ACTA ARITHMETICA
164.3 (2014)

Sumsets in quadratic residues

by

I. D. Shkredov (Moscow and Yaroslavl')

1. Introduction. Let p be a prime number, $\mathbb{F}_p$ the finite field, and R the set of all quadratic residues. In other words, R is the set of all squares in $\mathbb{F}_p \setminus \{0\}$. There are many interesting conjectures about the set R (see e.g. [6, 15, 17]). We begin with one of A. Sárközy [17]:

Conjecture A. *The set R cannot be represented as $R = A + B$ where the cardinality of each set A, B is at least 2.*

Here, as usual,

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

We also define, for a set $A \subseteq \mathbb{F}_p$,

$$A \hat{+} A := \{a + a' : a, a' \in A,\, a \neq a'\}.$$

In [17] the following result was obtained (see also [7]).

Theorem 1.1. *Let p be a prime number. Suppose that $R = A + B$ with $|A|, |B| \geq 2$. Then*

$$\frac{p^{1/2}}{3 \log p} < |A|, |B| < p^{1/2} \log p.$$

Some generalizations and improvements of Theorem 1.1 can be found in [7, 21].

Another well-known conjecture (see e.g. [6]) states, in particular, the following:

Conjecture B. *Let $\varepsilon \in (0, 1)$ and let p be a sufficiently large prime number. Suppose that $A + A \subseteq R$ or $A - A \subseteq R \sqcup \{0\}$. Then $|A| \ll p^{\varepsilon}$.*

Some results in this direction can be found in [1, 5, 10]. At the moment the best known bound has the form $|A| \ll \sqrt{p}$ (see e.g. [1]). A lower bound for the case $A - A \subseteq R \sqcup \{0\}$ is due to S. Graham and C. Ringrose [10]. It asserts that $|A| \gg \log p \cdot \log\log\log p$ for infinitely many primes p. A uniform

2010 *Mathematics Subject Classification*: 11B13, 11B50, 11B75.
Key words and phrases: quadratic residues, sumsets.

DOI: 10.4064/aa164-3-2

lower bound of the form $|A| \geq (1/2 + o(1)) \log p$, where p is an arbitrary prime, can be found in [5]. Conjecture B can be reformulated in terms of the clique number of the Paley graph P_p (see e.g. [3]).

Exponential sums with multiplicative characters over sumsets have been studied by various authors (see e.g. [4], [8], [9], [13]–[15]). The classical general result of [8], [9] states that

$$\sigma(A,B) := \Big| \sum_{x\in B,\, y\in A} \chi(x+y)\Big| \leq \sqrt{|A|\,|B|p} \tag{1}$$

for any sets $A, B \subseteq \mathbb{F}_p$ and an arbitrary nonprincipal multiplicative character χ. The bound is nontrivial if $|A|\,|B| > p^{1+\delta}$ with some $\delta > 0$. A. A. Karatsuba and M.-C. Chang contributed significantly to the theory of such exponential sums. For example, Karatsuba proved a nontrivial upper bound for $\sigma(A,B)$ provided $|A| > p^{\varepsilon_1}$ and $|B| > p^{1/2+\varepsilon_2}$ with $\varepsilon_1, \varepsilon_2 > 0$. Chang obtained plenty of results for specific A and B, e.g. when A has small sumset or, conversely, A is a well-spaced set (see [4] for details). In his survey [15] Karatsuba formulated the following conjecture (see Problem 6 there).

Conjecture C. *Let $A, B \subseteq \mathbb{F}_p$ with $|A|, |B| \sim \sqrt{p}$. Then*

$$\Big| \sum_{x\in B,\, y\in A} \chi(x+y)\Big| \leq c(\delta)|A|\,|B|p^{-\delta}, \quad \delta > 0. \tag{2}$$

The last conjecture in this section, also called the Paley graph conjecture (see e.g. [4]), predicts a nontrivial upper bound for the sum (1) for $|A|, |B| > p^{\varepsilon}$ with $\varepsilon > 0$.

Conjecture D. *Let $A, B \subseteq \mathbb{F}_p$ with $|A|, |B| > p^{\varepsilon}$ for some $\varepsilon > 0$. Then*

$$\Big| \sum_{x\in B,\, y\in A} \chi(x+y)\Big| \leq c(\varepsilon)|A|\,|B|p^{-\delta}, \quad \text{where } \delta = \delta(\varepsilon) > 0. \tag{3}$$

Clearly, Conjecture D is the strongest one and implies the others. Trivially, Conjecture A follows from Conjecture B or C. It is known that the corresponding functional version of Conjecture C is false: see e.g. Section 5.

In this paper we give a partial result on Conjecture A. Let us formulate our main theorem.

Theorem 1.2. *Let p be a prime number, $R \subseteq \mathbb{F}_p$ be the set of all quadratic residues and $A \subseteq \mathbb{F}_p$ be a set.*

(i) *If $A + A = R$ then $p = 3$ and $A = \{2\}$.*
(ii) *If $A \hat{+} A = R$ then $p = 3, 7, 13$ and there are just four possibilities for A: see Example* 4.1.

Also, we improve Theorem 1.1 a little as well as consider the cases of approximate equalities, in some sense, that is, $A+A \approx R$ and $A\hat{+}A \approx R$ (see

Sections 3, 4). Note that an improvement of Sárközy's theorem was obtained independently by I. Shparlinski [21] using Karatsuba's bound from [14]. As for Conjecture B, we reprove a recent result of C. Bachoc, M. Matolcsi and I. Z. Ruzsa [1] in this direction. Interestingly, our method does not use the main lemma of [1].

In their proof the authors of [17, 7, 21] used the well-known Weil bound for exponential sums with multiplicative characters (see e.g. [12])

$$\Big|\sum_x \chi(x)\chi(x+x_1)\dots\chi(x+x_d)\Big| \le (d-1)\sqrt{p} \tag{4}$$

for distinct nonzero $x_1,\dots,x_d \in \mathbb{F}_p$ and any nonprincipal character χ, as well as some combinatorial tools. Our main idea exploits the fact that quadratic residues are "more random than a random set", and hence are far from being random. The last statement is the most transparent in the case $p \equiv 3 \pmod 4$ (or, equivalently, $\left(\frac{-1}{p}\right) = -1$, in terms of the Legendre symbol). It is known that R is then a perfect difference set (see e.g. Lemma 2.8 from Section 2), that is, the number of solutions $x = a - b$ with $a, b \in R$ does not depend on $x \neq 0$. Of course a random set of density $1/2$ has this property with probability zero. So, since we use these properties of R instead of its random behavior it is very natural that perfect difference sets appear in our proofs. For example, all sets A from the second part of Theorem 1.2 turn out to be perfect difference sets.

2. Notation and auxiliary results. We start with definitions and notation used in the paper. Let $\mathbf{G}$ be a finite abelian group. It is well-known [16] that the dual group $\widehat{\mathbf{G}}$ is isomorphic to $\mathbf{G}$. Let f be a function from $\mathbf{G}$ to $\mathbb{C}$. We denote the Fourier transform of f by $\widehat{f}$,

$$\widehat{f}(\xi) = \sum_{x\in\mathbf{G}} f(x)e(-\xi\cdot x), \tag{5}$$

where $e(x) = e^{2\pi i x}$. We rely on the following basic identities:

$$\sum_{x\in\mathbf{G}} f(x)\overline{g}(x) = \frac{1}{|\mathbf{G}|}\sum_{\xi\in\widehat{\mathbf{G}}} \widehat{f}(\xi)\,\overline{\widehat{g}(\xi)}, \tag{6}$$

$$\sum_{y\in\mathbf{G}}\Big|\sum_{x\in\mathbf{G}} f(x)g(y-x)\Big|^2 = \frac{1}{|\mathbf{G}|}\sum_{\xi\in\widehat{\mathbf{G}}} |\widehat{f}(\xi)|^2|\widehat{g}(\xi)|^2. \tag{7}$$

Set

$$(f*g)(x) := \sum_{y\in\mathbf{G}} f(y)g(x-y),$$

$$(f\circ g)(x) := \sum_{y\in\mathbf{G}} f(y)g(y+x) = (g\circ f)(-x).$$

Then

$$\widehat{f*g} = \widehat{f}\,\widehat{g} \quad \text{and} \quad \widehat{f\circ g} = \widehat{\overline{f}}\,\widehat{g} = \widehat{f^c}\widehat{g}. \tag{8}$$

Note also that

$$\begin{aligned}(f*g)(x) &= (f^c\circ g)(x) = (f\circ g^c)(-x),\\ (f\circ g)(x) &= (f^c * g)(x) = (f * g^c)(-x),\end{aligned} \tag{9}$$

where for a function $f:\mathbf{G}\to\mathbb{C}$ we put $f^c(x) := f(-x)$. Clearly, $(f*g)(x) = (g*f)(x)$ for all $x\in\mathbf{G}$. By $\langle f,g\rangle$ denote the scalar product of two complex functions f and g. Put $\langle f\rangle = \langle f,1\rangle$, where 1 is the constant function on $\mathbf{G}$. We will write $\sum_x$ and $\sum_\xi$ instead of $\sum_{x\in\mathbf{G}}$ and $\sum_{\xi\in\widehat{\mathbf{G}}}$ for simplicity.

We use the same letter to denote a set $S\subseteq\mathbf{G}$ and its characteristic function $S:\mathbf{G}\to\{0,1\}$. We let $|S|$ denote the cardinality of S. Given $a\in\mathbf{G}$ we write $\delta_a(x)$ for the delta function at a. For a positive integer n, we set $[n]=\{1,\dots,n\}$. All logarithms are of base 2. The signs $\ll$ and $\gg$ are the usual Vinogradov symbols.

For a sequence $s=(s_1,\dots,s_k)\in\mathbf{G}^k$ put $A_s = A\cap(A-s_1)\cap\dots\cap(A-s_k)$. Let

$$\mathsf{E}_{k+1}(A) = \sum_{x\in\mathbf{G}}(A\circ A)^{k+1}(x) = \sum_{s_1,\dots,s_k\in\mathbf{G}}|A_s|^2. \tag{10}$$

If $k=1$ then $\mathsf{E}_2(A)$ is denoted by $\mathsf{E}(A)$ and is called the *additive energy* of A (see [22]). Some results on the quantities $\mathsf{E}_k(A)$ can be found in [18, 20]. For any complex function f and positive integer k denote

$$\mathcal{C}_{k+1}(f)(x_1,\dots,x_k) = \sum_z f(z)f(z+x_1)\dots f(z+x_k).$$

The next lemma is a very special case of [19, Lemma 4] and is the simplest generalization of the second formula from (10).

LEMMA 2.1. *Let f,g be complex functions on an abelian group $\mathbf{G}$, and k a positive integer. Then*

$$\sum_{x_1,\dots,x_k}\mathcal{C}_{k+1}(f)(x_1,\dots,x_k)\mathcal{C}_{k+1}(g)(x_1,\dots,x_k) = \sum_z (f\circ g)^{k+1}(z).$$

Now consider the case when $\mathbf{G}$ is a field. If $q=p^s$ with p a prime number then we write $\mathbb{F}_q$ for the finite field of order q. In the case $q=p$ we denote by R and N the sets of quadratic residues and nonresidues of $\mathbb{F}_p$, respectively. Clearly, $|R|=|N|=(p-1)/2=:t$, and $0\notin R$, $0\notin N$. Let χ_0 denote the principal character, and χ the character induced by the Legendre symbol on $\mathbb{F}_p$. Given a nonzero $\lambda\in\mathbb{F}_p$ and a set $A\subseteq\mathbb{F}_p$ we will write

$$\lambda\cdot A := \{\lambda\cdot a : a\in A\}.$$

Thus $2A := A+A \neq 2\cdot A$ in general.

DEFINITION 2.2. Let φ, ψ be characters on $\mathbb{F}_q$. The *Jacobi sum* $J(\chi, \psi)$ is defined by

$$J(\varphi, \psi) = \sum_x \varphi(x)\psi(1-x).$$

We need a lemma (see [2, Chapters 1, 2]).

LEMMA 2.3. *For any nonprincipal character ψ, we have*

$$J(\psi, \overline{\psi}) = -\psi(-1). \tag{11}$$

Hence

$$(\psi \circ \overline{\psi})(x) = p\delta_0(x) - 1, \qquad (\psi * \overline{\psi})(x) = \chi(-1)(p\delta_0(x) - 1). \tag{12}$$

Further

$$G(p) := \sum_x \chi(x) e^{2\pi i x/p} = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \bmod 4, \\ i\sqrt{p} & \text{if } p \equiv -1 \bmod 4. \end{cases}$$

In particular, $|\widehat{R}(x)| \le (\sqrt{p}+1)/2$ for any $x \ne 0$.

Proof. Indeed, by the definition of the Gauss sum, for all $x \in \mathbb{F}_p$ we have

$$\widehat{R}(x) = \tfrac{1}{2}(p\delta_0(x) - 1 + G(p)\chi(-x)),$$

and the result follows. ∎

The following formulas are well-known and can also be derived from Lemma 2.3.

LEMMA 2.4. *Let $g, h : \mathbb{F}_p \to \mathbb{C}$ be any functions. Then*

$$\Big|\sum_{x,y} g(x)h(y)\chi(x+y)\Big| \le \|g\|_2 (p\|h\|_2^2 - |\langle h \rangle|^2)^{1/2} \le \|g\|_2 \|h\|_2 \sqrt{p}, \tag{13}$$

and

$$((g \circ \chi) \circ (h \circ \chi))(x) = p(h \circ g)(x) - \langle g \rangle \cdot \langle h \rangle. \tag{14}$$

In particular

$$\sum_z (g \circ \chi)(x)\, \overline{(h \circ \chi)(x)} = p\langle g, h \rangle - \langle g \rangle \cdot \langle \overline{h} \rangle. \tag{15}$$

Note that inequality (13) is sharp (see e.g. Section 5). Formula (15) of the lemma above implies the "Cauchy–Schwarz" inequality in $\mathbb{F}_p$:

COROLLARY 2.5. *For any complex function $f : \mathbb{F}_p \to \mathbb{C}$, we have*

$$\|f\|_2^2 = \frac{|\langle f \rangle|^2}{p} + \frac{1}{p}\sum_x |(f \circ \chi)(x)|^2 \ge \frac{|\langle f \rangle|^2}{p}. \tag{16}$$

Also, using Lemma 2.4 one can obtain simple upper bounds for the cardinalities of sets A, B such that $A+B \subseteq R$ or $A+B \subseteq N$ (see e.g. the proof of Theorem 3.2 below or [3, 6]).

Applying Lemma 2.1 we can easily improve [17, Theorem 1.1] (a similar result was obtained in [21]).

COROLLARY 2.6. *Let $A+B=R$. Then as $p\to\infty$,*

$$(1/6-o(1))\sqrt{p}\le |A|,|B|\le (3+o(1))\sqrt{p}.$$

Proof. We can assume that the sets A and B are sufficiently large (see [17]). By Lemma 2.1, we have

$$|A|^4|B|=\sum_{x\in B}(\chi\circ A)^4(x)\le\sum_x(\chi\circ A)^4(x)=\sum_{x,y,z}\mathcal{C}_4(\chi)(x,y,z)\mathcal{C}_4(A)(x,y,z).$$

Formula (4) gives

$$|\mathcal{C}_4(\chi)(x,y,z)|\le 3\sqrt{p}$$

with three exceptions: $x=y\ne 0$, $z=0$; $x=z\ne 0$, $y=0$; and $y=z\ne 0$, $x=0$. Thus

$$|A|^4|B|\le 3\sqrt{p}\,|A|^4+3p|A|^2$$

and we infer that $|A|,|B|\le(3+o(1))\sqrt{p}$. Because $|A|\,|B|\ge t=(p-1)/2$, we get $|A|,|B|\ge(1/6-o(1))\sqrt{p}$. ∎

To end this section, we recall the notion of perfect difference sets.

DEFINITION 2.7. Let $\mathbf{G}$ be a group. A set $A\subseteq\mathbf{G}$ is called a *perfect difference set* if the convolution $(A\circ A)(x)$ does not depend on the choice of $x\ne 0$.

Since $(A\circ A)(0)=|A|$, the definition above says that $(A\circ A)(x)=(|A|-\lambda)\delta_0(x)+\lambda$, where $\lambda\ge 1$ is some constant. We will say that A is a *λ-perfect difference set* in this case and just a *perfect difference set* for $\lambda=1$. Generally speaking, let $\mathcal{L}$ be the algebra of functions of the form $a\delta_0(x)+b$, where a and b are some complex constants. Clearly, $\varphi\in\mathcal{L}$ iff $\widehat{\varphi}\in\mathcal{L}$.

Denote by $\mathcal{D}$ the set of all *perfect difference functions*, that is, all functions φ such that $\varphi\circ\varphi$, or equivalently $\widehat{\varphi}^c\cdot\widehat{\varphi}$, belongs to $\mathcal{L}$. For example, Lemma 2.3 says that $\chi\in\mathcal{D}$. It is easy to check that $\mathcal{D}$ is closed under both convolutions $*$ and $\circ$. Moreover, if $\varphi\in\mathcal{D}$ with $\widehat{\varphi}(x)\ne 0$ for all $x\in\mathbf{G}$ and $\varphi\circ\psi$ or $\varphi*\psi$ is in $\mathcal{D}$ then $\psi\in\mathcal{D}$. Finally, if $f\in\mathcal{D}$ then $\alpha+\beta f\in\mathcal{D}$ for any $\alpha,\beta\in\mathbb{C}$.

We need a simple lemma.

LEMMA 2.8. *For all $x\ne 0$, we have*

$$(R\circ R)(x)=\frac{p-3}{4}-\frac{\chi(x)}{4}\left(1+\chi(-1)\right). \tag{17}$$

Proof. Since $R(x) = \frac{1}{2}(\chi_0(x) + \chi(x))$, it follows that for $x \neq 0$,

$$(R \circ R)(x) = \frac{1}{4}\sum_z (\chi_0(z) + \chi(z))(\chi_0(z+x) + \chi(z+x))$$
$$= \frac{p-2}{4} - \frac{1}{4}(\chi(x) + \chi(-x)) + \frac{1}{4}\sum_z \chi(z(z+x)),$$

and the result follows from Lemma 2.3. ∎

In particular, if $p \equiv -1 \pmod 4$ then $R \in \mathcal{D}$.

Let $A \subseteq \mathbb{Z}_P$ be a perfect difference set. A residue m is called a *multiplier* of A if $mA = A$. We recall the multiplier theorem (see e.g. [11]).

THEOREM 2.9. *Let $A \subseteq \mathbb{Z}_P$ be a λ-perfect difference set and m be any prime number such that $m \,|\, (|A| - \lambda)$, $(m, P) = 1$ and $m > \lambda$. Then m is a multiplier of some translation of A.*

Clearly, the set of multipliers of A forms a group and, moreover, one can choose a translation of A fixed by the group (see [11]).

Recall also a beautiful theorem of Singer (see e.g. [11]) related to finite projective geometries.

THEOREM 2.10. *Suppose that P is a number of the form $P = n^2 + n + 1$, $n = q^s$, where $s \geq 1$ and q is a prime number. Then there is a perfect difference set $A \subseteq \mathbb{Z}_P$ such that $(A \circ A)(x) = 1$ for all $x \neq 0$.*

3. Sumsets and differences. We begin with a simple lemma.

LEMMA 3.1. *Let c be an integer and $\psi : \mathbf{G} \to \mathbb{Z}$ be a function. Then*

$$\|\psi\|_2^2 \geq c\Big|\sum_x \psi(x)\Big| - (c-1)\cdot\Big|\sum_{x:\, 0<|\psi(x)|<c} \psi(x)\Big|. \tag{18}$$

Further

$$\|\psi\|_2^2 = c\sum_x \psi(x) + \sum_k |\{x : \psi(x) = k\}|\cdot(k^2 - ck). \tag{19}$$

Proof. Let $\sigma = \sum_x \psi(x)$. We can suppose that $\sigma > 0$, otherwise consider the function $-\psi$. For any integer k put

$$p_k = |\{x : \psi(x) = k\}|.$$

Then

$$\sigma = \sum_k k p_k = \sum_{k:\, |k| \geq c} k p_k + \sum_{k:\, 0<|k|<c} k p_k =: \sigma_1 + \sigma_2,$$

and hence

$$\|\psi\|_2^2 = \sum_k k^2 p_k = \sum_{k:\,|k|\ge c} k^2 p_k + \sum_{k:\,0<|k|<c} k^2 p_k \ge c\sigma_1 + \sigma_2 = c\sigma - (c-1)\sigma_2$$
$$\ge c\sigma - (c-1)|\sigma_2|$$

as required. Formula (19) follows similarly. ∎

Now we can prove a minor generalization of the first part of our main Theorem 1.2.

THEOREM 3.2. *Let p be a prime number, $R \subseteq \mathbb{F}_p$ be the set of quadratic residues and $A \subseteq \mathbb{F}_p$ be a set. If $A + A = R$ then $p = 3$ and $A = \{2\}$. Moreover for all sufficiently large p, we have*

$$\max\Big\{|R \setminus (A+A)|, \sum_{x\in(A+A)\setminus R} (A*A)(x)\Big\} \ge (1/6 - o(1))|A|. \tag{20}$$

Proof. Suppose that A, B are sets such that $A + B \subseteq R$. Let $a = |A|$ and $b = |B|$. Define the function $\varepsilon(x)$ by the formula

$$(A \circ \chi)(x) = aB(x) + \varepsilon(x). \tag{21}$$

We have $\varepsilon(x) = 0$ for all $x \in B$. Using Lemma 2.4, we get

$$\|\varepsilon\|_2^2 = pa - a^2 - a^2 b. \tag{22}$$

Further

$$\langle \varepsilon \rangle = -ab, \tag{23}$$

thus, by the Cauchy–Schwarz inequality,

$$a^2 b^2 \le (p-b)(pa - a^2 - a^2 b),$$

that is,

$$p + \frac{ab}{p} \ge ab + a + b. \tag{24}$$

On the other hand, by formula (13) of Lemma 2.4 or just by equality (22), one has $ab < p$.

Now suppose that $A = B$ and $A + A = R$. If $a = 1$ then $(p-1)/2 = 1$, whence $p = 3$ and clearly $A = \{2\}$. Thus, suppose that $a > 1$. From $A + A = R$, we obtain $\binom{a}{2} + a \ge (p-1)/2$, so $a^2 + a \ge p - 1$. Using this estimate, the fact that $a^2 < p$ and inequality (24), we get

$$p + 1 > p + \frac{a^2}{p} \ge a^2 + 2a \ge p - 1 + a,$$

a contradiction.

Now, let us prove the "moreover" part of the theorem. Put

$$|R \setminus (A+A)| =: \zeta_1 a \quad \text{and} \quad \sum_{x \in (A+A)\setminus R} (A*A)(x) =: \zeta_2 a.$$

Let also $\zeta = \max\{\zeta_1, \zeta_2\}$. We will obtain a lower bound for ζ. Suppose that $\zeta \le 1/6 + o(1)$ as $p \to \infty$. We have

$$\binom{a}{2} + a \ge \frac{p-1}{2} - \zeta_1 a \ge \frac{p-1}{2} - \zeta a,$$

so that

$$a^2 + a(1+2\zeta) \ge p - 1. \tag{25}$$

Put

$$(A \circ \chi)(x) = aA(x) + \varepsilon(x).$$

As in (23), the average value of ε equals $-a^2$, and we compute the l_2-norm of ε as in (22):

$$\begin{aligned} \|\varepsilon\|_2^2 &= \sum_x ((A\circ\chi)(x) - aA(x))^2 = pa - a^2 + a^3 - 2a\sum_{x\in A}(A\circ\chi)(x) \\ &= pa - a^2 - a^3 + 2a\sum_x (1-\chi(x))(A*A)(x) \\ &= pa - a^2 - a^3 + 2a \sum_{x\in(A+A)\setminus R} (1-\chi(x))(A*A)(x) \\ &\le pa - a^2 - a^3 + 4\zeta a^2. \end{aligned} \tag{26}$$

By the Cauchy–Schwarz inequality,

$$a^4/p \le \|\varepsilon\|_2^2 \le pa - a^2 - a^3 + 4\zeta a^2. \tag{27}$$

Note that this yields $a \ll \sqrt{p}$. Using (27) and (25), after some calculations we obtain $\zeta \ge 1/6 - o(1)$. This completes the proof. ∎

Now we reprove a result of C. Bachoc, M. Matolcsi and I. Z. Ruzsa from [1].

THEOREM 3.3. *Let p be a prime number, $R \subseteq \mathbb{F}_p$ be the set of quadratic residues and $A \subseteq \mathbb{F}_p$ be a set. If $A - A \subseteq R \sqcup \{0\}$ then*

$$p \ge \begin{cases} |A|^2 + |A| - 1 & \text{if } |A| \text{ is even,} \\ |A|^2 + 2|A| - 2 & \text{if } |A| \text{ is odd.} \end{cases}$$

Proof. Put $|A| = a$. Clearly, $p \equiv 1 \pmod 4$. As in the previous theorem, we have

$$(A * \chi)(x) = (a-1)A(x) + \varepsilon(x), \tag{28}$$

where $\varepsilon(x) = 0$ for $x \in A$. As above

$$\|\varepsilon\|_2^2 = pa - a^2 - a(a-1)^2 \quad \text{and} \quad \langle \varepsilon \rangle = -a(a-1).$$

Further

$$\varepsilon(x) = |R \cap (x-A)| - |N \cap (x-A)| = 2|R \cap (x-A)| - a \tag{29}$$

for all $x \notin A$. First of all consider the case where a is even. By (29) the values of $\varepsilon(x)$ are even for all x (recall that $\varepsilon(x) = 0$ on A). Using Lemma 3.1 with $c = 2$, we obtain

$$\|\varepsilon\|_2^2 = pa - a^2 - a(a-1)^2 \geq 2a(a-1),$$

so $p \geq a^2 + a - 1$, as required.

Now suppose that a is odd and $a > 1$. Of course $\varepsilon(x) = 0$ on A, and by (29) all other values of $\varepsilon(x)$ are odd. Note that there is $x \notin A$ such that $\varepsilon(x) \neq -1$. Indeed, otherwise, applying (28), we get

$$\langle A, \chi\rangle = \langle \varepsilon, \chi\rangle = pA(0) - a - (a-1)\langle A, \chi\rangle. \tag{30}$$

Shifting, we can suppose that $0 \in A$, and hence $\langle A, \chi\rangle = a - 1$. Substituting into (30) gives $p = a^2$, a contradiction. (Note that nevertheless there is no contradiction for the field $\mathbb{F}_q$ with q a prime power, and moreover our result does not hold for the field, see [1].)

Another proof of the fact that there is $x \notin A$ with $\varepsilon(x) \neq -1$ is the following. Put $p_k := |\{x \in \mathbb{F}_p : \varepsilon(x) = k\}|$ for $k \in \mathbb{Z}$. Consider $\varepsilon(x) \pmod p$ and note that $\chi(x) \equiv x^{(p-1)/2} \pmod p$. Then we see that the quantity p_{-1} does not exceed $(p-1)/2$.

As before, using formula (19) of Lemma 3.1 with $c = -2$ and the bound $p_{-1} \leq (p-1)/2$, we obtain

$$\begin{aligned}\|\varepsilon\|_2^2 = pa - a^2 - a(a-1)^2 &= -2\langle\varepsilon\rangle + \sum_k (k^2+2k)p_k \\ &\geq 2a(a-1) - p_{-1} + 3\sum_{k\neq -1,0} p_k \\ &= 2a(a-1) + 3p - 4p_{-1} - 3a \geq 2a(a-1) + p + 2 - 3a,\end{aligned}$$

so

$$p \geq a^2 + a - 4 + \frac{p+2}{a}.$$

After some calculations we get $p \geq a^2 + 2a - 2$, provided $a > 1$. ∎

4. Restricted sumsets. The aim of the section is to prove the second part of our main Theorem 1.2.

Write any prime p as $p = n^2 + \Delta$, $1 \leq \Delta \leq 2n$. We are interested in sets $A \subseteq \mathbb{F}_p$ such that $A \hat{+} A = R$. Let us consider some examples.

Example 4.1. The following are examples of *perfect difference sets* $A \subseteq \mathbb{F}_p$ with $A \hat{+} A = R$:

(a) $p = 3$, $A = \{0, 1\}$,

(b) $p=7$, $A=\{3,5,6\}$,
(c) $p=13$, $A=\{0,1,3,9\}$, $A=\{0,4,10,12\}$.

Note that in all these examples $p=n^2+n+1$, $|A|=n+1$, $n=q^s$, q is a prime number or 1. In particular $\Delta=n+1$. The existence of a perfect difference set in $\mathbb{F}_p$ for p of such a form is guaranteed by Singer's Theorem 2.10. Note also that it is easy to check using the multiplier theorem and other tools (see the beginning of the proof of Proposition 4.2 and Theorem 4.3 below) that the sets above form a complete list of (perfect difference) sets $A\subseteq\mathbb{F}_p$ with $A\hat{+}A=R$ for $p=3,7,13$.

In our proof of the second part of Theorem 1.2 we begin with the situation when A is a perfect difference set. Surprisingly, it turns out that this is the most important case.

PROPOSITION 4.2. *Let p be a prime number, $p=n^2+n+1$, $R\subseteq\mathbb{F}_p$ be the set of quadratic residues and $A\subseteq\mathbb{F}_p$ be a perfect difference set. Suppose that $A\hat{+}A=R$. Then A is one of the sets in Example* 4.1.

Proof. Let $a=|A|$. Because A is a perfect difference set, we have $a=n+1$. First, $(A\hat{+}A)\cap 2\cdot A=\emptyset$ and so $R\cap 2\cdot A=\emptyset$. In particular, either $A\subseteq R\sqcup\{0\}$ or $A\subseteq N$. Second, by Theorem 2.9 there is $s\in\mathbb{F}_p$ such that the set $A+s$ is fixed by a multiplier $m\neq 1$. Then $(A+s)\hat{+}(A+s)=R+2s$ and hence $m(R+2s)=mR+2sm=R+2s$. If $m\in R$, we have automatically $s=0$. If $m\in N$ then $mR=N$, and hence $N(x)=R(x+2s(m-1))$. In other words

$$\chi_0(x)-\chi(x)=\chi_0(x+2s(m-1))+\chi(x+2s(m-1)).$$

Clearly, the case $s=0$ is impossible. Multiplying by $\chi(x)$, summing and using Lemma 2.3, we get

$$p-1=1-\chi(-2s(m-1)).$$

That implies $p=1$ or $p=3$. The case $p=3$ is Example 4.1(a). Thus for $p>3$, any multiplier of A belongs to R. Below we assume that $n>1$, and hence $p>3$. By Theorem 2.9 and the previous arguments any prime factor of n is a quadratic residue, which implies that n belongs to R itself. We have $p=n^2+n+1$, $n^3\equiv 1 \pmod p$ and hence the order of n is three (in particular $p\equiv 1 \pmod 3$). The same follows from the fact that $n\equiv 0 \pmod 3$ if $0\in A$, and $n\equiv -1 \pmod 3$ if $0\notin A$. Take an arbitrary nonzero $x\in A$. Because $n>1$, we see that x, xn, xn^2 are different and belong to A. Hence $x+xn^2\equiv x-(n+1)x\equiv -nx\in R$, so $x\in -R$. This is equivalent to $A\setminus\{0\}\subseteq -R$.

Our arguments rest on the identity

$$R(x)=\tfrac{1}{2}((A*A)(x)-(2\cdot A)(x)), \tag{31}$$

which is a consequence of the fact that A is a perfect difference set.

First of all suppose that $A \subseteq N$. Then $A \subseteq -R$, and hence $-1 \in N$, $p \equiv -1 \pmod 4$ and $2 \in R$. Since $R \in \mathcal{D}$ and simultaneously $A \in \mathcal{D}$, it follows from (31) that $((A*A)\circ 2\cdot A)(x) + (2\cdot A \circ (A*A))(x) \in \mathcal{L}$. Using identity (31) again, we see that $(R\circ(2\cdot A))(x) + ((2\cdot A)\circ R)(x) \in \mathcal{L}$. It follows that

$$|R\cap(2\cdot A + x)| + |R\cap(2\cdot A - x)| = a, \quad \forall x \neq 0. \tag{32}$$

We know that 2 belongs to R. If $x \in 2\cdot A$ then

$$|R\cap(2\cdot A + x)| = |R\cap(A + x/2)| = a - 1,$$

because $x/2 \in A$ and $A \hat{+} A = R$. On the other hand, using the fact that $2 \in R$ again, we get

$$\sum_{x\in 2\cdot A} |R\cap(2\cdot A - x)| = \sum_x R(x)(A\circ A)(x) = t, \tag{33}$$

and hence there is $x \in 2\cdot A$ such that $|R\cap(2\cdot A - x)| \geq t/a$. Combining this with (32), we obtain

$$a - 1 + t/a \leq a,$$

or $t \leq a$, and hence $a \leq 3$. This is Example 4.1(b).

It remains to consider the situation $A \subseteq R \sqcup \{0\}$. In this case we have $p \equiv 1 \pmod 4$ and $2 \in N$ but, unfortunately, $R \notin \mathcal{D}$, and thus we need more delicate arguments. Using (31), one can see that

$$\begin{aligned}(R\circ R)(x) = \tfrac14\big(((A*A)\circ(A*A))(x) + ((2\cdot A)\circ(2\cdot A))(x) - ((2R+2\cdot A)\circ 2\cdot A)(x)\\ - 2\cdot A\circ(2R + 2\cdot A)\big)\\ = \tfrac14\big(((A*A)\circ(A*A))(x) - ((2\cdot A)\circ(2\cdot A))(x)\\ - 2(R\circ 2\cdot A)(x) - 2(2\cdot A\circ R)(x)\big).\end{aligned}$$

Because $\mathsf{E}(A) = 2a^2 - a$ and $A*A \in \mathcal{D}$, we have

$$((A*A)\circ(A*A))(x) = \frac{a^4 - \mathsf{E}(A)}{p-1} = \frac{a^4 - 2a^2 + a}{p-1} = a^2 + a - 1, \quad \forall x \neq 0.$$

Combining this with Lemma 2.8 and the fact that $A \in \mathcal{D}$, we obtain

$$p - 3 - 2\chi(x) = a^2 + a - 1 - 1 - 2(R\circ 2\cdot A)(x) - 2(2\cdot A\circ R)(x), \quad \forall x \neq 0.$$

In other words

$$a + \chi(x) = (R\circ 2\cdot A)(x) + (2\cdot A\circ R)(x), \quad \forall x \neq 0. \tag{34}$$

Let $A^* = A \setminus \{0\}$. Using arguments similar to (32)–(33), we see that for all $x \in 2\cdot A^*$ the following holds: $|R\cap(2\cdot A + x)| = |N\cap(A + x/2)| = 1$ and

$$\begin{aligned}\sum_{x\in 2\cdot A^*} |R\cap(2\cdot A - x)| &= \sum_x N(x)(A^*\circ A)(x)\\ &= \sum_x N(x)(A\circ A)(x) - |A\cap N| = t.\end{aligned}$$

Hence there is $x \in 2 \cdot A^*$ such that $|R \cap (2 \cdot A - x)| \le t/(a-1)$. For any $x \in 2 \cdot A^*$, we have $\chi(x) = -1$. Applying (34), we obtain

$$a - 1 \le 1 + \frac{t}{a-1},$$

so $a \le 4$ (if $0 \notin A$ then it is easy to check similarly that $a \le 3$). This is Example 4.1(c). Indeed, $A \subseteq R \sqcup \{0\}$, $R = \{1,3,4,9,10,12\}$ and it is easy to see that A is either $\{0,1,3,9\}$ or $\{0,4,10,12\}$ (note that $|A| - 1 = 3$ is a multiplier of A). ∎

Note that Example 4.1 shows the possibility of the cases $\Delta = 2, 3$ as well as $\Delta = n + 1$.

Now we can consider the general situation. Of course, the third part of the theorem below is the main one but it follows from the first part. The second part shows that A with $A \hat{+} A = R$ is close to a perfect difference set in some sense.

THEOREM 4.3. *Let p be a prime number, $p = n^2 + \Delta$, $1 \le \Delta \le 2n$, $R \subseteq \mathbb{F}_p$ be the set of quadratic residues and $A \subseteq \mathbb{F}_p$ be a set.*

(i) *If $A \hat{+} A = R$ and A is not from Example* 4.1(a) *then $|A| = n + 1$, $3 \le \Delta \le n+1$ and $|2 \cdot A \cap R| \le \sqrt{|A|\Delta - 3|A| + 1}/2$. If $0 \notin A$ then $\chi(2) = 1$ and $|A| \le 6$. If $0 \in A$ then $\chi(2) = -1$, and if $\Delta = n + 1$ then A is a perfect difference set.*

(ii) *If $A \hat{+} A = R$ then A is close to a perfect difference set in the sense that*

$$\mathsf{E}(A) = 2|A|^2 - |A| + \mathcal{E}_1, \tag{35}$$

where

$$\mathcal{E}_1 \le 6(|A| - \Delta) + 2|A| + \min\{(|A| - \Delta)|A|, |A|\sqrt{3(|A| - \Delta)}, (|A| - \Delta)^2\},$$

and

$$(A \circ A)(x) = (|A| - 1)\delta_0(x) + 1 + \mathcal{E}_2(x), \tag{36}$$

where $\sum_x \mathcal{E}_2(x) = |A| - \Delta$ and $\|\mathcal{E}_2\|_2^2 = \mathcal{E}_1 + \Delta - |A|$.

(iii) *If $A \hat{+} A = R$ then A is a perfect difference set such that if $|A|$ is even then $|A| \le 6$, and if $|A|$ is odd then $|A| \le 5$.*

Proof. (i) Put $a = |A|$. The assumption $A \hat{+} A = R$ implies that $\binom{a}{2} \ge (p-1)/2$, so $a^2 - a \ge p - 1$. This is equivalent to $a \ge n + 1$. We can assume that $a \ge 3$ because otherwise we have Example 4.1(a). One can also check that for $a \ge 3$ the case $p = 5$ is impossible, and hence we will assume that $p \ge 7$. Below we will use the fact that $A \hat{+} A \subseteq R$ only. Put

$$d := \sum_{x \in A} (\chi(2x) - 1) = \eta a.$$

Clearly, $\eta \in [-2,0]$. We will further estimate d and η. By Lemma 2.4, we get

$$\sum_x (A\circ\chi)^2(x) = pa - a^2. \tag{37}$$

Further, similarly to (21), we have

$$(A\circ\chi)(x) = (a-1+\chi(2x))A(x) + \varepsilon(x) \tag{38}$$

where $\varepsilon(x) = 0$ for all $x \in A$. Hence

$$a(a-1)^2 + 2(a-1)(d+a) + a - \omega = \sum_{x\in A}(a-1+\chi(2x))^2 \le pa - a^2$$

where $\omega = 1$ if $0 \in A$ and $\omega = 0$ otherwise. The last inequality and the bound $a^2 - a \ge p-1$ easily imply that

$$d \le -a - \frac{a-\omega}{2(a-1)} < -a. \tag{39}$$

In particular, $\eta \in [-2,-1)$.

In the case $0 \notin A$, we have

$$(d+a)^2 + a(a-1)^2 + 2(a-1)(d+a) + a \le pa - a^2$$

and after some manipulations, we obtain

$$d \le -2a + 1 + \sqrt{a^2 - 3a + 1}, \tag{40}$$

and

$$d \le -2a + 1 + \sqrt{a\Delta - 3a + 1} \tag{41}$$

in the case $p = (a-1)^2 + \Delta$. Note that in this case $\Delta \ge 3$.

Now suppose that $0 \in A$. Write $A^* = A \sqcup \{0\}$. Then $A^* \subseteq R$, and the set $2\cdot A^*$ is included in either R or N. In the first case $d = -1$, which is impossible by (39). If $2\cdot A^* \subseteq N$ then $d = -2a+1$, $\chi(2) = -1$ and (40), (41) hold. Thus in any case

$$|2\cdot A \cap R| \le \frac{\sqrt{a^2-3a+1}}{2}, \tag{42}$$

and

$$|2\cdot A \cap R| \le \frac{\sqrt{a\Delta-3a+1}}{2} \tag{43}$$

in the case $p = (a-1)^2 + \Delta$. One of the main ideas of the further proof is to exploit inequalities (39), (42), (43). They mean that the distribution of the intersections $|R\cap(A+x)|$ for $x \in \mathbb{F}_p$ is somewhat asymmetric.

Returning to (38), for all $x \notin A$ we get

$$\varepsilon(x) = |R\cap(A+x)| - |N\cap(A+x)| = 2|R\cap(A+x)| - a + A(-x). \tag{44}$$

Clearly,

$$\langle \varepsilon \rangle = -a^2 - d. \tag{45}$$

As above, we have

$$\sum_{x\in A}(a-1+\chi(2x))^2 = a(a-1)^2+2(a-1)(d+a)+a-\omega = a^3+2(a-1)d-\omega$$

where, as before, $\omega = |A \cap \{0\}|$. As in Theorem 3.2, we obtain an analog of (22),

$$\|\varepsilon\|_2^2 = pa - a^2 - a^3 - 2(a-1)d + \omega. \tag{46}$$

Thus by the Cauchy–Schwarz inequality and identity (45), we get

$$\frac{(a^2+d)^2}{p-a} \le pa - a^2 - a^3 - 2(a-1)d + \omega. \tag{47}$$

In other words

$$\begin{aligned} &a^2(p-1) + ab(\eta) - c(\eta) \\ &\quad := a^2(p-1) + a(\eta^2 + 2\eta + 2\eta p + 2p) - 2\eta p - p^2 - \omega\frac{p-a}{a} \le 0. \end{aligned} \tag{48}$$

It is easy to check that the formula for the right root of (48), namely,

$$x(\eta) = \frac{-b(\eta) + \sqrt{b^2(\eta) + 4(p-1)c(\eta)}}{2(p-1)}$$

contains a decreasing function $-b(\eta)$ and an increasing function

$$\begin{aligned} g(\eta) &:= b^2(\eta) + 4(p-1)c(\eta) \\ &= \eta^4 + (4+4p)\eta^3 + (4+4p^2+12p)\eta^2 + 16\eta p^2 + 4p^3 + \omega\frac{4(p-1)(p-a)}{a} \end{aligned}$$

of $\eta \in [-2,-1)$. Indeed, one can see that $g'(-2) = 0$ and g'' grows on $[-2,-1)$. Put $e = \omega 4(p-1)(p-a)/a$. Because $a \ge \sqrt{p}$, we have $e \le 4p^{3/2}$. Hence, we should substitute $\eta = -2$ into $b(\eta)$, $\eta = -1$ into $g(\eta)$, and check that

$$a \le \frac{2p + \sqrt{4p^3 - 12p^2 + 8p + 1 + e}}{2(p-1)} \le \sqrt{p} + 1 < n + 2. \tag{49}$$

Indeed, one can check that the second bound from (49) holds provided that $p \ge 7$. Thus, for any η, we have $a = n+1$. Recalling $a^2 - a \ge p - 1$, we obtain

$$a^2 - a = n^2 + n \ge p - 1 = n^2 + \Delta - 1. \tag{50}$$

Hence $3 \le \Delta \le n+1$ and in the case $\Delta = n+1$, all sums $a' + a''$ are different for different $a', a'' \in A$. Using the arguments above, we see that if $0 \in A$ and $\Delta = n+1$ then A is a perfect difference set.

Finally, consider the case $0 \notin A$. We will prove, in particular, that $\chi(2) = 1$ in this situation. By (38) one has

$$\varepsilon(0) = \sum_{x\in A} \chi(x) = \chi(2) \sum_{x\in A} \chi(2x) = \chi(2)(d+a).$$

Identity (38) and the last formula imply

$$\sum_x \varepsilon(x)\chi(x) = -a - \chi(2)(a^2 + da - d).$$

Hence, as in (47), considering the function $\varepsilon(x)$ restricted to $\mathbb{F}_p \setminus \{0\}$ only, and additionally using Corollary 2.5, we get

$$\frac{(a^2 + d + \chi(2)(d+a))^2 + (a + \chi(2)(a^2 + da - d))^2}{p} \le pa - a^2 - a^3 - 2(a-1)d - (d+a)^2. \tag{51}$$

After some manipulations, for $\chi(2) = -1$ we obtain

$$h_{a,d}(\Delta) := a\Delta^2 + (a^3 - 6a^2 + 2a - 4da + 2d - d^2)\Delta - 6a^4 + 13a^3 - 8a^2 + 14a^2d - 2d^2a^2 - 6da^3 + a - 10da + 4d^2a + 2d - 2d^2 \ge 0. \tag{52}$$

The maximum of $h_{a,d}(\Delta)$ is attained at $\Delta = a$ and is equal to

$$-(2a^2 - 3a + 2)d^2 - (6a^3 - 10a^2 + 8a - 2)d - 5a^4 + 8a^3 - 6a^2 + a.$$

The integer maximum of the last expression is attained at $d \in [-1.5a, -1.5a + 1]$. Substituting the integer values of d from this interval into the last expression, we obtain a contradiction with the nonnegativity of (52).

Almost the same is true in the case $\chi(2) = 1$. In this situation

$$h^*_{a,d}(\Delta) := a\Delta^2 + (a^3 - 6a^2 + 2a - 4da + 2d - d^2)\Delta + a - 2d^2a^2 - 6d^2 + 5a^3 - 8a^2 + 2d - 6a^4 + 4d^2a - 10da + 6a^2d - 6da^3 \ge 0. \tag{53}$$

Again the maximum of $h^*_{a,d}(\Delta)$ is attained at $\Delta = a$ and is equal to

$$-(2a^2 - 3a + 6)d^2 - (6a^3 - 2a^2 + 8a - 2)d - 5a^4 - 6a^2 + a \ge 0.$$

Here the integer maximum is attained at $d \in (-1.5a-3, -1.5a]$. Substituting the integer values of d from this interval into the last inequality, we obtain a contradiction for $a \ge 7$. Thus, we have proved (i).

Let us make some additional remarks which we will use later. If $a = 3$ then $p = 7$, $\chi(2) = 1$, $\Delta = a$, $|A \hat{+} A| = \binom{3}{2} = 3$, $R = \{1, 2, 4\}$. If $A \cap R = \emptyset$ then A is from Example 4.1(b). Further, it is easy to see that $0 \notin A$, and A can intersect R at just one point. If $1 \in A$ then we have a contradiction because $5, 6$ cannot belong to A in this case. The same is true for $2 \in A$ and $4 \in A$. Thus A is from Example 4.1(b), provided that $a = 3$. Finally, if $a = 5$ then $p = 19$ because $\Delta \ge 3$. Hence $\chi(2) = -1$, $0 \in A$, $d = -2a + 1 = -9$. Substituting this into (47), we obtain a contradiction. The remaining cases

$a = 4, 6$ as well as the situation $0 \in A$ will be considered in the third part of the proof.

(ii) The fact that $R = A \hat{+} A$ implies

$$(A * A)(x) = 2R(x) + (2 \cdot A)(x) + Z(x), \tag{54}$$

where $Z(x) \geq 0$. It is easy to see that $\operatorname{supp} Z \subseteq R$. Summing (54), we obtain

$$\|Z\|_1 = a^2 - 2t - a = n + 1 - \Delta = a - \Delta := z.$$

Using this, the Gauss sum bound of Lemma 2.3, the inequality $\Delta \geq 3$ and identity (54), we get

$$|\widehat{A}(x)|^2 \leq 3n + 2 < 3a, \quad \forall x \neq 0. \tag{55}$$

Further, multiplying (54) by $(A * A)(x)$ and summing, we have

$$\begin{aligned}\mathsf{E}(A) &= \sum_x (2R(x) + (2 \cdot A)(x))(A * A)(x) + \sum_x Z(x)(A * A)(x) \\ &= 4t + a + 2z + 4\sum_x R(x)(2 \cdot A)(x) + \sum_x (2 \cdot A)(x)Z(x) + \sum_x Z(x)(A * A)(x).\end{aligned}$$

Applying the Fourier transform and estimates (39), (41), (43), (55), we get

$$\begin{aligned}\mathsf{E}(A) &= 2p - 2 + a + 2z + 4\langle 2 \cdot A, R\rangle + \langle 2 \cdot A, Z\rangle \\ &\quad + \theta_1(\min\{za, a^2 z/p + a\sqrt{3z}\}) \\ &\leq 2a^2 - a + \theta_2(4(a - \Delta) + 2a + \min\{az, a\sqrt{3z}\}),\end{aligned} \tag{56}$$

where $|\theta_1|, |\theta_2| \leq 1$. Thus $\mathcal{E}_1 \leq 4z + 2a + \min\{az, a\sqrt{3z}\}$. Squaring (54), summing and using (41), (43), we obtain

$$\begin{aligned}\mathsf{E}(A) &= 4t + a + 4z + 2\langle 2 \cdot A, Z\rangle + 4\langle 2 \cdot A, R\rangle + \|Z\|_2^2 \\ &= 2a^2 - a + \theta_3(6(a - \Delta) + 2a + z^2),\end{aligned}$$

where $0 \leq \theta_3 \leq 1$. Hence $\mathcal{E}_1 \leq 6z + 2a + z^2$.

Finally,

$$\begin{aligned}(a-1)^2 + \sum_x \mathcal{E}_2^2(x) &= (a-1)^2 + \sum_{x \neq 0} ((A \circ A)(x) - 1)^2 \\ &= \sum_x ((A \circ A)(x) - 1)^2 = \mathsf{E}(A) - 2a^2 + p.\end{aligned} \tag{57}$$

From $p = (a-1)^2 + \Delta$, the last identity and formula (35), we obtain $\|\mathcal{E}_2\|_2^2 = \mathcal{E}_1 + \Delta - a$.

(iii) Let a be even. Recalling (44) we see that $\varepsilon(x)$ is even for $x \notin -A$. Using Lemma 3.1 with $c = -2$, we get

$$\|\varepsilon\|_2^2 = pa - a^2 - a^3 - 2(a-1)d + \omega \geq 2(a^2 + d) - (a - \omega).$$

After some computations, we obtain

$$2+\Delta-2d\ge 5a. \tag{58}$$

Thus, either $\Delta=a=n+1$ and $d=-2a+1,-2a$, or $\Delta=a-1,a-2$ and $d=-2a$. In the first case A is a perfect difference set. Now suppose that A is not a perfect difference set and consider the second case. Because $d=-2a$, we see that $0\notin A$. Returning to (50), we get $\Delta=a-2=n-1$. This means, in particular, that inequality (58) is actually an equality. Using formula (19) of Lemma 3.1, we see that $\varepsilon(x)=0$ on A, $\varepsilon(x)=-1$ on $-A$ and $\varepsilon(x)=0,-2$ on the rest. But $2\cdot A\subseteq N$, hence $A\subseteq R$ or $A\subseteq N$, and thus by (44), we have $\varepsilon(0)=\pm a$, a contradiction. In particular, we have thus considered the remaining cases $a=4,6$.

Now we deal with the case when a is odd and $0\in A$. Hence $d=-2a+1$ and we can suppose that $\Delta\le a-1$ because A is a perfect difference set otherwise. Using (19) with $c=-2$, and applying the arguments from the proof of Theorem 3.3, we obtain

$$\begin{aligned}\|\varepsilon\|_2^2 &= pa-a^3+3a^2-6a+3\ge 2(a^2-2a+1)+\sum_k (k^2+2k)p_k\\ &\ge 2(a^2+2a-1)-p_{-1}+3\sum_{k\ne 0,-1,-2}p_k\\ &= 2(a^2-2a+1)+3p-4p_{-1}-3(p_0+p_{-2}).\end{aligned}$$

Here, again $p_k:=|\{x\in\mathbb{F}_p:\varepsilon(x)=k\}|$ for $k\in\mathbb{Z}$. Clearly, $p_0+p_{-2}\le 2a-1$. As above, $p_{-1}\le (p-1)/2$. Hence

$$pa-a^3+3a^2-6a+3\ge 2(a^2-2a+1)+p+2-6a+3.$$

In other words,

$$\Delta(a-1)-2a^2+7a-5\ge 0,$$

a contradiction for $a\ge 5$ because A is not a perfect difference set by our assumption and hence $\Delta\le a-1$. This completes the proof. ∎

Clearly, combining the third part of Theorem 4.3 with Proposition 4.2 we get the second part of the main Theorem 1.2.

Remark 4.4. The method of proving Theorem 4.3 above is analytical, so we can say something about the structure of the set A in a somewhat more general situation. This was the reason to include the second part of the theorem. More precisely, suppose that

$$(A*A)(x)=2R(x)+(2\cdot A)(x)+Z(x) \tag{59}$$

with a "small" function Z. Then summing (59), we have

$$p-1+|A|-\|Z\|_1\le |A|^2\le p-1+|A|+\|Z\|_1 \quad\text{and}\quad \langle Z\rangle=|A|^2-2t-a.$$

Further, for all $x \neq 0$,

$$|\widehat{A}(x)|^2 \le \sqrt{p} + 1 + |A| + \|Z\|_1,$$

and

$$\begin{aligned}(60)\qquad \mathsf{E}(A) &= \sum_x \big(2R(x) + (2\cdot A)(x)\big)(A*A)(x) + \sum_x Z(x)(A*A)(x)\\ &\le 4t + 5a + 3\|Z\|_1 + \sum_x Z(x)(A*A)(x)\\ &\le 4t + 6a + 3\|Z\|_1 + (\sqrt{p} + 1 + |A| + \|Z\|_1)^{1/2}|A|^{1/2}\|Z\|_2,\end{aligned}$$

provided that $\langle Z\rangle \le pa^{-1}$, say. Similarly, if we put

$$(A\circ A)(x) = (|A|-1)\delta_0(x) + 1 + \mathcal{E}_2(x)$$

then, as in (57), by (60) we get

$$\begin{aligned}\sum_x \mathcal{E}_2^2(x) &= \sum_x \big((A\circ A)(x) - 1\big)^2 - (a-1)^2 = \mathsf{E}(A) - 2a^2 + p - (a-1)^2\\ &\le 3p - 3 + 8a - 3a^2 + 3\|Z\|_1\\ &\quad + (\sqrt{p} + 1 + |A| + \|Z\|_1)^{1/2}|A|^{1/2}\|Z\|_2.\end{aligned}$$

Thus, if $|R\Delta(A \dot{+} A)|$ is small then A is close to a perfect difference set.

5. Concluding remarks. Now we describe an alternative way to obtain the results of Sections 3, 4.

Our aim is to define an analog of "Fourier transform" with respect to a multiplicative character χ. Put

$$\mathrm{f}(x) = \frac{1}{\sqrt{p}}\left(\chi(x) - \frac{1}{\sqrt{p}}\right).$$

Clearly, f is a perfect difference function. Note that

$$(61)\qquad \|\mathrm{f}\|_\infty \le \frac{1}{\sqrt{p}}\left(1 + \frac{1}{\sqrt{p}}\right).$$

Let g be an arbitrary function. We write $g_s(x)$ for $g(x+s)$. By Lemma 2.3,

$$(62)\qquad \langle \mathrm{f}_s, \mathrm{f}_t\rangle = \delta_{s,t} \quad\text{and}\quad \sum_y \mathrm{f}_y(s)\overline{\mathrm{f}_y(t)} = \delta_{s,t},$$

for all $s,t \in \mathbb{F}_p$. Further $\langle \mathrm{f}_s, 1\rangle = \langle 1, \mathrm{f}_s\rangle = -1$ and

$$(63)\qquad (\mathrm{f}_s \circ \bar{\mathrm{f}}_t)(x) = \sum_z \mathrm{f}_s(z)\overline{\mathrm{f}_t(x+z)} = \langle \mathrm{f}_s, \mathrm{f}_{t+x}\rangle = \delta_{s,t+x}.$$

For an arbitrary function g, write $g^\lambda(x) = g(\lambda x)$. We have

$$(64)\qquad \mathrm{f}_s^\lambda(x) = \chi(\lambda)\mathrm{f}_{s/\lambda}(x) + \frac{\chi(\lambda)-1}{p}$$

for all $\lambda \in \mathbb{F}_p \setminus \{0\}$. Applying (12) once more, we obtain

$$(\mathrm{f}_s^\lambda \circ \bar{\mathrm{f}}_t^\mu)(x) = \chi(\lambda)\overline{\chi(\mu)} \cdot \delta_{s/\lambda, x+t/\mu} + \frac{1-\chi(\lambda)\overline{\chi(\mu)}}{p}. \tag{65}$$

Now we can define the "Fourier transform" corresponding to the character χ.

Definition 5.1. Let $\varphi : \mathbb{F}_p \to \mathbb{C}$ be a function. Denote by $\tilde{\varphi}$ the function

$$\tilde{\varphi}(x) = \sum_y \varphi(y)\overline{\mathrm{f}_x(y)} = \langle \varphi, \mathrm{f}_x \rangle = (\varphi \circ \bar{\mathrm{f}})(x). \tag{66}$$

For example $\tilde{1} = -1$, $\tilde{\delta}_s(x) = \overline{\mathrm{f}_s(x)}$ and $\tilde{\mathrm{f}}_s(x) = \delta_s(x)$.

Because $\mathcal{D}$ is closed under the convolutions $*$, $\circ$, and $\widehat{\mathrm{f}}(x) \neq 0$ for $x \in \mathbb{F}_p$, we see that $\varphi \in \mathcal{D}$ iff $\tilde{\varphi} \in \mathcal{D}$ (formula (70) below also implies this fact). The next lemma follows from the definitions.

Lemma 5.2. *Let $\varphi, \psi : \mathbb{F}_p \to \mathbb{C}$ be any functions. Then*

$$(\varphi_s)\tilde{} = (\tilde{\varphi})_{-s}, \quad \forall s \in \mathbb{F}_p, \tag{67}$$

$$(\overline{\varphi})\tilde{}(x) = \overline{\varphi}(x) \quad \textit{and} \quad (\tilde{\varphi})\tilde{}(x) = \varphi(x) \qquad \textit{if } \chi \in \mathbb{R}, \tag{68}$$

$$(\varphi^\lambda)\tilde{}(x) = \chi(\lambda)\tilde{\varphi}^\lambda(x) + \frac{\langle\varphi\rangle(\chi(\lambda)-1)}{p}, \quad \forall \lambda \neq 0, \tag{69}$$

$$\varphi(x) = \sum_y \tilde{\varphi}(y)\mathrm{f}_x(y), \tag{70}$$

$$\sum_x \varphi(x)\overline{\psi(x)} = \sum_y \tilde{\varphi}(y)\overline{\tilde{\psi}(y)}, \tag{71}$$

$$(\varphi \circ \psi)\tilde{}(x) = (\varphi * \tilde{\psi})(x). \tag{72}$$

Further for any $\lambda, \mu \neq 0$, we have

$$(\varphi^\lambda \circ \overline{\psi^\mu})(x) = \chi(\lambda)\overline{\chi(\mu)} \cdot (\overline{\tilde{\psi}^\mu} \circ \tilde{\varphi}^\lambda)(x) + \frac{1-\chi(\lambda)\overline{\chi(\mu)}}{p} \cdot \langle\varphi\rangle\langle\overline{\psi}\rangle. \tag{73}$$

In particular

$$(\varphi \circ \overline{\psi})(x) = (\tilde{\varphi} \circ \overline{\tilde{\psi}})(-x) = (\overline{\tilde{\psi}} \circ \tilde{\varphi})(x), \tag{74}$$

$$(\varphi * \overline{\psi})(x) = \chi(-1)(\tilde{\varphi} * \overline{\tilde{\psi}})(-x) + \frac{1-\chi(-1)}{p}\langle\varphi\rangle\langle\overline{\psi}\rangle. \tag{75}$$

Proof. We just need to check (73) because the other formulas are almost trivial. Applying (69), (70) and the fact that $\langle \mathrm{f}_s \rangle = -1$ for all $s \in \mathbb{F}_p$, we obtain

$$
\begin{aligned}
(\varphi^\lambda \circ \overline{\psi^\mu})(x) &= \sum_z \varphi^\lambda(z)\overline{\psi^\mu(z+x)} \\
&= \sum_{y,y',z} \left(\chi(\lambda)\tilde{\varphi}^\lambda(y) + \frac{\langle\varphi\rangle(\chi(\lambda)-1)}{p}\right) \\
&\qquad \times \overline{\left(\chi(\mu)\tilde{\psi}^\mu(y') + \frac{\langle\psi\rangle(\chi(\mu)-1)}{p}\right)} \mathrm{f}_z(y)\overline{\mathrm{f}_{z+x}(y')} \\
&= \chi(\lambda)\overline{\chi(\mu)} \cdot \sum_y \tilde{\varphi}^\lambda(y)\overline{\tilde{\psi}^\mu(y-x)} + \frac{1-\chi(\lambda)\overline{\chi(\mu)}}{p} \cdot \langle\varphi\rangle\langle\overline{\psi}\rangle \\
&= \chi(\lambda)\overline{\chi(\mu)} \cdot (\overline{\tilde{\psi}^\mu} \circ \tilde{\varphi}^\lambda)(x) + \frac{1-\chi(\lambda)\overline{\chi(\mu)}}{p} \cdot \langle\varphi\rangle\langle\overline{\psi}\rangle. \ \blacksquare
\end{aligned}
$$

In particular, formula (74) says that $\mathsf{E}(A) = \mathsf{E}(\tilde{A})$. The transform above can be used to obtain the results of Sections 3, 4. Indeed, the arguments here are just calculation of $\tilde{A}$, $\tilde{B}$. Similarly, one can define the "Fourier transform" with respect to any perfect difference set as well as a function from $\mathcal{D}$.

There is a general question about "Fourier coefficients" of subsets of $\mathbb{F}_p$. Partial answers to this question are given by the proofs of the statements of Sections 3, 4.

Suppose that $A \subset \mathbb{F}_p$ is a set, and χ is an arbitrary character. Consider the function

$$E(x) = E_A(x) = E_{A,\chi}(x) := (A \circ \chi)(x).$$

Alternatively, one can take convolutions of A with the function f above, that is, $\tilde{A}$. Our question is the following: what can we say about the function $E(x)$? There is a list of simple properties of $E(x)$. Clearly,

$$\langle E_A\rangle = 0 \quad \text{and} \quad \|E_A\|_2^2 = p|A| - |A|^2.$$

Higher moments of E can be estimated using the Weil bound (4) and Lemma 2.1, as in the proof of Corollary 2.6. Of course, there is the "cocycle" property of $E(x)$, namely,

$$E_A(xy) = \chi(x)E_{x^{-1}A}(y), \qquad x \neq 0.$$

In particular, $|E_A(x)|$ is fixed by the multiplier group of A, that is, the set $\{x \in \mathbb{F}_p : xA = A\}$. Further,

$$\sum_{x,y} \chi(x+y)A(x)E_A(y) = \sum_z (A \circ \chi)^2(z) = p|A| - |A|^2,$$

and hence

$$\left|\sum_{x,y} \chi(x+y)A(x)E_A(y)\right| \gg \sqrt{p}\,\|A\|_2\|E_A\|_2 \tag{76}$$

provided $|A| \ll p$. In particular, formula (76) shows that inequality (13) of Lemma 2.4 is tight. Using estimate (61) and Lemma 5.2 one can easily prove an uncertainty principle for any function g (in particular for A),

$$p(1+1/\sqrt{p})^{-2} \le |\operatorname{supp} g| \cdot |\operatorname{supp} \tilde{g}|.$$

If A is a Singer perfect difference set then the character χ can be represented as the convolution $(A * E_{A,\chi})(x)$. Indeed,

$$\begin{aligned}(A * E_A)(x) &= (A * (A \circ \chi))(x) = (\chi * (A \circ A))(x)\\ &= \big(\chi * ((|A|-1)\delta_0 + 1)\big)(x) = (|A|-1)\chi(x).\end{aligned}$$

Finally, the size of each level set

$$L_c := \{x \in \mathbb{F}_p : E_A(x) = c\}, \qquad c \in \mathbb{F}_p,$$

is bounded by $(p-1)/2$ because $E(x) \pmod p$ is a nonzero polynomial from $\mathbb{F}_p[x]$ of degree $(p-1)/2$ with leading term $|A|x^{(p-1)/2}$. Are there further properties of $E(x)$? For example, what can we say about the maximum/minimum value of $E(x)$?

Acknowledgements. The author is grateful to S. Yekhanin for very useful discussion and to S. Konyagin for his interest in this paper.

This work was supported by grant RFFI NN 11-01-00759, Russian Government project 11.G34.31.0053, Federal Program "Scientific and scientific–pedagogical staff of innovative Russia" 2009–2013, grant mol_a_ved 12–01–33080 and grant Leading Scientific Schools N 2519.2012.1.

References

[1] C. Bachoc, M. Matolcsi and I. Z. Ruzsa, *Squares and difference sets in finite fields*, Integers 13 (2013), paper no. A77, 5 pp.
[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.
[3] B. Bollobás, *Random Graphs*, Cambridge Univ. Press, Cambridge, 2001.
[4] M.-C. Chang, *On a question of Davenport and Lewis and new character sum bounds in finite fields*, Duke Math. J. 145 (2008), 409–442.
[5] S. D. Cohen, *Clique numbers of Paley graphs*, Quaest. Math. 11 (1988), 225–231.
[6] E. Croot and V. Lev, *Open problems in additive combinatorics*, in: Additive Combinatorics, CRM Proc. Lecture Notes 43, Amer. Math. Soc., Providence, RI, 2007, 207–233.
[7] C. Dartyge and A. Sárközy, *On additive decompositions of the set of primitive roots modulo p*, Monatsh. Math. 169 (2013), 317–328.
[8] H. Davenport and P. Erdős, *The distribution of quadratic and higher residues*, Publ. Math. Debrecen 2 (1952), 252–265.
[9] P. Erdős and H. N. Shapiro, *On the least primitive roots of a prime*, Pacific J. Math. 7 (1957), 861–865.
[10] S. Graham and C. Ringrose, *Lower bounds for least quadratic nonresidues*, in: Analytic Number Theory (Allerton Park, IL, 1989), Progr. Math. 85, Birkhäuser, 1990, 269–309.

[11] M. Hall, *Combinatorial Theory*, Blaisdell, 1967.
[12] J. Johnsen, *On the distibution of powers in finite fields*, J. Reine Angew. Math. 251 (1971), 10–19.
[13] A. A. Karatsuba, *Distribution of power residues and non-residues in additive sequences*, Soviet Math. Dokl. 11 (1970), 235–236.
[14] A. A. Karatsuba, *The distribution of values of Dirichlet characters on additive sequences*, Soviet Math. Dokl. 44 (1992), 145–148.
[15] A. A. Karatsuba, *Arithmetic problems in the theory of Dirichlet characters*, Russ. Math. Surv. 63 (2008), 43–92.
[16] W. Rudin, *Fourier Analysis on Groups*, Wiley, 1990 (reprint of the 1962 original).
[17] A. Sárközy, *On additive decompositions of the set of quadratic residues modulo p*, Acta Arith. 155 (2012), 41–51.
[18] T. Schoen and I. D. Shkredov, *Higher moments of convolutions*, J. Number Theory 133 (2013), 1693–1737.
[19] I. D. Shkredov, *Some new inequalities in additive combinatorics*, Moscow J. Combin. Number Theory 3 (2013), 237–288.
[20] I. D. Shkredov and I. V. Vyugin, *On additive shifts of multiplicative subgroups*, Mat. Sb. 203 (2012), no. 6, 81–100 (in Russian).
[21] I. E. Shparlinski, *Additive decompositions of subgroups of finite fields*, SIAM J. Discrete Math. 27 (2013), 1870–1879.
[22] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Univ. Press, 2006.

I. D. Shkredov
Division of Algebra and Number Theory
Steklov Mathematical Institute
Gubkina St. 8
Moscow, Russia 119991
and
Delone Laboratory of Discrete and Computational Geometry
Yaroslavl' State University
Sovetskaya St. 14
Yaroslavl', Russia 150000
and
IITP RAS
Bol'shoy Karetny per. 19
Moscow, Russia 127994
E-mail: ilya.shkredov@gmail.com

Received on 24.5.2013
and in revised form on 21.12.2013 and 26.5.2014 (7458)