More exact solutions to Waring’s problem for finite fields

by

KEIJO KONONEN (Oulu)

1. Introduction. Let $\mathbb{F}_q$ be a finite field of $q$ elements. For a positive exponent $k$, Waring’s problem for $\mathbb{F}_q$ is the question of how many summands $n$ are minimally needed to express every element of $\mathbb{F}_q$ in the form

$$\sum_{i=1}^{n} x_i^k,$$

where $x_i \in \mathbb{F}_q$ for all $i$. We define the Waring function $g(k, q)$ to be that minimal number of summands.

We shall prove the following results.

**Theorem 1.1.** Let $m$ be a positive integer and $p, r$ primes such that $p$ is a primitive root modulo $r^m$. Then

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

where $\varphi$ is Euler’s phi-function.

**Theorem 1.2.** Let $m$ be a positive integer and $p, r$ odd primes such that $p$ is a primitive root modulo $r^m$. Then

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

We note that Theorems 1.1 and 1.2 generalize Theorems 1.2 and 1.3 respectively of [3], which cover the case $m = 1$. A prime $p$ is a primitive root modulo $r^m$ for every $m \in \mathbb{Z}_+$ if $p$ is a primitive root modulo $r^2$ and $r$ is an odd prime (see [2, Theorem 9.10]). This makes it rather easy to find primes.
$p, r$ satisfying our assumptions for all values $m \in \mathbb{Z}_+$. For example a prime $p$ is a primitive root modulo $3^m$ for all $m \in \mathbb{Z}_+$ if and only if $p \equiv 2 \pmod{9}$ or $p \equiv 5 \pmod{9}$.

2. Proof of Theorem 1.1. Put $t = r^{m-1}$, $q = p^{\varphi(r^m)}$ and $k = (q-1)/r^m$. Let $\gamma$ be a primitive element of the finite field $\mathbb{F}_q$ and denote $\zeta = \gamma^k$. Then $\zeta$ is a primitive $r^m$th root of unity and all the nonzero $k$th powers in the field $\mathbb{F}_q$ are $1, \zeta, \ldots, \zeta^{r^m-1}$. Since $p$ is a primitive root modulo $r^m$, $\mathbb{F}_q$ is in fact the smallest extension field of $\mathbb{F}_p$ containing $\zeta$. Thus $\mathbb{F}_q = \mathbb{F}_p(\zeta)$ and the minimal polynomial of $\zeta$ is the $r^m$th cyclotomic polynomial $\Phi_{r^m}(x) = \Phi_r(x^t) = x^{(r-1)t} + \cdots + x^t + 1$ (see for example [3, p. 65]).

We shall use the brief notation $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ for the integers modulo $n$. A vector $\mathbf{a} = (a_0, \ldots, a_{r^m-1}) \in \mathbb{Z}_p^{r^m}$ will be called a representation for an element $a \in \mathbb{F}_q$ if

$$a = \sum_{i=0}^{r^m-1} a_i \zeta^i.$$ 

Since $\mathbb{F}_q = \mathbb{F}_p(\zeta)$, every element $a \in \mathbb{F}_q$ has such a representation. Let $\bar{x}$ denote the smallest nonnegative integer in the equivalence class $x \in \mathbb{Z}_p$ for any given class $x$. Obviously, we may then represent $a$ as a sum of $k$th powers in such a way that there are $\bar{a}_i$ summands $\zeta^i$ for every $i$ and the total number of summands is

$$||a||_1 = \sum_{i=0}^{r^m-1} a_i.$$ 

Using the terminology introduced in [3] we call a vector $\mathbf{a} \in \mathbb{Z}_p^{r^m}$ admissible (with respect to $|| \ ||_1$) if $||a||_1 \leq ||b||_1$ whenever $\mathbf{b}$ is a representation for the same element $a \in \mathbb{F}_q$ as $\mathbf{a}$. The solution $g(k, q)$ for Waring’s problem will now be the maximal value $||x||_1$ for an admissible vector $\mathbf{x} \in \mathbb{Z}_p^{r^m}$.

A vector $\mathbf{b} = (b_0, \ldots, b_{r^m-1})$ is a representation for the same element $a$ as a vector $\mathbf{a}$ if and only if there exist $c_0, \ldots, c_{t-1} \in \mathbb{Z}_p$ satisfying the equation

$$\sum_{i=0}^{r^m-1} a_i x^i = \sum_{i=0}^{r^m-1} b_i x^i + \Phi_{r^m}(x) \sum_{j=0}^{t-1} c_j x^j = \sum_{i=0}^{r^m-1} b_i x^i + \sum_{j=0}^{t-1} c_j x^j \Phi_{r^m}(x)$$

in the polynomial ring $\mathbb{Z}_p[x]$. Here

$$x^j \Phi_{r^m}(x) = x^j + x^{t+j} + \cdots + x^{(r-1)t+j}$$

for every $j = 0, \ldots, t - 1$. We define subvectors $\mathbf{a}^{(0)}, \ldots, \mathbf{a}^{(t-1)} \in \mathbb{Z}_p^r$ by the equations $\mathbf{a}^{(j)} = (a_j, a_{t+j}, \ldots, a_{(r-1)t+j})$ and similarly for $\mathbf{b}$. Also, let $\mathbf{e} = (1, \ldots, 1) \in \mathbb{Z}_p^r$. Notice that a vector $\mathbf{y} \in \mathbb{Z}_p^r$ (i.e. in the case $m = 1$)}
is admissible if and only if \( \|y\|_1 \leq \|y + ze\|_1 \) for every \( z \in \mathbb{Z}_p \). The vectors \( a, b \in \mathbb{Z}_p^m \) represent the same element if and only if all subvectors satisfy \( a^{(i)} \equiv b^{(i)} \pmod{(e)} \), where \( (e) \) denotes the submodule generated by \( e \) in the free module \( \mathbb{Z}_p^r \).

It follows that \( a \in \mathbb{Z}_p^m \) is admissible if and only if each subvector \( a^{(i)} \in \mathbb{Z}_p^r \) is admissible. Moreover, the maximal norm for an admissible vector in \( \mathbb{Z}_p^r \) is \( (p - 1)(r - 1)/2 \) by \cite{3} Theorem 2.5. Thus the maximal norm for an admissible vector \( a \in \mathbb{Z}_p^m \) is achieved precisely when all the subvectors are admissible in \( \mathbb{Z}_p^r \) of maximal norm, and it equals

\[
\|a\|_1 = \sum_{i=0}^{t-1} \|a^{(i)}\|_1 = t \cdot (p - 1)(r - 1)/2.
\]

### 3. Proof of Theorem 1.2

We shall use the notations from the previous section. Now all the \( (k/2) \)th powers in the field \( \mathbb{F}_q \) are \( 0, \pm 1, \pm \zeta, \ldots, \pm \zeta^{r^m-1} \). Suppose \( a \in \mathbb{F}_q^* \) is written as a sum of \( (k/2) \)th powers in the form

\[
a = \sum_{i=0}^{r^m-1} a_i^{(+)} \zeta^i + \sum_{i=0}^{r^m-1} a_i^{(-)} (-\zeta^i),
\]

where \( a_i^{(+)}, a_i^{(-)} \in \mathbb{Z}_p \) for every \( i \). Putting \( a_i = a_i^{(+)} - a_i^{(-)} \in \mathbb{Z}_p \) we again get a representation of the form \( (2.1) \). The corresponding vector \( a = (a_0, \ldots, a_{r^m-1}) \in \mathbb{Z}_p^m \) will again also be called a representation for \( a \).

For every \( x \in \mathbb{Z}_p \) put

\[
|x| = \min\{\bar{x}, p - \bar{x}\}.
\]

There exist \( p \) different choices of \( a_i^{(+)} \) and \( a_i^{(-)} \) that lead to the same value \( a_i \). Among these choices the smallest possible total number of summands \( \pm \zeta^i \) is \( |a_i| \). To see this, note that if we choose \( a_i^{(-)} \) arbitrarily then \( a_i^{(+)} = a_i + a_i^{(-)} \) and

\[
\bar{a}_i^{(+)} + \bar{a}_i^{(-)} = \begin{cases}
\bar{a}_i + \bar{a}_i^{(-)} + \bar{a}_i^{(-)} \geq \bar{a}_i & \text{if } 0 \leq \bar{a}_i^{(-)} < p - \bar{a}_i, \\
\bar{a}_i + \bar{a}_i^{(-)} - p + \bar{a}_i^{(-)} \geq p - \bar{a}_i & \text{if } p - \bar{a}_i \leq \bar{a}_i^{(-)} < p.
\end{cases}
\]

So instead of the norm \( \|a\|_1 \) we are interested in the so-called \textit{Lee norm}

\[
\|a\|_2 = \sum_{i=0}^{r^m-1} |a_i|.
\]

Again the solution of Waring’s problem \( g(k/2, q) \) will be the maximal norm of an admissible element; the only difference is that “admissible” is now with respect to the Lee norm \( \| \|_2 \). The rest of the proof goes as before: again \( a \) is admissible if and only if each subvector \( a^{(i)} \) is admissible and according
to [3, Theorem 2.6] the maximal Lee norm of an admissible vector of \( \mathbb{Z}_p^r \) is

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

References


Keijo Kononen
Department of Mathematical Sciences
University of Oulu
P.O. Box 3000
FIN-90014 Oulun yliopisto, Finland
E-mail: keijo.kononen@oulu.fi

Received on 19.1.2010