On the reducibility of large sets of residues modulo p

Katalin Gyarmati, Sergei Konyagin, András Sárközy

Abstract

It is shown that if $p > 2$ and $\mathcal{C}$ is a subset of $\mathbb{F}_p$ with $|\mathcal{C}| \geq p - C_1 \frac{p}{\log p}$ then there are $\mathcal{A} \in \mathbb{F}_p$, $\mathcal{B} \in \mathbb{F}_p$ with $\mathcal{C} = \mathcal{A} + \mathcal{B}$, $|\mathcal{A}| \geq 2$, $|\mathcal{B}| \geq 2$. On the other hand, for every prime p there is a subset $\mathcal{C} \subset \mathbb{F}_p$ with $|\mathcal{C}| > p - C_2 \frac{\log \log p}{(\log p)^{1/2}} p$ such that there are no $\mathcal{A}, \mathcal{B}$ with these properties.

1 Introduction

Ostmann [6] introduced the following definitions:

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

Keywords and phrases: sumset, reducible set.

The first and the third authors are partially supported by the Hungarian National Foundation for Scientific Research, grants no. K72731 and K100291 and the János Bolyai Research Fellowship. The second author is partially supported by Russian Fund for Basic Research, Grant N. 11-01-00329, and by the Grant of the President of Russian Federation Nsh-6003.2012.1.

Definition 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*

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

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

Definition 2 *An* infinite *set $\mathcal{C}$ of non-negative integers is said to be* total-primitive *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, [6]) *The set of the prime numbers is totalprimitive.*

This conjecture is still wide open, although there are remarkable partial results (see [5] and the papers listed in it).

There are some further papers written on reducibility and totalprimitivity of infinite sequences of non-negative integers, in particular, Sárközy [7], [8] proved the following results:

Theorem A *If C is a small enough positive number then every sequence $\mathcal{C} = \{a_1, a_2, \dots\}$ of non-negative integers satisfying*

$$n + 1 - \mathcal{C}(n) < C\left(\frac{n(\log\log n)^2}{(\log n)^4}\right) \quad \text{for all } n \geq 3$$

(where $\mathcal{C}(n)$ denotes the counting function of $\mathcal{C}$: $\mathcal{C}(n) = |\mathcal{C} \cap \{0, 1, \dots, n\}|$) is reducible.

Theorem B *If $\mathcal{C} = \{a_1, a_2, \dots\}$ is any infinite sequence of non-negative integers then one can achieve by changing at most $O\left(\frac{n \log\log n}{\log n}\right)$ elements of $\mathcal{C}$ up to n that the modified sequence should be totalprimitive.*

Some further papers written on reducibility and totalprimitivity of infinite sequences are listed in [9].

In [9] Sárközy proposed to study *finite* analogues of problems of this type. He remarked that the definitions of reducibility and primitivity can be extended to any additive group, thus the reducibility and primitivity of subsets of $\mathbb{F}_p$ can be defined in the same way as in Definition 1. (While clearly the definition of totalprimitivity cannot be adapted to finite sets thus we will not use it.) We will identify $\mathbb{F}_p$ with the set of modulo p residue classes and, as it is customary, we will not distinguish between residue classes and the integers representing them. Using this convention, Sárközy proposed to study the reducibility, resp. primitivity of sets of residues modulo p. First in [9] he studied the set of the quadratic residues modulo p, and then in [4] Dartyge and Sárközy studied the set of the primitive roots modulo p.

In this paper our goal is to study the finite analogues of Theorems A and B: we will show that every large subset of $\mathbb{F}_p$ is reducible. More precisely, let $f(p)$ denote the cardinality of the largest primitive subset of $\mathbb{F}_p$; our goal is to estimate this function $f(p)$. The methods used in the infinite case in [7] and [8] cannot be used in this finite case.

Gowers and Green [3] and Alon [1] studied a closely related problem: they studied representations of large subsets $\mathcal{C}$ of $\mathbb{F}_p$ in form

$$\mathcal{A} + \mathcal{A} = \mathcal{C}. \tag{1.2}$$

Let $g(p)$ denote the cardinality of the largest subset $\mathcal{C}$ of $\mathbb{F}_p$ which cannot be represented in the form (1.2). Clearly we have

$$f(p) \leq g(p). \tag{1.3}$$

Improving on results of Gowers and Green [3], Alon [1] proved that

$$p - C_1 \frac{p^{2/3}}{(\log p)^{1/3}} < g(p) < p - C_2 \frac{p^{1/2}}{\log p}.$$

By (1.3), it follows from the upper bound here that

$$f(p) < p - C_2 \frac{p^{1/2}}{\log p}. \tag{1.4}$$

In this paper first we will prove that if $|\mathcal{C}|$ is "very large", i.e., $p - |\mathcal{C}|$ is very small then $\mathcal{C}$ can be represented in the form (1.1) with the further restriction $|\mathcal{B}| = 2$:

Theorem 1 *If p is a prime number with $p > 3$, $\mathcal{C} \subset \mathbb{F}_p$ and*

$$|\mathcal{C}| \geq p - p^{1/2}, \tag{1.5}$$

then $\mathcal{C}$ can be represented in the form

$$\mathcal{A} + \mathcal{B} = \mathcal{C} \quad \text{with } |\mathcal{A}| \geq 2, |\mathcal{B}| = 2. \tag{1.6}$$

Note that Alon, Granville and Ubis in [2] (see Theorem 3 in [2]) gave an estimate for the number of the sets $\mathcal{C} \subset \mathbb{F}_p$ having a representation of form (1.6).

It follows trivially from Theorem 1 that

Corollary 1 *For $p > 3$ we have*

$$f(p) < p - p^{1/2}.$$

This improves slightly on (1.4). However, if we replace the strong $|\mathcal{B}| = 2$ restriction in (1.6) by $|\mathcal{B}| \geq 2$, then we get a much better upper bound for $f(p)$:

Theorem 2 *There is a positive absolute constant C_3 such that if p is a prime number large enough then we have*

$$f(p) < p - C_3 \frac{p}{\log p}. \tag{1.7}$$

From the opposite side we will prove

Theorem 3 *There is an absolute constant p_0 such that if p is a prime number with $p > p_0$ then we have*

$$f(p) > p - 1.3 \frac{\log \log p}{(\log p)^{1/2}} p.$$

2 Proof of Theorem 1.

We have to show that if $p > 3$, $\mathcal{C} \subset \mathbb{F}_p$ and (1.5) holds then there are $\mathcal{A}, \mathcal{B}$ satisfying (1.6). Let $\overline{\mathcal{C}} = \mathbb{F}_p \setminus \mathcal{C}$. We claim that for any $h \in \{1, 2, \ldots, p-1\}$ there are c_h, c'_h with

$$c_h - c'_h = 2h, \ c_h \in \overline{\mathcal{C}}, \ c'_h \in \overline{\mathcal{C}}. \tag{2.1}$$

Indeed, take $h \in \{1, 2, \ldots, p-1\}$ and

$$\mathcal{A} = \{x \in \mathbb{F}_p : \ x \in \mathcal{C}, \, x + h \in \mathcal{C}\}, \quad \mathcal{B} = \{0, h\}.$$

Clearly, $\mathcal{A} + \mathcal{B} \subset \mathcal{C}$. If $\mathcal{A} + \mathcal{B} = \mathcal{C}$ with $|\mathcal{A}| \geq 2$ then we are done. Suppose that $\mathcal{A} + \mathcal{B} \neq \mathcal{C}$. Then there is $x \in \mathcal{C} \setminus (\mathcal{A} + \mathcal{B})$. We have $c_h := x + h \in \overline{\mathcal{C}}$

since otherwise $x \in \mathcal{A}$ and $x = x + 0 \in \mathcal{A} + \mathcal{B}$ contrary to our supposition. Similarly, $c'_h = x - h \in \overline{\mathcal{C}}$ since otherwise $x - h \in \mathcal{A}$ and $x = (x-h)+h \in \mathcal{A}+\mathcal{B}$ contrary to our supposition. Thus, the elements c_h and c'_h satisfy (2.1).

The number of the values of h is $p-1$, to each of them there is an ordered pair $(c_h, c'_h) \in \overline{\mathcal{C}}^2$ assigned by (2.1), and to different h values different ordered pairs are assigned. Thus the number $2\binom{|\overline{\mathcal{C}}|}{2}$ of the ordered pairs $(c_h, c'_h) \in \overline{\mathcal{C}}^2$ with $c_h \neq c'_h$ must be at least as large as the number of the h values:

$$2\binom{|\overline{\mathcal{C}}|}{2} \geq p - 1$$

whence

$$\left|\overline{\mathcal{C}}\right| \left(\left|\overline{\mathcal{C}}\right| - 1\right) \geq p - 1. \tag{2.2}$$

The left hand side is an increasing function of $\left|\overline{\mathcal{C}}\right|$ for $\left|\overline{\mathcal{C}}\right| \geq 1$, and by (1.5) we have

$$\left|\overline{\mathcal{C}}\right| = p - |\mathcal{C}| \leq p^{1/2}.$$

Thus we have

$$\left|\overline{\mathcal{C}}\right| \left(\left|\overline{\mathcal{C}}\right| - 1\right) \leq p^{1/2}\left(p^{1/2} - 1\right) = p - p^{1/2}$$

which contradicts (2.2), and this proves

$$\mathcal{A} + \mathcal{B} = \mathcal{C} \text{ with } |\mathcal{B}| = 2. \tag{2.3}$$

It remains to show that for $p > 3$ (2.3) also implies $|\mathcal{A}| \geq 2$. By a trivial counting argument it follows from (2.3) that

$$|\mathcal{A}|\,|\mathcal{B}| \geq |\mathcal{C}|$$

whence, by (1.5), (2.3) and $p > 3$ (and thus $p \geq 5$),

$$|\mathcal{A}| \geq \frac{|\mathcal{C}|}{|\mathcal{B}|} \geq \frac{p - p^{1/2}}{2} = p^{1/2}\frac{p^{1/2} - 1}{2} > 2 \cdot \frac{1}{2} = 1.$$

Since $|\mathcal{A}|$ is an integer this proves $|\mathcal{A}| \geq 2$ which completes the proof of the theorem. (Note that if p is 2 or 3 then the only reducible subset of $\mathbb{F}_p$ is $\mathbb{F}_p$ itself thus the condition $p > 3$ is necessary.)

3 Proof of Theorem 2.

We have to show that if C_3 is small enough and p_0 is large enough, then for $p > p_0$, $\mathcal{C} \subset \mathbb{F}_p$ and

$$|\mathcal{A}| \geq p - C_3 \frac{p}{\log p} \tag{3.1}$$

the set $\mathcal{C}$ is reducible, i.e., it can be represented in the form

$$\mathcal{A} = \mathcal{B} + \mathcal{C} \quad \text{with } \mathcal{B}, \mathcal{C} \subset \mathbb{F}_p,\ |\mathcal{B}|, |\mathcal{C}| \geq 2. \tag{3.2}$$

Write $\overline{\mathcal{A}} = \mathbb{F}_p \setminus \mathcal{A}$ and $n = \left|\overline{\mathcal{A}}\right|$. Let r denote a positive integer with $r > 2$, $r = o(p)$ which will be fixed later. We consider all the r-dimensional vectors $\mathbf{x} = (x_1, x_2, \ldots, x_r) \in \mathbb{F}_p^r$. We say that the vector $\mathbf{x}$ is *non-degenerate* if it contains at least two distinct components thus

$$|\{x_1, \ldots, x_r\}| \geq 2. \tag{3.3}$$

For every $\mathbf{x} \in \mathbb{F}_p^r$ we define the set $\mathcal{Y} = \mathcal{Y}(\mathbf{x})$ by

$$\mathcal{Y} = \{y \in \mathbb{F}_p :\ x_i + y \in \mathcal{A} \quad \text{for } i = 1, 2, \ldots, r\}.$$

Clearly, we have

$$\{x_1, x_2, \ldots, x_r\} + \mathcal{Y} \subset \mathcal{A}. \tag{3.4}$$

We will show that (choosing r in the appropriate way) there is a non-degenerate $\mathbf{x}$ such that

$$\{x_1, x_2, \ldots, x_r\} + \mathcal{Y} = \mathcal{A}. \tag{3.5}$$

Indeed, then (3.2) holds with $\mathcal{B} = \{x_1, x_2, \ldots, x_r\}$, $\mathcal{C} = \mathcal{Y}$ by (3.3), (3.5) and $r = o(p)$ so that this will complete the proof of the theorem.

Assume that for some non-degenerate $\mathbf{x}$ (3.5) does not hold. Then by (3.4) there is an $a \in \mathcal{A}$ such that

$$a \notin \{x_1, \ldots, x_r\} + \mathcal{Y}. \tag{3.6}$$

It follows from (3.6) that for every $i \in \{1, 2, \ldots, r\}$ there is an

$$f(i) \in \{1, 2, \ldots, r\} \tag{3.7}$$

such that

$$a - (x_i - x_{f(i)}) \in \overline{\mathcal{A}}. \tag{3.8}$$

Namely, if some i there was no $f(i)$ satisfying (3.7) and (3.8) then for this i and all $j \in \{1, 2, \ldots, r\}$ we had

$$a - (x_i - x_j) = (a - x_i) + x_j \in \mathcal{A} \quad (\text{for all } j \in \{1, 2, \ldots, r\}).$$

By the definition of $\mathcal{Y} = \mathcal{Y}(\mathbf{x})$ this implies that $a - x_i \in \mathcal{Y}$ whence, by (3.4),

$$a = x_i + (a - x_i) \in \{x_1, x_2, \ldots, x_r\} + \mathcal{Y}$$

which contradicts (3.6). Thus, indeed, for every $i \in \{1, 2, \ldots, r\}$ there is an $f(i)$ satisfying (3.7) and (3.8). Note that it follows from (3.8) that $f(i) \neq i$.

Let $\mathcal{F}$ denote the set of the mappings

$$f:\ \{1,2,\dots,r\} \to \{1,2,\dots,r\} \quad \text{with } f(i) \neq i \text{ for } i = 1,2,\dots,r. \tag{3.9}$$

For a fixed $f \in \mathcal{F}$ let X_f denote the set of the non-degenerate vectors

$$\mathbf{x} = (x_1, x_2, \dots, x_r) \in \mathbb{F}_p^r \tag{3.10}$$

such that (3.8) holds for some $a \in \mathcal{A}$, and write $M_f = |X_f|$. Now we will estimate M_f.

To any $f \in \mathcal{F}$ we assign the directed graph G_f with vertices $1,2,\dots,r$ and edges joining i with $f(i)$ and directed from i to $f(i)$. In order to study these graphs G_f we will use the following terminology:

We will consider finite *directed* graphs, i.e., finite graphs such that every edge has a *starting point* P and an *endpoint* Q, and then the edge is considered to be directed from P to Q. We denote this edge by $P \to Q$, and two vertices P, Q can be joined with at most two edges: $P \to Q$ and $Q \to P$. The number of vertices of G is denoted by $|G|$. *Path* is a sequence $V_1, V_2, \dots, V_n$ of vertices of the graph such that each of the pairs V_i, V_{i+1} $(i = 1,2,\dots,n-1)$ is joined. If for every $i \in \{1,2,\dots,n-1\}$ the edge joining V_i and V_{i+1} is directed as $V_i \to V_{i+1}$, then the path is called a *directed path* and we denote this directed path by $V_1 \to V_2 \to \cdots \to V_n$. If $V_1 \to V_2 \to \cdots \to V_n$ is a directed path such that the vertices $V_1, V_2, \dots, V_n$ are pairwise distinct then the directed path is called *simple.* If $V_1 \to V_2 \to \cdots \to V_n \to V_{n+1}$ is a directed path such that $V_1, V_2, \dots, V_n$ are pairwise distinct and $V_{n+1} = V_1$ then we say that it is a *directed cycle* of *size* n and this directed cycle is denoted by $(V_1 \to V_2 \to \cdots \to V_n)$. (Note that this definition also includes the $n = 2$

special case $(V_1 \rightarrow V_2)$ when V_1, V_2 are joined with both edges $V_1 \rightarrow V_2$ and $V_2 \rightarrow V_1$.) The number of edges starting out from the vertex V is called the outdegree of V and it will be denoted by $d(V)$. We will also introduce

Definition 3 *A directed graph is called an* admissible graph *if it is the union of a directed cycle and several directed rooted trees such that the root of each of them is a vertex belonging to this directed cycle, the directed cycle and the trees have no other common vertex than the root of the tree, the trees are pairwise disjoint, and every edge of any tree is directed towards the root. (See Figure 1 for an admissible graph.)*

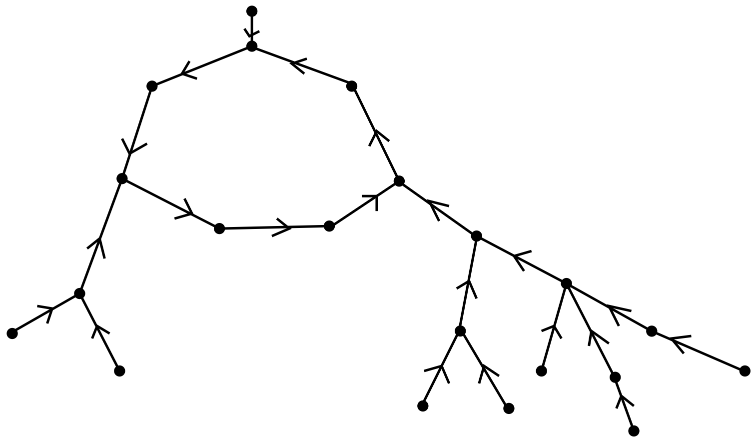

Figure 1.

An admissible graph

We will need

Lemma 1 *If the outdegree of every vertex V of a directed graph G is 1:*

$$d(V) = 1 \quad \textit{for every vertex } V \textit{ of } G, \tag{3.11}$$

then the graph is the disjoint union of admissible graphs.

(The graph G is the disjoint union of certain graphs $G_1, G_2, \dots, G_k$ if for every $i \neq j$ the vertex sets of G_i and G_j are disjoint and no vertex of G_i is joined with a vertex of G_j.)

Proof of Lemma 1. We will prove by induction on $|G|$. It follows from (3.11) that the smallest possible value of $|G|$ is 2. Then G has 2 edges which form a directed cycle of size 2, and this is an admissible graph.

Now assume that $k \in \mathbb{N}$, $k > 2$ and the statement of the lemma is true for graphs of $2, 3, \dots, k-1$ vertices, and consider a graph G with $|G| = k$ which satisfies assumption (3.11). Let V_1 be an arbitrary vertex of G. By (3.11) and the finiteness of G there is a unique simple directed path $V_1 \to V_2 \to \cdots \to V_i$ starting from V_1 such that the endpoint of the single edge starting from V_i is one of $V_1, V_2, \dots, V_{i-1}$, say V_j (with $1 \le j < i$). Then the directed cycle $(V_j \to V_{j+1} \to \cdots \to V_i)$ is a directed cycle contained in G; denote it by C. Now consider any vertex V_ℓ of this directed cycle. By (3.11) there is a single edge starting from V_ℓ, and its endpoint must be the next vertex of the directed cycle; there is no other edge starting from V_ℓ. On the other hand, there may exist several edges whose endpoint is V_ℓ, and consider the starting points of all these edges. By (3.11) the single edge starting from them ends in V_ℓ; on the other hand, each of them can be the endpoint of several edges. Consider the starting points of all these edges, and repeat the previous argument with each of these vertices. Continuing this algorithm, we end up with a directed rooted tree whose root is V_ℓ and every edge is directed towards the root, and whose vertices different from the root are not joined with any vertex not belonging to the tree. If we consider the directed cycle C and all the trees rooted at the vertices of C and generated in the way described above, then clearly we get an admissible graph G_0. Drop the vertices and edges of this graph from G. Then we get a graph G' which also satisfies the assumptions in the lemma, and for which $|G'| < |G| = k$; thus by our assumption the statement of the lemma holds with G' in place of G, i.e., G' is the disjoint union of admissible graphs. Adding G_0 to these admissible graphs we get that G is the disjoint union of admissible graphs which completes the proof of the lemma.

Now we return to the estimate of M_f (for fixed f satisfying (3.9)). By (3.9) the graph G satisfies (3.11) with G_f in place of G thus G_f can be written as the disjoint union of admissible graphs. Let $v = v(f)$ denote the number of these admissible graphs $G_f(1), G_f(2), \dots, G_f(v)$ and let $C(1), C(2), \dots, C(v)$ denote the directed cycles in these graphs. For every $j \in \{1, 2, \dots, v\}$ we fix an arbitrary vertex $i_j \in C(j)$. Let $I = \{i_1, i_2, \dots, i_v\}$ and $I' = \{1, 2, \dots, r\} \backslash I$.

Define the linear mapping $\Lambda_f : \ \mathbb{F}_p^r \to \mathbb{F}_p^{r-v}$ by setting

$$\Lambda_f(\mathbf{x}) = \Lambda_f((x_1, x_2, \dots, x_r)) = \mathbf{y} = (y_i)_{i \in I'} \tag{3.12}$$

where

$$y_i = x_i - x_{f(i)}. \tag{3.13}$$

We claim that Λ_f is a mapping from $\mathbb{F}_p^r$ *onto* $\mathbb{F}_p^{r-v}$, more precisely, for every $\mathbf{y} \in \mathbb{F}_p^{r-v}$ there are exactly p^v vectors $\mathbf{x} \in \mathbb{F}_p^r$ satisfying (3.12) and (3.13).

Indeed, by removing the edges $i_j \to f(i_j)$ for $j = 1, 2, \dots, v$ from G_f we get a graph G'_f. Then G'_f is a disjoint union of the graphs $G'_f(j)$ that we get from the admissible graph $G_f(j)$ by removing the edge $i_j \to f(i_j)$. Suppose that each vertex i of G'_f $(1 \le i \le r)$ has a value $x_i \in \mathbb{F}_p$, and then we assign a value to each edge of G'_f, namely we assign the value $x_i - x_{f(i)}$ to the edge $i \to f(i)$ (where $i \in I'$). Clearly, our claim holds, i.e., for every $\mathbf{y} \in \mathbb{F}_p^{r-v}$ there are exactly p^v vectors $\mathbf{x} \in \mathbb{F}_p^r$ satisfying (3.12) and (3.13) if for fixed $\mathbf{y} = (y_i)_{i \in I'} \in \mathbb{F}_p^{r-v}$ there are exactly p^v tuples $\{x_1, x_2, \dots, x_r\}$ such that if the vertex i of G'_f has the value x_i for $1 \le i \le r$ then the edge $i \to f(i)$ has the value $y_i (= x_i - x_{f(i)})$ for $i \in I'$. It follows from the structure of admissible graphs that if h is any vertex of $G'_f(j)$ then there is a *unique* path P in $G'_f(j)$ (where edges are directed but it need not be a *directed* path in the sense that the endpoint of an edge need not be the starting point of the next one) leading from i_j to h (indeed, we removed the edge $i_j \to f(i_j)$ from the cycle $C(j)$ to achieve this). Starting out from the vertex i_j and moving along this path P towards h, and using (3.13) for the subscripts i which are vertices belonging to the path P, we can determine the x_i's with these subscripts successively, and it turns out that all these $x_i's$ assume a uniquely defined value. This is so for every vertex h of $G'_f(j)$. So far the starting x_i value, x_{i_j} has been fixed. If we let x_{i_j} run over the elements of $\mathbb{F}_p$, then we obtain that the x_i values belonging to the vertices i of $G'_f(j)$ may assume p values. Since the graphs $G_f(1), G_f(2), \dots, G_f(v)$ are disjoint, thus we finally obtain that for fixed $\mathbf{y}$ in (3.12) the vector $\mathbf{x}$ in (3.12) and (3.13) can be chosen in p^v ways which proves our claim above.

We are ready to estimate M_f, i.e., the number of vectors $\mathbf{x}$ satisfying (3.10) and (3.8) for some a. This a can be chosen in at most $|\mathcal{A}| \le p$ ways. Now we fix a. For every $i \in I'$ we have $a - y_i \in \overline{\mathcal{A}}$. Thus we can choose each y_i with $i \in I'$ in n ways. (Recall that $n = |\overline{\mathcal{A}}|$.) Finally by our claim above, for any $\mathbf{y} = (y_i)_{i \in I'}$ we have p^v vectors $\mathbf{x}$ with $\Lambda_f(\mathbf{x}) = \mathbf{y}$. It follows that

$$M_f \le p \cdot n^{|I'|} \cdot p^v = p^{v+1} n^{r-v} = p^{r+1} \left(\frac{n}{p}\right)^{r-v}. \tag{3.14}$$

Now we will estimate the number $N(v,u)$ of functions f such that $v(f) = v$ and the total size of directed cycles in G_f is u:

$$u = \sum_{j=1}^{v} |C_j|.$$

Clearly, if $N(v,u) \ne 0$ then we must have

$$0 < 2v \le u \le r. \tag{3.15}$$

There are $\binom{r}{u} < 2^r$ ways to choose the union $\mathcal{J}$ of the vertices of all directed cycles with $|\mathcal{J}| = u$. The vertices in $\mathcal{J}$ have $u! < r^u$ orderings; for any splitting of $\mathcal{J}$ into v directed cycles we can concatenate all the directed cycles to get one of these orderings in at least $v!$ ways. For a fixed ordering we have $\binom{u-1}{v-1} < 2^{u-1} < 2^r$ ways to split the elements of $\mathcal{J}$ into v directed cycles according to the chosen order (the order of the vertices of the directed cycle also defines the direction of the edges). Moreover, we can define the function f on $\{1, 2, \ldots, r\} \setminus \mathcal{J}$ in at most r^{r-u} ways. Thus we get

$$N(v,u) < 2^r r^u (v!)^{-1} 2^r r^{r-u} = 4^r r^r / v!. \tag{3.16}$$

Now let $N(v)$ denote the number of functions f of type (3.9) such that $v(f) = v$. Then by (3.15) and (3.16) we have

$$N(v) = \sum_{0<u\le r} N(v,u) < \sum_{0<u\le r} \frac{4^r r^r}{v!} = \frac{4^r r^{r+1}}{v!} = 4^r r \frac{r^r}{v!} < 6^r \frac{r^r}{v!} \tag{3.17}$$

since $4^r r < 6^r$ for $r > 2$ which can be proved easily by induction. It follows from (3.14), (3.15) and (3.17) that the number N of the non-degenerate vectors $\mathbf{x}$ such that (3.5) fails is at most

$$\begin{aligned} N &\le \sum_f M_f \le \sum_{v \le r/2} \sum_{v(f)=v} p^{r+1} \left(\frac{n}{p}\right)^{r-v} = \sum_{v \le r/2} p^{r+1} \left(\frac{n}{p}\right)^{r-v} \sum_{v(f)=v} 1 \\ &= p^{r+1} \left(\frac{n}{p}\right)^{r-v} \sum_{v \le r/2} N(v) < p^{r+1} \left(\frac{n}{p}\right)^{r-v} \sum_{v \le r/2} 6^r \frac{r^r}{v!} \\ &= p^{r+1} \sum_{v \le r/2} (6r)^r \left(\frac{n}{p}\right)^{r-v} \cdot \frac{1}{v!}. \end{aligned} \tag{3.18}$$

For $v \in \mathbb{N}$ we have

$$\left(\frac{e}{v}\right)^v > \frac{1}{v!}$$

thus

$$\left(\frac{n}{p}\right)^{r-v} \cdot \frac{1}{v!} < \left(\frac{n}{p}\right)^r \left(\frac{ep}{nv}\right)^v \qquad \text{for } v \in \mathbb{N}. \tag{3.19}$$

Now we assume that

$$\frac{r}{2} < \frac{p}{n}. \tag{3.20}$$

The function $\left(\frac{ep}{nx}\right)^x$ is increasing for $0 < x < \frac{p}{n}$, thus by (3.20) for $v \le r/2$ we have

$$\left(\frac{ep}{nv}\right)^v \le \left(\frac{2ep}{nr}\right)^{r/2} \qquad (\text{for } v \le r/2). \tag{3.21}$$

It follows from (3.18), (3.19) and (3.21) that

$$N < p^{r+1} \sum_{v \le r/2} (6r)^r \left(\frac{n}{p}\right)^r \left(\frac{2ep}{nr}\right)^{r/2} \le p^{r+1} \frac{r}{2} \left(\frac{6rn}{p}\right)^r \left(\frac{2ep}{nr}\right)^{r/2} \tag{3.22}$$

$$= p^{r+1} \frac{r}{2} \left(\frac{72enr}{p}\right)^{r/2}. \tag{3.23}$$

Now we fix r: we take

$$r = (1 + o(1)) 2 \log p \tag{3.24}$$

then (3.20) holds if $C_3 < 1$ for every large p by (3.1), more precisely, we may take r as $r = [2 \log p]$. Finally, we take $C_3 = \frac{1}{1100}$ in (1.7) and (3.1) so that

$$n = |\overline{\mathcal{A}}| \le \frac{1}{1100} \frac{p}{\log p}. \tag{3.25}$$

Then it follows from (3.23), (3.24) and (3.25) with a little computation that for p large enough we have

$$N < \frac{1}{2} p^r.$$

Thus there are more than $(1 + o(1)) \frac{p^r}{2}$ non-degenerate vectors $\mathbf{x}$ for which (3.5) holds and this completes the proof of Theorem 2.

4 Proof of Theorem 3.

Throughout the proof we will assume that p is a prime number large enough.

We introduce the following notations:

$$t \stackrel{\text{def}}{=} \left[\frac{\log \log p - 2 \log \log \log p + 1}{\log 4} \right], \tag{4.1}$$

$$B \stackrel{\text{def}}{=} [0.71 \log p], \tag{4.2}$$

$$T \stackrel{\text{def}}{=} \left[1.01 p \left(1 - \frac{1}{2^t} \right)^B \right], \tag{4.3}$$

$$H \stackrel{\text{def}}{=} 3T. \tag{4.4}$$

Let $u_1, u_2, \ldots, u_t$ be t arbitrary different quadratic non-residues modulo p. (The number of u_i's is the number t defined by (4.1).) Moreover, we define two sets by

$$\mathcal{C}_0 \stackrel{\text{def}}{=} \left\{ x \in \mathbb{F}_p : \ \exists 1 \le i \le t, \text{ such that } \left(\frac{x^2 - u_i}{p} \right) = -1 \right\},$$
$$\mathcal{D}_0 \stackrel{\text{def}}{=} \left\{ x \in \mathbb{F}_p : \ \forall 1 \le i \le t \text{ we have } \left(\frac{x^2 - u_i}{p} \right) = 1 \right\}.$$

Then

$$\mathcal{C}_0 \cap \mathcal{D}_0 = \emptyset, \quad \mathcal{C}_0 \cup \mathcal{D}_0 = \mathbb{F}_p. \tag{4.5}$$

Moreover, let

$$\mathbb{W} = \left\{ \mathcal{C} : \ \mathcal{C} \subset \mathcal{C}_0 \text{ and } |\mathcal{C}| = |\mathcal{C}_0| - H \right\}.$$

It suffices to prove:

Lemma 2 *For all $\mathcal{C} \in \mathbb{W}$ we have*

$$|C| > \left(1 - 1.3 \cdot \frac{\log \log p}{(\log p)^{1/2}} \right) p.$$

Lemma 3 *There exists a set $\mathcal{C} \in \mathbb{W}$ which is primitive.*

Indeed, Theorem 3 follows trivially from Lemma 2 and Lemma 3. In Sections 4.1 and 4.2 we will prove Lemma 2 and Lemma 3, respectively. In both Sections 4.1 and 4.2 we will use the following estimates for the constants t, B, T and H:

Lemma 4

$$t < 0.01 \frac{\log\log p}{(\log p)^{1/2}} p \tag{4.6}$$

$$2tp^{1/2} < 0.01 \frac{\log\log p}{(\log p)^{1/2}} p \tag{4.7}$$

$$2tp^{1/2} < 0.005p < 0.01 \left(1 - \frac{1}{2^t}\right) p \tag{4.8}$$

$$t^2 4^t < 1.45 \log p \tag{4.9}$$

$$1 - \frac{1}{2^t} > 1 - 1.24 \frac{\log\log p}{(\log p)^{1/2}} \tag{4.10}$$

$$-\frac{3.61}{t} > -0.002 \frac{\log p}{t2^t} \tag{4.11}$$

$$H < 0.01 \frac{\log\log p}{(\log p)^{1/2}} p \tag{4.12}$$

$$H < 0.005p < 0.01 \left(1 - \frac{1}{2^t}\right) p \tag{4.13}$$

$$T < p/11 < p/2 \tag{4.14}$$

$$H > 0.25p^{0.51} \tag{4.15}$$

$$T > 0.08p^{0.51}. \tag{4.16}$$

Proof of Lemma 4. By (4.1)

$$\frac{\log\log p - 2\log\log\log p + 1}{\log 4} - 1 \le t \le \frac{\log\log p - 2\log\log\log p + 1}{\log 4}, \tag{4.17}$$

from which (4.6), (4.7) and (4.8) follows immediately.

By (4.17) we get

$$\frac{e}{4} \cdot \frac{\log p}{(\log\log p)^2} \le 4^t \le e \cdot \frac{\log p}{(\log\log p)^2}$$

$$0.67 \cdot \frac{\log p}{(\log\log p)^2} < 4^t < 2.72 \cdot \frac{\log p}{(\log\log p)^2} \tag{4.18}$$

By (4.17) and (4.18)

$$t^2 4^t < \left(\frac{\log\log p}{\log 4}\right)^2 \cdot 2.72 \cdot \frac{\log p}{(\log\log p)^2} < 1.45 \log p,$$

which proves (4.9).

By (4.18)

$$0.81 \cdot \frac{(\log p)^{1/2}}{\log\log p} < 2^t < 1.65 \cdot \frac{(\log p)^{1/2}}{\log\log p}. \tag{4.19}$$

(4.10) and (4.11) follow from (4.19) immediately.

By $1 + x \leq e^x$, (4.2) and (4.19) we have

$$\begin{aligned}\left(1 - \frac{1}{2^t}\right)^B &\leq e^{-B/2^t} < e^{-0.7 \log p / \left(1.65 \frac{(\log p)^{1/2}}{\log\log p}\right)} \\ &< e^{-0.42 (\log p)^{1/2} \log\log p},\end{aligned}$$

from which (4.12), (4.13) and (4.14) follow.

By $1 + x \leq e^x$, (4.2) and (4.19) we have

$$\begin{aligned}\left(1 - \frac{1}{2^t}\right)^B &= \frac{1}{\left(1 + \frac{1}{2^t - 1}\right)^B} \geq \frac{1}{e^{B/(2^t-1)}} = e^{-B/(2^t-1)} \\ &\geq e^{-0.71 \log p / \left(0.81 \frac{(\log p)^{1/2}}{\log\log p} - 1\right)} > e^{-0.71 \log p / \left(0.8 \frac{(\log p)^{1/2}}{\log\log p}\right)} \\ &> e^{-0.89 (\log p)^{1/2} \log\log p},\end{aligned}$$

from which (4.15) and (4.16) follow.

4.1 Proof of Lemma 2.

We will derive Lemma 2 from the following:

Lemma 5 *Let $f_1(x), f_2(x), \ldots, f_r(x)$ be different monic irreducible polynomials of degree ≥ 2. Let k denote the maximum of the degrees of the polynomials $f_1(x), f_2(x), \ldots, f_r(x)$:*

$$k = \max_{1 \leq i \leq r} \deg f_i(x).$$

Moreover, let $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r \in \{-1, +1\}$*. Then*

$$\left|\left\{x:\ \left(\frac{f_i(x)}{p}\right) = \varepsilon_i \textit{ for } 1 \le i \le r\right\}\right| = \frac{p}{2^r} + \delta r k p^{1/2}, \tag{4.20}$$

where $-1 < \delta < 1$*.*

Proof of Lemma 5. Since $f_i(x) \in \mathbb{F}_p[x]$ is irreducible, for $x \in \mathbb{F}_p$ we have $f_i(x) \ne 0$. Thus $\left(\frac{f_i(x)}{p}\right) = +1$ or -1. For $\varepsilon_i \in \{-1, +1\}$ we have

$$\left(\frac{f_i(x)}{p}\right) + \varepsilon_i = \begin{cases} 2\varepsilon_i & \text{if } \left(\frac{f_i(x)}{p}\right) = \varepsilon_i, \\ 0 & \text{if } \left(\frac{f_i(x)}{p}\right) = -\varepsilon_i. \end{cases}$$

Thus

$$\frac{1}{2^r \varepsilon_1 \cdots \varepsilon_r} \prod_{i=1}^{r} \left(\left(\frac{f_i(x)}{p}\right) + \varepsilon_i\right) = \begin{cases} 1 & \text{if } \left(\frac{f_i(x)}{p}\right) = \varepsilon_i \text{ for all } 1 \le i \le r \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$\begin{aligned} S &\stackrel{\text{def}}{=} \left|\left\{x:\ \left(\frac{f_i(x)}{p}\right) = \varepsilon_i \ \text{ for all } 1 \le i \le r\right\}\right| \\ &= \frac{1}{2^r \varepsilon_1 \cdots \varepsilon_r} \sum_{x=0}^{p-1} \prod_{i=1}^{r} \left(\left(\frac{f_i(x)}{p}\right) + \varepsilon_i\right). \end{aligned} \tag{4.21}$$

Since the Legendre symbol is multiplicative it is easy to see that there exist polynomials $g_1(x), g_2(x), \dots, g_{2^r-1}(x)$ (which are products of different $f_i(x)$'s) with degree $\le rk$ such that

$$\prod_{i=1}^{r} \left(\left(\frac{f_i(x)}{p}\right) + \varepsilon_i\right) = \varepsilon_1 \cdots \varepsilon_r + \sum_{i=1}^{2^r-1} \left(\frac{g_i(x)}{p}\right). \tag{4.22}$$

By (4.21), (4.22), $\varepsilon_1 \cdots \varepsilon_r = \pm 1$ and the triangle inequality we get

$$\begin{aligned} S &= \frac{p}{2^r} + \frac{1}{2^r \varepsilon_1 \cdots \varepsilon_r} \sum_{i=1}^{2^r-1} \sum_{x=0}^{p-1} \left(\frac{g_i(x)}{p}\right) \\ &\le \frac{p}{2^r} + \frac{1}{2^r} \sum_{i=1}^{2^r-1} \left|\sum_{x=0}^{p-1} \left(\frac{g_i(x)}{p}\right)\right|. \end{aligned}$$

Similarly, by the triangle inequality

$$\begin{aligned} S &= \frac{p}{2^r} + \frac{1}{2^r\varepsilon_1\cdots\varepsilon_r}\sum_{i=1}^{2^r-1}\sum_{x=0}^{p-1}\left(\frac{g_i(x)}{p}\right) \\ &\geq \frac{p}{2^r} - \frac{1}{2^r}\sum_{i=1}^{2^r-1}\left|\sum_{x=0}^{p-1}\left(\frac{g_i(x)}{p}\right)\right|. \end{aligned}$$

Thus there exists an $-1 \leq \delta_0 \leq 1$ with

$$\begin{aligned} S &= \frac{p}{2^r} + \frac{1}{2^r\varepsilon_1\cdots\varepsilon_r}\sum_{i=1}^{2^r-1}\sum_{x\in\mathbb{F}_p}\left(\frac{g_i(x)}{p}\right) \\ &= \frac{p}{2^r} + \delta_0\frac{1}{2^r}\sum_{i=1}^{2^r-1}\left|\sum_{x\in\mathbb{F}_p}\left(\frac{g_i(x)}{p}\right)\right|. \end{aligned} \tag{4.23}$$

Next we use Weil's theorem [11]:

Lemma 6 *Suppose that p is a prime, χ is a non-principal character modulo p of order d, $f \in \mathbb{F}_p[x]$ has s distinct roots in $\overline{\mathbb{F}}_p$, and it is not the constant multiple of the d-th power of a polynomial over $\mathbb{F}_p$. Then*

$$\left|\sum_{x\in\mathbb{F}_p}\chi(f(x))\right| < sp^{1/2}.$$

Proof of Lemma 6. See [11] and an elementary proof can be found in [10].

The factorization of $g_i(x)$ contains different monic irreducible factors $f_j(x)$, thus $g_i(x)$ is not of the form $ch(x)^2$ with $c \in \mathbb{F}_p$, $h(x) \in \mathbb{F}_p[x]$ so that we may use Lemma 6. For $1 \leq i \leq 2^r - 1$ there exists an $0 \leq \delta_i < 1$ such that

$$\left|\sum_{x\in\mathbb{F}_p}\left(\frac{g_i(x)}{p}\right)\right| = \delta_i rkp^{1/2}.$$

Then (4.23) can be rewritten as

$$S = \left|\left\{x :\ \left(\frac{f_i(x)}{p}\right) = \varepsilon_i \ \text{ for all } 1 \leq i \leq r\right\}\right| = \frac{p}{2^r} + \delta rkp^{1/2},$$

where $\delta = \frac{1}{2^r}\delta_0 \left(\delta_1 + \cdots + \delta_{2^r-1}\right)$, so $-1 < \delta < 1$ which was to be proved.

Next we return to the proof of Lemma 2. Using Lemma 5 for $f_i(x) = x^2 - u_i$ (where $1 \le i \le t$) we get

$$|\mathcal{D}_0| = \frac{p}{2^t} + 2\delta t p^{1/2}$$

with $-1 < \delta < 1$. Then by (4.5) we have

$$\begin{aligned} |\mathcal{C}_0| &= \left(1 - \frac{1}{2^t}\right) p - 2\delta t p^{1/2} \\ &> \left(1 - \frac{1}{2^t}\right) p - 2tp^{1/2}. \end{aligned}$$

Thus

$$|\mathcal{C}_0| - H > \left(1 - \frac{1}{2^t}\right) p - 2tp^{1/2} - H. \tag{4.24}$$

Using this, (4.7), (4.10) and (4.12) we get

$$|\mathcal{C}_0| - H > \left(1 - 1.3 \cdot \frac{\log\log p}{(\log p)^{1/2}}\right) p. \tag{4.25}$$

Since for $\mathcal{C} \in \mathbb{W}$ we have

$$|\mathcal{C}| = |\mathcal{C}_0| - H,$$

we get

$$|C| > \left(1 - 1.3 \cdot \frac{\log\log p}{(\log p)^{1/2}}\right) p,$$

which was to be proved.

4.2 Proof of Lemma 3.

In order to prove Lemma 3 we need several auxiliary lemmas and definitions.

Definition 4 *We will represent the elements of* $\mathbb{F}_p$ *by the integers* $0, 1, 2, \ldots, p-1$*. Then every* $\mathcal{A} \subseteq \mathbb{F}_p$ *is of form*

$$\mathcal{A} = \{a_1, a_2, \ldots, a_K\}$$

with $0 \le a_1 < a_2 < \cdots < a_K \le p-1$*. For* $|\mathcal{A}| \ge 2$*, define* $\Delta(\mathcal{A})$ *by*

$$\Delta(\mathcal{A}) = \{a_1 - a_2, a_1 - a_3, \ldots, a_1 - a_K\} \cup \{a_2 - a_1\} \ (\subseteq \mathbb{F}_p).$$

Clearly

$$|\Delta(\mathcal{A})| = |\mathcal{A}| \quad \text{or} \quad |\Delta(\mathcal{A})| = |\mathcal{A}| - 1.$$

Lemma 7 *Let* $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$ *with* $|\mathcal{A}| \ge 2$*. Then for every* $x \in \mathcal{A} + \mathcal{B}$ *there exists an* $a \in \Delta(\mathcal{A})$ *such that* $x + a \in \mathcal{A} + \mathcal{B}$*.*

Proof of Lemma 7. Let $\mathcal{A} = \{a_1, a_2, \ldots, a_K\} \subseteq \mathbb{F}_p$ and $\mathcal{B} = \{b_1, b_2, \ldots, b_L\} \subseteq \mathbb{F}_p$ where $0 \le a_1 < a_2 < \cdots < a_K \le p-1$ and $0 \le b_1 < b_2 < \cdots < b_L \le p-1$. Then $\Delta(\mathcal{A}) = \{a_1 - a_2, a_1 - a_3, \ldots, a_1 - a_K\} \cup \{a_2 - a_1\}$. We distinguish two cases. First consider the case when $x \in \mathcal{A} + \mathcal{B}$ is of the form $a_i + b_j$ with $2 \le i \le K$, $1 \le j \le L$. Then for $a = a_1 - a_i \in \Delta(\mathcal{A})$ we have

$$x + a = (a_i + b_j) + (a_1 - a_i) = a_1 + b_j \in \mathcal{A} + \mathcal{B}.$$

Next consider the case when $x \in \mathcal{A} + \mathcal{B}$ is of the form $a_1 + b_j$ with $1 \le j \le L$. Then for $a = a_2 - a_1 \in \Delta(\mathcal{A})$ we have

$$x + a = (a_1 + b_j) + (a_2 - a_1) = a_2 + b_j,$$

which completes the proof of Lemma 7.

Definition 5 *For $\mathcal{A} \subseteq \mathbb{F}_p$, $|\mathcal{A}| \geq 2$ define $\mathcal{U}(\mathcal{A})$ by*

$$\mathcal{U}(\mathcal{A}) = \Big\{ x \in \mathbb{F}_p : \left(\frac{x^2 - u_1}{p}\right) = -1 \text{ and for } a \in \Delta(\mathcal{A}),\ 1 \leq i \leq t, \\ \text{we have } \left(\frac{(x+a)^2 - u_i}{p}\right) = 1 \Big\}.$$

Lemma 8 *For $\mathcal{A} \subseteq \mathbb{F}_p$, $|\mathcal{A}| \geq 2$ we have*

$$|\mathcal{U}(\mathcal{A})| > \frac{1}{2^{|\mathcal{A}|t+1}} p - 2(|\mathcal{A}|\, t + 1) p^{1/2}. \tag{4.26}$$

Proof of Lemma 8. Next we prove (4.26). Let $f_1(x) = x^2 - u_1$ and $f_2(x), f_3(x), \dots, f_{|\Delta(\mathcal{A})|t+1}(x)$ denote the polynomials in the set

$$S = \left\{ (x+a)^2 - u_i :\ a \in \Delta(\mathcal{A}), 1 \leq i \leq t \right\}.$$

Clearly the polynomials $f_i(x)$ $(1 \leq i \leq |\Delta(\mathcal{A})|\, t + 1)$ are irreducible over $\mathbb{F}_p$, since u_i is a quadratic non-residue modulo p. Moreover, the monic irreducible polynomials $f_i(x)$ $(1 \leq i \leq |\Delta(\mathcal{A})|\, t + 1)$ are pairwise different: Indeed, suppose that for two polynomials we have

$$(x+a)^2 - u_i = (x+a')^2 - u_j$$

where $a, a' \in \Delta(\mathcal{A}) \cup \{0\}$, $1 \leq i, j, \leq t$. Then

$$x^2 + 2ax + a^2 - u_i = x^2 + 2a'x + (a')^2 - u_j$$

whence

$$2a = 2a'$$

$$a^2 - u_i = (a')^2 - u_j.$$

It follows that $a = a'$, $u_i = u_j$. Since $\Delta(\mathcal{A})$ does not contain 0, from this we get that the monic irreducible polynomials $f_i(x)$ $(1 \le i \le |\Delta(\mathcal{A})|\, t + 1)$ are pairwise different.

Using Lemma 5 for the polynomials $f_i(x)$ $(1 \le i \le |\Delta(\mathcal{A})|\, t + 1)$ we get (4.26).

Lemma 9 *Suppose that* $\mathcal{A} + \mathcal{B} \subseteq \mathcal{C}_0$ *with* $|\mathcal{A}| \ge 2$. *Then* $\mathcal{U}(\mathcal{A}) \subseteq \mathcal{C}_0$ *and* $\mathcal{U}(\mathcal{A}) \cap (\mathcal{A} + \mathcal{B}) = \emptyset$.

Proof of Lemma 9. Clearly,

$$\begin{aligned} \mathcal{U}(\mathcal{A}) &\subseteq \left\{ x \in \mathbb{F}_p : \ \left(\frac{x^2 - u_1}{p} \right) = -1 \right\} \\ &\subseteq \left\{ x \in \mathbb{F}_p : \ \exists 1 \le i \le t, \text{ such that } \left(\frac{x^2 - u_i}{p} \right) = -1 \right\} = \mathcal{C}_0. \end{aligned}$$

Suppose that $x \in \mathcal{U}(\mathcal{A})$ and $x \in \mathcal{A} + \mathcal{B}$. Then by Lemma 7 there exists $a \in \Delta(\mathcal{A})$ such that $x + a \in \mathcal{A} + \mathcal{B} \subseteq \mathcal{C}_0$, so $x + a \in \mathcal{C}_0$. Thus there exists $1 \le j \le t$ such that

$$\left(\frac{(x+a)^2 - u_j}{p} \right) = -1.$$

But then $x \notin \mathcal{U}(\mathcal{A})$, which contradicts our assumption.

From Lemma 9 immediately follows:

Lemma 10 *If* $\mathcal{A} + \mathcal{B} \subseteq \mathcal{C}_0$ *with* $|\mathcal{A}| \ge 2$, *then*

$$|\mathcal{U}(\mathcal{A})| + |\mathcal{A} + \mathcal{B}| \le |\mathcal{C}_0|.$$

Next we prove

Lemma 11 *If $\mathcal{C} \in \mathbb{W}$ can be written in the form $\mathcal{C} = \mathcal{A} + \mathcal{B}$ with $|\mathcal{A}| \geq 2$, then*

$$|\mathcal{A}| > \frac{\log(p/(4H))}{t \log 2}. \tag{4.27}$$

Proof of Lemma 11. Suppose that

$$|\mathcal{A}| \leq \frac{\log(p/(4H))}{t \log 2}. \tag{4.28}$$

Since $\mathcal{A} + \mathcal{B} \in \mathbb{W}$ we have

$$|\mathcal{C}_0| - |\mathcal{A} + \mathcal{B}| = H.$$

Since $\mathcal{A} + \mathcal{B} \subseteq \mathcal{C}_0$, by Lemma 10 we have

$$|\mathcal{U}(\mathcal{A})| + |\mathcal{A} + \mathcal{B}| \leq |\mathcal{C}_0|$$

$$|\mathcal{U}(\mathcal{A})| \leq |\mathcal{C}_0| - |\mathcal{A} + \mathcal{B}| = H.$$

By this and Lemma 8

$$\frac{1}{2^{|\mathcal{A}|t+1}} p - 2(|\mathcal{A}|\, t + 1) p^{1/2} \leq H. \tag{4.29}$$

Next we prove that

$$2(|\mathcal{A}|\, t + 1) p^{1/2} < \frac{1}{2} \cdot \frac{1}{2^{|\mathcal{A}|t+1}} p. \tag{4.30}$$

Indeed, since by (4.15)

$$H > 0.25 p^{0.51},$$

by (4.28), we have

$$|\mathcal{A}| \leq \frac{\log(p/(4H))}{t \log 2} < \frac{0.49}{\log 2} \cdot \frac{\log p}{t}.$$

Thus if p is large enough then

$$|\mathcal{A}| < \frac{\log(p^{1/2}/8) - \log\log p}{t\log 2}$$

whence

$$|\mathcal{A}|\,t + 1 < \frac{\log(p^{1/2}/4) - \log\log p}{\log 2}.$$

Thus

$$2^{|\mathcal{A}|t+1} < \frac{p^{1/2}}{4\log p}, \tag{4.31}$$

and

$$|\mathcal{A}|\,t + 1 < \log p. \tag{4.32}$$

(4.30) follows from (4.31) and (4.32).

By (4.29) and (4.30) we get

$$\frac{1}{2}\cdot\frac{1}{2^{|\mathcal{A}|t+1}}p < H.$$

This is equivalent with

$$|\mathcal{A}| > \frac{\log(p/(4H))}{t\log 2},$$

which contradicts (4.28). Thus (4.28) does not hold, and this completes the proof of Lemma 11.

Lemma 12 *If $\mathcal{C} \in \mathbb{W}$ can be written of the form $\mathcal{C} = \mathcal{A} + \mathcal{B}$ with $|\mathcal{A}| \geq 2$, then*

$$|\mathcal{A}| > 0.7t2^t.$$

Proof of Lemma 12. We will estimate the right hand side of (4.27). By (4.3), (4.4) and $1+x \le e^x$, we get that if p is large enough then

$$p/(4H) = \frac{p}{12\left[1.01p\left(1-\frac{1}{2^t}\right)^B\right]} \ge \frac{p}{12.12p\left(1-\frac{1}{2^t}\right)^B} = \frac{1}{12.12\left(1-\frac{1}{2^t}\right)^B}$$
$$\ge \frac{1}{12.12e^{-B/2^t}} = \frac{1}{12.12}e^{B/2^t}.$$

Thus

$$\log(p/(4H)) > -2.5 + B/2^t.$$

So

$$\frac{\log(p/(4H))}{t\log 2} > \frac{-3.61}{t} + \frac{B}{\log 2\cdot t2^t} = \frac{-3.61}{t} + \frac{[0.71\log p]}{\log 2\cdot t2^t}$$
$$> \frac{-3.61}{t} + \frac{0.709\log p}{\log 2\cdot t2^t} > \frac{-3.61}{t} + \frac{1.022\log p}{t2^t}.$$

By (4.11)

$$\frac{\log(p/(4H))}{t\log 2} > \frac{1.02\log p}{t2^t} > 0.7\cdot\frac{1.45\log p}{t2^t}.$$

By this and (4.9)

$$\frac{\log(p/(4H))}{t\log 2} > 0.7\frac{t^2 4^t}{t2^t} = 0.7t2^t. \tag{4.33}$$

Using Lemma 11 and (4.33) we get the conclusion of the lemma.

Lemma 13 *Suppose that $\mathcal{A}+\mathcal{B} \subseteq \mathcal{C}_0$ and $|\mathcal{A}| \ge k$. Then*

$$|\mathcal{B}| < \left(1-\frac{1}{2^t}\right)^k \left(p + 2^{k+1}tkp^{1/2}\right).$$

Proof of Lemma 13. Suppose that $x \in \mathbb{F}_p$. Then for an $a \in \mathcal{A}$ it holds that $x+a$ is in $\mathcal{C}_0$ if there exists an $1 \le i \le t$ such that

$$\left(\frac{(x+a)^2 - u_i}{p}\right) = -1.$$

By this we have

$$1-\frac{1}{2^t}\prod_{i=1}^{t}\left(\left(\frac{(x+a)^2-u_i}{p}\right)+1\right)=\begin{cases}1 & \text{if there exists } 1\le i\le t \\ & \quad\text{such that } \left(\frac{(x+a)^2-u_i}{p}\right)=-1 \\ 0 & \text{if for all } 1\le i\le t \\ & \quad\text{we have } \left(\frac{(x+a)^2-u_i}{p}\right)=1.\end{cases}$$

Let $a_1,a_2,\dots,a_k\in\mathcal{A}$ be k different elements from $\mathcal{A}$. Then

$$\prod_{j=1}^{k}\left(1-\frac{1}{2^t}\prod_{i=1}^{t}\left(\left(\frac{(x+a_j)^2-u_i}{p}\right)+1\right)\right)=\begin{cases}1 & \text{if for all } a_j\ \exists 1\le i\le t \\ & \quad\text{such that} \\ & \quad\left(\frac{(x+a_j)^2-u_i}{p}\right)=-1 \\ 0 & \text{otherwise.}\end{cases} \tag{4.34}$$

If $\mathcal{A}+\mathcal{B}\subseteq\mathcal{C}_0$, then for all $x\in\mathcal{B}$ and $a_j\in\mathcal{A}$ we have $x+a_j\in\mathcal{C}_0$ and thus there exists u_i such that

$$\left(\frac{(x+a_j)^2-u_i}{p}\right)=-1.$$

By (4.34) we have

$$\prod_{j=1}^{k}\left(1-\frac{1}{2^t}\prod_{i=1}^{t}\left(\left(\frac{(x+a_j)^2-u_i}{p}\right)+1\right)\right)=1 \text{ for all } x\in\mathcal{B}.$$

Clearly, for $x\in\mathbb{F}_p\setminus\mathcal{B}$ the value of $\prod_{j=1}^{k}\left(1-\frac{1}{2^t}\prod_{i=1}^{t}\left(\left(\frac{(x+a_j)^2-u_i}{p}\right)+1\right)\right)$ is 0 or 1. By this

$$|\mathcal{B}|\le\sum_{x\in\mathbb{F}_p}\prod_{j=1}^{k}\left(1-\frac{1}{2^t}\prod_{i=1}^{t}\left(\left(\frac{(x+a_j)^2-u_i}{p}\right)+1\right)\right).$$

After taking the term-by-term product in the second product, we get that there exist monic polynomials $f_1(x),f_2(x),\dots,f_{2^t-1}(x)$ (of degree $\le 2t$) such that

$$|\mathcal{B}| \leq \sum_{x\in\mathbb{F}_p}\prod_{j=1}^{k}\left(1-\frac{1}{2^t}-\frac{1}{2^t}\sum_{s=1}^{2^t-1}\left(\frac{f_s(x+a_j)}{p}\right)\right). \tag{4.35}$$

Let

$$F(a_i) = \{f_s(x+a_i):\ 1\leq s\leq 2^t-1\}.$$

By taking the term-by-term product in (4.35) and using the triangle inequality we get

$$\begin{aligned}
|\mathcal{B}| &\leq \sum_{x\in\mathbb{F}_p}\left(1-\frac{1}{2^t}\right)^k + \sum_{x\in\mathbb{F}_p}\sum_{s=1}^{k}\left(1-\frac{1}{2^t}\right)^{k-s}\left(-\frac{1}{2^t}\right)^s \sum_{1\leq i_1<i_2<\cdots<i_s\leq k} \\
&\quad \sum_{g_1\in F(a_{i_1})}\sum_{g_2\in F(a_{i_2})}\cdots\sum_{g_s\in F(a_{i_s})}\left(\frac{\prod_{j=1}^{s}g_j(x)}{p}\right) \\
&= \left(1-\frac{1}{2^t}\right)^k p + \sum_{s=1}^{k}\left(1-\frac{1}{2^t}\right)^{k-s}\left(-\frac{1}{2^t}\right)^s \sum_{1\leq i_1<i_2<\cdots<i_s\leq k} \\
&\quad \sum_{g_1\in F(a_{i_1})}\sum_{g_2\in F(a_{i_2})}\cdots\sum_{g_s\in F(a_{i_s})}\sum_{x\in\mathbb{F}_p}\left(\frac{\prod_{j=1}^{s}g_j(x)}{p}\right) \\
&\leq \left(1-\frac{1}{2^t}\right)^k p + \sum_{s=1}^{k}\left(1-\frac{1}{2^t}\right)^{k-s}\left(\frac{1}{2^t}\right)^s \sum_{1\leq i_1<i_2<\cdots<i_s\leq k} \\
&\quad \sum_{g_1\in F(a_{i_1})}\sum_{g_2\in F(a_{i_2})}\cdots\sum_{g_s\in F(a_{i_s})}\left|\sum_{x\in\mathbb{F}_p}\left(\frac{\prod_{j=1}^{s}g_j(x)}{p}\right)\right|.
\end{aligned}$$

Since each $f_s(x+a_j)$ is a product of different monic irreducible polynomials $(x+a_j)^2-u_i$, a product $\prod_{j=1}^{s}g_j(x)$ for $g_1\in F(a_{i_1}), g_2\in F(a_{i_2}),\ldots,g_s\in F(a_{i_s})$ (where $1\leq i_1<i_2<\cdots<i_s\leq k$) is not of the form $cg(x)^2$ with $c\in\mathbb{F}_p$ and $g(x)\in\mathbb{F}_p[x]$. Moreover, deg $\prod_{j=1}^{s}g_j(x)\leq k\max_{1\leq j\leq s}\deg g_j(x)\leq$

$k\max_{1\le i\le 2^t-1}\deg f_i(x)\le 2tk$. Thus by using Lemma 6 we get

$$\begin{aligned}
|\mathcal{B}| &< \left(1-\frac{1}{2^t}\right)^k p+\sum_{s=1}^{k}\left(1-\frac{1}{2^t}\right)^{k-s}\left(\frac{1}{2^t}\right)^s \sum_{1\le i_1<i_2<\cdots<i_s\le k} \\
&\quad \sum_{g_1\in F(a_{i_1})}\sum_{g_2\in F(a_{i_2})}\cdots\sum_{g_s\in F(a_{i_s})} 2tkp^{1/2} \\
&= \left(1-\frac{1}{2^t}\right)^k p+2tkp^{1/2}\sum_{s=1}^{k}\left(1-\frac{1}{2^t}\right)^{k-s}\left(\frac{1}{2^t}\right)^s \sum_{1\le i_1<i_2<\cdots<i_s\le k} \\
&\quad \sum_{g_1\in F(a_{i_1})}\sum_{g_2\in F(a_{i_2})}\cdots\sum_{g_s\in F(a_{i_s})} 1 \\
&= \left(1-\frac{1}{2^t}\right)^k p+2tkp^{1/2}\sum_{s=1}^{k}\left(1-\frac{1}{2^t}\right)^{k-s}\left(\frac{1}{2^t}\right)^s \sum_{1\le i_1<i_2<\cdots<i_s\le k}\left(2^t-1\right)^s \\
&= \left(1-\frac{1}{2^t}\right)^k p+2tkp^{1/2}\sum_{s=1}^{k}\left(1-\frac{1}{2^t}\right)^{k} \sum_{1\le i_1<i_2<\cdots<i_s\le k} 1 \\
&= \left(1-\frac{1}{2^t}\right)^k p+2tkp^{1/2}\sum_{s=1}^{k}\binom{k}{s}\left(1-\frac{1}{2^t}\right)^{k} \\
&< \left(1-\frac{1}{2^t}\right)^k \left(p+2^{k+1}tkp^{1/2}\right),
\end{aligned}$$

which was to be proved.

Lemma 14 *Suppose that* $\mathcal{A}+\mathcal{B}\subseteq\mathcal{C}_0$ *and* $\min\{|\mathcal{A}|,[0.71\log p]\}\ge k$. *Then*

$$|\mathcal{B}|<1.01\left(1-\frac{1}{2^t}\right)^k p.$$

Proof of Lemma 14. Since p is large enough, by the conditions of the lemma we have

$$k<\frac{\log(p^{1/2}/(300t))}{\log 2}-\frac{\log\log(p^{1/2}/(300t))}{\log 2}.$$

Then

$$k2^k < \frac{\log(p^{1/2}/(300t))}{\log 2} \frac{p^{1/2}/(300t)}{\log(p^{1/2}/(300t))} < 0.005\frac{p^{1/2}}{t}$$

$$2^{k+1}tkp^{1/2} < 0.01p.$$

Using this and Lemma 13 we get

$$|\mathcal{B}| < \left(1 - \frac{1}{2^t}\right)^k \left(p + 2^{k+1}tkp^{1/2}\right) < 1.01\left(1 - \frac{1}{2^t}\right)^k p.$$

Lemma 15 *Suppose that $\mathcal{A} + \mathcal{B} \in \mathbb{W}$ where $|\mathcal{A}| \geq 2$. Then*

$$|\mathcal{A}| > [0.71 \log p].$$

Proof of Lemma 15. By $\mathcal{A} + \mathcal{B} \in \mathbb{W}$ we have

$$|C_0| - H = |\mathcal{A} + \mathcal{B}| \leq |\mathcal{A}|\,|\mathcal{B}|\,.$$

By (4.24) we have

$$\left(1 - \frac{1}{2^t}\right)p - 2tp^{1/2} - H < |\mathcal{A}|\,|\mathcal{B}|\,. \tag{4.36}$$

Let $|\mathcal{A}| = f$. Then by Lemma 12 $f > 0.7t2^t$. Suppose that contrary to Lemma 15 we have

$$0.7t2^t < f \leq [0.71 \log p].$$

By using Lemma 14 with $k = |\mathcal{A}| = f$ and (4.36) we have

$$\left(1 - \frac{1}{2^t}\right)p - 2tp^{1/2} - H < 1.01f\left(1 - \frac{1}{2^t}\right)^f p.$$

By (4.8) and (4.13) we get

$$0.98\left(1 - \frac{1}{2^t}\right)p < 1.01f\left(1 - \frac{1}{2^t}\right)^f p.$$

So

$$f\left(1-\frac{1}{2^t}\right)^{f-1} > \frac{0.98}{1.01} > 0.97. \tag{4.37}$$

Here $f\left(1-\frac{1}{2^t}\right)^{f-1}$ is monotone decreasing in f for $f \in [2^t, \infty)$, since using $\log(1+x) \le x$ and $f \ge 2^t$ we get for the derivative

$$\begin{aligned}\frac{df\left(1-\frac{1}{2^t}\right)^{f-1}}{df} &= \left(1-\frac{1}{2^t}\right)^{f-1}\left(1+f\log\left(1-\frac{1}{2^t}\right)\right)\\ &\le \left(1-\frac{1}{2^t}\right)^{f-1}\left(1-\frac{f}{2^t}\right) \le 0.\end{aligned}$$

Since $f\left(1-\frac{1}{2^t}\right)^{f-1}$ is monotone decreasing in f and $f > 0.7t2^t$, by (4.37) and $1+x \le e^x$ we have

$$\begin{aligned}0.97 < f\left(1-\frac{1}{2^t}\right)^{f-1} &\le 0.7\cdot t2^t\left(1-\frac{1}{2^t}\right)^{0.7t2^t-1} \le 1.4\cdot t2^t\left(1-\frac{1}{2^t}\right)^{0.7t2^t}\\ &\le 1.4\cdot t2^t e^{-0.7\cdot t2^t/2^t} = 1.4t\left(\frac{2}{e^{0.7}}\right)^t < 1.4t(0.994)^t,\end{aligned}$$

which is impossible, if p (and thus t) is large enough.

Lemma 16 *Define B and T by* (4.2) *and* (4.3). *Suppose that $\mathcal{A}+\mathcal{B} \in \mathbb{W}$ with $|\mathcal{A}|, |\mathcal{B}| \ge 2$. Then*

$$|\mathcal{A}|, |\mathcal{B}| \le \left[1.01\left(1-\frac{1}{2^t}\right)^B p\right] = T.$$

Proof of Lemma 16. By symmetry reasons, it is enough to prove that

$$|\mathcal{B}| \le T. \tag{4.38}$$

By Lemma 15 we have

$$|\mathcal{A}| > [0.71\log p] = B.$$

Thus using Lemma 14 with $k = B$ we get (4.38), which was to be proved.

Now we are ready to prove Lemma 3.

Proof of Lemma 3. Let S denote the number of reducible sets in $\mathbb{W}$. We will prove that

$$S < |\mathbb{W}|,$$

from which the lemma follows. Suppose that $\mathcal{C} \in \mathbb{W}$ is reducible, thus there exist sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$ such that $|\mathcal{A}|, |\mathcal{B}| \geq 2$ and

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

By Lemma 16 we have

$$|\mathcal{A}|, |\mathcal{B}| \leq \left[1.01 \left(1 - \frac{1}{2^t}\right)^B p\right] = T.$$

Thus if $\mathcal{C} = \mathcal{A} + \mathcal{B}$ with $|\mathcal{A}|, |\mathcal{B}| \geq 2$ then $\mathcal{A}$ and $\mathcal{B}$ can be chosen from

$$\sum_{i=2}^{T} \binom{p}{i} < p \max_{1 \leq i \leq T} \binom{p}{i} \leq p \binom{p}{T}$$

different subsets of $\mathbb{F}_p$ (here we also use (4.14)). Thus there are at most

$$p^2 \binom{p}{T}^2$$

different sums $\mathcal{A} + \mathcal{B}$ whence

$$S \leq p^2 \binom{p}{T}^2 < p^2 \frac{p^{2T}}{(T!)^2}.$$

Clearly

$$|\mathbb{W}| = \binom{|C_0|}{H}.$$

By (4.25), we have

$$|\mathcal{C}_0| - H > 0.99p$$

whence

$$|\mathbb{W}| > \frac{(|\mathcal{C}_0| - H)^H}{H!} > \frac{(0.99p)^H}{H!}.$$

Thus $S < |\mathbb{W}|$ follows from

$$p^2 \frac{p^{2T}}{(T!)^2} < \frac{(0.99p)^H}{H!}. \tag{4.39}$$

Next we prove (4.39). If p is large enough, then T and H are large enough, thus by Stirling's formula

$$T! > 0.99\sqrt{2\pi T}\left(\frac{T}{e}\right)^T$$
$$H! < 1.01\sqrt{2\pi H}\left(\frac{H}{e}\right)^H.$$

Thus (4.39) (and $S < |\mathbb{W}|$ also) follows from

$$p^2 \frac{p^{2T}}{\left(0.99\sqrt{2\pi T}\left(\frac{T}{e}\right)^T\right)^2} < \frac{(0.99p)^H}{1.01\sqrt{2\pi H}\left(\frac{H}{e}\right)^H}. \tag{4.40}$$

(4.40) is equivalent with

$$p^2 \frac{\sqrt{H}}{T}\frac{H^H}{T^{2T}} e^{2T-H} \frac{p^{2T}}{(0.99p)^H} < \frac{0.99^2\sqrt{2\pi}}{1.01}. \tag{4.41}$$

In order to complete the proof of Lemma 3 we need to prove (4.41). Indeed, if p is large enough, then by (4.4), (4.14) and (4.16) we get

$$\begin{aligned} p^2 \frac{\sqrt{H}}{T}\frac{H^H}{T^{2T}} e^{2T-H} \frac{p^{2T}}{(0.99p)^H} &= p^2 \frac{\sqrt{3}}{\sqrt{T}}\left(\frac{3^3}{0.99^3 e}\cdot\frac{T}{p}\right)^T \le p^2\sqrt{3}\left(\frac{3^3}{0.99^3 e}\cdot\frac{T}{p}\right)^T \\ &< p^2\sqrt{3}\left(\frac{3^3}{0.99^3\cdot 11\cdot e}\right)^T < p^2\sqrt{3}\,(0.94)^T \\ &< p^2\sqrt{3}\,(0.94)^{0.08p^{0.51}} < e^{-0.004p^{0.51}+2\log p+\log\sqrt{3}} \\ &< \frac{0.99^2\sqrt{2\pi}}{1.01}, \end{aligned}$$

which was to be proved.

References

[1] N. Alon, *Large sets in finite fields are sumsets*, J. Number Theory 126 (2007), 110-118.

[2] N. Alon, A. Granville and A. Ubis, *The number of sumsets in a finite field*, Bull. London Math. Soc. 42 (2010), 784-794.

[3] B. J. Green, *Essay submitted for the Smith's Prize*, Cambridge University, 2001.

[4] C. Dartyge and A. Sárközy, *On additive decompositions of the set of the primitive roots modulo p*, Monatsh. Math., to appear.

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

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

[7] A. Sárközy, *Über reduzible Folgen*, Acta Arith. 10 (1965), 399-408.

[8] A. Sárközy, *Über totalprimitive*, Folgen, Acta Arith. 8 (1962), 21-31.

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

[10] W. M. Schmidt, *Equations Over Finite Fields: An Elementary Approach*, Berlin ; Springer-Verlag, 1976.

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

Katalin Gyarmati
Eötvös Loránd University
Department of Algebra and Number Theory
H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary
email: gykati@cs.elte.hu

Sergei Konyagin
Moscow State University
Department of Mechanics and Mathematics
Moscow 119992, Russia
email: konyagin23@gmail.com

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