Large zero-free subsets of $\mathbb{Z}/p\mathbb{Z}$

Jean-Marc Deshouillers, Gyan Prakash

Abstract

A finite subset $A$ of an abelian group $G$ is said to be zero-free if the identity element of $G$ cannot be written as a sum of distinct elements from $A$. In this article we study the structure of zero-free subsets of $\mathbb{Z}/p\mathbb{Z}$ the cardinality of which is close to largest possible. In particular, we determine the cardinality of the largest zero-free subset of $\mathbb{Z}/p\mathbb{Z}$, when $p$ is a sufficiently large prime.

For a finite abelian group $(G, +)$ and a subset $A$ of $G$, we set $A^\sharp = \{ \sum_{b \in B} b : B \subset A, B \neq \emptyset \}$. We say $A$ is zero-free if $0 \not\in A^\sharp$; in other words $A$ is zero-free if $0$ can not be expressed as a sum of distinct elements of $A$.

In 1964, Erdős and Heilbronn [5] made the following conjecture, supported by examples showing that the upper bound they conjectured is, if correct, very close to being best possible.

Conjecture 1. Let $A$ be a subset of $\mathbb{Z}/p\mathbb{Z}$. If $A$ is zero-free, we have $\text{Card}(A) \leq \sqrt{2p}$.

Up to recently, the best result concerning zero-free subsets of $\mathbb{Z}/p\mathbb{Z}$ was that of Hamidoune and Zémor [3] who proved in 1996 that their cardinality is at most $\sqrt{2p} + 5 \ln p$, thus showing that the constant $\sqrt{2}$ in the above conjecture is sharp.

The study of this question has been revived more recently. Freiman and the first named author introduced a method based on trigonometrical sums which led to the description of large incomplete subsets [1] as well as that of large zero-free subsets [1] of $\mathbb{Z}/p\mathbb{Z}$. Recall that a subset $A$ of $G$ is said to be incomplete if $A^\sharp \cup \{0\}$ is not equal to $G$. Szemerédi and Van Vu [6], as a consequence of their result on long arithmetic progressions in sumsets, gave structure results for zero-free subsets leading to the optimal bound for the total number of such subsets of $\mathbb{Z}/p\mathbb{Z}$. As it was noticed independently by Nguyen, Szemerédi and Van Vu [4] on one side and us on the other one, both methods readily lead to a proof of the Erdős-Heilbronn conjecture for zero-free subset[5].

The aim of the present paper is to study the description of rather large zero-free subsets of $\mathbb{Z}/p\mathbb{Z}$. We start by reviewing the present knowledge on zero-free subsets of $\mathbb{Z}/p\mathbb{Z}$.

Notation 2. We denote by $\sigma_p$ the canonical homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}/p\mathbb{Z}$; for an element $a$ in $\mathbb{Z}/p\mathbb{Z}$, we denote by $\bar{a}$ be the integer in $(-\frac{p}{2}, \frac{p}{2}]$ such that $a = \sigma_p(\bar{a})$ and let $|a|_p = |\bar{a}|$. Given a set $A \subset \mathbb{Z}/p\mathbb{Z}$, we denote by $\bar{A}$ the set $\{ \bar{a} : a \in A \}$. For $d \in \mathbb{Z}/p\mathbb{Z}$, we write $d \cdot A := \{ da : a \in A \}$. Given any real numbers $x, y$ with $x \leq y$, we write $[x, y]_p$\footnote{Van H. Vu and the first named author exchanged this information during a private conversation held in Spring 2006.}
to denote the set \( \sigma_p([x, y] \cap \mathbb{Z}) \). Given a set \( \mathcal{B} \subset \mathbb{Z} \) and non negative real numbers \( x, y \), we write \( \mathcal{B}(x, y) \) to denote the set \( \{ b \in \mathcal{B} : x \leq |b| \leq y \} \) and simply write \( \mathcal{B}(x) \) to denote the set \( \mathcal{B}(0, x) \).

It is evident that \( A \subset \mathbb{Z}/p\mathbb{Z} \) is zero-free if and only if the set \( (\tilde{A})^2 \) does not contain any multiple of \( p \). This leads to the following examples of zero-free subsets of \( \mathbb{Z}/p\mathbb{Z} \).

**Examples 3.**

(i) Any subset \( A \) of \( \mathbb{Z}/p\mathbb{Z} \) which satisfy the properties that \( \tilde{A} \) is a subset of \( [1, \frac{2}{p}] \) and \( \sum_{a \in A} |a| \leq p - 1 \) is a zero-free subset of \( \mathbb{Z}/p\mathbb{Z} \).

(ii) Given any integer \( k \) with \( k(k + 1)/2 \leq p + 1 \), the subset \( A \) of \( \mathbb{Z}/p\mathbb{Z} \) with \( A = \{-2, 1\}_p \cup [3, k]_p \) is a zero-free subset of \( \mathbb{Z}/p\mathbb{Z} \) which has cardinality equal to \( k \).

Moreover, one readily sees that if a subset \( A \) of \( \mathbb{Z}/p\mathbb{Z} \) is zero-free, then it is also the case for the set \( s \cdot A \), for any \( s \) coprime with \( p \).

Building on [2], the first named author proved in [1] the following result.

**Theorem 4.** Let \( c > 1 \), \( p \) a sufficiently large prime and \( A \) a zero-free subset of \( \mathbb{Z}/p\mathbb{Z} \) with cardinality larger than \( c\sqrt{p} \). Then, there exists \( d \) coprime with \( p \) such that

\[
\sum_{a \in A} |da|_p < p + O(p^{3/4} \ln p) \quad \text{and} \quad \sum_{a \in A, da < 0} |da|_p = O(p^{3/4} \ln p),
\]

where the constants implied in the \( O \) symbol depend upon \( c \),

and built examples showing moreover that none of the above error-terms can be replaced by \( o(p^{1/2}) \).

The error-terms in [1] were reduced to the best possible \( O(p^{1/2}) \) by Nguyen, Szemerédi and Van Vu in [4, Theorem 1.9].

The above mentioned paper of Szemerédi and Van Vu [6] implicitly contains the following result, formally stated in [4] as Theorem 2.1.

**Theorem 5.** Let \( A \) be a zero-free subset of \( \mathbb{Z}/p\mathbb{Z} \). Then for some non zero element \( d \in \mathbb{Z}/p\mathbb{Z} \) the set \( d \cdot A \) can be partitioned into two disjoint sets \( A' \) and \( A'' \), where

(i) \( A' \) has negligible cardinality: \( |A'| = O(p^{1/2}/\log^2 p) \).

(ii) We have \( A'' \subset [1, p/2]_p \) and \( \sum_{a'' \in A''} |a''|_p \leq p - 1 \).

We first consider the maximal zero-free subsets of \( \mathbb{Z}/p\mathbb{Z} \). The description given in the following theorem is a synthesis of the results established in Sections 1 and 2.

**Theorem 6.** Let \( p \) be a sufficiently large prime and \( A \) a zero-free subset of \( \mathbb{Z}/p\mathbb{Z} \) with maximal cardinality. Then

\[
\text{card}(A) \text{ is the largest integer } k \text{ such that } k(k + 1)/2 \leq p + 1,
\]

and one may thus write \( \text{card}(A) = \left\lfloor \sqrt{2p + 9/4} - 1/2 \right\rfloor = \left\lfloor \sqrt{2p} \right\rfloor - \delta(p), \) with \( \delta(p) \in \{0, 1\} \).

Furthermore, there exists a non-zero element \( d \) in \( \mathbb{Z}/p\mathbb{Z} \) such that the set \( d \cdot A \) is the union of two sets \( A' \) and \( A'' \), with
(i) \( A' \subset [-2(1 + \delta(p)), -1]_p \), \( A'' \subset [1, p/2]_p \), \( A'' \cap (-A') = \emptyset \) and \( \text{card}(A') \leq 1 + \delta(p) \).

(ii) \( \sum_{a' \in A'} |a'|_p \leq 2(1 + \delta(p)) \) and \( \sum_{a'' \in A''} |a''|_p \leq p - 1 + 3\delta(p) \).

The Reader will find a more detailed description of extremal zero-free sets in Section 2. In this Introduction, we limit ourselves to a few remarks and examples.

Writing \( \sqrt{2p + 9/4} - 1/2 = \sqrt{2p} + \alpha_p - 1/2 \), we have \( \alpha_p = O(1/\sqrt{p}) \). One readily sees that \( \delta(p) \) takes the values 1 or 0 according as the fractional part of \( \sqrt{2p} \) is smaller than \( 1/2 - \alpha_p \) or larger. Thus the density of the primes \( p \) for which the maximal zero-free of \( \mathbb{Z}/p\mathbb{Z} \) subset has cardinality \( \lfloor \sqrt{2p} \rfloor \) is 1/2.

The sum \( \sum_{a'' \in A''} |a''|_p \) can take the values \( p + 1 \) or \( p + 2 \) only in very special cases, namely when one of \( p + 2, p + 3, p + 4, p + 5, p + 6, \) or \( p + 7 \) is a value of the polynomial \( x(x + 1)/2 \) at some integral point \( x \). The number of such primes \( p \) up to \( P \) is \( O(\sqrt{P}) \); the existence of infinitely many such primes is not known and would result from the validity of some standard conjectures, like Schinzel’s hypothesis. The set \( A = \{-3, 1, 4, 5, 6, \cdots 14, 15\}_{113} \) is an example of a zero-free subset of \( \mathbb{Z}/113\mathbb{Z} \) which satisfies Theorem 6 with \( \text{card}(A) = \lfloor \sqrt{2p} \rfloor - 1 \), \( \sum_{a'' \in A''} |a''|_p = p + 2 \) and \( p + 7 = x(x + 1)/2 \).

We now turn our attention to very large zero-free subsets \( A \) of \( \mathbb{Z}/p\mathbb{Z} \), i.e. subsets such that \( \sqrt{2p} - \text{card}(A) = o(\sqrt{p}) \). From now on, we fix a function \( \psi \) from \( [2, \infty) \) to \( \mathbb{R}^+ \) which tends to 0 at \( \infty \) and assume that
\[
\epsilon(A) := |\sqrt{2p} - \text{card}(A)| \leq \psi(p)\sqrt{p}
\]
the term sufficiently large implicitly referring to the function \( \psi \).

The following result gives the structure of large zero-free subsets of \( \mathbb{Z}/p\mathbb{Z} \). It shows that any given large zero-free subset \( A \) has a dilate, which is a union of sets \( A' \) and \( A'' \), where \( A'' \) is a set closely related to the one given in Example 3 (i) and the cardinality of \( A' \) is small.

**Theorem 7.** When \( p \) is sufficiently large, then given any zero-free subset \( A \) of \( \mathbb{Z}/p\mathbb{Z} \) with \( \epsilon(A) \) satisfying (3), there exists a non-zero element \( d \in \mathbb{Z}/p\mathbb{Z} \) such that \( d \cdot A \) can be partitioned into disjoint sets \( A' \) and \( A'' \) with the following properties

(i) The set \( A'' \) is included in \( [1, \frac{\epsilon(A)}{2c}] \) and we have \( \sum_{a'' \in A''} |a''|_p \leq p - 1 \).

(ii) The set \( A' \) is included in \( [-c\epsilon(A), c\epsilon(A)] \) for some absolute constant \( c \) and the cardinality of \( A' \) is \( O \left( \frac{\sqrt{\epsilon(A)} + 2 \ln(\epsilon(A) + 2)}{\sqrt{\epsilon(A)}} \right) \),

where \( \epsilon(A) \) is defined in (3).

To prove Theorems 6 and 7, we prove the following proposition.

**Proposition 8.** Let \( p \) be a prime and \( A \) a zero-free subset \( A \) of \( \mathbb{Z}/p\mathbb{Z} \) with \( \epsilon(A) \) satisfying (3). When \( p \) is sufficiently large, there exists a non-zero element \( d \in \mathbb{Z}/p\mathbb{Z} \) such that
\[
\sum_{a \in A} |da|_p \leq p + O \left( \epsilon(A)^{3/2} \ln(\epsilon(A) + 2) \right),
\]
\[
\sum_{a \in A, da < 0} |da|_p = O \left( \epsilon(A)^{3/2} \ln(\epsilon(A) + 2) \right)
\]
Remark 9. Noticing that for any zero-free subset $A$ of $\mathbb{Z}/p\mathbb{Z}$, the corresponding set $\bar{A} \subset \mathbb{Z}$ can contain at most one element from the set $\{x, -x\}$ for any integer $x$ we have $\sum_{\bar{a} \in \bar{A}}|\bar{a}| \geq \frac{|\bar{A}|(|\bar{A}|+1)}{2}$. Using this, Conjecture 1 is an immediate corollary of Proposition 8.

To prove Proposition 8 we use Theorem 4 and the following result from [2].

Theorem 10. ([2, Theorem 2]) Let $I > L > 100$ and $B > 2C\ln L$ be positive integers such that
\[ C^2 > 500L(\ln L)^2 + 2000I\ln L. \]
Let $B$ be a set of $B$ integers included in $[-L, L]$. Then there exist $d > 0$ and a subset $C$ of $B$ with cardinality $C$ such that
(i) all the elements of $C$ are divisible by $d$,
(ii) $C^*$ contains an arithmetic progression with $I$ terms and common difference $d$,
(iii) at most $C\ln L$ elements of $B$ are not divisible by $d$.

1 Proof of Proposition 8

Let $p$ be a sufficiently large prime and $A \subset \mathbb{Z}/p\mathbb{Z}$ be as given in Proposition 8. From Theorem 4 there exists a non-zero element $d \in \mathbb{Z}/p\mathbb{Z}$ such that (1) holds. Without loss of generality, we may indeed assume that $d = 1$ or, equivalently, replace $d \cdot A$ by $A$. We then get
\[ \sum_{\bar{a} \in \bar{A}}|\bar{a}| = \sum_{a \in A}|a|_p \leq p + O(p^{3/4}\ln p). \]  
(6)
We prove Proposition 8 by showing that if $\bar{A} \subset [-\frac{p}{2}, \frac{p}{2}]$ is as above then we have
\[ \sum_{\bar{a} \in \bar{A}}|\bar{a}| \leq p + O \left(e(A)^{3/2}\ln (e(A) + 2)\right). \]  
(7)
We shall first show how one can deduce (7) from the following proposition.

Proposition 11. Let $p$ be a sufficiently large prime and $K \subset \mathbb{Z}$ such that $K^2$ does not contain any multiple of $p$. We recall that $\psi$ is a fixed function from $[2, \infty)$ to $\mathbb{R}^+$ which tends to $0$ at $\infty$. Let us suppose that we have
\[ e(K) := |\sqrt{2p-\text{card}(K)}| \leq \psi(p)\sqrt{2p} \quad \text{and} \quad \sum_{k \in K}|k| \leq p + s(K), \quad \text{with} \quad 0 \leq s(K) \leq p^{0.9}. \]  
(8)
Then, we have in fact
\[ \sum_{k \in K}|k| \leq p + O \left(\kappa^{3/2}\ln \kappa\right), \]  
(9)
where $\kappa = s(K)/\sqrt{p} + e(K) + 2$. Moreover we have
\[ \min\{\sum_{k \in K, k > 0}|k|, \sum_{k \in K, k < 0}|k|\} = O(\kappa^{3/2}\ln \kappa). \]
The fact that \( \mathcal{A} \) is zero-free and Relations (1) and (3) permit to apply Proposition (1) with \( \mathcal{K} = \mathcal{A} \). When \( e(\mathcal{K}) \geq p^{1/4} \), then (9) directly implies (7). But, when \( e(\mathcal{K}) \leq p^{1/4} \), we first obtain from (9) the following weaker inequality

\[
\sum_{a \in \mathcal{A}} |a| \leq p + O(p^{3/8} \ln p).
\]

As such, it is weaker than (7) in this case, we may use \( s(\mathcal{K}) = p^{3/8} \ln p \), so that \( \kappa = e(\mathcal{K}) + O(1) \), and a further application of Proposition (1) leads to Relation (7).

To prove Proposition (11) we need a few lemmas.

**Lemma 12.** Let \( m \in \mathbb{Z}, \ell \in \mathbb{N} \) and let \( B \) be a subset of \([-\ell, \ell] \cap \mathbb{Z} \). We have

\[
\left( \{m, \ldots, m + \ell - 1\} \cup B^* \right) \cap \mathbb{Z} = \left( \left[ m - \sum_{b \in B, b < 0} |b|, m + \ell - 1 + \sum_{b \in B, b > 0} |b| \right] \right) \cap \mathbb{Z}.
\]

**Proof.** We write \( k = |B| \) and \( B = \{b_1 < b_2 < \ldots < b_h < 0 \leq b_{h+1} < \ldots < b_k\} \), where \( h = 0 \) if all the elements of \( B \) are nonnegative. For \( 0 \leq u \leq k \), we define

\[
\beta_u = \begin{cases} 
\sum_{i=1}^{h-u} b_i & \text{if } 0 \leq u \leq h - 1, \\
0 & \text{if } u = h, \\
\sum_{j=h+1}^{u} b_j & \text{if } h + 1 \leq u \leq k.
\end{cases}
\]

Simply notice that \( \beta_0 = \min \{s : s \in B^*\} \), \( \beta_k = \max \{s : s \in B^*\} \) and that \( \{\beta_0 < \ldots < \beta_k\} \) is a subset of \( B^* \) such that the difference between two consecutive elements of which is at most \( \ell \). \( \square \)

**Lemma 13.** Let \( B \subset \mathbb{Z}, c \in \mathbb{Z}, x \in \mathbb{N}, \ell \geq x + 1 \) be such that \( B(x)^2 \) contains \([c, c + \ell] \cap \mathbb{Z}\). Then, if there exists an integer \( y \) in \([x + 1, \infty)\) such that \( B(y)^2 \) does not contain \([\{c - \sum_{b \in B(x+1,y), b < 0} |b|, c + \ell - 1 + \sum_{b \in B(x+1,y), b > 0} |b|\}] \cap \mathbb{Z}, and z is the least such integer, then we have

\[
z \geq \ell + \sum_{b \in B(x+1,z-1)} |b| + 1.
\]

**Proof.** We notice that \( B(z)^2 \supseteq B(x)^2 + B(x + 1, z)^* \). Lemma (12) implies if \( z \) has the required property, then \( z \geq x + 2 \). Since \( z \geq x + 2 \), the minimal property of \( z \) implies that the set \( B(z - 1)^2 \) does contain

\[
I = ([c - \sum_{b \in B(x+1,z-1), b < 0} |b|, c + \ell - 1 + \sum_{b \in B(x+1,z-1), b > 0} |b|]) \cap \mathbb{Z}.
\]

By our assumption, the set \( I \cup \bigcup_{b \in B, |b| = z} (I + b) \) is not an interval. This implies (special case of Lemma 12) that \( z \geq \ell + \sum_{b \in B(x+1,z-1)} |b| + 1 \). \( \square \)

**Lemma 14.** Let \( \mathcal{K} \) be as given in Proposition (11). Then for any \( k \in \mathcal{K} \), the element \(-k\) does not belong to \( \mathcal{K} \).

**Proof.** If claim is not true, then evidently \( 0 \in \mathcal{K}^2 \) which is contrary to the assumption. \( \square \)

**Lemma 15.** We keep the notation of Proposition (11). For \( x \leq 0.9 \sqrt{2p} \), the cardinality of \( \mathcal{K}(x) \) is \( x + O(e(\mathcal{K}) + s(\mathcal{K})/\sqrt{p}) \).
Proof. Lemma 14 immediately implies that the cardinality of \( K(x) \) is at most \( x \). Let us suppose that the cardinality of \( K(x) \) is \( x - \lambda(x) \). Then using Lemma 14 we get

\[
\sum_{k \in K} |k| \geq \sum_{i=1}^{x-\lambda(x)} i + \sum_{i=x+1}^{\text{card}(K) + \lambda(x)} i
\]

Writing each summand in the second sum on the right hand side of the above inequality as \((i - \lambda(x)) + \lambda(x)\) and then noticing that the number of terms in the second sum is \( \text{card}(K) - x \), we get the following inequality

\[
\sum_{k \in K} |k| \geq \sum_{i=1}^{\text{card}(K)} i + \lambda(x)(\text{card}(K) - x).
\] (10)

Since \( x \leq 0.9\sqrt{2p} \) and \( \text{card}(K) \geq \sqrt{2p} - e(K) \geq \sqrt{2p} - \psi(p)\sqrt{p} \), the second term in the right hand side of the above inequality is larger than \( 0.05\sqrt{2p}\lambda(x) \), whereas the first term is \( p - O(e(K)\sqrt{2p}) \). Now comparing the above inequality with (8) we obtain

\[
\lambda(x) \leq c(e(K) + s(K)/\sqrt{p}),
\]

for some absolute constant \( c \). The lemma readily follows from this fact. \qed

Lemma 16. We keep the notation of Proposition 11. The largest integer \( y_0 \) belonging to \( K \cup -K \) satisfies \( y_0 = O(e(K)\sqrt{2p} + s(K)) \).

Proof. Using Lemma 14 we obtain

\[
\sum_{k \in K} |k| \geq \sum_{i=1}^{\text{card}(K) - 1} i + y_0.
\] (11)

Now the first term on the right hand side of the above inequality is \( p - O(e(K)\sqrt{2p}) \). Therefore comparing the above inequality with (8), the assertion follows. \qed

Lemma 17. We keep the notation of Proposition 11 and let \( x \) be a sufficiently large integer. Suppose that the cardinality of \( K(x) \) is at least \( 0.99x \). Then there exists a subset \( C \) of \( A(x) \) with \( |C| = O(\sqrt{x} \ln x) \) such that \( C^x \) contains an arithmetic progression of length \( x \) and common difference \( d \), with \( d \in \{1, 2\} \).

Proof. Applying Theorem 10 with \( B = K(x) \), \( L = x, I = x + 1 \), \( C = |100\sqrt{x} \ln x| \), we get that there exists a subset \( C \) of \( K(x) \) with \( |C| = O(\sqrt{x} \ln x) \) such that \( C^x \) contains an arithmetic progression of length \( x \) and common difference \( d \) dividing at least \( 0.8x \) elements of \( K(x) \). Since \( K(x) \) is contained in an interval of length \( 2x \), we obtain that \( d \in \{1, 2\} \). \qed

Lemma 18. Let \( x \) and \( C \) be as in Lemma 17. Then there exists \( k \in K(x) \setminus C \) such that the element \( k + 1 \) also belongs to \( K(x) \setminus C \).

Proof. Let \( L \) be the set consisting of those elements \( l \in [1, x] \) such that one of the elements \( l \) or \(-l\) belongs to the set \( K(x) \setminus C \). Then \( L \) is a set of cardinality at least \( 0.9x \) contained in an interval of length \( x \). Therefore there exists \( l \in L \) such that \( \{l, l+1, l+2, l+3, l+4\} \subset L \). Now by the definition of \( L \), for any \( 0 \leq i \leq 4 \), either \( l+i \in K(x) \setminus C \) or \(-l+i \in K(x) \setminus C \). The lemma follows evidently by showing that there exists \( i \) with \( 0 \leq i \leq 3 \) for which one
of the following two sets, \{l+i, l+i+1\} and \{-(l+i), -(l+i+1)\} is included in \(K(x) \setminus C\). If not, then replacing \(K\) by \(-K\) if necessary we have that \{-l, l+1, l+3, -(l-4) \subset K(x) \setminus C\}. This would contradict the assumption that \(0\) does not belong to \(K^\sharp\). Hence the lemma follows.

We are now in a position to prove Proposition 11.

**Proof of Proposition 11** From Lemma 15 there is an integer \(x\) which satisfies the assumption of Lemma 17 and at the same time \(x = O(e(K) + s(K) \sqrt{p})\). For this choice of \(x\), let \(C\) be a subset of \(K(x)\), as provided by Lemma 17. From Lemma 18 we obtain a subset \(\{k, k + 1\}\) of \(K(x) \setminus C\). Then the set \(C_1 = C \cup \{k, k + 1\}\) is a subset of \(K(x)\) with \(\text{card}(C_1) = O(\sqrt{x} \ln x)\) and \((C_1)^{\sharp}\) contains an interval \([y, y + x]\) of length \(x\). With this interval \(I\) applying Lemma 12 with \(B = K(x) \setminus C_1\), we obtain that \(K(x)^{\sharp}\) contains the interval \([y - \sum_{k \in K(x) \setminus C_1} |k|, y + x + \sum_{k \in K(x) \setminus C_1} |k|]\) of length \(x + \sum_{k \in K(x) \setminus C_1} |k|\). Then using Lemmas 13 and 15 after an elementary calculation, it follows that for some positive absolute constant \(c_0\), the set \(K(p/c_0)\) contains the interval \([y - \sum_{k \in K(p/c_0) \setminus C_1} |k|, y + x + \sum_{k \in K(p/c_0) \setminus C_1} |k|]\) of length \(x + \sum_{k \in K(p/c_0) \setminus C_1} |k|\). Replacing \(K\) by \(-K\) we may assume that \(y > 0\). Then since \(K^\sharp\) does not contain any multiple of \(p\) we obtain the following inequalities

\[
\sum_{k \in K(p/c_0) \setminus C_1} |k| \leq p - 1
\]

and

\[
\sum_{k \in K(p/c_0) \setminus C_1} |k| \leq \sum_{c_1 \in C_1} |c_1| + \sum_{k \in K(p/c_0) \setminus C_1, k < 0} |k| \leq \sum_{c_1 \in C_1} |c_1| + y.
\]

From Lemma 16 we have that \(K(p/c_0) = K\). Moreover it is also evident from the construction of \(C_1\) that \(\sum_{c_1 \in C_1} |c_1| = O(x^{3/2} \ln x)\). Since \(y \in C_1^\sharp\) we have \(y \leq \sum_{c_1 \in C_1} |c_1|\). Therefore the assertion follows.

## 2 Proof of Theorem 6

Let \(p\) be a sufficiently large prime and \(A\) a zero-free subset of \(\mathbb{Z}/p\mathbb{Z}\) of the largest cardinality. From Proposition 8 and Remark 9 we have that \(\text{card}(A) \leq \sqrt{|2p|}\). Moreover, since for any prime \(p\) the set \([1, [\sqrt{2p}] - 1]_p\) is an example of a zero-free subset of \(\mathbb{Z}/p\mathbb{Z}\), it follows that \(\text{card}(A) = [\sqrt{2p}] - \delta(p)\) with \(\delta(p) \in \{0, 1\}\). We set

\[
s(\sqrt{2p}) = \sum_{i=1}^{[\sqrt{2p}]} i = \frac{[\sqrt{2p}] [\sqrt{2p} + 1]}{2}.
\]

From Example 3(ii), it follows that when \(s(\sqrt{2p}) \leq p + 1\), then \(\delta(p) = 0\). In this section we shall show that \(\delta_p = 0\), only when \(s(\sqrt{2p}) \leq p + 1\).

Using Proposition 8 there exists a \(d \in (\mathbb{Z}/p\mathbb{Z})^*\) such that replacing \(A\) by \(dA\), we have

\[
\sum_{a \in A} |a|_p \leq p + O(1).
\]

Using (11) with \(K = A\) and (12), the following lemma is immediate.

**Lemma 19.** The largest integer \(y\) in \(A \cup -A\) is \(O(\sqrt{2p})\).
Let $G(A)$ be the collection of all natural numbers $g$ which satisfy the property that none of the integers $g$ and $-g$ belong to the set $A$, where $\bar{A}$ is the subset of integers as defined earlier. For the brevity of notation we shall write $G$ to denote the set $G(A)$. Let $G = \{g_0 < g_1 < g_2 < \ldots \}$.

From Lemma [15] we obtain that the cardinality of $G(x)$ is $O(1)$ for any $x \leq 0.9\sqrt{2p}$. The arguments identical to those used in the proof of Lemma [15] in fact leads to the following lemma.

**Lemma 20.** The set $\bar{A} \cup (-\bar{A})$ contains all the integers in $[1, \sqrt{2p}/5]$ with at most $\delta(p)$ exception.

**Proof.** The lemma is equivalent to showing that in case $\text{card}(A) = \lfloor \sqrt{2p} \rfloor$, then $g_0 > \sqrt{2p}/5$, whereas in case $\text{card}(A) = \lfloor \sqrt{2p} \rfloor - 1$, then $g_1 > \sqrt{2p}/5$. Suppose that this is not true. Then if $\delta(p) = 0$, we have

$$\sum_{a \in A} |a|_p = \sum_{\bar{a} \in A} \bar{a}^g \geq \sum_{i=1}^{g_0-1} i + \sum_{i=g_0+1}^{Card(A)+1} i \geq \frac{\sqrt{2p} + 1}{2} \frac{\sqrt{2p} + 2}{2} - \sqrt{2p}/5,$$

whereas in case $\delta(p) = 1$, we have

$$\sum_{a \in A} |a|_p \geq \sum_{i=1}^{g_0-1} i + \sum_{i=g_0+1}^{g_1-1} i + \sum_{i=g_1+1}^{Card(A)+2} i \geq \frac{\sqrt{2p} + 1}{2} \frac{\sqrt{2p} + 2}{2} - 2\sqrt{2p}/5.$$

Using the facts that $\lfloor \sqrt{2p} \rfloor \geq \sqrt{2p} - 1$ and for any integer $i$, we have $\lfloor \sqrt{2p} + i \rfloor = \lfloor \sqrt{2p} \rfloor + i$, it follows that either of these inequalities are contrary to [12]. Hence the lemma follows. \qed

Now we determine all the possible structure of $\bar{A}(\sqrt{2p}/5)$, first under the assumption that $g_0 \geq 5$.

**Lemma 21.** When $g_0 \geq 5$, then replacing $A$ by $-A$, if necessary, the set $\bar{A}$ contains the whole interval $[\sqrt{2p}/5, \sqrt{2p}/5]$ with at most $\delta(p)$ exception and $\bar{A}(4)$ is equal to one of the three sets described in the the first three rows of the second column of Table 1.

**Proof.** Since we have assumed that $g_0 \geq 5$, replacing $A$ by $-A$, if necessary, we may assume that $3 \in \bar{A}$. Then the set $\bar{A}(3)$ is equal to one of the following four sets, \{1,2,3\}, \{-1,2,3\}, \{1, -2, 3\}, \{-1, -2, 3\}. Since $A$ is zero-free, among these four possibilities, the last one cannot occur. We verify that in all the other three possible cases the following always hold

$$\{1,2,3,4\} \subseteq \bar{A}(3)^5.$$

This implies that the set $\bar{A}(4)$ is equal to one of the three sets described in the second column of the first three rows of Table 1; that is, the set $\bar{A}(4)$ is equal to one of the following three sets \{1,2,3,4\}, \{-1,2,3,4\}, \{1, -2, 3, 4\}. We claim that there does not exist any integer $z \in [\sqrt{2p}/5, \sqrt{2p}/5]$ with $-z \in \bar{A}$. The lemma follows immediately using this claim and Lemma 20. To verify the claim, suppose that the claim is not true and $z_0$ is the least integer which violates the claim. Then since \{1,2,3,4,5,6\} is always a subset of $\bar{A}(4)^5$, we have that $z_0$ is at least 6. Now if $z_0 \neq g_0 + 1$, then we have $z_0 - 1 \in \bar{A}$ and thus $z_0 \in \bar{A}(3)^5 \cup z_0 - 1 \subseteq \bar{A}(z_0 - 1)^5$. Since $A$ is zero-free, this implies that $-z_0$ can not belong to the set $\bar{A}$ which contradicts the assumption that $z_0$ is the least integer violating the claim. Thus if the claim is not true then $z_0 = g_0 + 1$. But in this case $z_0 - 2 \in \bar{A}$ and thus $z_0 \in \bar{A}(3)^5 \cup z_0 - 2 \subseteq \bar{A}(z_0 - 2)^5$. This implies that $-z_0$ cannot belong to $\bar{A}$. Hence the claim and thus the lemma hold. \qed
Structure of $A$ when $|A| = \lfloor\sqrt{2p}\rfloor - \delta_p$, with $\delta_p \in \{0,1\}$

Here $s'' = s''(A) = \sum_{\bar{a} \in \bar{A}, \bar{a} > 0} \bar{a}$.

| # | $\{a \in A/|a| \leq 4\}$ | $\delta_p$ | $g_0$ | $(A)^{\bar{a}}$ |
|---|-------------------|------|------|----------------|
| 1 | $\{1,2,3,4\}$    | $\geq 5$ | $\{1, s''\}$ |
| 2 | $\{-1,2,3,4\}$   | $\geq 5$ | $\{-1\} \cup [1, s'']$ |
| 3 | $\{1,-2,3,4\}$   | $\geq 5$ | $\{-2,-1\} \cup [1, s'']$ |
| 4 | $\{1,2,3\}$      | 1     | 4    | $[1, s'']$ |
| 5 | $\{-1,2,3\}$     | 1     | 4    | $\{-1\} \cup [1, s'']$ |
| 6 | $\{1,-2,3\}$     | 1     | 4    | $\{-1,-2\} \cup [1, s'']$ |
| 7 | $\{-1,2,-3\}$    | 1     | 4    | $[-4,-1] \cup [1, s'']$ |
| 8 | $\{1,2,4\}$      | 1     | 3    | $[1, s'']$ |
| 9 | $\{-1,2,4\}$     | 1     | 3    | $\{-1\} \cup [1, s'']$ |
| 10| $\{1,-2,4\}$     | 1     | 3    | $\{-2,-1\} \cup [1, s'']$ |
| 11| $\{1,2,-4\}$     | 1     | 3    | $[-4,-1] \cup [1, s'']$ |
| 12| $\{-1,-2,4\}$    | 1     | 3    | $[-3,-1] \cup [1, s'']$ |
| 13| $\{1,3,4\}$      | 1     | 2    | $[1, s''] \setminus \{2, s'' - 2\}$ |
| 14| $\{-1,3,4\}$     | 1     | 2    | $\{-1\} \cup [1, s''] \setminus \{1, s'' - 2\}$ |
| 15| $\{1,-3,4\}$     | 1     | 2    | $\{-3,-2\} \cup [1, s''] \setminus \{s'' - 2\}$ |
| 16| $\{2,3,4\}$      | 1     | 1    | $[2, s''] \setminus \{s'' - 1\}$ |
| 17| $\{-2,3,4\}$     | 1     | 1    | $\{-2,-1\} \cup [1, s''] \setminus \{s'' - 1\}$ |
| 18| $\{2,-3,4\}$     | 1     | 1    | $\{-3,-1\} \cup [1, s''] \setminus \{s'' - 1\}$ |
| 19| $\{2,3,-4\}$     | 1     | 1    | $\{-4,-2,-1\} \cup [1, s''] \setminus \{s'' - 1\}$ |

Table 1: Subset sum of a largest zero-free set
Lemma 22. Let $A$ be as in Lemma 21. $A' = A \cap [-\frac{p}{2}, -1]_p$ and $A'' = A \cap [1, \frac{p}{2}]_p$. Then we have $A' \subset [-2, -1]_p$. Moreover the set $(A')^2$ contains the interval $[1, s'']_p$ with $s'' = \sum_{a'' \in A''} |a''|_p$ and is equal to one of the sets described in the fifth column of the first three rows of Table 1, the three possibilities corresponding to three possible structures for $\bar{A}(4)$. We have

$$s'' \leq p - 1.$$ 

Proof. For any integer $z$ we set

$$s''(z) = \sum_{a'' \in A''(z)} a''.$$ 

We claim that there is an absolute constant $c$ such that for any integer $z$ with $5 \leq z \leq \frac{p}{c}$, the set $(\bar{A}(z))^2$ contains the interval $[1, s''(z)]$. The claim is easily verified with $z = 5$. Suppose the claim is not true and $z_0$ is the least integer violating the claim. Since using the previous lemma we always have $s''(5) \geq 5 + 1 = 6$, we apply Lemma 13 with $x = 5$ and obtain the following inequality.

$$z_0 \geq s''(z_0 - 1) + 1.$$ 

(13)

Using the previous lemma, for any integer $y$ with $y \in [6, \sqrt{2p}/5]$, we have

$$s''(y) = \frac{y(y + 1)}{2} - \sum_{a' \in A(4)} |a'| - \epsilon,$$

where $\epsilon = 0$ if $y \leq g_0$ and $\epsilon = g_0$ if $y > g_0$. Using this it follows that (13) cannot hold with $z_0 \leq \sqrt{2p}/5$. Therefore we have

$$z_0 \geq s''(\sqrt{2p}/5) \geq \frac{p}{c},$$

where $c$ is an absolute constant. Hence the claim follows. Using the claim and Lemma 19 it follows that the set $(A)^2$ contains the interval $[1, s'']_p$. Since $A$ is zero-free, it follows that

$$s'' \leq p - 1.$$ 

Since $(\bar{A}(\sqrt{2p}/5))^2$ contains the interval $[1, s''(\sqrt{2p}/5)]$, it follows that there is no integer $y \in \left[ -\frac{p}{c}, -\sqrt{2p}/5 \right]$ with $y \in \bar{A}'$. Using the previous lemma and Lemma 19 it follows that $\bar{A}' = \bar{A} \cap [-4, -1] \subset [-2, -1]$. Using this it may be easily verified that the set $(A)^2$ is equal to one of the sets described in the fifth column of the first three rows of Table 1. Hence the lemma follows.

Theorem 23. Let $p$ be a sufficiently large prime and $A$ a zero-free subset of $\mathbb{Z}/p\mathbb{Z}$ of the largest cardinality. Then $\text{card}(A) = \left(\sqrt{2p} - \delta(p) \right)$, where $\delta(p) = 0$ if $s(\sqrt{2p}) \leq p + 1$ and is equal to 1 otherwise. In other words, $\text{card}(A)$ is the largest integer $k$ with the property that $\frac{k(k + 1)}{2} \leq p + 1$; that is $\text{card}(A) = \left(\sqrt{2p} + 9/4 - 1/2 \right)$.

Proof. From the remarks made in the beginning of this section, it follows that $\text{card}(A) = \lfloor \sqrt{2p} \rfloor - \delta(p) \in \{0, 1\}$. If $s(\sqrt{2p}) \leq p + 1$, then the set $\{-2, -1\}_p \cup [3, \sqrt{2p}]_p$ is an example of a zero-free subset of $\mathbb{Z}/p\mathbb{Z}$ and since $A$ is a largest zero-free subset, we have $\delta(p) = 0$, in this case. Now in case $\delta(p) = 0$, then from the remarks made in the beginning of this section there is a $d \in (\mathbb{Z}/p\mathbb{Z})^*$, such that replacing $A$ by $dA$, the
inequality (12) holds with $d = 1$. Using Lemma 20 it also follows that $g_0 \geq \sqrt{2p}/5 \geq 5$. Therefore it follows that replacing $A$ by $-A$, if necessary, the set $A$ is as in Lemma 22.

Since $\delta(p) = 0$, we also have that

$$s(\sqrt{2p}) \leq s'' + \sum_{a' \in A'} |a'| \leq s'' + 2,$$

where $s''$ is as in the Lemma 22 and is at most $p - 1$. Thus $s(\sqrt{2p}) \leq p + 1$. Hence the theorem follows.

**Lemma 24.** Let $A$ be a largest zero-free subset of $\mathbb{Z}/p\mathbb{Z}$ which satisfy (12). When $g_0 \leq 4$, then, replacing $A$ by $-A$ if necessary, the set $A$ contains the whole interval $[5, \sqrt{2p}/5]$.

**Proof.** Since $g_0 \leq 4$, then using Lemma 20 for any integer $z \geq 5$ either $z$ or $-z$ belongs to $A$. Replacing $A$ by $-A$, if necessary, we may assume that the integer 5 belongs to the set $A$. If the statement of the lemma is not true then there is an integer $z \in [6, \sqrt{2p}/5]$ with $-z \notin A$. Let $z_0$ be the least among such integers. Then since $-z_0$ belongs to $A$ and $A$ is zero-free, it follows that $z_0 - 5$ does not belong to the set $A$. From the definition of $z_0$ it follows that $z_0 - 5 \leq 4$ and thus $z_0 \leq 9$. In other words, $z_0 \in \{6, 7, 8, 9\}$. On the other hand we shall show that $z_0$ cannot be equal to any of this four possible integers.

Case 1: If $z_0 = 9$. In this case we have $\{5, 6, 7, 8, -9\} \subset A$. Since $2 + 7 - 9 = 6 + 5 - 9 - 2 = 3 + 6 - 9 = 7 + 5 - 3 - 9 = 0$, it follows that none of the integers in the set $\{2, 3, -2, -3\}$ belongs to the set $A$. This is in contradiction to Lemma 20. Thus $z_0$ cannot be equal to 9.

Case 2: If $z_0 = 8$. In this case we have that $\{5, 6, 7, -8\} \subset A$. Since we have $3 + 5 - 8 = -3 + 6 + 5 - 8 = 1 + 7 - 8 = -4 + 7 + 5 - 8 = 0$, none of the integers from the set $\{1, 2, 3, -3, -4\}$ belongs to $A$. From Lemma 20 it follows that $\{-1, -2, 4, 5, 6, 7, -8\} \subset A$. Since $-1 + 5 + 4 - 8 = 0$, this is in contradiction to the fact that $A$ is zero-free. Therefore $z_0$ cannot be equal to 8.

Case 3: If $z_0 = 7$. In this case we have $\{5, 6, -7\} \subset A$. Since $-4 + 5 + 6 - 7 = 2 + 5 - 7 = 1 + 6 - 7 = 0$, it follows that none of the integers from the set $\{1, 2, -4\}$ belongs to $A$. Now if $4 \notin A$, in other words if $\{4, 5, 6, -7\} \subset A$, then since we have $-2 + 5 + 4 - 7 = -3 + 4 + 6 - 7 = 0$, it follows that there is no integer in $\{2, -2, -3\}$ which belongs to $A$. Therefore we have $g_0 = 2$ and using Lemma 20 the set $\{-1, 3, 4, 5, 6, -7\}$ is included in $A$. Since $-1 + 3 + 5 - 7 = 0$, this is in contradiction to the fact that $A$ is zero-free. Therefore it follows that neither the integer 4 nor $-4$ can belong to $A$. Therefore using Lemma 20 we have $\{-1, -2, 5, 6, -7\} \subset A$. Since $3 - 1 - 2 = -3 - 1 - 2 + 6 = 0$, this implies that neither the integer 3 nor $-3$ can belong to $A$. In other words none of the integers from the set $\{-3, 3, -4, 4\}$ can belong to $A$. This is in contradiction to Lemma 20. Hence $z_0$ cannot be equal to 7.

Case 4: If $z_0 = 6$. In this case we have $\{5, -6\} \subset A$. Since $1 + 5 - 6 = 0$, it follows that the integer 1 cannot belong to $A$. We have two subcases to discuss in this case, the first one when $g_0 \neq 1$ and the second one when $g_0 = 1$.

In case $g_0 \neq 1$, then we have $-1 \notin A$; that is $\{-1, 5, -6\} \subset A$. Since $-1 - 6 + 7 = 0$, this implies that $-7 \notin A$. This in turn implies that $-8 \notin A$. Thus we have $\{-1, 5, -6, -7, -8\} \subset A$. Since $4 + 5 - 8 - 1 = -4 - 1 + 5 = 0$, it follows that none the
integers 4 nor −4 belongs to \( \mathcal{A} \) and hence \( g_0 = 4 \). Since \( 3 + 5 - 8 = 2 + 5 - 7 = 0 \), it follows that none of the integers from the set \( \{2, 3\} \) belongs to \( \mathcal{A} \). Hence using Lemma 20 we have \( \{-2, -3, 5\} \subset \mathcal{A} \). Since \( \mathcal{A} \) is zero-free, this is not possible. Hence if \( z_0 = 6 \), then \( g_0 = 1 \).

In case \( g_0 = 1 \), then either 3 or −3 belongs to \( \mathcal{A} \).

If 3 belongs to \( \mathcal{A} \); that is \( \{3, 5, -6\} \subset \mathcal{A} \), then since \( -2 + 3 + 5 - 6 = 0 \), it follows that \( 2 \in \mathcal{A} \). Thus we have \( \{2, 3, 5, -6\} \subset \mathcal{A} \). Since \( 4 + 2 - 6 = -4 + 2 + 3 + 5 - 6 = 0 \), it follows that none of the integers from the set \( \{1, -1, 4, -4\} \) belongs to \( \mathcal{A} \). This is in contradiction to Lemma 20.

In case \( -3 \in \mathcal{A} \), in other words \( \{-3, 5, -6\} \subset \mathcal{A} \). Since \( 4 + 5 - 3 - 6 = 0 \), it follows that \( -4 \in \mathcal{A} \), that is \( \{-3, -4, 5, -6\} \subset \mathcal{A} \). Since \( -2 - 3 + 5 = 2 - 3 - 4 + 5 = 0 \), it follows that none of the integers from the set \( \{1, -1, 2, -2\} \) can belong to \( \mathcal{A} \). This is in contradiction to Lemma 20.

Hence we have shown that \( z_0 \notin \{6, \sqrt{2p}/5\} \) and thus the lemma follows.

\( \square \)

**Lemma 25.** Let \( \mathcal{A} \) be as in the previous lemma. Then the set \( \mathcal{A}(4) \) is equal to one of the sets described in the second column of the last sixteen rows of Table 1.

**Proof.** Let \( N \) be the set of integers \( n_i \) which belongs to \([1, 4]\) with \( -n_i \in \mathcal{A} \). Then it follows using the previous lemma that

\[
\sum_{n_i \in N} n_i \leq 4. \tag{14}
\]

This implies that the cardinality of \( N \) is at most 2.

When \( \text{card}(N) = 2 \). It follows from (13) that \( N \) is either equal to \( \{1, 2\} \) or is equal to \( \{1, 3\} \); that is, in this case either \( \{-1, -2\} \) or \( \{-1, -3\} \) is a subset of \( \mathcal{A} \). In case \( \{-1, -2\} \) is a subset of \( \mathcal{A} \), then since \( 3 - 1 - 2 = 0 \), it follows that \( g_0 = 3 \) and \( \mathcal{A}(4) \) is equal to \( \{-1, -2, 4\} \). In case \( \{-1, -3\} \) is a subset of \( \mathcal{A} \), then since \( 4 - 1 - 3 = 0 \), it follows that \( g_0 = 4 \) and \( \mathcal{A}(4) \) is equal to \( \{-1, -3, 2\} \).

When \( \text{card}(N) = 1 \). We have the following four sub-cases to discuss.

- **When** \( N = \{1\} \). In this case \( \mathcal{A}(4) \) can be equal to any of the following three sets, namely, \( \{-1, 2, 3\}, \{-1, 2, 4\}, \{-1, 3, 4\} \).

- **When** \( N = \{2\} \). In this case \( \mathcal{A}(4) \) can be equal to any of the following three sets, namely, \( \{-2, 1, 3\}, \{-2, 1, 4\}, \{-2, 3, 4\} \).

- **When** \( N = \{3\} \). Since \( 1 + 2 - 3 = 0 \), in this case either \( g_0 \) is equal to 1 or is equal to 2. Moreover the set \( \mathcal{A}(4) \) is equal to one of the following two sets, namely, \( \{-3, 1, 4\}, \{-3, 2, 4\} \).

- **When** \( N = \{4\} \). Since \( 1 + 3 - 4 = 0 \), it follows that either \( g_0 \) is equal to 1 or is equal to 3. In this case \( \mathcal{A}(4) \) is equal to one of the following two sets, namely \( \{-4, 1, 2\}, \{-4, 2, 3\} \).

When \( \text{card}(N) = 0 \). In this case \( \mathcal{A}(4) \) is equal to any one of the following four sets, namely, \( \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\} \).

\( \square \)

**Lemma 26.** Let \( \mathcal{A} \) be as in Lemma 24. \( \mathcal{A}' = \mathcal{A} \cap \left[ \frac{-p}{2}, -1 \right]_p \) and \( \mathcal{A}'' = \mathcal{A} \cap \left[ 1, \frac{p}{2} \right]_p \). Then we have

\[
\mathcal{A}' \subset \left[ -4, -1 \right]_p, \quad \left[ 5, \sqrt{2p} - 9 \right]_p \subset \mathcal{A}'' \subset \left[ 1, \sqrt{2p} + 8 \right]_p.
\]
Moreover, the set $A''$ contains $[3, s'' - 3]_p$ with $s'' = \sum_{a' \in A'} |a'|$ and is equal to one of the set described in the fifth column of the last sixteen rows of Table 1; the sixteen possibilities correspond to sixteen possibilities for $A(4)$ as given by Lemma 25. We also have $s'' \leq p + 2$.

**Proof.** For any positive integer $z$ we set

$$s''(z) = \sum_{a'' \in A''(z)} |a''|.$$  

We claim that there is an absolute constant $c$ such that for any integer $z$ with $6 \leq z \leq \frac{p}{c}$, the set $(A(z))^2$ contains the interval $[3, s''(z) - 3]$. Suppose the claim is not true and let $z_0$ be the least integer in $[6, \frac{p}{c}]$ such that $(A(z_0))^2$ does not contains the interval $[3, s''(z_0) - 3]$. Since the claim is easily verified when $z = 6$, it follows that $z_0 \geq 7$. Moreover we also verify that the length of the interval $[3, s''(6) - 3]$ is at least 7. Therefore using Lemma 13 with $x = 6$, it follows that

$$z_0 \geq s''(z_0 - 1) - 4 + 1.$$  

Using Lemmas 24 and 25 it follows that the above inequality does not hold for any $z_0$ with $z_0 \in [6, \sqrt{2p}/5]$. Therefore we have

$$z_0 \geq s''(\sqrt{2p}/5 - 1) - 3 \geq \frac{p}{c},$$

where $c$ is an absolute constant. Hence the claim follows. Using Lemma 19 it follows that $(A)^2$ contains the interval $[3, s'' - 3]$. Since $A$ is zero-free, it follows that $s'' \leq p + 2$. Since $(A(\sqrt{2p}/5))^2$ contains the interval $[3, \frac{2}{5}]$ it follows there is no $y \in [-p/c, -\sqrt{2p}/5]$ with $y \in A'$. Then using Lemma 24 it follows that $A' = A \cap [-4, -1] \subset [-4, -1]$. Using this, it is easy to verify that the set $(A)^2$ is equal to one of the sets described in the fifth column of the last sixteen rows of Table 1. We shall now show that

$$[5, \sqrt{2p} - 9] \subset A''.$$  

Since $A' \subset [-4, -1]$, this follows by showing that

$$g_1 \geq \lfloor \sqrt{2p} \rfloor - 8.$$  

For proving this we may assume that $g_1 \leq \sqrt{2p}$. Then we observe that the following inequality holds

$$\sum_{a \in A} |a| \geq s(\sqrt{2p}) + \left\lfloor \sqrt{2p} \right\rfloor + 1 - g_0 - g_1.$$  

The left hand side of the above inequality is equal to $s'' = \sum_{a' \in A'} |a'|$ and is thus at most $p + 6$. Moreover using Lemma 20 and Theorem 23 we have $s(\sqrt{2p}) \geq p + 2$. Using this and rearranging the terms of (16), we obtain that $g_1 \geq \sqrt{2p} - 8$. We shall now show that

$$A'' \subset \left[1, \lfloor \sqrt{2p} \rfloor + 8 \right].$$  

This is equivalent to showing that the largest integer $y \in A$ is at most $\lfloor \sqrt{2p} \rfloor + 8$. Now we have the following inequality

$$\sum_{a \in A} |a| \geq s(\sqrt{2p}) - g_0 - \lfloor \sqrt{2p} \rfloor + y.$$  

Rearranging the terms of the above inequality we obtain the desired upper bound for $y$. Hence the lemma follows. \Box
Theorem 27. Let $p$ be a sufficiently large prime and $A$ be a zero-free subset of $\mathbb{Z}/p\mathbb{Z}$ of the largest cardinality. We write $\delta(p)$ to denote the integer $\lfloor \sqrt{2p} \rfloor - \text{card}(A)$, as in Theorem 23. Then there exists $d \in (\mathbb{Z}/p\mathbb{Z})^*$ such that the set $dA$ is union of sets $A'$ and $A''$ satisfying the following properties:

(i) $A' \subset \{-2(1 + \delta(p)), -1\}_p$, $A'' \subset [1, p/2]_p$, $A'' \cap (-A') = \emptyset$ and $\text{card}(A') \leq 1 + \delta(p)$,

(ii) the set $A''$ contains the whole interval $[5, \sqrt{2p}/5]_p$ with at most $\delta(p)$ exception,

(iii) the set $(-A') \cup A''$ contains the whole interval $[1, 4]_p$, with at most $\delta(p)$ exception,

(iv) the set $(dA)^2$ contains the whole interval $[3, s'']_p$ with at most $\delta(p)$ exception, where $s'' = \sum_{a'' \in A''} |a''|_p$,

(v) $\sum_{a' \in A'} |a'|_p \leq 2(1 + \delta(p))$ and $\sum_{a'' \in A''} |a''|_p \leq p - 1 + 3\delta(p)$.

Further, if $s'' = \sum_{a'' \in A''} |a''|_p > p - 1$, then we have $s(\sqrt{2p}) = \lfloor \sqrt{2p} + 1/p \rfloor \in [p + 2, p + 7]$.

Proof. It is sufficient to show that there exists $d \in (\mathbb{Z}/p\mathbb{Z})^*$ such that replacing $A$ by $dA$, the conclusion of the theorem holds with $d = 1$. From Proposition 8 there exists $d \in (\mathbb{Z}/p\mathbb{Z})^*$ such that replacing $A$ by $dA$, the inequality (12) holds. Let $g_0$ be the least positive integer which does not belong to $A \cup -A$. When $g_0 \geq 5$, replacing $A$ by $-A$ if necessary, let $A$ be as in Lemma 21. When $g_0 \leq 4$, then replacing $A$ by $-A$ if necessary, let $A$ be as in Lemma 21. For such $A$, let $A' = A \cap [-2, -1]_p$ and $A'' = A \cap [1, 2]_p$. Then claims (i)-(v) follow from Lemmas 20, 21 and 22 in case $g_0 \geq 5$ and from Lemmas 24, 25 and 26 in case $g_0 \leq 4$.

To prove the theorem, we need to show that if $s'' > p - 1$, then $s(\sqrt{2p}) \in [p + 2, p + 7]$. From claim (v) and Lemma 21 it follows that when $s'' > p - 1$, then we have $\delta(p) = 1$. From Theorem 23 it follows that

$$s(\sqrt{2p}) \geq p + 2.$$  \hfill (17)

Moreover from Lemmas 22 and 26 it follows that the set $[3, s'']_p$ is contained in $(A)^2$ in case $g_0 \notin \{1, 2\}$. Therefore it follows that if $s'' > p - 1$, then we have

$$g_0 \in \{1, 2\}.$$  \hfill (18)

When $g_0 \in \{1, 2\}$, then we have

$$s(\sqrt{2p}) - g_0 \leq \sum_{a \in A} |a|_p = \sum_{a' \in A'} |a'|_p + s''$$ \hfill (19)

and from Lemma 26 it follows that either $s'' \leq p - 1$ or we have $s'' = p + g_0$. We also know all the possibilities of $A'$ from Lemma 25 and claim (i). Using this and rearranging the terms in (18), we obtain that when $s'' > p - 1$, then we have

$$s(\sqrt{2p}) \leq p + 7.$$  \hfill (19)

Therefore if $s'' \geq p - 1$ then from (17) and (19), we have $s(\sqrt{2p}) \in [p + 2, p + 7]$. Hence the theorem follows.

The Theorem readily follows from Theorems 23 and 27.
3 Proof of Theorem 7

Let \( \mathcal{A} \) be as in Theorem 7. From the assumptions we have

\[
e(\mathcal{A}) := |\sqrt{2p} - \text{card}(\mathcal{A})| \leq \psi(p)\sqrt{p} \quad \text{and} \quad p \text{ is sufficiently large,}
\]

where \( \psi \) is a function from \([2, \infty)\) to \(\mathbb{R}^+\) which tends to 0 at \(\infty\). In what follows \( \psi \) will denote this function.

From Proposition 8, replacing \( \mathcal{A} \) by \( d.\mathcal{A} \) for some non-zero element \( d \in \mathbb{Z}/p\mathbb{Z} \) we have

\[
\sum_{a \in \mathcal{A}} |a|_p \leq p + O \left( (e(\mathcal{A})^{3/2}\ln(e(\mathcal{A}) + 2) \right) \quad \text{(21)}
\]

and

\[
\sum_{a \in \mathcal{A}, a < 0} |a|_p = O \left( e(\mathcal{A})^{3/2}\ln(e(\mathcal{A}) + 2) \right). \quad \text{(22)}
\]

As before we find it more convenient to work with \( \tilde{\mathcal{A}} \) than \( \mathcal{A} \). We partition the set of natural numbers into the three disjoint sets \( P, N \) and \( G \) which are defined as follows.

\[
P = \{ k \in \mathbb{N} : k \in \tilde{\mathcal{A}} \}, \quad N = \{ k : k \in -\tilde{\mathcal{A}} \}, \quad G = \{ k : k \notin \tilde{\mathcal{A}} \cup -\tilde{\mathcal{A}} \}.
\]

An immediate corollary of (22) is that the cardinality of \( N \) is \( O \left( e(\mathcal{A})^{3/4}\ln(e(\mathcal{A})) \right) \). We shall prove the following result.

**Proposition 28.** The cardinality of \( N \) is \( O(\sqrt{e(\mathcal{A})}) \). Moreover there exists an absolute constant \( c \) such that \( N \subset [1, ce(\mathcal{A})] \).

We first deduce Theorem 7 from Proposition 28.

**Proof of Theorem 7.** From Proposition 8 there exists a \( d \in (\mathbb{Z}/p\mathbb{Z})^* \) such that replacing \( \mathcal{A} \) by \( d.\mathcal{A} \), the inequalities (21) and (22) hold. Let \( \mathcal{K} = \tilde{\mathcal{A}} \setminus (-N) \). Then we have

\[
e(\mathcal{K}) := |\sqrt{2p} - \text{card}(\mathcal{K})| \leq e(\mathcal{A}) + \text{card}(N) = O \left( \psi(p)\sqrt{p} \right), \text{ the last equality follows using Proposition 28.}
\]

Moreover we have

\[
\sum_{k \in \mathcal{K}} |k| \leq \sum_{a \in \mathcal{A}} |\bar{a}| \leq p + O(e(\mathcal{A})^{3/4}\ln(e(\mathcal{A}) + 2)).
\]

Therefore it follows that \( \mathcal{K} \) satisfies the assumption of Proposition 11 with \( s(\mathcal{K}) = O(e(\mathcal{A})^{3/4}\ln(e(\mathcal{A}) + 2)) \). Let \( \mathcal{C}_1 \) be a subset of \( \mathcal{K} \) as in the proof of Proposition 11. Then we have \( \mathcal{C}_1 \subset [1, ce(\mathcal{A})] \), \( \text{card}(\mathcal{C}_1) = O(\sqrt{e(\mathcal{A})}\ln(e(\mathcal{A})) \) and \( \sum_{k \in \mathcal{K} \setminus \mathcal{C}_1} |k| \leq p - 1 \). Let \( \mathcal{A}' = \sigma_p(N \cup \mathcal{C}_1) \) and \( \mathcal{A}'' = \mathcal{A} \setminus \mathcal{A}' \). Then using Proposition 28 and the properties of \( \mathcal{C}_1 \) just stated, we have that \( \mathcal{A}' \subset [-ce(\mathcal{A}), ce(\mathcal{A})]_p \) for some absolute positive constant \( c \) and \( \text{card}(\mathcal{A}') = \text{card}(\mathcal{C}_1) + \text{card}(N) = O(\sqrt{e(\mathcal{A})}\ln(e(\mathcal{A}) + 2)) \). From the definition of \( N \) and \( \mathcal{A}'' \), we have that \( \mathcal{A}'' \subset [1, \frac{p}{2}]_p \). Moreover we have

\[
\sum_{a'' \in \mathcal{A}''} |a''| = \sum_{k \in \mathcal{K} \setminus \mathcal{C}_1} |k| \leq p - 1.
\]

Hence Theorem 7 follows. \( \square \)
3.1 Proof of Proposition 28

Lemma 29. The cardinality of $P(0.9\sqrt{2p})$ is equal to $0.9\sqrt{2p} - O(e(A))$.

Proof. Applying Lemma [15] with $K = \bar{A}$ and $e(p) = e(A)^{3/2} \ln e(A)$ we obtain that
$$\text{card}(P(0.9\sqrt{2p})) + \text{card}(N(0.9\sqrt{2p})) = 0.9\sqrt{2p} - O(e(A))$$
and using [22] it also follows that the cardinality of $N$ is $O(e(A)^{3/4} \ln e(A))$. Hence the lemma follows. \hfill \Box

Lemma 30. Let $q$ be a sufficiently large positive integer and $B \subset [1, q]$ with $\text{card}(B) \geq \frac{7}{8}q$. Then the interval $[q + 1, \frac{13}{8}q]$ is contained in $2^*B$.

Proof. For any $n \in [q+1, \frac{13}{8}q]$ there are $q - \left\lceil \frac{n}{q} \right\rceil - 1$ pairs of elements $(a_i, b_i)$ with $n = a_i + b_i$, $a_i < b_i$ and both $a_i, b_i \in [1, q]$. Among these pairs if there is a pair $(a_i, b_i)$ with both $a_i, b_i \in B$ then the assertion follows. If not then $\text{card}(B) \leq q - (q - \left\lceil \frac{n}{q} \right\rceil - 1) = \left\lceil \frac{n}{q} \right\rceil + 1$ which is strictly less than $\frac{7}{8}q$, since $n \leq \frac{13}{8}q$. This is contrary to the assumption. Hence the lemma follows. \hfill \Box

Lemma 31. Let $q$ be a sufficiently large positive integer and $B \subset [1, q]$ with $\text{card}(B) = q - O(\psi(q)q)$. Then the interval $[q + 1, \psi(q)^{1/2}q^2]$ is contained in the set $B^2$.

Proof. For any $n \in [q+1, \frac{13}{8}q]$ it follows from the previous lemma that $n \in B^2$. Let $B(0.2q, 0.4q) = B \cap [0.2q, 0.4q] = \{b_1 > b_2 > .... > b_I\}$. Then from the assumptions of the lemma we have $\text{card}(B(0.2q, 0.4q)) \geq 0.2q - O(\psi(q)q)$. Let $C$ be the sequence $\{c_i\}_{i=1}$ with $c_i = \sum_{i=1}^i b_i$. Then the following properties of $c_i$ are evident.

(i) $c_i \geq 0.2qi,$

(ii) $c_{i+1} - c_i \leq 0.4q.$

Now for every $n \in [\frac{13}{8}q, \psi(q)^{1/2}q^2]$, let $n_i$ be the least integer with $1 \leq n_i \leq I$ such that $n - c_{n_i}$ belongs to the interval $[1.01q, \frac{13}{8}q]$. From the properties of $c_i$ it follows that such a $n_i$ exists and $n_i \leq \psi(q)^{1/2}q$. Moreover we also have $c_i \in B_{n_i}$, where $B_{n_i} = \{b_1, b_2, ..., b_{n_i}\} \subset B$ and is of cardinality $n_i$. Now $\text{card}(B \setminus B_{n_i}) \geq q - O(\psi(q)^{1/2}q)$. Therefore using Lemma 30, the element $n - c_{n_i}$ can be written as a sum of distinct elements of the set $B \setminus B_{n_i}$. Hence $n \in B^2$. Hence the lemma follows. \hfill \Box

Lemma 32. The set $P^2$ contains the interval $[0.9\sqrt{2p} + 1, \psi(p)^{1/2}p]$.

Proof. From Lemma 29 the cardinality of $P(0.9\sqrt{2p})$ is $0.9\sqrt{2p} - O(e(A)) \geq 0.9\sqrt{2p} - O(\psi(p)\sqrt{p})$. Therefore the assertion follows from Lemma 31. \hfill \Box

Lemma 33. The cardinality of $N$ is $O(\sqrt{e(A)})$.

Proof. From Lemma 16 the largest integer $y_0$ belonging to $P \cup N$ is $O(e(A)^{1/2}p)$. Since $\bar{A}$ does not contain any multiple of $p$ and hence does not contain zero, the sets $P^2$ and $N$ are disjoint. Therefore using Lemma 32 it follows that $N \subset [1, 0.9\sqrt{2p}]$. Since the cardinality of $N$ is $O(e(A)^{3/4} \ln e(A))$, it follows that $N^2 \subset [1, c_0 e(A)^{3/4} \ln e(A)^{1/2}]$. Since $e(A) \leq \psi(p)^{1/2}p$, using Lemma 32 it follows that $N^2 \subset [1, 0.9\sqrt{2p}]$. Now using Lemma 29 and the fact that $P$ and $N^2$ are disjoint sets, it follows that the cardinality of $N^2$ is $O(e(A))$. Since we also have that the cardinality of $N^2$ is at least $\frac{(\text{card}(N))^2}{2}$, the assertion follows. \hfill \Box
Lemma 34. There exists a positive absolute constant $c_0$ such that $N \subset [1, c_0 e(A)]$.

Proof. Let $x$ be a sufficiently large integer such that $\text{card}(P(x)) \geq \frac{7}{8} x$, then using Lemma 31 the set $N$ does not contain any element from the interval $[x + 1, \frac{13}{8} x]$. From Lemma 29 there exists an integer $x_0$ such that $x_0 = O(e(A))$ and for any integer $x$ with $x_0 \leq x \leq 0.9 \sqrt{2p}$, we have $\text{card}(P(x)) \geq \frac{5}{8} x$. Therefore the set $N$ does not contain any integer in the interval $[x_0, 0.9 \sqrt{2p}]$. As it was observed during the proof of Lemma 33 we have $N \subset [1, 0.9 \sqrt{2p}]$, it follows that $N \subset [1, x_0]$. Hence the lemma follows. \qed

From Lemmas 33 and 34, Proposition 28 follows.

References

[1] Jean-Marc Deshouillers. Quand seule la sous-somme vide est nulle modulo $p$. Journal de Theorie des Nombres de Bordeaux, 19:71–79, 2007.

[2] Jean-Marc Deshouillers and Gregory A. Freiman. When subsets-sums do not cover all the residues modulo $p$. Journal of Number Theory, 104:255–262, 2004.

[3] Yahya Ould Hamidoune and Gilles Zémor. On zero-free subset sums. Acta Arith., 78(2):143–152, 1996.

[4] Hoi H. Nguyen, Endre Szemerédi, and Van H. Vu. Subset sums modulo $\mathbb{Z}_p$. Acta Arith., 131(4):303–316, 2008.

[5] P. Erdős and H. A. Heilbronn. On the addition of residue classes modulo $p$. Acta Arith., 9:149–159, 1964.

[6] Endre Szemerédi and Van H. Vu. Long arithmetic progressions in sumsets and the number of $x$-free sets. Proc. London Math. Soc., 90:273–296, 2005.

Jean-Marc Deshouillers
Institut Mathématique de Bordeaux,
Université de Bordeaux et CNRS
F-33405 TALENCE Cedex,
France.
E-mail: jean-marc.deshouillers@math.u-bordeaux1.fr

Gyan Prakash
Institut Mathématique de Bordeaux,
Université de Bordeaux 1,
F-33405 TALENCE Cedex,
France.
E-mail: gyan.prakash@math.u-bordeaux1.fr
gyan.jp@gmail.com