On additive decompositions of the set of primitive roots modulo p

Cécile Dartyge, András Sárközy

On additive decompositions of the set of primitive roots modulo p

Cécile Dartyge (Nancy) and András Sárközy (Budapest) *

Abstract. It is conjectured that the set $\mathcal{G}$ of the primitive roots modulo p has no decomposition (modulo p) of the form $\mathcal{G} = \mathcal{A}+\mathcal{B}$ with $|\mathcal{A}| \geqslant 2$, $|\mathcal{B}| \geqslant 2$. This conjecture seems to be beyond reach but it is shown that if such a decomposition of $\mathcal{G}$ exists at all, then $|\mathcal{A}|$, $|\mathcal{B}|$ must be around $p^{1/2}$, and then this result is applied to show that $\mathcal{G}$ has no decomposition of the form $\mathcal{G} = \mathcal{A}+\mathcal{B}+\mathcal{C}$ with $|\mathcal{A}| \geqslant 2$, $|\mathcal{B}| \geqslant 2$, $|\mathcal{C}| \geqslant 2$.

1. Introduction

Ostmann [4] 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 $\mathcal{A}+\mathcal{B} = \mathcal{C}$, $|\mathcal{A}| \geqslant 2$, $|\mathcal{B}| \geqslant 2$. If there are no sets $\mathcal{A}, \mathcal{B}$ with these properties, then $\mathcal{C}$ is said to be primitive.*

Definition 1.2. *An infinite set $\mathcal{C}$ of non-negative integers is said to be totalprimitive if every set $\mathcal{C}'$ which is equal to $\mathcal{C}$ apart from a finite number of exceptions (i.e. there is a number K such that $\mathcal{C}' \cap [K, +\infty[= \mathcal{C} \cap [K, +\infty[$) is primitive.*

He formulated the following conjecture :

Conjecture 1 (Ostmann, [4]). *The set $\mathcal{P}$ of the prime numbers is totalprimitive.*

This conjecture is still open and it seems to be beyond reach at present, although many partial results have been proved (see [6] for a list of these papers.) In particular, estimates have been given for the counting functions of sets $\mathcal{A}$, $\mathcal{B}$ with $\mathcal{A}+\mathcal{B} = \mathcal{P}'$ where $\mathcal{P}'$ is a set which is equal to $\mathcal{P}$ apart from a finite number of exceptions. Elsholtz has given the sharpest estimates of this type, and using these estimates he also proved:

Theorem 1.3 (Elsholtz, [1]). *If $\mathcal{P}'$ is equal to $\mathcal{P}$ apart from a finite number of exceptions, then there are no sets $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ of non-negative integers with*

$$\mathcal{A}+\mathcal{B}+\mathcal{C} = \mathcal{P}', \ \min(|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|) \geqslant 2.$$

In [6] Sárközy proposed to study finite problems of this type. He remarked that the definitions of reducibility and primitivity can be extended to any group, in particular, to the additive group of $\mathbb{F}_p$, thus the reducibility and primitivity of sets of residue classes (or residues) mod p can be defined in the same way as in Definition 1.1. He also introduced the following terminology :

2010 Mathematics Subject Classification: Primary 11P70; Secondary 11Bxx.

Key words and phrases: sumset, additive decomposition, inverse theorem, primitive roots.

* Research partially supported by the Hungarian National Foundation for Scientific Research, Grant K 67676 and K72731 and the Agence Nationale de la Recherche, grant ANR-10-BLAN 0103 MUNUM.

Definition 1.4. *If* $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_k \subset \mathbb{F}_p$,

$$\mathcal{A}_1 + \mathcal{A}_2 + \cdots + \mathcal{A}_k = \mathcal{B} \tag{1·1}$$

and

$$\min(|\mathcal{A}_1|, \dots, |\mathcal{A}_k|) \geqslant 2, \tag{1·2}$$

then (1·1) *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* (1·2)*.*

Here we will be interested in 2-decompositions and 3-decompositions only.

In [6], Sárközy formulated and studied the following conjecture:

Conjecture 2 (Sárközy [6]). *Let* p *be a prime number and let* $Q = Q(p)$ *denote the set of the quadratic residues modulo* p*. If* p *is large enough, then* $Q = Q(p)$ *is primitive, i.e., it has no (non-trivial)* 2 *decomposition.*

It turned out that the situation is similar to Ostmann's conjecture: conjecture 2 also seems beyond reach but the following partial results have been proved in [6].

Theorem 1.5 (Sárközy [6]). *If* p *is a prime large enough and*

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

is a non-trivial 2*-decomposition of* $Q = Q(p)$*, then we have*

$$\frac{p^{1/2}}{3\log p} < \min\{|\mathcal{U}|, |\mathcal{V}|\} \text{ and } \max\{|\mathcal{U}|, |\mathcal{V}|\} < p^{1/2}\log p.$$

Theorem 1.6 (Sárközy [6]). *If* p *is a prime large enough then* Q *has no (non-trivial)* 3*-decomposition*

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

There is another subset of $\mathbb{F}_p$ which is of special interest : the set of the modulo p primitive roots which we will denote by $\mathcal{G} = \mathcal{G}(p)$. The aim of this paper is to study this set. We conjecture that the analogue of conjecture 2 also holds:

Conjecture 3. *If* p *is a prime number large enough then the set* $\mathcal{G} = \mathcal{G}(p)$ *is primitive, i. e., it has no non-trivial* 2*-decomposition.*

Again this conjecture seems to be beyond reach but we will be able to prove partial results analogous to Theorem 1.3, Theorem 1.5, and Theorem 1.6. The crucial tool in the proofs will be an estimate for sums of the form

$$\sum_{g\in\mathcal{G}} \chi(f(g))$$

which can be derived from Weil's theorem [8] and we will use some ideas from [6], but we will also need some further ideas.

2. 2-decomposition of $\mathcal{G}$.

We will prove

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

$$\mathcal{U} + \mathcal{V} = \mathcal{G} \tag{2·1}$$

is a non-trivial 2-decomposition of $\mathcal{G} = \mathcal{G}(p)$, then we have:

$$\min(|\mathcal{U}|, |\mathcal{V}|) > \frac{\varphi(p-1)}{\tau(p-1)p^{1/2}\log p} \tag{2·2}$$

and

$$\max(|\mathcal{U}|, |\mathcal{V}|) < \tau(p-1)p^{1/2}\log p \tag{2·3}$$

where $\varphi(n)$ is Euler's function and $\tau(n)$ denotes the divisor function.

Note that by Wigert's theorem ([9], [3] p. 220),

$$\tau(n) < 2^{(1+\varepsilon)\frac{\log n}{\log\log n}} \text{ for } n > n_0(\varepsilon), \tag{2·4}$$

and we also have [3] p. 217

$$\varphi(n) \gg \frac{n}{\log\log n} \tag{2·5}$$

so that the bounds in (2·2) an (2·3) are by at most a factor $O(\exp(c\frac{\log p}{\log\log p}))$ apart.
Proof. We may assume that

$$2 \leqslant |\mathcal{U}| \leqslant |\mathcal{V}|. \tag{2·6}$$

Let

$$\mathcal{U} = \{u_1, u_2, \ldots, u_k\} \text{ with } 0 \leqslant u_1 < u_2 < \ldots < u_k < p. \tag{2·7}$$

For $i = 1, \ldots, k$ define u_i' by $u_i' = u_i - u_1$, let $\mathcal{U}' = \{u_1', u_2', \ldots, u_k'\} = \mathcal{U} - \{u_1\}$ 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

$$u_1 = 0 \tag{2·8}$$

in (2·7). By (2·6) and (2·7) we have

$$2 \leqslant |\mathcal{U}| = k \leqslant |\mathcal{V}|. \tag{2·9}$$

Now we will prove several lemmas.

Lemma 2.2. *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 over the algebraic closure of $\mathbb{F}_p$ and it is not the constant multiple of the D-th power of a polynomial over $\mathbb{F}_p$. Then*

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

Proof. This is a special case of Weil's theorem [8] (see also [7] p.43).

Lemma 2.3. *Let χ be a multiplicative character modulo p of order δ. Let $f(X) \in \mathbb{F}_p[X]$ be such that for all $d|p-1$, $f(X^d)$ is not a constant times the δ-th power of a polynomial of $\mathbb{F}_p[X]$. Then we have*

$$\Big| \sum_{g \in \mathcal{G}(p)} \chi(f(g)) \Big| \leqslant \tau(p-1)(s-1)\sqrt{p}, \tag{2·10}$$

where s is the number of distinct zeros of f over the algebraic closure of $\mathbb{F}_p$.

Proof. Let g_0 be a fixed primitive root of $\mathbb{F}_p$. The other primitive roots are g_0^k with $(k, p-1) = 1$. Thus we have :

$$\sum_{g \in \mathcal{G}_p} \chi(f(g)) = \sum_{\substack{k=1 \\ (k,p-1)=1}}^{p-1} \chi(f(g_0^k)).$$

Next we use the Möbius function to handle the coprimality condition :

$$\sum_{g \in \mathcal{G}_p} \chi(f(g)) = \sum_{d|p-1} \mu(d) \sum_{1 \leqslant k \leqslant \frac{p-1}{d}} \chi(f(g_0^{kd})) = \sum_{d|p-1} \frac{\mu(d)}{d} \sum_{x \in \mathbb{F}_p^*} \chi(f(x^d)),$$

since g_0^{kd} is periodic in k with period $\frac{p-1}{d}$. By the condition of Lemma 2.3 we can apply Weil's Theorem for the last character sum and this gives (2·10).

Lemma 2.4. *If $f(X) \in \mathbb{F}_p[X]$ is not of the form $f(X) = KX^t Q(X)^\delta$ with $K \in \mathbb{F}_p^*$, $t \in \mathbb{N}$, $Q(X) \in \mathbb{F}_p[X]$ and it satisfies $Q(0) \neq 0$ (Q can be constant) then f satisfies the condition of Lemma 2.3.*

Proof of Lemma 2.4. If f satisfies the conditions in the lemma then f can be written in the form $f(X) = X^t P(X)$ where $P \in \mathbb{F}_p[X]$ is of degree $\geqslant 1$, is not a constant times the δ-th power of a polynomial and satisfies $P(0) \neq 0$.

Thus we have to study the polynomials $f(Y^d) = Y^{dt} P(Y^d)$ for all $d|p-1$.

We write $P = P_1^{m_1} \cdots P_s^{m_s}$ where $P_1, \ldots, P_s$ are the distinct irreducible factors of P in $\mathbb{F}_p[X]$. Since P is not a constant times the δ-th power of a polynomial, there exists i such that $m_i \not\equiv 0 \,(\mathrm{mod}\, \delta)$. We can suppose that $m_1 \not\equiv 0 \,(\mathrm{mod}\, \delta)$.

Let $\alpha_1, \ldots, \alpha_r$ be the distinct roots of P_1 in $\overline{\mathbb{F}}_p$. For each $1 \leqslant i \leqslant r$, the equation $Y^d = \alpha_i$ has d distinct solutions $\beta_{i,1}, \ldots, \beta_{i,d}$.

Then $\beta_{1,1}$ is a root of $P(X^d)$ of multiplicity m_1 with $m_1 \not\equiv 0 \,(\mathrm{mod}\, \delta)$. We deduce that $f(X^d)$ is not a constant times the δ-th power of a polynomial.

Lemma 2.5. *With the notations and assumptions above we have*

$$(|\mathcal{U}| = k) \neq 2. \tag{2·11}$$

Proof. Assume that contrary to (2·11) we have:

$$k = 2. \tag{2·12}$$

Then by (2·1) and (2·8) we have

$$\{0, u_2\} + \mathcal{V} = \mathcal{G}. \tag{2·13}$$

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

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

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

$$g_0 \in \mathcal{G} \tag{2·14}$$

with

$$\gamma(g_0 + u_2) = 1 \tag{2·15}$$

and

$$\gamma(g_0 - u_2) = 1. \tag{2·16}$$

We remark that it follows trivially from (2·15) and (2·16) that

$$g_0 + u_2 \notin \mathcal{G} \text{ and } g_0 - u_2 \notin \mathcal{G} \tag{2·17}$$

and this is that we will need; thus (2·15) and (2·16) seem to "overshoot" our goal (2·17). However, the more demanding conditions (2·15) and (2·16) can be handled more easily than the milder condition (2·17), and this simplification will pay here and later in a similar situation as well.

Let $\mathcal{R}$ denote the set of the numbers g_0 satisfying (2·14), (2·15) and (2·16), and write $F(x) = (\gamma(x + u_2) + 1)(\gamma(x - u_2) + 1)$. If $g \in \mathcal{G}$ then $\gamma(g) = -1$, thus clearly we have

$$F(g) = 4 \text{ for } g \in \mathcal{R}, \tag{2·18}$$

$$F(g) = 0 \text{ for } g \in \mathcal{G} \setminus \mathcal{R},\ (g + u_2)(g - u_2) \neq 0, \tag{2·19}$$

$$|F(g)| \leqslant 2 \text{ for } g \in \mathcal{G} \setminus \mathcal{R},\ (g + u_2)(g - u_2) = 0 \tag{2·20}$$

and

$$|\{g : g \in \mathbb{F}_p, (g + u_2)(g - u_2) = 0\}| \leqslant 2. \tag{2·21}$$

It follows from (2·18), (2·19), (2·20) and (2·21) that

$$\begin{aligned} \Big|\frac{1}{4}\sum_{g\in\mathcal{G}} F(g)\Big| &= \Big|\frac{1}{4}\sum_{g\in\mathcal{R}} F(g) + \frac{1}{4}\sum_{g\in\mathcal{G}\setminus\mathcal{R}} F(g)\Big| \\ &= \Big||\mathcal{R}| + \frac{1}{4}\sum_{g\in\mathcal{G}\setminus\mathcal{R}} F(g)\Big| \leqslant |\mathcal{R}| + \frac{1}{4}\sum_{\substack{g\in\mathcal{G}\\(g+u_2)(g-u_2)=0}} |F(g)| \\ &\leqslant |\mathcal{R}| + \frac{1}{2}\big|\{g : g \in \mathbb{F}_p,\ (g + u_2)(g - u_2) = 0\}\big| \leqslant |\mathcal{R}| + 1. \end{aligned} \tag{2·22}$$

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

$$\begin{aligned} \frac{1}{4}\sum_{g\in\mathcal{G}} F(g) &= \frac{1}{4}\sum_{g\in\mathcal{G}} (\gamma(g + u_2) + 1)(\gamma(g - u_2) + 1) \\ &= \frac{|\mathcal{G}|}{4} + \frac{1}{4}\sum_{g\in\mathcal{G}} (\gamma((g + u_2)(g - u_2)) + \gamma(g + u_2) + \gamma(g - u_2)) \\ &= \frac{\varphi(p-1)}{4} + \frac{1}{4}\sum_{i=1}^{3}\sum_{g\in\mathcal{G}} \gamma(f_i(g)) \end{aligned} \tag{2·23}$$

where

$$f_1(X) = (X+u_2)(X-u_2),\ f_2(X) = X+u_2 \text{ and } f_3(X) = X-u_2. \tag{2·24}$$

It follows from (2·23) that

$$\Big|\frac{1}{4}\sum_{g\in\mathcal{G}} F(g)\Big| \geqslant \frac{\varphi(p-1)}{4} - \frac{1}{4}\sum_{i=1}^{3}\Big|\sum_{g\in\mathcal{G}}\gamma(f_i(g))\Big|. \tag{2·25}$$

We have $u_2 \neq u_1 = 0$, and if $p > 2$, then $-u_2 \neq u_2$ also holds. Thus each of the polynomials $f_i(X)$ in (2·24) satisfies the condition in Lemma 2.4 with 2 in place of D so that Lemma 2.3 can be applied with γ and f_i in place of χ and f, respectively. Thus we obtain from (2·25) that

$$\Big|\frac{1}{4}\sum_{g\in\mathcal{G}} F(g)\Big| \geqslant \frac{\varphi(p-1)}{4} - \frac{1}{4}\tau(p-1)(2+1+1)\sqrt{p} = \frac{\varphi(p-1)}{4} - \tau(p-1)\sqrt{p}. \tag{2·26}$$

It follows from (2·22) and (2·26) that

$$|\mathcal{R}|+1 \geqslant \Big|\frac{1}{4}\sum_{g\in\mathcal{G}} F(g)\Big| \geqslant \frac{\varphi(p-1)}{4} - \tau(p-1)\sqrt{p}$$

whence

$$|\mathcal{R}| \geqslant \frac{1}{4}\varphi(p-1) - \tau(p-1)\sqrt{p} - 1 > 0$$

for p large enough by (2·4) and (2·5). Thus, indeed, there is a g_0 satisfying (2·14), (2·15) and (2·16). By (2·13) and (2·14) for this g_0 we have

$$g_0 \in \mathcal{G} = \{0, u_2\} + \mathcal{V}.$$

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

$$g_0 = 0 + v \tag{2·27}$$

or

$$g_0 = u_2 + v \tag{2·28}.$$

If (2·27) holds then by (2·1) we also have

$$u_2 + g_0 = u_2 + v \in \mathcal{U} + \mathcal{V} = G$$

whence $\gamma(u_2+g_0) = -1$ which contradicts (2·15), while if (2·28) holds, then we have

$$g_0 - u_2 = v = 0 + v \in \mathcal{U} + \mathcal{V} = \mathcal{G}$$

whence $\gamma(g_0-u_2) = -1$ which contradicts (2·16). Thus our indirect assumption (2·12) leads to a contradiction which completes the proof of Lemma 2.5.

Lemma 2.6. *If* $\ell \in \mathbb{N}$, $\ell < p$, $\mathcal{S} = \{s_1, \dots, s_\ell\} \subset \mathbb{F}_p$,

$$s_1 = 0, \tag{2·29}$$

$\mathcal{T} \subset \mathbb{F}_p$ *and*

$$\mathcal{S} + \mathcal{T} \subset \mathcal{G}, \tag{2·30}$$

then we have

$$|\mathcal{T}| < \frac{\varphi(p-1)}{2^{\ell-1}} + \frac{\ell\tau(p-1)\sqrt{p}}{2}. \tag{2·31}$$

Proof. By (2·29) and (2·30) we have

$$\mathcal{T} = \{0\} + \mathcal{T} \subset \mathcal{S} + \mathcal{T} \subset \mathcal{G}. \tag{2·32}$$

Write $H(x) = 2^{-\ell}\prod_{i=1}^{\ell}(1 - \gamma(x + s_i))$. Then clearly

$$H(x) \geqslant 0 \ \forall x \in \mathbb{F}_p. \tag{2·33}$$

Moreover by (2·30), for all $t \in \mathcal{T}$ and $i = 1, 2, \dots, \ell$ we have $s_i + t \in \mathcal{G}$, thus $\gamma(s_i + t) = -1$. It follows that

$$H(t) = 1 \ \forall t \in \mathcal{T}. \tag{2·34}$$

By (2·32), (2·33) and (2·34) we have

$$\sum_{g\in\mathcal{G}} H(g) \geqslant \sum_{t\in\mathcal{T}} H(t) = |\mathcal{T}|. \tag{2·35}$$

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

$$\begin{aligned} 2^\ell \sum_{g\in\mathcal{G}} H(g) &= |\mathcal{G}| + \sum_{g\in\mathcal{G}}\sum_{j=1}^{\ell}(-1)^j \sum_{1\leqslant i_1<\dots<i_j\leqslant\ell} \gamma((g+s_{i_1})\cdots(g+s_{i_j})) \\ &= \varphi(p-1) + \sum_{j=1}^{\ell}(-1)^j \sum_{1\leqslant i_1<\dots<i_j\leqslant\ell} \sum_{g\in\mathcal{G}} \gamma((g+s_{i_1})\cdots(g+s_{i_j})) \\ &\leqslant \varphi(p-1) + \sum_{j=1}^{\ell}(-1)^j \sum_{1\leqslant i_1<\dots<i_j\leqslant\ell} \Big|\sum_{g\in\mathcal{G}} \gamma((g+s_{i_1})\cdots(g+s_{i_j}))\Big|. \end{aligned} \tag{2·36}$$

Each of the innermost sums is of the type (2·10), thus we would like to estimate them by using Lemma 2.3 with γ in place of χ. In order to ensure the applicability of Lemma 2.3, the conditions of Lemma 2.4 must hold. Indeed, all but one of these sums satisfy these conditions so that, indeed, Lemma 2.3 can be applied. The only exception is the sum with $j = 1$ when the only s_i is 0, so that this sum is $|\sum_{g\in\mathcal{G}}\gamma(g)\Big|$. The contribution of this sum is $|\mathcal{G}| = \varphi(p-1)$, so that by using Lemma 2.3 we get from (2·36) that

$$\begin{aligned} 2^\ell \sum_{g\in\mathcal{G}} H(g) &\leqslant 2\varphi(p-1) + \sum_{j=1}^{\ell} \sum_{1\leqslant i_1<\dots<i_\ell\leqslant\ell} \tau(p-1)(j-1)\sqrt{p} \\ &\leqslant 2\varphi(p-1) + \tau(p-1)\sqrt{p}\sum_{j=1}^{\ell}\binom{\ell}{j}(j-1) \\ &< 2\varphi(p-1) + \tau(p-1)\sqrt{p}\sum_{j=1}^{\ell}\binom{\ell}{j}j = 2\varphi(p-1) + \ell 2^{\ell-1}\tau(p-1)\sqrt{p} \end{aligned}$$

whence

$$\sum_{g\in\mathcal{G}} H(g) < \frac{\varphi(p-1)}{2^{\ell-1}} + \frac{\ell}{2}\tau(p-1)\sqrt{p}. \tag{2·37}$$

Then (2·31) follows from (2·35) and (2·37).

Lemma 2.7. *If p is large enough then we cannot have*

$$3 \leqslant k = |\mathcal{U}| \leqslant \Big\lfloor \frac{\log p}{\log 2} \Big\rfloor + 1. \tag{2·38}$$

Proof. Assume that contrary to the statement of the lemma (2·38) holds. Then using Lemma 2.6 with $\ell = k$, $\mathcal{S} = \mathcal{U}$, $\mathcal{T} = \mathcal{V}$ (so that (2·30) holds by (2·1)) we get that

$$|\mathcal{V}| < \frac{\varphi(p-1)}{2^{k-1}} + \frac{k}{2}\tau(p-1)\sqrt{p}. \tag{2·39}$$

Moreover, it follows from (2·1) by a trivial counting argument that

$$|\mathcal{U}||\mathcal{V}| = |\{(u,v) : u \in \mathcal{U}, v \in \mathcal{V}\}| \geqslant |\mathcal{U}+\mathcal{V}| = |\mathcal{G}| = \varphi(p-1),$$

whence

$$|\mathcal{V}| \geqslant \frac{\varphi(p-1)}{|\mathcal{U}|} = \frac{\varphi(p-1)}{k}. \tag{2·40}$$

It follows from (2·39) and (2·40) that

$$\frac{\varphi(p-1)}{k} \leqslant |\mathcal{V}| < \frac{\varphi(p-1)}{2^{k-1}} + \frac{k}{2}\tau(p-1)\sqrt{p}$$

so that

$$\varphi(p-1)\Big(\frac{1}{k} - \frac{1}{2^{k-1}}\Big) < \frac{k}{2}\tau(p-1)\sqrt{p}. \tag{2·41}$$

It can be shown by induction that $2^{k-1} \geqslant \frac{4k}{3}$ for $k \geqslant 3$. Thus it follows from (2·41) that

$$\varphi(p-1)\Big(\frac{1}{k} - \frac{3}{4k}\Big) < \frac{k}{2}\tau(p-1)\sqrt{p}$$

whence

$$\varphi(p-1) < 2k^2\tau(p-1)\sqrt{p}.$$

By (2·4) and (2·5) and (2·38) this cannot hold for large p and this contradiction completes the proof of Lemma 2.7.

Now we are ready to prove the upper bound (2·3) in Theorem 2.1. By Lemma 2.5 and Lemma 2.7 (and since (2·1) is a non-trivial decomposition of $\mathcal{G}$ so that $k > 1$) we have $k > \big\lfloor \frac{\log p}{\log 2} \big\rfloor + 1$. Thus writing $\ell = \big\lfloor \frac{\log p}{\log 2} \big\rfloor + 1$ we have $k > \ell$ so that

$$\{u_1, u_2, \dots, u_\ell\} \subset \{u_1, u_2, \dots, u_k\} = \mathcal{U}$$

whence, by (2·1)

$$\{u_1, u_2, \dots, u_\ell\} + \mathcal{V} \subset \mathcal{U} + \mathcal{V} = \mathcal{G}.$$

Thus we may apply Lemma 2.6 with $\mathcal{S} = \{u_1, u_2, \dots, u_\ell\}$ and $\mathcal{T} = \mathcal{V}$. We obtain for p large enough that

$$|\mathcal{V}| < \frac{\varphi(p-1)}{2^{\ell-1}} + \frac{\ell}{2}\tau(p-1)\sqrt{p} < \frac{2\varphi(p-1)}{2^{(\log p)/(\log 2)}} + \frac{1}{2}\Big(\frac{\log p}{\log 2} + 1\Big)\tau(p-1)\sqrt{p} < \tau(p-1)\sqrt{p}\log p$$

which, together with (2·5), proves the upper bound (2·3). Finally it follows from (2·3) and (2·40) for large p that

$$|\mathcal{U}| \geqslant \frac{\varphi(p-1)}{|\mathcal{V}|} > \frac{\varphi(p-1)}{\tau(p-1)\sqrt{p}\log p}$$

which proves (2·2) and this completes the proof of Theorem 2.1.

3. 3-decomposition of $\mathcal{G}$

Now we will prove that

Theorem 3.1. *If p is a prime large enough then $\mathcal{G}$ does not have a non-trivial 3-decomposition*

$$\mathcal{A}+\mathcal{B}+\mathcal{C}=\mathcal{G}. \tag{3·1}$$

Proof. This can be derived from Theorem 2.1 in the same way as Theorem 1.6 was derived in [6] from Theorem 1.5. Assume that contrary to the statement of the theorem (3·1) holds. We may write (3·1) as

$$(\mathcal{A}+\mathcal{B})+\mathcal{C}=(\mathcal{A}+\mathcal{C})+\mathcal{B}=(\mathcal{B}+\mathcal{C})+\mathcal{A}=\mathcal{G}.$$

Here we have three non trivial 2-decompositions of $\mathcal{G}$. Thus for p large enough it follows from Theorem 2.1 that

$$\max(|\mathcal{A}+\mathcal{B}|,|\mathcal{A}+\mathcal{C}|,|\mathcal{B}+\mathcal{C}|)<\tau(p-1)\sqrt{p}\log p. \tag{3·2}$$

Now we need the following result of Ruzsa

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

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

Proof. This is Theorem 5.1 in [5] (see also [2]).

$\mathcal{A},\mathcal{B},\mathcal{C}$ are subsets of the additive group of $\mathbb{Z}/p\mathbb{Z}$, thus by Lemma 3.2 and (3·2) we have

$$|\mathcal{A}+\mathcal{B}+\mathcal{C}|^2\leqslant|\mathcal{A}+\mathcal{B}||\mathcal{A}+\mathcal{C}||\mathcal{B}+\mathcal{C}|<(\tau(p-1))^3p^{3/2}(\log p)^3. \tag{3·3}$$

On the other hand, it follows from (3·1) that

$$|\mathcal{A}+\mathcal{B}+\mathcal{C}|^2=|\mathcal{G}|^2=(\varphi(p-1))^2.$$

By (2·4) and (2·5), for p large enough this contradicts (3·3) which completes the proof of Theorem 3.1.

References

[1] C. Elsholtz, The inverse Goldbach problem, Mathematika 48 (2001), 151-158.

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

[3] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, I-II, 2nd ed., Chelsea Publ. Co., New-York, 1953.

[4] H.-H. Ostmann, *Additive Zahlentheorie*, 2 vols, Springer, Berlin, 1956.

[5] I. Z. Ruzsa, Cardinality questions about sumsets, in : *Additive Combinatorics*, eds. A. Granville et al., CRM Proc. Lecture Notes, vol. 43, AMS, Providence, Rhode Island, USA, 2007; pp. 195-205.

[6] A. Sárközy, On additive decompositions of the set of the quadratic residues modulo p, Acta Arith., to appear.

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

[8] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Acta Sci. Ind. 1041, Hermann, Paris, 1948.

[9] S. Wigert, Sur l'ordre de grandeur du nombre des diviseurs d'un entier, Arkiv för mathematik, astronomi och fysik, Bd. 3, No. 18, 9S.; 1906-1907.

Cécile Dartyge
Institut Élie Cartan
Université Henri Poincaré–Nancy 1,BP 239
54506 Vandœuvre Cedex, France
dartyge@iecn.u-nancy.fr

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