Functiones et Approximatio
52.2 (2015), 223–227
doi: 10.7169/facm/2015.52.2.3

COUNTING ADDITIVE DECOMPOSITIONS OF QUADRATIC RESIDUES IN FINITE FIELDS

Simon R. Blackburn, Sergei V. Konyagin, Igor E. Shparlinski

Abstract: We say that a set $\mathcal{S}$ is additively decomposed into two sets $\mathcal{A}$ and $\mathcal{B}$ if $\mathcal{S} = \{a+b \ : \ a \in \mathcal{A}, \ b \in \mathcal{B}\}$. A. Sárközy has recently conjectured that the set $\mathcal{Q}$ of quadratic residues modulo a prime p does not have nontrivial decompositions. Although various partial results towards this conjecture have been obtained, it is still open. Here we obtain a nontrivial upper bound on the number of such decompositions.

Keywords: additive decompositions, finite fields, quadratic nonresidues character sums.

1. Introduction

Given two subsets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ of the finite field $\mathbb{F}_q$ of q elements, we define their sum as

$$\mathcal{A} + \mathcal{B} = \{a + b : a \in \mathcal{A}, \ b \in \mathcal{B}\}.$$

A set $\mathcal{S} \subseteq \mathbb{F}_q$ is called *additively decomposable* into two sets if $\mathcal{S} = \mathcal{A} + \mathcal{B}$ for some sets $\mathcal{A}, \mathcal{B}$ with

$$\min\{\#\mathcal{A}, \#\mathcal{B}\} \geqslant 2.$$

Sárközy [6] has conjectured that the set $\mathcal{Q}$ of quadratic residues modulo a prime p does not have additive decompositions and shown towards this conjecture that any additive decomposition

$$\mathcal{Q} = \mathcal{A} + \mathcal{B}$$

satisfies

$$\frac{p^{1/2}}{3 \log p} \leqslant \min\{\#\mathcal{A}, \#\mathcal{B}\} \leqslant \max\{\#\mathcal{A}, \#\mathcal{B}\} \leqslant p^{1/2} \log p.$$

During the preparation of the work, the second author was supported by Russian Fund for Basic Research, Grant N. 14-01-00332, and Program Supporting Leading Scientific Schools, Grant Nsh-3082.2014.1; the third author was supported by the Australian Research Council, Grant DP140100118.

2010 Mathematics Subject Classification: primary: 11B13; secondary: 11L40

The method also works for an arbitrary finite field of odd characteristic. In [8] this result has been improved to

$$cq^{1/2} \leqslant \min\{\#\mathcal{A}, \#\mathcal{B}\} \leqslant \max\{\#\mathcal{A}, \#\mathcal{B}\} \leqslant Cq^{1/2}, \qquad (1)$$

for some absolute constants $C \geqslant c > 0$ (and also generalised to other multiplicative subgroups of $\mathbb{F}_q^*$).

Shkredov [7] has recently made remarkable progress towards the conjecture of Sárközy [6] by showing that the conjecture holds with $\mathcal{A} = \mathcal{B}$. That is, $\mathcal{Q} \neq \mathcal{A} + \mathcal{A}$ for any set $\mathcal{A} \subseteq \mathbb{F}_p$.

Furthermore, Dartyge and Sárközy [1] have made a similar conjecture for the set $\mathcal{R}$ of primitive roots modulo p. We also refer to [1, 2, 6] for further references about set decompositions.

For an odd prime power q we denote by $N(q)$ the total number of pairs $(\mathcal{A}, \mathcal{B})$ of sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ that provide an additive decomposition of the set of quadratic residues of $\mathbb{F}_q$, that is, the set $\mathcal{Q} = \{x^2 \ : \ x \in \mathbb{F}_q^*\}$. The conjecture of Sárközy [6] is equivalent to the statement that $N(q) = 0$ when q is an odd prime (and is probably true for any odd prime power as well).

The bound (1) implies

$$N(q) \leqslant \exp\left(O(q^{1/2} \log q)\right).$$

Here we obtain a more precise estimate:

Theorem 1. *For any odd prime power q, we have*

$$N(q) \leqslant \exp\left(O(q^{1/2})\right).$$

Finally, we remark that the argument we use to prove Theorem 1 can be extended to prove results on additive decompositions of many other "multiplicatively" defined sets, such as cosets of multiplicative groups and sets of primitive elements of $\mathbb{F}_q^*$. See [1, 8] for analogues of (1) for such sets.

2. Bounds of multiplicative character sums

As usual, we use the expressions $A \ll B$ and $A = O(B)$ to mean $|A| \leqslant cB$ for some constant c.

We recall the following bound on a double character sum due to Karatsuba [4], see also [5, Chapter VIII, Problem 9], which can easily be derived from the Weil bound (see [3, Corollary 11.24]) and the Hölder inequality.

Lemma 2. *For any integer $\nu \geqslant 1$, sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_q$ and nontrivial multiplicative character χ of $\mathbb{F}_q$, we have*

$$\sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \chi(u+v) \ll (\#\mathcal{U})^{1-1/2\nu} \#\mathcal{V} q^{1/4\nu} + (\#\mathcal{U})^{1-1/2\nu} (\#\mathcal{V})^{1/2} q^{1/2\nu},$$

where the implied constant depends only on ν.

We obtain the following result as a corollary of Lemma 2:

Lemma 3. *For any $\varepsilon > 0$ if for two sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_q$ with $\#\mathcal{V} \geqslant q^{\varepsilon}$ and a nontrivial multiplicative character χ of $\mathbb{F}_q$, we have $\chi(u+v) = 1$ for all pairs $(u, v) \in \mathcal{U} \times \mathcal{V}$, then $\#\mathcal{U} \ll q^{1/2}$ where the implied constant depends only on ε.*

Proof. We see from Lemma 2 that

$$\begin{aligned}\#\mathcal{U}\#\mathcal{V} &= \sum_{u\in\mathcal{U}}\sum_{v\in\mathcal{V}} \chi(u+v) \\ &\ll (\#\mathcal{U})^{1-1/2\nu}\#\mathcal{V}q^{1/4\nu} + (\#\mathcal{U})^{1-1/2\nu}(\#\mathcal{V})^{1/2}q^{1/2\nu}.\end{aligned}$$

Taking ν sufficiently large so that the first term dominates (for example, taking $\nu = \lceil (2\varepsilon)^{-1} \rceil$ so that $\#\mathcal{V} \geqslant q^{1/2\nu}$) we find that

$$\#\mathcal{U}\#\mathcal{V} \ll (\#\mathcal{U})^{1-1/2\nu}\#\mathcal{V}q^{1/4\nu},$$

which implies the result. ∎

We remark that the bounds (1) follow from Sárközy's result [6] and Lemma 3. To see this, note that the upper bound follows by taking χ to be the quadratic character in Lemma 3, and taking $\mathcal{U} = \mathcal{A}$ and $\mathcal{V} = \mathcal{B}$ (and then $\mathcal{U} = \mathcal{B}$ and $\mathcal{V} = \mathcal{A}$). The lower bound now follows since $\#\mathcal{Q} \leqslant \#\mathcal{A}\#\mathcal{B}$.

3. Proof of Theorem 1

The proof of Theorem 1 is instant from the following result, which is of independent interest.

For positive integers k and m, let $N(k, m, q)$ denote the number of pairs $(\mathcal{A}, \mathcal{B})$ of sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ with $\#\mathcal{A} = k$, $\mathcal{B} = m$ such that $\mathcal{Q} = \mathcal{A} + \mathcal{B}$.

To simplify formulas we extend the definition of binomial coefficients to all non-negative real numbers. More precisely, for a real $z \geqslant 0$ and an integer n we set

$$\binom{z}{n} = \binom{\lfloor z \rfloor}{n}.$$

Lemma 4. *For any fixed $\varepsilon > 0$ there is a constant $c > 0$ such that for all integers k and m with $q > k > q^{\varepsilon}$ and $q > m > q^{\varepsilon}$, we have*

$$N(k, m, q) \leqslant \binom{cq^{1/2}}{k}\binom{cq^{1/2}}{m}.$$

Proof. We fix a set $\mathcal{V} \subseteq \mathbb{F}_q$ of size $\#\mathcal{V} = \lfloor q^{\varepsilon/2} \rfloor$. We estimate the number $N(\mathcal{V}, k, m, q)$ of sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ with $\#\mathcal{A} = k$, $\mathcal{B} = m$ such that

$$\mathcal{Q} = \mathcal{A} + \mathcal{B} \qquad \text{and} \qquad \mathcal{V} \subseteq \mathcal{B}.$$

Let χ be the quadratic character. Let $\mathcal{U}$ be the set of elements $u \in \mathbb{F}_q$ such that for every $v \in \mathcal{V}$ we have $\chi(u+v) = 1$. We see from Lemma 3 that $\#\mathcal{U} \ll q^{1/2}$.

Any set $\mathcal{A}$ which contributes to $N(\mathcal{V}, k, m, q)$ satisfies $\mathcal{A} \subseteq \mathcal{U}$. Hence there are at most

$$\binom{\#\mathcal{U}}{k} \leqslant \binom{c_1 q^{1/2}}{k} \tag{2}$$

possibilities for $\mathcal{A}$ (where $c_1 > 0$ is some constant that depends only on ε).

Suppose now that $\mathcal{A}$ is chosen. Fixing an arbitrary set of $\lfloor q^{\varepsilon/2} \rfloor$ elements of $\mathcal{A}$ and using the same argument we see that that the remaining elements of $\mathcal{B}$ always belong to some fixed set $\mathcal{W} \subseteq \mathbb{F}_q$ of size $\#\mathcal{W} \ll q^{1/2}$. Therefore, there are at most

$$\binom{\#\mathcal{W}}{k} \leqslant \binom{c_2 q^{1/2}}{m} \tag{3}$$

possibilities for the remaining elements of $\mathcal{B}$ (where $c_2 > 0$ is some constant that depends only on ε). Hence, combining (2) and (3), we obtain

$$N(\mathcal{V}, k, m, q) \leqslant \binom{c_1 q^{1/2}}{k} \binom{c_2 q^{1/2}}{m}.$$

Summing over all choices for $\mathcal{V}$ yields

$$\begin{aligned} N(k, m, q) &\leqslant \binom{q}{q^{\varepsilon/2}} \binom{c_1 q^{1/2}}{k} \binom{c_2 q^{1/2}}{m} \\ &\leqslant q^{q^{\varepsilon/2}} \binom{c_1 q^{1/2}}{k} \binom{c_2 q^{1/2}}{m}, \end{aligned}$$

which concludes the proof. ■

Now, using the fact that $N(k, m, q) \neq 0$ only if $q^{1/2} \ll k \ll q^{1/2}$ and $q^{1/2} \ll m \ll q^{1/2}$, see (1), we easily derive Theorem 1 from Lemma 4.

References

[1] C. Dartyge, A. Sárközy, *On additive decompositions of the set of primitive roots modulo p*, Monat. Math. **169** (2013), 317–328.

[2] C. Elsholtz, *A survey on additive and multiplicative decompositions of sumsets and of shifted sets*, Combinatorial Number Theory and Additive Group Theory, Birkhäuser, 2009, 213–231.

[3] H. Iwaniec, E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[4] A.A. Karatsuba, *The distribution of values of Dirichlet characters on additive sequences*, Doklady Acad. Sci. USSR **319** (1991), 543–545 (in Russian).

[5] A.A. Karatsuba, *Basic analytic number theory*, Springer-Verlag, 1993.

[6] A. Sárközy, *On additive decompositions of the set of quadratic residues modulo p*, Acta Arith. **155** (2012), 41–51.

[7] I.D. Shkredov, *Sumsets in quadratic residues*, Acta Arith. **164** (2014), 221–243.
[8] I.E. Shparlinski, *Additive decompositions of subgroups of finite fields*, SIAM J. Discr. Math. **27** (2013), 1870–1879.

Addresses: Simon R. Blackburn: Department of Mathematics, Royal Holloway University of London, Egham, Surrey, TW20 0EX, UK;
Sergei V. Konyagin: Steklov Mathematical Institute, 8, Gubkin Street, Moscow, 119991, Russia;
Igor E. Shparlinski: Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052 Australia.

E-mail: s.blackburn@rhul.ac.uk, konyagin@mi.ras.ru, igor.shparlinski@unsw.edu.au

Received: 11 March 2014; **revised:** 6 May 2014