Exact values for Waring's problem in finite fields

Christiaan van de Woestijne
Institut für Mathematik B
Technische Universität Graz, Austria

25th Journées Arithmétiques,
Edinburgh, Scotland,
2–6 July 2007

Waring's problem in finite fields

joint work with Arne Winterhof

Over a ring R, Waring's problem in degree n asks whether every element a of R can be written in the form

$$a = \sum_i a_i^n \tag{1}$$

for some $a_i \in R$, and whether the number of terms needed can be uniformly bounded for all $a \in R$.

The problem is best known over $\mathbb{Z}$, but was also much studied in the case where R is a finite field (see Winterhof (1998) for a survey).

We define the Waring function $g(k, q)$ as follows: if all $a \in \mathbb{F}_q$ have an expansion (1), then $g(k, q)$ is the maximal number of terms needed for any a; otherwise, $g(k, q)$ is undefined.

Some results on the Waring function

- We may assume that the exponent k divides $q-1$.
- If $k^2 < q$ or if q is prime, then $g(k,q)$ exists.
- A counterexample: q nonprime, $k = q-1$.
- If $g(k,q)$ exists, then $g(k,q) \leq k$ (inhomogeneous Chevalley-Warning); there is then a deterministic polynomial time algorithm to solve

$$a_1^k + \ldots + a_k^k = a.$$

- If $(k-1)^4 < q$, then $g(k,q) = 1$ or 2 (Weil bound). Assuming this, in fact, whenever $abc \neq 0$, then

$$ax^k + by^k = c$$

is solvable.

Reduction to the prime field

We have the following nice inequality: if $g(k, p^n)$ exists, then

$$g(k, p^n) \leq n g(d, p),$$

with $d = \dfrac{k}{\text{gcd}(k, \frac{p^n-1}{p-1})}$.

This follows because $g(k, p^n)$ exists if and only if

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha^k)$$

for some $\alpha \in \mathbb{F}_{p^n}$, so we have

$$a = a_0 + a_1 \alpha^k + \ldots + a_{n-1} \alpha^{(n-1)k},$$

and we write each a_i as a sum of dth powers in $\mathbb{F}_p$. Finally, more elements of $\mathbb{F}_p$ may become dth powers in the extension field.

We use this reduction in the sequel.

Basic setup and results

We have odd primes p and r, with p a primitive root modulo r. Thus,

$$\mathbb{F}_{p^{r-1}} \text{ is generated over } \mathbb{F}_p \text{ by } \zeta_r.$$

We let $k = \dfrac{p^{r-1}}{r}$ or $\dfrac{p^{r-1}}{2r}$, so kth powers are rth or $2r$th roots of unity. We compute $g(k, p^{r-1})$ for these cases:

Theorem We have

$$\begin{cases} g\left(\dfrac{p^{r-1}-1}{r}, p^{r-1}\right) = \dfrac{(p-1)(r-1)}{2}. \\ g\left(\dfrac{p^{r-1}-1}{2r}, p^{r-1}\right) = \begin{cases} \left\lfloor \dfrac{pr}{4} - \dfrac{p}{4r} \right\rfloor & \text{if } r < p; \\ \left\lfloor \dfrac{pr}{4} - \dfrac{r}{4p} \right\rfloor & \text{if } r \geq p. \end{cases} \end{cases}$$

Norm and weight

Let's call the minimal number of k'th powers needed to form a the Waring weight of a. For a vector $\mathbf{a} \in \mathbb{F}_p^r$, we write

$$\|\mathbf{a}\| = |a_0| + \ldots + |a_{r-1}|,$$

where $|a|$ is the Waring weight of a (depending on the exponent k).

Lemma Let $a = a_0 + a_1\zeta_r + \ldots + a_{r-1}\zeta_r^{r-1}$. Then the weight of a is equal to

$$\min\{\|\mathbf{a} + x\mathbf{e}\| : x \in \{0, 1, \ldots, p-1\}\}.$$

Lemma If $k = \dfrac{p^{r-1} - 1}{r}$, then $|a| =$ "a" for all $a \in \mathbb{F}_p$.

Lemma If $k = \dfrac{p^{r-1} - 1}{2r}$, then $|a| =$ "$\min\{a, p-a\}$" for all $a \in \mathbb{F}_p$.

Reformulation of the problem

We can now reformulate the Waring problem for these cases as follows.

Let $V = (\mathbb{Z}/m\mathbb{Z})^r$, let $|\cdot| : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}$ be some weight function on $\mathbb{Z}/m\mathbb{Z}$, and for $\mathbf{a} \in V$, let $\|\mathbf{a}\| = |a_0| + \ldots + |a_{r-1}|$.

We say $\mathbf{a}$ is admissible if

$$\|\mathbf{a}\| \leq \|\mathbf{a} + x\mathbf{e}\| \text{ for all } x \in \mathbb{Z}/m\mathbb{Z}.$$

Now we want to know the maximal norm of an admissible vector.

We use the weights defined earlier, i.e.,

$|a|_1$ is the smallest nonnegative integer representative of a;
$|a|_2$ is the absolute value of the symmetric integer representative of a.

An upper bound on $\|\mathbf{a}\|$

If $\|\mathbf{a}\|_i \leq \|\mathbf{a} + x\mathbf{e}\|_i$ for all x, add these and get

$$m\|\mathbf{a}\|_i \leq r \sum_{x=0}^{m-1} |x|_i. \tag{2}$$

Lemma We have

$$\sum_x |x|_1 = \frac{m(m-1)}{2} \quad ; \quad \sum_x |x|_2 = \begin{cases} \frac{m^2}{4} & \text{if } m \text{ is even} \\ \frac{m^2-1}{4} & \text{if } m \text{ is odd.} \end{cases}$$

We refine (2) a little bit by noting that

$$\|\mathbf{a} + x\mathbf{e}\|_1 \equiv \|\mathbf{a}\| + rx \pmod{m},$$

so in fact we have $\|\mathbf{a}\|_1 \leq \|\mathbf{a} + x\mathbf{e}\|_1 - |rx|_1$, and get the sharp

$$\|\mathbf{a}\|_1 \leq \frac{mr - m - r + \gcd(m,r)}{2}.$$

An aside, with an open problem

In general, assume q is a positive integer and $p \equiv 1 \pmod{q}$ is prime. Let ζ_q be a primitive qth root of unity in $\mathbb{F}_p$, and define

$$|x|_q = \min\{\,|\zeta^i x|_1 : 0 \le i \le q-1\}.$$

Note that this agrees with our earlier definition of $|\cdot|_2$.

Proposition We have for $q \ge 2$

$$\sum_x |x|_q = \left(\frac{1}{q+1} - \frac{B_q}{q!}\right) p^2 + O(p^{2-\varepsilon}),$$

where B_q is the qth Bernoulli number.

Conjecture We have

$$\sum_x |x|_3 = \frac{p^2-1}{4}.$$

Any takers??

An upper bound for $\|\mathrm{a}\|$ (continued)

Recall that $\mathbf{a} \in V = (\mathbb{Z}/m\mathbb{Z})^r$, and $|x|_2 = \min\{x, m-x\}$.

For $|\cdot|_2$, the upper bound on $\|\mathbf{a}\|_2$ for admissible vectors $\mathbf{a}$ that we get is sharp whenever $r \geq m$ or r is even. If $r < m$ and r is odd, we consider the norm sequence

$$N_x = \|\mathbf{a} + x\mathbf{e}\|,$$

and using symmetry properties of this sequence, we derive a sharp bound in this case also.

We have, for admissible $\mathbf{a} \in V$,

$$\|\mathbf{a}\|_2 \leq \begin{cases} \frac{mr}{4} & \text{if } m \text{ and } r \text{ are even;} \\ \lfloor \frac{mr}{4} - \frac{1}{2} \rfloor & \text{if } m \text{ is even, } r \text{ is odd, and } r > m; \\ \lfloor \frac{mr}{4} - \frac{r}{4m} \rfloor & \text{if } m \text{ is odd and } r \geq m; \\ \lfloor \frac{mr}{4} - \frac{1}{2} \rfloor & \text{if } m \text{ is odd, } r \text{ is even, and } r < m; \\ \lfloor \frac{mr}{4} - \frac{m}{4r} \rfloor & \text{if } r \text{ is odd and } r < m. \end{cases}$$

Matching up

To show that the given upper bounds are sharp, we need to construct admissible vectors attaining the bound.

If m and r are even, $(0,\dots,0,\frac{m}{2},\dots,\frac{m}{2})$ is admissible of norm $mr/4$, which is maximal.

If m is odd and r is even, we use $(0,\frac{m-1}{2})$ as a building block, with some cunning.

For odd r, the constructions are rather involved. First, by induction we reduce to the case that $r < 2m$. Then, we solve some integer programming problems with the goal to make the norm sequence, which has $N_{x+1} \neq N_x$ for all x, as smooth and as flat as possible. Finally, the case of odd m is derived from the case of even m.

Recapitulation

Theorem Let p and r be odd primes, with p a primitive root modulo r. Then we have

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

$$g\left(\frac{p^{r-1}-1}{2r}, p^{r-1}\right) = \begin{cases} \left\lfloor \frac{pr}{4} - \frac{p}{4r} \right\rfloor & \text{if } r < p; \\ \\ \left\lfloor \frac{pr}{4} - \frac{r}{4p} \right\rfloor & \text{if } r \geq p. \end{cases}$$

Furthermore, there exists an algorithm that shows elements in $\mathbb{F}_{p^{r-1}}$ that need this many terms when writing them as sum of kth powers (KASH 2.5 code available...).

Note that all bounds are symmetric in p and r!