#A34 INTEGERS 9 (2009), 435-440

WARING'S NUMBER IN A FINITE FIELD

James Arthur Cipra
Department of Mathematics, Kansas State University, Manhattan, Kansas
cipra@math.ksu.edu

Received: 9/24/08, Accepted: 5/8/09

Abstract

Let p be a prime, n be an integer, $k \mid p^n - 1$, and $\gamma(k, p^n)$ be the minimal value of s such that every number in $\mathbb{F}_{p^n}$ is a sum of s k^{th} powers. A known upper bound is improved to $\gamma(k, p^n) \ll nk^{1/n}$ and generalizations of Heilbronn's conjectures are proven for an arbitrary finite field.

1. Introduction

Let p be a prime, n be a positive integer, $q = p^n$, and $\mathbb{F}_q$ be the field of q elements. The smallest s (should it exist) such that

$$x_1^k + x_2^k + \cdots + x_s^k = \alpha \tag{1}$$

has a solution for all $\alpha \in \mathbb{F}_q$ is called Waring's number, denoted $\gamma(k, q)$. We will assume throughout that Waring's number exits. It is easy to show that $\gamma(k, q) = \gamma(\gcd(k, q-1), q)$; thus, we will assume that $k \mid q-1$. Similarly we define $\delta(k, q)$ to be the smallest s (should it exist) such that every element of $\mathbb{F}_q$ can be represented as sums or differences of s k^{th} powers. Note that $\delta(k, q)$ exists if and only if $\gamma(k, q)$ exists.

Let $A_k := \{x^k : x \in \mathbb{F}_q\}$, $A'_k := A_k \cap \mathbb{F}_p$. Note that $A_k^* := A_k \setminus \{0\}$ and $(A'_k)^* := (A'_k) \setminus \{0\}$ are multiplicative subgroups of $\mathbb{F}_q^*$. For any subset A in an additive group and $s \in \mathbb{N}$, we set $sA := \{a_1 + a_2 + \cdots + a_s : a_i \in A, 1 \le i \le s\}$.

Tornheim shows [11, Lemma 1] that the collection of all possible sums of k^{th} powers in $\mathbb{F}_q$ forms a subfield of $\mathbb{F}_q$. Bhaskaran shows [1, Theorem G] that this subfield is proper if and only if there exists $d \mid n$, $d \neq n$, such that $\frac{p^n-1}{p^d-1} \mid k$. Hence, to ensure the existence of $\gamma(k, q)$, we must have $\frac{p^n-1}{p^d-1} \nmid k$ for all $d \mid n$, $d \neq n$.

Winterhof has shown in [13] that, provided $\gamma(k, q)$ exists,

$$\gamma(k, q) \le 6.2n(2k)^{1/n} \ln(k). \tag{2}$$

Winterhof and van de Woestijne prove in [14] that for p and r primes with p a primitive root (mod r) we have $\gamma\left(\frac{p^{r-1}-1}{r}, p^{r-1}\right) = \frac{(r-1)(p-1)}{2}$. Thus, with $k =$

$\frac{p^{r-1}-1}{r}$ and $n = r-1$ one has the bounds:

$$\frac{n}{2}(k^{1/n}-1) \leq \gamma(k,p^n) \leq n(k+1)^{1/n}. \tag{3}$$

In light of inequality (3), we see that $nk^{1/n}$ is essentially the best possible order of magnitude for Waring's number without further restrictions. In this paper, by using some results of [5], we show the $\ln k$ factor in Winterhof's bound (2) can be dropped.

Theorem 1 *If $\gamma(k,q)$ exists, then*

$$\gamma(k,q) \leq 8n \left\lceil \frac{(k+1)^{1/n}-1}{|A_k'|-1} \right\rceil.$$

Furthermore, if $|A_k'| \geq 3$, then

$$\gamma(k,q) \leq 4n \left\lceil \frac{(k+1)^{1/n}-1}{|A_k'|-1} + 2 \right\rceil.$$

Under more stringent conditions on the number of k^{th} powers falling in the base field we can improve the exponent $1/n$ at the cost of increasing the constant.

Theorem 2 *If $\gamma(k,q)$ exists, then*

$$\gamma(k,q) \ll n(k+1)^{\frac{\log(4)}{n\log|A_k'|}} \log\log(k).$$

Furthermore, if

$$|A_k'|^{\left\lceil \frac{\log(\frac{8}{3}(k+1)^{1/n})}{\log|A_k'|} + 8/7 \right\rceil} \leq \frac{p-1}{2},$$

then

$$\gamma(k,p) \ll n(k+1)^{\frac{\log 4}{n\log|A_k'|}}.$$

In the case when q is prime, Heilbronn conjectured in [7] (and Konyagin proved in [8]) that for any $\varepsilon > 0$ we have $\gamma(k,p) \ll_\varepsilon k^\varepsilon$ for $|A_k| > c(\varepsilon)$. It is interesting to note that in this case $A_k = A_k'$. By placing the size condition on A_k' instead of A_k, we extend Heilbronn's conjecture to a general finite field.

Theorem 3 *For any $\varepsilon > 0$, if $|A_k'| \geq 4^{\frac{2}{\varepsilon n}}$, then $\gamma(k,q) \ll_\varepsilon k^\varepsilon$.*

Heilbronn further conjectured that $\gamma(k,p) \ll k^{1/2}$ for $\frac{p-1}{k} > 2$. This was established in [2, Theorem 1] and [3] gives an explicit constant: $\gamma(k,p) \leq 83k^{1/2}$. For $n \geq 2$ we obtain here:

Theorem 4

- *If $n = 2$ and $\gamma(k,p^2)$ exists, then $\gamma(k,p^2) \leq 16\sqrt{k+1}$.*
- *If $n \geq 3$ and $\gamma(k,q)$ exists, then $\gamma(k,q) \leq 10\sqrt{k+1}$.*

2. Preliminaries

Definition 5 A subset $A \subset \mathbb{F}_q$ is said to be symmetric if $A = -A$, where $-A = \{-a : a \in A\}$, and antisymmetric if $A \cap (-A) = \emptyset$.

Note that $A_k^* := A_k \backslash \{0\}$ is either symmetric or antisymmetric depending on whether $-1 \in A_k$ or not.

The next lemma is a result of Glibichuk [5, Theorems 7,8 and 9].

Lemma 6 *Let $A \subset \mathbb{F}_q$ and $B \subset \mathbb{F}_q$ with $|A||B| > q$. Then $16AB = \mathbb{F}_q$. Moreover, if B is symmetric or antisymmetric, then $8AB = \mathbb{F}_q$.*

Glibichuk [4, Corollary 4] noted that if A is a subgroup of $\mathbb{F}_q^*$ with $|A| > \sqrt{q}$, then $8A = \mathbb{F}_q$. This is an immediate consequence of Lemma 6 with $A = B$, because multiplicative subgroups are either symmetric or antisymmetric.

Corollary 7 *If $\gamma(k, q)$ exists and $k < \sqrt{q}$ then $\gamma(k, q) \leq 8$.*

Proof. The statement is trivial for $q \leq 5$, and so we may assume that $q \geq 6$. We apply Lemma 6 with $A = A_k$, $B = A_k^*$. If $k \leq \sqrt{q}$, then $|A_k||A_k^*| > q$ provided that $\left(\frac{q-1}{\sqrt{q}} + 1\right)\left(\frac{q-1}{\sqrt{q}}\right) > q$, that is, $q^{3/2} > 2q + \sqrt{q} - 1$. The latter holds for $q \geq 6$. □

Corollary 8 *If $\gamma(k, q)$ exists and $|sA_k| \geq k + 1$ for some $s \in \mathbb{N}$, then $\gamma(k, q) \leq 8s$.*

Proof. We use Lemma 6, with $A = sA_k$ and $B = A_k^*$. Note that $(sA_k)A_k^* = sA_k$ and $|A_k^*||sA_k| \geq \frac{q-1}{k}(k+1) = q - 1 + \frac{q-1}{k} > q$. □

The next three statements are useful for estimating the growth of additive sets in $\mathbb{F}_p$. The first is a reformulation of the classical result due to Cauchy and Davenport. The second is a sharpening of Cauchy–Davenport for multiplication groups from Nathanson's book [9], and the third is a recent lemma due to Glibichuk and Konyagin in [6].

Lemma 9 (Cauchy–Davenport) *For any $A \subset \mathbb{F}_p$ we have*

$$|lA| \geq \min(l(|A| - 1) + 1, p).$$

Lemma 10 ([9, Theorem 2.8]) *For any $A := \{x^k : x \in \mathbb{F}_p\} \subset \mathbb{F}_p$ with $1 < \gcd(k, p - 1) < \frac{p-1}{2}$,*

$$|lA| \geq \min((2l - 1)(|A| - 1) + 1, p).$$

Lemma 11 ([6, Lemmas 5.2 and 5.3]) *Let $N_l = \frac{5}{24}4^l - \frac{1}{3}$. If $A \subset \mathbb{F}_p$, then $|N_lA^l - N_lA^l| \geq \frac{3}{8}\min(|A|^l, (p-1)/2)$. Furthermore, if $2 \leq l \leq 1 + \frac{\log((p-1)/2)}{\log|A|}$, then $|N_lA^l| \geq \frac{3}{8}|A|^{l-8/7}$.*

Lemma 12 is a well-known corollary of Rusza's triangle inequality [9, Lemma 7.4] ($|S+T| \geq |S|^{1/2}|T-T|^{1/2}$), while Lemma 13 is a consequence of the pigeonhole principle.

Lemma 12 *[3, Equation 2.2] For any subset S of an abelian group and any positive integer j, $|jS| \geq |S-S|^{1-\frac{1}{2^j}}$. The inequality is strict for $|S| > 1$.*

Lemma 13 *If A is a subset of an abelian group G such that $|A| > |G|/2$, then $A + A = G$.*

The next lemma generalizes [3, Theorem 4.1c] from $\mathbb{F}_p$ to $\mathbb{F}_q$.

Lemma 14 *We have $\gamma(k,q) \leq 2\lceil \log\log(q) \rceil \delta(k,q)$.*

Proof. Let $j \geq \log\log(q)$ be an integer. By Lemma 12 with $S = \delta(k,q)A_k$, we have $|j\delta(k,q)A_k| > |\delta(k,q)A_k - \delta(k,q)A_k|^{1-\frac{1}{2^j}} = q^{1-\frac{1}{2^j}} \geq q/2$. Hence by Lemma 13 we have $2j\delta(k,q)A = \mathbb{F}_q$. □

3. Proofs of Theorems 1 and 2

Let $\{b_1, b_2, ..., b_n\}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ consisting of k^{th} powers in $\mathbb{F}_q$. Then the set $B_l := \{a_1b_1 + \cdots + a_nb_n : a_j \in lA'_k\}$ is a subset of $(nl)(A_k)$ with $|B_l| \geq |l(A'_k)|^n$.

To prove Theorem 1, we first take $l \geq \frac{(k+1)^{1/n}-1}{|A'_k|-1}$, giving (by Cauchy-Davenport) that $|lA'_k| \geq \min\left((k+1)^{1/n}, p\right)$. In either case $|(nl)A_k| \geq k+1$ and Corollary 8 yields the first result of Theorem 1. Now Taking $l \geq \frac{(k+1)^{1/n}-1}{2(|A'_k|-1)} + \frac{1}{2}$ gives (by Lemma 10) that $|lA'_k| \geq \min\left((k+1)^{1/n}, p\right)$. Again in either case $|(nl)A_k| \geq k+1$ and Corollary 8 yields the second result of Theorem 1.

To prove Theorem 2, we first note that Corollary 7 lets us restrict our attention to $k > \sqrt{q}$. Now set $l = \left\lceil \frac{\log(\frac{8}{3}(k+1)^{1/n})}{\log(|A'_k|)} + \frac{8}{7} \right\rceil$ and let N_l be as in Lemma 11.

`Case 1:` If $|A'_k|^l \geq \frac{p-1}{2}$ then we use the first part of Lemma 11 with the result that $|N_lA'_k - N_lA'_k| \geq \frac{3}{16}(p-1)$. By Lemma 9, $|48(N_lA'_k - N_lA'_k)| \geq \min(9p-56, p) = p$ for $p \geq 7$. If $p < 7$ we use the fact that $|A'_k| \geq 2 \geq \frac{p-1}{2}$ and $p \geq |48(N_lA'_k - N_lA'_k)| \geq |4A'_k| = p$ to establish $|48(N_lA'_k - N_lA'_k)| = p$. We now have an upper bound on $\delta(k,q)$ and hence on $\gamma(k,q)$:

$$\gamma(k,q) \ll \log\log(q)\delta(k,q) \ll \log\log(q)nN_l \ll n(k+1)^{\frac{\log 4}{n \log |A'_k|}} \log\log(k).$$

Case 2: If $|A'_k|^l \le \frac{p-1}{2}$ then we use the second part of Lemma 11 with the result that $|N_l A'_k| \ge (k+1)^{1/n}$. Hence

$$\begin{aligned}\gamma(k,q) \le 8nN_l &= 8n\left[\tfrac{5}{3}2^{\frac{15}{7}}4^{\frac{\log\frac{8}{3}}{\log|A'_k|}}(k+1)^{\frac{\log 4}{n\log|A'_k|}} - 1/3\right] \ll n(k+1)^{\frac{\log 4}{n\log|A'_k|}}\\ &\ll n(k+1)^{\frac{\log 4}{n\log|A'_k|}}\log\log(k).\end{aligned}$$

Alone this case gives the second part of the theorem. Combined with Case 1, we have the first part of the theorem.

4. Proofs of Theorems 3 and 4

Corollary 7 permits us to restrict our attention to $k > \sqrt{q}$. To prove Theorem 3 we make the further assumption: $|A'_k| > 4^{2/n\varepsilon}$. Then, $n \ll \log(k)$. Using Theorem 2, we see that

$$\gamma(k,q) \ll n(k+1)^{\frac{\log 4}{n\log|A'_k|}}\log\log(k) \ll (\log(k))^2(k)^{\frac{\log 4}{n\log|A'_k|}} \ll (\log(k))^2 k^{\varepsilon/2}.$$

The first part of Theorem 4 is easily derived from Theorem 1. For the second part of Theorem 4, we first note that for $k \le 396$ the result follows from the bound $\gamma(k,q) \le \frac{k}{2}+1$ (for $p=2$ see [12, Theorem 3], for $p \ne 2$ see [10, Theorem 1]). Thus we may assume $k \ge 396$. Corollary 7 lets us also assume $k > \sqrt{q}$. In particular, $k > 2^{n/2}$. By Theorem 1, we have, for $n \ge 18$,

$$\frac{\gamma(k,q)}{\sqrt{k+1}} \le 8n(k+1)^{1/n-1/2} \le 8n2^{\frac{n}{2}(\frac{1}{n}-\frac{1}{2})} = \frac{8\sqrt{2}n}{2^{n/4}} \le 10.$$

For $3 \le n \le 17$, we have

$$\frac{\gamma(k,q)}{\sqrt{k+1}} \le 8n(k+1)^{1/n-1/2} \le \frac{8n}{396^{1/2-1/n}} \le 10.$$

References

[1] M. Bhaskaran, *Sums of mth powers in algebraic and abelian number fields,* Arch. Math. (Basel) **17** (1966), 497-504; Correction, ibid. **22** (1972), 370-371.

[2] J. A. Cipra, T. Cochrane, and C. Pinner, *Heilbronn's conjecture on Waring's number (mod p)*, J. Number Theory **125** (2007), 289-297.

[3] T. Cochrane and C. Pinner, *Sum-product estimates applied to Waring's problem mod p*, Integers **8** (2008), A46.

[4] A. A. Glibichuk, *Combinational Properties of Sets of Residues Modulo a Prime and the Erdős-Graham Problem*, Mathematical Notes **79** (2006), No. 3 , 356-365.

[5] A. A. Glibichuk, *Additive properties of product sets in an arbitrary finite field*, preprint arXiv:0801.2021v1 [math.NT] (2008).

[6] A. A. Glibichuk and S. V. Konyagin, *Additive properties of product sets in fields of prime order,* Additive Combinatorics, CRM Proceedings and Lecture Notes **43** (2007), 279-286.

[7] H. Heilbronn, *Lecture Notes on Additive Number Theory mod p*, California Institute of Technology (1964).

[8] S.V. Konyagin, *On estimates of Gaussian sums and Waring's problem for a prime modulus*, Trudy Mat. Inst. Stelov. **198** (1992) 111-124 (Russian); Proc. Steklov Inst. Math. 1 (1994) 105-117 (English trans.).

[9] M. B. Nathanson, *Additive Number Theory*, Springer, (1996).

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

[11] L. Tornheim, *Sums of n-th Powers in Fields of Prime Characteristic,* Duke Math. J. **4** (1938), 359-362.

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

[13] A. Winterhof, *A note on Waring's problem in finite fields,* Acta Arith. **4** (2001), 365-368.

[14] A. Winterhof and C. van de Woestijne, *Exact solutions to Waring's problem for finite fields*, preprint arXiv:0810.0485v1 [math.NT] (2007).