ACTA ARITHMETICA
155.1 (2012)

On additive decompositions of the set of quadratic residues modulo p

by

ANDRÁS SÁRKÖZY (Budapest)

Dedicated to Professor Andrzej Schinzel
on the occasion of his 75th birthday

1. Introduction. Ostmann [15] introduced the following definitions:

DEFINITION 1.1. If $\mathcal{C}$ is a finite or infinite set of non-negative integers, then it is said to be *reducible* if there are sets $\mathcal{A}$, $\mathcal{B}$ of non-negative integers with

$$\mathcal{A}+\mathcal{B}=\mathcal{C}, \quad |\mathcal{A}|,|\mathcal{B}|\ge 2. \tag{1.1}$$

If there are no sets $\mathcal{A}$, $\mathcal{B}$ with these properties, then $\mathcal{C}$ is said to be *primitive.*

DEFINITION 1.2. Two sets $\mathcal{A}$, $\mathcal{B}$ of non-negative integers are said to be *asymptotically equal* if they are equal apart from a finite number of exceptions, i.e., there is a number K such that

$$\mathcal{A}\cap[K,+\infty)=\mathcal{B}\cap[K,+\infty);$$

we then write $\mathcal{A}\sim\mathcal{B}$.

DEFINITION 1.3. An infinite set $\mathcal{C}$ of non-negative integers is said to be *totalprimitive* if every $\mathcal{C}'$ with $\mathcal{C}'\sim\mathcal{C}$ is primitive.

Ostmann formulated the following conjecture:

CONJECTURE 1.4 (Ostmann [15]). *The set $\mathcal{P}$ of prime numbers is totalprimitive.*

Partial results in this direction have been proved by Hornfeck [14], Hofmann and Wolke [13], Elsholtz [4]–[6] and Puchta [16] (but Conjecture 1.4 is still unproved). In these papers the counting functions of sets $\mathcal{A}$, $\mathcal{B}$ with

2010 *Mathematics Subject Classification*: Primary 11P70; Secondary 11B99.
Key words and phrases: sumset, additive decomposition, inverse theorem, quadratic residues.

DOI: 10.4064/aa155-1-4

$\mathcal{A}+\mathcal{B}\sim\mathcal{P}$ (if there are such $\mathcal{A}$, $\mathcal{B}$ at all) have been estimated, and using estimates of this type Elsholtz also proved:

THEOREM A (Elsholtz [5]). *If $\mathcal{P}'\sim\mathcal{P}$, then there are no sets $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ of non-negative integers with*

$$\mathcal{A}+\mathcal{B}+\mathcal{C}=\mathcal{P}', \qquad |\mathcal{A}|,|\mathcal{B}|,|\mathcal{C}|\geq 2.$$

It is trivial that the set $\mathcal{N}=\{1^2,2^2,3^2,\dots\}$ of all squares is totalprimitive (this follows from the fact that the limit of the gaps between the consecutive squares is infinite). Erdős conjectured that every set $\mathcal{N}'$ which can be obtained from $\mathcal{N}$ by changing only $o(x^{1/2})$ elements of it up to x is also totalprimitive. Sárközy and Szemerédi [19] have proved a slightly weaker result: all the sets $\mathcal{N}'$ obtained by changing only $o\big(x^{1/2}\exp\big(-c\frac{\log x}{\log\log x}\big)\big)$ elements of $\mathcal{N}$ up to x are totalprimitive.

One might wish to study the finite analogues of these problems. The most natural question of this type is to consider the set of quadratic residues in $\mathbb{F}_p$ and to look for additive decompositions of it. (We will identify $\mathbb{F}_p$ with the set of residue classes modulo p and, as is customary, we will not distinguish between residue classes and the integers representing them.)

Clearly, the definitions of reducibility and primitivity can be extended to any additive group, thus the reducibility and primitivity of sets of residue classes (or residues) modulo p can be defined in the same way as in Definition 1.1. We will also use the following terminology:

DEFINITION 1.5. If $\mathcal{A}_1,\dots,\mathcal{A}_k\subset\mathbb{F}_p$,

$$\mathcal{A}_1+\dots+\mathcal{A}_k=\mathcal{B} \tag{1.2}$$

and

$$|\mathcal{A}_1|,\dots,|\mathcal{A}_k|\geq 2, \tag{1.3}$$

then (1.2) will be called an (additive) *k-decomposition* of $\mathcal{B}$; a k-decomposition will always mean a *non-trivial* one, that is, a decomposition satisfying (1.3). (Here we will be interested in 2-decompositions and 3-decompositions only.)

On the other hand, clearly the definition of totalprimitivity cannot be adapted to finite sets, thus we will not use it.

There are many papers on the connection of sumsets and quadratic residues [1]–[3], [7]–[9], [11], [12], [17]. A further problem of this type is to study the reducibility of the set of quadratic residues modulo p. The following conjecture seems to be very plausible:

CONJECTURE 1.6. *Let p be a prime number and let $\mathcal{Q}=\mathcal{Q}(p)$ denote the set of quadratic residues modulo p. If p is large enough, then $\mathcal{Q}=\mathcal{Q}(p)$ is primitive, i.e., it has no* (*non-trivial*) *2-decomposition.*

(Note that $\mathcal{Q}$ is a "large", "dense" subset of $\mathbb{F}_p$ which makes this problem very different from the case of squares mentioned above.) This paper is devoted to the study of this problem. Here the situation is similar to the case of Ostmann's conjecture: Conjecture 1.6 seems to be beyond reach at present. On the other hand, one can prove partial results similar to the ones proved in the case of Ostmann's conjecture. First in Section 2 we will estimate the cardinalities of the subsets $\mathcal{A}$, $\mathcal{B}$ occurring in a (non-trivial) 2-decomposition $\mathcal{A}+\mathcal{B}=\mathcal{Q}$ (if there is any). Then in Section 3 we will apply these results to prove the Elsholtz-type result that $\mathcal{Q}$ has no (non-trivial) 3-decomposition. (While here the nature of the results is similar to the ones proved in connection with Ostmann's conjecture, the methods used are completely different: there sieve methods, in particular, the large sieve and Gallagher's larger sieve are used, while here Weil's theorem will be the crucial tool and we will also apply a theorem of Ruzsa.)

2. 2-decompositions of $\mathcal{Q}$.

We will prove

THEOREM 2.1. *If p is a prime large enough and*

$$\mathcal{U}+\mathcal{V}=\mathcal{Q} \tag{2.1}$$

is a (non-trivial) 2-decomposition of $\mathcal{Q}=\mathcal{Q}(p)$, then

$$\min\{|\mathcal{U}|,|\mathcal{V}|\}>\frac{1}{3}\frac{p^{1/2}}{\log p}, \tag{2.2}$$

$$\max\{|\mathcal{U}|,|\mathcal{V}|\}<p^{1/2}\log p. \tag{2.3}$$

Proof. We may assume that

$$(2\le)\ |\mathcal{U}|\le|\mathcal{V}|. \tag{2.4}$$

Let

$$\mathcal{U}=\{u_1,\dots,u_k\}\quad\text{with } 0\le u_1<\dots<u_k<p, \tag{2.5}$$

for $i=1,\dots,k$ define u_i' by $u_i'=u_i-u_1$ and let

$$\mathcal{U}'=\{u_1',\dots,u_k'\}\quad(=\mathcal{U}-\{u_1\})$$

where $u_1'=0$, and set

$$\mathcal{V}'=\mathcal{V}+\{u_1\}.$$

Then clearly (2.1) also holds with $\mathcal{U}'$ and $\mathcal{V}'$ in place of $\mathcal{U}$ and $\mathcal{V}$, and we have $|\mathcal{U}'|=|\mathcal{U}|$, $|\mathcal{V}'|=|\mathcal{V}|$ and $0\in\mathcal{U}'$; thus it suffices to prove the theorem when we have

$$u_1=0 \tag{2.6}$$

in (2.5).

By (2.4) and (2.5) we have

$$2\le|\mathcal{U}|=k\le|\mathcal{V}|. \tag{2.7}$$

Now we will prove several lemmas.

Lemma 2.2. *With the notation and assumptions above we have*

$$k \neq 2. \tag{2.8}$$

Proof. Assume that contrary to (2.8) we have

$$k = 2. \tag{2.9}$$

Then by (2.1) and (2.6),

$$\{0, u_2\} + \mathcal{V} = \mathcal{Q}. \tag{2.10}$$

Let γ denote the quadratic character of $\mathbb{F}_p$ so that

$$\gamma(n) = \begin{cases} \left(\dfrac{n}{p}\right) & \text{for } n \neq 0, \\ 0 & \text{for } n = 0 \end{cases}$$

($\left(\frac{n}{p}\right)$ denotes the Legendre symbol). We will prove that there is a

$$q \in \mathcal{Q} \tag{2.11}$$

with

$$\gamma(q + u_2) = -1, \tag{2.12}$$

$$\gamma(q - u_2) = -1. \tag{2.13}$$

Let $\mathcal{R}$ denote the set of q's satisfying (2.11)–(2.13), and write

$$f(x) = (\gamma(x) + 1)(\gamma(x + u_2) - 1)(\gamma(x - u_2) - 1).$$

Then clearly

$$f(x) = 8 \quad \text{for } x \in \mathcal{R}, \tag{2.14}$$

$$f(x) = 0 \quad \text{for } x \notin \mathcal{R},\ x(x + u_2)(x - u_2) \neq 0, \tag{2.15}$$

$$|f(x)| \leq 4 \quad \text{for } x \notin \mathcal{R},\ x(x + u_2)(x - u_2) = 0 \tag{2.16}$$

and

$$|\{x : x \in \mathbb{F}_p,\ x(x + u_2)(x - u_2) = 0\}| \leq 3. \tag{2.17}$$

It follows from (2.14)–(2.17) that

$$\begin{aligned} \left| \frac{1}{8} \sum_{x \in \mathbb{F}_p} f(x) \right| &= \left| \frac{1}{8} \sum_{x \in \mathcal{R}} f(x) + \frac{1}{8} \sum_{x \in \mathbb{F}_p \setminus \mathcal{R}} f(x) \right| \\ &= \left| |\mathcal{R}| + \frac{1}{8} \sum_{\substack{x \in \mathbb{F}_p \setminus \mathcal{R} \\ x(x+u_2)(x-u_2)=0}} f(x) \right| \end{aligned} \tag{2.18}$$

$$\le |\mathcal{R}| + \frac{1}{8} \sum_{\substack{x\in\mathbb{F}_p\setminus\mathcal{R}\\ x(x+u_2)(x-u_2)=0}} |f(x)|$$

$$\le |\mathcal{R}| + \frac{1}{2}\big|\{x : x\in\mathbb{F}_p,\ x(x+u_2)(x-u_2)=0\}\big| \le |\mathcal{R}| + \frac{3}{2}.$$

On the other hand, by using the multiplicativity of γ we get

$$\frac{1}{8}\sum_{x\in\mathbb{F}_p} f(x) = \frac{1}{8}\sum_{x\in\mathbb{F}_p}(\gamma(x)+1)(\gamma(x+u_2)-1)(\gamma(x-u_2)-1) \tag{2.19}$$

$$= \frac{1}{8}p + \frac{1}{8}\sum_{i=1}^{7}\varepsilon_i \sum_{x\in\mathbb{F}_p}\gamma(f_i(x))$$

where $\varepsilon_1 = \varepsilon_4 = \varepsilon_7 = +1$, $\varepsilon_2 = \varepsilon_3 = \varepsilon_5 = \varepsilon_6 = -1$, and $f_1(x),\ldots,f_7(x)$ denote the polynomials

$$x,\ x+u_2,\ x-u_2,\ (x+u_2)(x-u_2),\ x(x-u_2),\ x(x+u_2),\ x(x+u_2)(x-u_2). \tag{2.20}$$

It follows from (2.19) that

$$\bigg|\frac{1}{8}\sum_{x\in\mathbb{F}_p} f(x)\bigg| \ge \frac{1}{8}p - \frac{1}{8}\sum_{i=1}^{7}\bigg|\sum_{x\in\mathbb{F}_p}\gamma(f_i(x))\bigg|. \tag{2.21}$$

Here the inner sum can be estimated by Weil's theorem:

Lemma 2.3. *Let χ be a multiplicative character of order $d>1$ of $\mathbb{F}_p$. Assume that $g(x)\in\mathbb{F}_p[x]$ has s distinct zeros in the algebraic closure of $\mathbb{F}_p$ and it is not a constant multiple of the dth power of a polynomial over $\mathbb{F}_p$. Then*

$$\bigg|\sum_{x\in\mathbb{F}_p}\chi(g(x))\bigg| \le (s-1)p^{1/2}.$$

Proof. This is a special case of Weil's theorem [21] (see also [20, p. 43]). ■

We have $u_2 \ne u_1 = 0$, and if $p>2$, then also $-u_2 \ne u_2$. Thus none of the polynomials in (2.20) has a multiple zero, so that Lemma 2.3 can be applied with γ and $f_i(x)$ $(i=1,\ldots,7)$ in place of χ and g, respectively. Then from (2.21) we get

$$\bigg|\frac{1}{8}\sum_{x\in\mathbb{F}_p} f(x)\bigg| \ge \frac{1}{8}p - \frac{1}{8}\sum_{i=1}^{7}2p^{1/2} = \frac{1}{8}p - \frac{7}{4}p^{1/2}. \tag{2.22}$$

It follows from (2.18) and (2.22) that

$$|\mathcal{R}| + \frac{3}{2} \ge \bigg|\frac{1}{8}\sum_{x\in\mathbb{F}_p} f(x)\bigg| \ge \frac{1}{8}p - \frac{7}{4}p^{1/2},$$

whence

$$|\mathcal{R}| \geq \frac{1}{8}p - \frac{7}{4}p^{1/2} - \frac{3}{2} > 0$$

for p large enough (for $p \geq 17$). Thus, indeed, there is a q satisfying (2.11)–(2.13). By (2.10) and (2.11) for this q we have

$$q \in \mathcal{Q} = \{0, u_2\} + \mathcal{V}.$$

It follows that there is a $v \in \mathcal{V}$ such that either

$$q = 0 + v \tag{2.23}$$

or

$$q = u_2 + v. \tag{2.24}$$

If (2.23) holds then we also have

$$u_2 + q = u_2 + v \in \mathcal{U} + \mathcal{V} = \mathcal{Q},$$

which contradicts (2.12), while if (2.24) holds, then

$$q - u_2 = v = 0 + v \in \mathcal{U} + \mathcal{V} = \mathcal{Q},$$

which contradicts (2.13). Thus our indirect assumption (2.9) leads to a contradiction, which completes the proof of Lemma 2.2. ■

Lemma 2.4. *If $\ell \in \mathbb{N}$, $\ell < p$, $\mathcal{S} = \{s_1, \dots, s_\ell\} \subset \mathbb{F}_p$, $\mathcal{T} \subset \mathbb{F}_p$ and*

$$\mathcal{S} + \mathcal{T} \subset \mathcal{Q}, \tag{2.25}$$

then

$$|\mathcal{T}| < \frac{p}{2^\ell} + \frac{\ell}{2}p^{1/2}. \tag{2.26}$$

We remark that by a theorem of Erdős and Shapiro [8] it follows from (2.25) that $|\mathcal{S}|\,|\mathcal{T}| = O(p)$. However, this information is not enough to handle the case when the sum $\mathcal{S} + \mathcal{T}$ is "unbalanced", i.e., $|\mathcal{S}|$ or $|\mathcal{T}|$ is small.

Proof of Lemma 2.4. Let $h(x) = \frac{1}{2^\ell}\prod_{i=1}^{\ell}(\gamma(x + s_i) + 1)$. Then clearly

$$h(x) \geq 0 \quad \text{for all } x \in \mathbb{F}_p. \tag{2.27}$$

Moreover, by (2.25), $\gamma(t + s_i) = +1$ for all $t \in \mathcal{T}$ and $i = 1, \dots, \ell$, so that

$$h(t) = 1 \quad \text{for all } t \in \mathcal{T}. \tag{2.28}$$

It follows from (2.27) and (2.28) that

$$\sum_{x \in \mathbb{F}_p} h(x) \geq \sum_{t \in \mathcal{T}} h(t) = |\mathcal{T}|. \tag{2.29}$$

On the other hand, by the multiplicativity of γ we have

$$\begin{aligned}2^\ell \sum_{x\in\mathbb{F}_p} h(x) &= p + \sum_{x\in\mathbb{F}_p}\sum_{j=1}^{\ell}\sum_{1\le i_1<\dots<i_j\le\ell} \gamma((x+s_{i_1})\dots(x+s_{i_j}))\\ &\le p + \sum_{j=1}^{\ell}\sum_{1\le i_1<\dots<i_j\le\ell}\Big|\sum_{x\in\mathbb{F}_p}\gamma((x+s_{i_1})\dots(x+s_{i_j}))\Big|.\end{aligned}$$

Since $s_{i_1},\dots,s_{i_j}$ are pairwise distinct, each of the innermost sums can be estimated by Lemma 2.3 (with γ in place of χ). Then we get

$$\begin{aligned}2^\ell \sum_{x\in\mathbb{F}_p} h(x) &\le p + \sum_{j=1}^{\ell}\sum_{1\le i_1<\dots<i_j\le\ell}(j-1)p^{1/2}\\ &= p + p^{1/2}\sum_{j=1}^{\ell}\binom{\ell}{j}(j-1) < p + p^{1/2}\sum_{j=1}^{\ell}\binom{\ell}{j}j = p+\ell 2^{\ell-1}p^{1/2},\end{aligned}$$

whence

$$\sum_{x\in\mathbb{F}_p} h(x) < \frac{p}{2^\ell} + \frac{\ell}{2}p^{1/2}. \tag{2.30}$$

Now (2.26) follows from (2.29) and (2.30). ∎

Lemma 2.5. *If p is large enough then we cannot have*

$$3 \le k = |\mathcal{U}| \le \left[\frac{\log p}{\log 2}\right] + 1. \tag{2.31}$$

Proof. Assume that contrary to the statement, (2.31) holds. Then using Lemma 2.4 with $\ell = k$, $\mathcal{S}=\mathcal{U}$, $\mathcal{T}=\mathcal{V}$ (so that (2.25) holds by (2.1)) we get

$$|\mathcal{V}| < \frac{p}{2^k} + \frac{k}{2}p^{1/2}. \tag{2.32}$$

Moreover, it follows from (2.1) by a trivial counting argument that

$$|\mathcal{U}|\,|\mathcal{V}| = |\{(u,v): u\in\mathcal{U},\ v\in\mathcal{V}\}| \ge |\mathcal{U}+\mathcal{V}| = |\mathcal{Q}| = \frac{p-1}{2},$$

whence

$$|\mathcal{V}| \ge \frac{p-1}{2|\mathcal{U}|} = \frac{p-1}{2k}. \tag{2.33}$$

It follows from (2.32) and (2.33) that

$$\frac{p-1}{2k} \le |\mathcal{V}| < \frac{p}{2^k} + \frac{k}{2}p^{1/2},$$

so that

$$p\Big(\frac{1}{k} - \frac{1}{2^{k-1}}\Big) < kp^{1/2} + \frac{1}{k}. \tag{2.34}$$

It can be shown by induction that $2^{k-1} \geq 4k/3$ for $k = 3, 4, \dots$. Thus it follows from (2.34) that

$$p\left(\frac{1}{k} - \frac{3}{4k}\right) < 2kp^{1/2},$$

whence

$$p^{1/2} < 8k^2,$$

which contradicts (2.31) for large p and completes the proof. ∎

Now we are ready to prove the upper bound (2.3) in Theorem 2.1. By Lemmas 2.3 and 2.5 (and since (2.1) is a non-trivial decomposition of $\mathcal{Q}$, so that $k > 1$) we have $k > \left[\frac{\log p}{\log 2}\right] + 1$. Thus writing $\ell = \left[\frac{\log p}{\log 2}\right] + 1$ we have $k > \ell$, so that

$$\{u_1, \dots, u_\ell\} \subset \{u_1, \dots, u_k\} = \mathcal{U},$$

whence, by (2.1),

$$\{u_1, \dots, u_\ell\} + \mathcal{V} \subset \mathcal{U} + \mathcal{V} = \mathcal{Q}.$$

Thus we may apply Lemma 2.4 with $\mathcal{S} = \{u_1, \dots, u_\ell\}$ and $\mathcal{T} = \mathcal{V}$. We obtain, for p large enough,

$$|\mathcal{V}| < \frac{p}{2^\ell} + \frac{\ell}{2}p^{1/2} < \frac{p}{2^{(\log p)/\log 2}} + \frac{1}{2}\left(\frac{\log p}{\log 2} + 1\right)p^{1/2} < p^{1/2}\log p,$$

which, together with (2.4), proves the upper bound (2.3).

Finally, it follows from (2.3) and (2.33) for large p that

$$|\mathcal{U}| \geq \frac{p-1}{2|\mathcal{V}|} > \frac{p-1}{2p^{1/2}\log p} > \frac{1}{3}\,\frac{p^{1/2}}{\log p},$$

which proves (2.2) and completes the proof of Theorem 2.1. ∎

3. 3-decompositions of $\mathcal{Q}$. Now we prove the following consequence of Theorem 2.1:

THEOREM 3.1. *If p is a prime large enough then $\mathcal{Q}$ has no* (*non-trivial*) 3-*decomposition*

$$\mathcal{A} + \mathcal{B} + \mathcal{C} = \mathcal{Q}. \tag{3.1}$$

Proof. Assume that contrary to the statement, (3.1) holds. We may rewrite (3.1) as

$$\mathcal{A} + (\mathcal{B} + \mathcal{C}) = \mathcal{Q},$$

which is a non-trivial 2-decomposition of $\mathcal{Q}$. Thus for p large enough it follows from Theorem 2.1 that

$$|\mathcal{B} + \mathcal{C}| < p^{1/2}\log p, \tag{3.2}$$

and in the same way we get

$$|\mathcal{A}+\mathcal{C}| < p^{1/2}\log p, \tag{3.3}$$

$$|\mathcal{A}+\mathcal{B}| < p^{1/2}\log p. \tag{3.4}$$

We will need the following result of Ruzsa:

LEMMA 3.2. *Let $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ be finite sets in a commutative group. Then we have*

$$|\mathcal{X}+\mathcal{Y}+\mathcal{Z}|^2 \le |\mathcal{X}+\mathcal{Y}|\,|\mathcal{Y}+\mathcal{Z}|\,|\mathcal{X}+\mathcal{Z}|.$$

Proof. This is Theorem 5.1 in [18] (see also [10]). ∎

Now, $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ are subsets of the additive group of $\mathbb{Z}/p\mathbb{Z}$, thus by Lemma 3.2 and (3.2)–(3.4) we have

$$|\mathcal{A}+\mathcal{B}+\mathcal{C}|^2 \le |\mathcal{A}+\mathcal{B}|\,|\mathcal{B}+\mathcal{C}|\,|\mathcal{A}+\mathcal{C}| < p^{3/2}(\log p)^3. \tag{3.5}$$

On the other hand, it follows from (3.1) that

$$|\mathcal{A}+\mathcal{B}+\mathcal{C}|^2 = |\mathcal{Q}|^2 = \left(\frac{p-1}{2}\right)^2 = \left(\frac{1}{4}+o(1)\right)p^2.$$

For p large enough this contradicts (3.5), which completes the proof of Theorem 3.1. ∎

4. Remarks. Let $\overline{\mathcal{Q}}$ denote the set of quadratic non-residues modulo p. Since $\overline{\mathcal{Q}}$ can be obtained from $\mathcal{Q}$ by multiplying it by a quadratic non-residue, it is easy to see that the statements of both Theorems 2.1 and 3.1 also hold with $\overline{\mathcal{Q}}$ in place of $\mathcal{Q}$.

Let $\mathcal{Q}^+ = \mathcal{Q}^+(p)$ denote the set of squares modulo p, so that $\mathcal{Q}^+ = \mathcal{Q}\cup\{0\}$. Then we have

$$\mathcal{Q}^+(5) = \{0,1,4\} = \{0,1\} + \{0,4\}, \tag{4.1}$$

so that $\mathcal{Q}^+(5)$ possesses a non-trivial 2-decomposition, while clearly $\mathcal{Q}(5) = \{1,4\}$ does not have such a decomposition. This shows that $\mathcal{Q}(p)$ and $\mathcal{Q}^+(p)$ may behave in a slightly different way. The proofs above can be easily adapted to show that our results also hold with $\mathcal{Q}^+$ in place of $\mathcal{Q}$ for p large enough. These facts suggest that, indeed, p must be large enough in Theorems 2.1 and 3.1. However, I have not been able to find an example of type (4.1) with $\mathcal{Q}$ in place of $\mathcal{Q}^+$.

Since both Weil's theorem and Ruzsa's Lemma 3.2 can also be used in finite fields, Theorems 2.1 and 3.1 can be extended to finite fields. On the other hand, the study of problems of this type can be much more complicated in $\mathbb{Z}/m\mathbb{Z}$, even the nature of the phenomena may change. In particular, for composite moduli one cannot use Weil's theorem; it might be of some interest to study how to replace it, and how far one can get in this way.

Acknowledgments. This research was partially supported by Hungarian National Foundation for Scientific Research, grants no. K67676 and K72731.

References

[1] N. Alon, O. Angel, I. Benjamini and E. Lubetzky, *Sums and products along sparse graphs*, Israel J. Math. 188 (2012), 353–384.

[2] P. Csikvári, *Subset sums avoiding quadratic nonresidues*, Acta Arith. 135 (2008), 91–98.

[3] R. Dietmann and C. Elsholtz, *Hilbert cubes in progression-free sets and in the set of squares*, Israel J. Math., to appear.

[4] C. Elsholtz, *A remark on Hofmann and Wolke's additive decompositions of the set of primes*, Arch. Math. (Basel) 76 (2001), 30–33.

[5] C. Elsholtz, *The inverse Goldbach problem*, Mathematika 48 (2001), 151–158.

[6] C. Elsholtz, *Additive decomposability of multiplicatively defined sets*, Funct. Approx. Comment. Math. 35 (2006), 61–77.

[7] P. Erdős and A. Sárközy, *On differences and sums of integers, I*, J. Number Theory 10 (1978), 430–450.

[8] P. Erdős and H. N. Shapiro, *On the least primitive root of a prime*, Pacific J. Math. 7 (1957), 861–865.

[9] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97 (2001), 53–65.

[10] K. Gyarmati, M. Matolcsi and I. Z. Ruzsa, *A superadditivity and submultiplicativity property for cardinalities of sumsets*, Combinatorica 30 (2010), 163–174.

[11] K. Gyarmati, A. Sárközy and C. L. Stewart, *On sums which are powers*, Acta Math. Hungar. 99 (2003), 1–24.

[12] N. Hegyvári and A. Sárközy, *On Hilbert cubes in certain sets*, Ramanujan J. 3 (1999), 303–314.

[13] A. Hofmann and D. Wolke, *On additive decompositions of the set of primes*, Arch. Math. (Basel) 67 (1996), 379–382.

[14] B. Hornfeck, *Ein Satz über die Primzahlmenge*, Math. Z. 60 (1954), 271–273 and 62 (1955), 502.

[15] H.-H. Ostmann, *Additive Zahlentheorie*, 2 Vols., Springer, Berlin, 1956.

[16] J.-P. Puchta, *On additive decompositions of the set of primes*, Arch. Math. (Basel) 78 (2002), 24–25.

[17] J. Rivat, A. Sárközy and C. L. Stewart, *Congruence properties of the Ω-function on sumsets*, Illinois J. Math. 43 (1999), 1–18.

[18] I. Z. Ruzsa, *Cardinality questions about sumsets*, in: Additive Combinatorics, A. Granville et al. (eds.), CRM Proc. Lecture Notes 43, Amer. Math. Soc., Providence, RI, 2007, 195–205.

[19] A. Sárközy and E. Szemerédi, *On the sequence of squares*, Mat. Lapok 16 (1965), 76–85 (in Hungarian).

[20] W. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Math. 536, Springer, New York, 1976.

[21] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Indust. 1041, Hermann, Paris, 1948.

András Sárközy
Department of Algebra and Number Theory
Eötvös Loránd University
Pázmány Péter sétány 1/C
H-1117 Budapest, Hungary
E-mail: sarkozy@cs.elte.hu

Received on 13.4.2011
and in revised form on 13.7.2011 (6669)