p^n}{2s}.$$

Since $|\sin m\varphi| \le |m\sin\varphi|$ and $\mathrm{Tr}(mx) = m\mathrm{Tr}(x)$ for $m = 1,\ldots,p-1$, we deduce that

$$\sum_{x\in\mathbb{F}_{p^n}} \sin^2\left(\frac{\pi}{p}(\mathrm{Tr}(mcx^k)-m\vartheta)\right) < \frac{m^2p^n \ln p^n}{2s},$$

whence

$$\sum_{x\in\mathbb{F}_{p^n}} \cos\left(2\frac{\pi}{p}(\mathrm{Tr}(mcx^k)-m\vartheta)\right) > p^n\left(1-\frac{m^2\ln p^n}{s}\right),$$

and thus

$$|S(mc)| > p^n\left(1-\frac{m^2\ln p^n}{s}\right). \blacksquare$$

LEMMA 3. *Suppose that* 2 *is a kth power in* $\mathbb{F}_{p^n}$ *and* $g(k,p^n)$ *exists. Then*

$$g(k,p^n) < n\left(\left\lfloor\frac{\ln p}{\ln 2}\right\rfloor+1\right).$$

P r o o f. If $g(k,p^n)$ exists, then there exists a basis $\{b_1,\ldots,b_n\}$ of kth powers. Let $x = a_1b_1 + \ldots + a_nb_n$ be any element of $\mathbb{F}_{p^n}$; $0 \le a_i < p$, $i = 1,\ldots,n$. For $i = 1,\ldots,n$ we can express a_i as

$$a_i = a_{i,0} + a_{i,1}2 + \ldots + a_{i,h_i}2^{h_i}; \qquad a_{i,j} \in \{0,1\},\ j = 0,\ldots,h_i-1,\ a_{i,h_i} = 1.$$

Since $2^{h_i} \le a_i < p$, x is a sum of at most $(h_1+1)+\ldots+(h_n+1) < n\big(\lfloor\frac{\ln p}{\ln 2}\rfloor+1\big)$ kth powers. $\blacksquare$

LEMMA 4. *If* $p^n > k^2$, *then* $g(k,p^n) < \lfloor 8\ln p^n\rfloor + 1$.

P r o o f. We suppose that for $s = \lfloor 8\ln p^n\rfloor + 1$ there exists an element $b \in \mathbb{F}_{p^n}$ that is not of the form $b = x_1^k + \ldots + x_s^k$ and obtain a contradiction.

By Lemma 2 there exists $c \in \mathbb{F}_{p^n}^*$ such that

$$|S(c)| > p^n\left(1-\frac{\ln p^n}{s}\right) > \frac{7}{8}p^n \quad\text{and}\quad |S(2c)| > p^n\left(1-\frac{4\ln p^n}{s}\right) > \frac{1}{2}p^n.$$

If 2 is not a kth power then c and $2c$ are representatives of two different classes in the sum of Lemma 1. Since $k^2 < p^n$ this gives

$$p^{2n} < \left(\frac{7}{8}\right)^2 p^{2n} + \left(\frac{1}{2}\right)^2 p^{2n} \le k(k-1)p^n < p^{2n}.$$

Hence 2 must be a kth power and Lemma 3 implies that b is a sum of $n\big(\lfloor\frac{\ln p}{\ln 2}\rfloor + 1\big) \le s$ kth powers. $\blacksquare$

COROLLARY 1. *If* $p^n/\theta \le k^2 < p^n$ *for some* $\theta > 1$, *then*

$$g(k,p^n) \le \lfloor 8\ln\theta k^2\rfloor + 1.$$

From Corollary 1 with $\theta = k^2$ and (14) with $s = 2$ we get:

THEOREM 1. *$g(k, p^n) \le \lfloor 32 \ln k \rfloor + 1$ for $p^n > k^2$.*

This generalizes [6], p. 151, (6).

4. A relation between $g(k, p^n)$ and $g(d, p)$

THEOREM 2. *If $g(k, p^n)$ exists, then*

$$g(k, p^n) \le n g(d, p); \qquad d = \frac{k}{\left(k, \frac{p^n-1}{p-1}\right)} = \frac{p-1}{\left(\frac{p^n-1}{k}, p-1\right)}.$$

Proof. If $g(k, p^n)$ exists, then there exists a basis $\{b_1, \ldots, b_n\}$ of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ consisting of kth powers.

The kth powers are exactly the $\frac{p^n-1}{k}$th roots of unity. Thus, the kth powers of elements of $\mathbb{F}_{p^n}^*$ in $\mathbb{F}_p^*$ are exactly the $\left(\frac{p^n-1}{k}, p-1\right)$th roots of unity which are the dth powers of elements of $\mathbb{F}_p^*$. Hence, all elements of $\mathbb{F}_p$ are sums of $g(d, p)$ kth powers of elements of $\mathbb{F}_{p^n}$, so that all elements of the form $b_i a$; $a \in \mathbb{F}_p$, $i = 1, \ldots, n$, are sums of $g(d, p)$ kth powers. Thus an arbitrary element $x = a_1 b_1 + \ldots + a_n b_n \in \mathbb{F}_{p^n}$; $a_i \in \mathbb{F}_p$, $i = 1, \ldots, n$, is a sum of $n g(d, p)$ kth powers. ∎

5. Extension of the Chowla/Mann/Straus bound

THEOREM 3. *If $g(k, 2^n)$ exists, then $g(k, 2^n) \le (k + 1)/2$.*

Proof. By Theorem 2 we have $g(k, 2^n) \le n$, which implies the result for

$$n \le (k + 1)/2. \tag{16}$$

Moreover, (14) with $s = 2$ implies the result for

$$2^n > (k - 1)^4. \tag{17}$$

Hence it is sufficient to consider $2 \le n \le 21$. By (4), (16) and (17) we have 12 pairs $(k, 2^n)$ to investigate: $g(3, 2^4)$, $g(7, 2^6)$, $g(5, 2^8)$, $g(7, 2^9)$, $g(11, 2^{10})$, $g(9, 2^{12})$, $g(13, 2^{12})$, $g(15, 2^{12})$, $g(21, 2^{12})$, $g(17, 2^{16})$, $g(27, 2^{18})$, and $g(33, 2^{20})$.

For $k \ge 5$ and $2^n > (k - 1)^3$ or $k \ge 7$ and $2^{3n} > (k - 1)^8$ we get the result by (14). Hence only $g(3, 2^4)$ and $g(7, 2^6)$ are undecided. It is well known that for $p^n \ne 4$ and 7 every element of $\mathbb{F}_{p^n}$ is a sum of two cubes (see [13]), which implies $g(3, 2^4) = 2$. As in the proof of Theorem 2 we get $g(7, 2^6) \le 3g(1, 2^2)$, which completes the proof. ∎

REMARK. For small k it is shown in [4] that $g(k, p^n) \le \lfloor k/2 \rfloor + 1$ for $k < \min(p, (p^n - 1)/2)$.

For arbitrary k but $p \ne 2$, [15], Theorem 1, implies $g(k, p^n) \le \lfloor k/2 \rfloor + 1$ for $k < (p^n - 1)/2$.

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] J. D. Bovey, *A new upper bound for Waring's problem* mod p, Acta Arith. 32 (1977), 157–162.

[3] 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.

[4] G. T. Diderrich and H. B. Mann, *Representations by k-th powers in* $GF(q)$, J. Number Theory 4 (1972), 269–273.

[5] M. M. Dodson, *Homogeneous additive congruences*, Philos. Trans. Roy. Soc. London Ser. A 261 (1967), 163–210.

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

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

[8] A. Garcia and J. F. Voloch, *Fermat curves over finite fields*, J. Number Theory 30 (1988), 345–356.

[9] D. R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from kth powers and for Heilbronn's exponential sum*, submitted to Quart. J. Math. Oxford.

[10] J. R. Joly, *Sommes de puissances d-ièmes dans un anneau commutatif*, Acta Arith. 17 (1970), 37–114.

[11] 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.

[12] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley, 1983.

[13] S. Singh, *Analysis of each integer as sum of two cubes in a finite integral domain*, Indian J. Pure Appl. Math. 6 (1975), 29–35.

[14] C. Small, *Sums of powers in large finite fields*, Proc. Amer. Math. Soc. 65 (1977), 35–36.

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

[16] L. Tornheim, *Sums of n-th powers in fields of prime characteristic*, Duke Math. J. 4 (1938), 359–362.

Institut für Algebra und Zahlentheorie
TU Braunschweig
Pockelsstr. 14
38106 Braunschweig, Germany
E-mail: A.Winterhof@tu-bs.de

Received on 13.3.1998
and in revised form on 13.8.1998 (3351)