CARRIES AND THE ARITHMETIC PROGRESSION STRUCTURE OF SETS

Francesco Monopoli
Dipartimento di Matematica, Università degli Studi di Milano, via Saldini 50, Milano, I-20133 Italy
fr.monopoli@gmail.com

Imre Z. Ruzsa[1]
Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Budapest, Pf. 127, H-1364 Hungary
ruzsa@renyi.hu

Received: 5/19/15, Revised: 10/3/16, Accepted: 3/9/17, Published: 4/14/17

Abstract

Adding integers in base m results in carries. The same happens modulo a generic integer q when the set of digits is a complete set of residues modulo m for some positive integer m such that m and q are composed of the same primes, and the exponent of each prime in q is strictly greater than in m. This paper proves that in this case any digital set inducing only two distinct carries is an arithmetic progression, thus generalizing results of Diaconis, Shao and Soundararajan.

1. Introduction

If we want to represent integers in base m, we need a set A of digits, which needs to be a complete set of residues modulo m. The most popular choices are the integers in $[0, m-1]$ and the integers in $(-m/2, m/2]$.

When adding two integers with last digits $a_1, a_2 \in A$, we find the unique $a \in A$ such that

$$a_1 + a_2 \equiv a \pmod{m},$$

which will be the last digit of the sum, and $(a_1 + a_2 - a)/m$ will be the *carry*. Diaconis, Shao and Soundararajan in the nice paper [4] and Alon in [1] show that the above two popular sets both have an extremal property: $(-m/2, m/2]$ minimizes the number of pairs a_1, a_2 for which there is a nonzero carry, while $[0, m-1]$ minimizes

[1]Author was supported by ERC–AdG Grant No. 321104 and Hungarian National Foundation for Scientific Research (OTKA), Grants No. 109789, and NK104183.

the number of distinct carries, and both examples are unique up to certain linear transformations.

The second extremal property is essentially equivalent to the following statement:

Let $A \subset \mathbb{Z}_{m^2}$ be a set which forms a complete set of residues modulo m. If $A + A \subset A + \{x, y\}$ with some $x, y \in \mathbb{Z}_{m^2}$, then A is an arithmetic progression.

In [4] this is proved for the case m prime.

From now on we call a set $A \subset \mathbb{Z}_q$ a *digital set,* if $m = |A|$ satisfies $m|q$, and A is a complete set of residues modulo m. A more general claim could sound as follows:

Let $A \subset \mathbb{Z}_{m^2}$ be a digital set with $|A| = m$. If $|A + A| \leq 2m$, then A is an arithmetic progression.

In [5] we find a complete description of finite sets in commutative groups satisfying $|A+A| \leq 2|A|$. This could be used to deduce the above claim. This deduction is not immediate, however, as this description contains a lot of subcases. We remark also that in [6] Hamidoune, Serra and Zémor prove a result somehow similar to our Theorem 2, which will be used to prove the claim above, albeit with different hypotheses and a weaker conclusion.

The aim of this paper is to provide a further generalization of the following form:

Let $A \subset \mathbb{Z}_{m^2}$ be a digital set with $|A| = m$. For every set B such that $1 < |B| < m^2 - m$ we have $|A + B| > m + |B|$, with certain exactly described exceptions.

Digital sets of cardinality m exist in $\mathbb{Z}_q$ whenever $m|q$. For our arguments we need a stronger assumption, which is, however, more general than the case $q = m^2$, namely, that m and q are composed of the same primes, and the exponent of each prime in q is strictly greater than in m. This is a natural restriction, as otherwise there are digital sets that are either contained in a nontrivial subgroup, or are unions of cosets of a nontrivial subgroup.

As we are looking for estimates that depend only on the cardinality of the other set B, it is comfortable to express this in terms of the *impact function* of the set A:

$$\xi(n) = \xi_A(n) = \min_{|B|=n} |A + B|,$$

defined for integers n that can serve as cardinality of a set; if we are in $\mathbb{Z}_q$, this means $|B| \leq q$.

Some values of ξ are determined by the size of A: we have $\xi(0) = 0$, $\xi(1) = m$, $\xi(n) = q$ for $q - m < n \leq q$ and $\xi(q - m) = q - 1$ by a familiar pigeonhole argument. A nontrivial estimate may exist for $1 < n < q - m$. The case $n = 2$ can be interpreted via the arithmetic progression structure of A. Given any $t \in \mathbb{Z}_q \setminus \{0\}$, A can be decomposed as the union of some cosets of the subgroup generated by t and some arithmetic progressions of difference t. Let $\alpha_t(A)$ be the number of arithmetic progressions in this decomposition. We have clearly

$$|A + \{x, x + t\}| = m + \alpha_t(A)$$

for every x, hence

$$\xi(2) = \min_t \alpha_t(A).$$

Thus, $\xi(2) > m + 2$ holds unless A is the union of at most two arithmetic progressions (as we shall soon see, digital sets do not contain nontrivial cosets). Hence the strongest result of this kind that may hold (save the lower bound on m) sounds as follows.

Theorem 1. *Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m. Let $A \subset \mathbb{Z}_q$ be a digital set with $|A| = m > 15$. We have*

$$\xi_A(n) > m + n$$

for $1 < n < q - m$, unless A is the union of at most two arithmetic progressions with a common difference.

A description of sets satisfying $|A + A| \leq 2m$ could be achieved by analyzing unions of two arithmetic progressions, a task not difficult which allows us to generalize the aforementioned result found in [4].

Corollary 1. *Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m. Let $A \subset \mathbb{Z}_q$ be a digital set with $|A| = m > 15$ such that $2A \subseteq \{x, y\} + A$ for some $x, y \in \mathbb{Z}_q$. Then there exist $c \in (\mathbb{Z}_q)^\times$ and $d \in m\mathbb{Z}_q$ such that $cA + d = \{0, 1, \ldots, m - 1\}$.*

In the first part of the paper we prove a somewhat weaker result. It turns out that the key to the claims above would be to understand (i) the cases when $\xi(2) = \xi(3)$, (ii) the cases when the decomposition of our set into the minimal $\xi(2)$ arithmetic progressions is not unique. The second part of the paper is devoted to these questions, including the proof of Theorem 1.

Our main result is as follows.

Theorem 2. *Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m. Let $A \subset \mathbb{Z}_q$ be a digital set with $|A| = m$ and $\xi = \xi_A$ its impact function. Let h be a nonnegative integer and $m_0(h) = \max(209, 3h)$. If the inequality*

$$\xi(n) \geq m + n + h \tag{1}$$

holds in the range

$$2 \leq n \leq \frac{3 + \sqrt{16h + 1}}{2}$$

and $m \geq m_0(h)$, then it holds in the range

$$2 \leq n \leq q - m - h - 1.$$

Corollary 2 (Case $h = 0$). *Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m, and $m \geq 5$. Let $A \subset \mathbb{Z}_q$ be a digital set with $|A| = m$. If A is not an arithmetic progression, then $\xi(n) \geq n + m$ in the range*

$$2 \leq n \leq q - m - 1.$$

Corollary 3 (Case $h = 1$). *Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m, and $m \geq 10$. Let $A \subset \mathbb{Z}_q$ be a digital set with $|A| = m$. If $\xi(2) \geq m + 3$ (that is, A is not a union of at most two arithmetic progressions of a common difference) and $\xi(3) \geq m + 4$, then $\xi(n) \geq n + m + 1$ in the range*

$$2 \leq n \leq q - m - 2.$$

2. Proof of Theorem 2

We fix the following assumptions: q and m are positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m, p is the smallest prime divisor of q, and A is our digital set with $|A| = m$. We will denote the greatest common divisor of integers a and b by (a, b).

First we consider adding a subgroup to A.

Lemma 1. *Let H be a subgroup of $\mathbb{Z}_q$, $H \neq \{\emptyset\}$, $H \neq \mathbb{Z}_q$.*

(i) For every t we have

$$|A \cap (H + t)| \leq \frac{\min(m, |H|)}{p} \leq \frac{\min(m, |H|)}{2} \tag{2}$$

(ii) For every nonempty subset A' of A we have

$$|A' + H| \geq p|A'| \geq 2|A'|. \tag{3}$$

(iii) We have

$$|A + H| \geq (m|H|, q) \geq \begin{cases} p \max(m, |H|) \geq (p-1)m + |H|, \\ \min\left(q, \frac{4}{3}m + |H|.\right) \end{cases} \tag{4}$$

Proof. Write $|H| = n$. We have $n|q$, $1 < n < q$ and

$$H = \left\{0, \frac{q}{n}, \frac{2q}{n}, \ldots, \frac{(n-1)q}{n}\right\}.$$

Some of these numbers are congruent modulo m, namely, if $m|(jq/n)$, then after j steps the residues modulo m are repeating. Clearly

$$m \,\Big|\, \frac{jq}{n} \text{ if and only if } mn \,\Big|\, jq \text{ if and only if } \frac{mn}{(mn,q)} \,\Big|\, j.$$

Hence

$$|A \cap (H+t)| \le \frac{mn}{(mn,q)} = \frac{m}{(m,q/n)} = \frac{n}{(n,q/m)}.$$

Since both m and q/m contain all prime divisors of q, both denominators are divisible by at least one prime factor of q, hence both are $\ge p$. This shows (2).

To show (3), let z be the number of cosets of H that intersect A'. In each intersection we have

$$|A' \cap (H+t)| \le |A \cap (H+t)| \le n/p,$$

so $|A'| \le zn/p$ while $|A'+H| = zn$.

To prove (4), observe that as any coset of H contains at most $m/(m,q/n)$ elements of A, then A must intersect at least $(m,q/n)$ cosets, which together have $n(m,q/n) = (mn,q)$ elements. Since

$$(mn,q) = n(m,q/n) \ge pn \tag{5}$$

and

$$(mn,q) = m(n,q/m) \ge pm, \tag{6}$$

we immediately get the bound in the upper line. It is stronger than the lower line unless $p = 2$.

If $p = 2$, then (5) becomes

$$(mn,q) = n(m,q/n) \ge 2n,$$

and (6) can be strengthened to

$$(mn,q) = m(n,q/m) \ge 3m,$$

unless $(n,q/m) = 2$. If both inequalities hold, then their arithmetic mean yields the stronger bound $(3/2)m + n$.

If the second inequality fails, then n is a power of 2, say $n = 2^j$. If $j = 1$, then we have

$$(mn,q) = (2m,q) = 2m \ge (4/3)m + n = \frac{4}{3}m + 2,$$

as $m \ge 3$.

If $j \ge 2$, then q/m must contain 2 exactly in the first power, say $q = 2^s q'$, $m = 2^{s-1}m'$ with odd q', m'. If $q' = m' = 1$, then $q|mn$ and $|A+H| = q$. Otherwise $m' \ge 3$, consequently $m \ge 3 \cdot 2^{s-1} \ge (3/2)n$ and

$$(mn,q) = 2m \ge \frac{4}{3}m + n.$$

□

Proof of Theorem 2. Let N be the least positive integer n such that $\xi(n) \geq q-1$.

In order to estimate $\xi(n)$ in the range $2 \leq n \leq q-m-h-1$ we will first prove (1) for $2 \leq n \leq N-1$. Once we prove this we have $m+N-1+h \leq \xi(N-1) < q-1$, and so $N \leq q-m-h-1$. Then for integers $N \leq n \leq q-m-h-1$, we have $\xi(n) = q-1 \geq m+n+h$ as required.

Let $2 \leq n \leq N-1$ be the number where $\xi(n)-n$ assumes its minimum, and if there are several such values, we take n to be the smallest of them. Write $\xi(n)-n = m+r$. If $r \geq h$, we are done, so we suppose that $r \leq h-1$.

Let B be a set such that $|B| = n$, $|A+B| = m+n+r$. We shall bound n from above in several stages.

The set $D = \mathbb{Z}_q \setminus (A+B)$ satisfies $|D| = q-(m+n+r)$ and

$$(A-D) \subset \mathbb{Z}_q \setminus (-B).$$

Hence $|A-D| \leq q-n = |D|+m+r$.

Since $|A+B| < q-1$ as $n < N$, we have $|D| \geq 2$. Then either $n < N \leq |D|$ or, if $|D| < N$, we have $n \leq |D|$ by the minimality of $|B|$.

In both cases we have

$$n \leq \frac{q-(m+r)}{2}.$$

Next we show that $A+B$ is aperiodic. To this end we use *Kneser's theorem*: for any finite sets A, B in a commutative group G we have

$$|A+B| \geq |A+H| + |B+H| - |H|,$$

where

$$H = \{t \in G : A+B+t = A+B\},$$

the group of periodes of $A+B$.

If $H = \mathbb{Z}_q$, then we get $|A+B| \geq |A+H| = q$ and we are done. If $H \neq \{0\}$, $H \neq \mathbb{Z}_q$, then we apply Lemma 1 to conclude

$$|A+H| \geq \frac{4}{3}m + |H|$$

and so

$$|A+B| \geq \frac{4}{3}m + |B+H| \geq \frac{4}{3}m + |B| \geq m+h+n$$

as wanted (here we use the bound $m \geq 3h$).

Next we show that B is a Sidon set, that is, for every $t \neq 0$ we have $|B \cap (B+t)| \leq 1$. Note that this fact can be deduced from [6, Corollary 9], which states that B has to be either a subgroup of $\mathbb{Z}_q$ or a Sidon set. Since $A+B$ is aperiodic, the first option is excluded and hence B is a Sidon set. Nevertheless, in order to avoid introducing the terminology from [6], we include a simple proof of this fact in the following.

Suppose then that B is not a Sidon set. Fix a t such that $|B \cap (B+t)| \geq 2$ and write

$$B_1 = B \cap (B+t),\ B_2 = B \cup (B+t).$$

These sets satisfy

$$|B_1| + |B_2| = 2|B| = 2n,$$
$$A + B_1 \subset (A+B) \cap (A+B+t),$$
$$A + B_2 = (A+B) \cup (A+B+t),$$

and consequently

$$|A+B_1| + |A+B_2| \leq 2|A+B| = 2(m+n+r). \tag{7}$$

B_1 must be a proper subset of B, since otherwise B and a fortiori $A+B$ would be periodic. Consequently we have

$$|A+B_1| > m + |B_1| + r \tag{8}$$

by the minimality of $|B|$. The set B_2 satisfies

$$|B_2| = 2n - |B_1| \leq 2n - 2 \leq q - (m+r+2). \tag{9}$$

If $2 \leq |B_2| < N$, then $|A+B_2| \geq m + |B_2| + r$.

If $|B_2| \geq N$, then $|A+B_2| \geq q - 1 > m + |B_2| + r$ by (9).

In both cases, we have

$$|A+B_2| \geq m + |B_2| + r. \tag{10}$$

By adding (8) and (10) we obtain

$$|A+B_1| + |A+B_2| > 2m + |B_1| + |B_2| + 2r = 2(m+n+r),$$

which contradicts (7).

Since B is a Sidon set, we have (see [9])

$$|A+B| \geq \frac{mn^2}{m+n-1}.$$

This inequality holds for every set of m elements and it is nearly best in this generality; to use the special properties of A we will need another approach.

Comparing this lower bound with the value $m+n+r$ yields the inequality

$$mn^2 \leq (m+n+r)(m+n-1) \leq (m+n+h-1)(m+n-1).$$

This is a quadratic inequality in n and it gives the bound

$$n \leq \frac{b + \sqrt{b^2+4ac}}{2a},\ a = m-1,\ b = 2m+h-2,\ c = (m-1)(m+h-1).$$

For large m this is asymptotic to $\sqrt{m}$; in particular, there is an m_0 depending on h such that

$$\beta = \frac{|A+B|}{|A|} = \frac{m+n+r}{m} < \sqrt{2}$$

for $m > m_0$.

Such a bound is easily found in the particular cases $h = 0, 1$; if $h = 0$, it holds for $m \geq 5$, if $h = 1$, it holds for $m \geq 10$. For general h, using the hypothesis of $m \geq 3h$, a routine check proves that this holds for $m \geq 209$.

Plünnecke's theorem (see [8]) implies the existence of a nonempty subset A' of A such that

$$|A' + 2B| \leq \beta^2 |A'| < 2|A'|. \tag{11}$$

We shall compare this to the Kneser bound

$$|A' + 2B| \geq |A' + H| + |2B + H| - |H|,$$

where H is the group of periods of $A' + 2B$. If H is a nontrivial subgroup, then

$$|A' + H| \geq 2|A'|$$

by (3); this also holds trivially if $H = \mathbb{Z}_q$, and this contradicts (11).

If $H = \{0\}$, then Kneser's bound reduces to

$$|A' + 2B| \geq |A'| + |2B| - 1 = |A'| + \frac{n(n+1)}{2} - 1,$$

as $|2B| = n(n+1)/2$ by the Sidon property. A comparison with the upper estimate (11) gives

$$|A'| + \frac{n(n+1)}{2} - 1 \leq \left(\frac{m+n+r}{m}\right)^2 |A'|,$$

$$\frac{n(n+1)}{2} - 1 \leq |A'| \left(\left(\frac{m+n+r}{m}\right)^2 - 1\right)$$

$$\leq m\left(\left(\frac{m+n+r}{m}\right)^2 - 1\right) = \frac{(2m+n+r)(n+r)}{m} \leq \frac{(2m+n+h-1)(n+h-1)}{m}.$$

This is again a quadratic inequality in n and it gives the bound

$$n \leq \frac{b + \sqrt{b^2 + 4ac}}{2a},\ a = m-2,\ b = 3m+4h-4,\ c = 2m + 2(h-1)(2m+h-1).$$

As $m \to \infty$, this bound tends to $\left(3 + \sqrt{16h+1}\right)/2$. The bound m_0 after which we can claim this bound for n depends on the fractional part of the square root inside, but it is easily found in the particular cases $h = 0, 1$; if $h = 0$, it holds for $m \geq 4$, if $h = 1$, it holds for $m \geq 9$. □

Remark. We remark that Theorem 2 also holds in a more general setting. In particular, as long as the set B appearing in the proof is not a subgroup, which happens in more general situations than just digital sets, the already mentioned Corollary 9 from [6] can be applied to prove that B is a Sidon set and continue in the proof. This would allow us to get rid of the arithmetic conditions on q and m.

3. Arithmetic progression structure of sets

In order to deduce Theorem 1 from Theorem 2 and its Corollary 3, we need to study the values at 2 and 3 of the impact function of a digital set $A \subseteq \mathbb{Z}_q$. In fact, if we are able to exclude the possibility of the equality $\xi_A(2) = \xi_A(3)$, Corollary 3 tells us that any digital set A inducing the minimal amount of distinct carries is the union of at most two arithmetic progressions.

For any set $A \subseteq \mathbb{Z}_q$, the equality $\xi_A(2) = \xi_A(3)$ is linked to the arithmetic progression structure of A, and is thus interesting to study even outside the context of digital sets.

In the following, let $A \subseteq \mathbb{Z}_q$ be a set containing no nontrivial cosets. This assumption is needed to avoid pathological cases and is always satisfied anyway by digital sets, as shown by Lemma 1. Moreover, let ξ_A be its impact function.

If equality $\xi_A(2) = \xi_A(3)$ holds, then there exist nonzero elements $d_1 \neq d_2$ such that

$$|A| + k = \xi_A(3) = |A + \{0, d_1, d_2\}| \geq |A + \{0, d_1\}| \geq \xi_A(2) = \xi_A(3),$$

so that $|A+\{0, d_1, d_2\}| = |A+\{0, d_1\}| = |A+\{0, d_2\}| = |A+\{d_1, d_2\}|$. In particular, this tells us that the set A can be written as the union of k arithmetic progressions of difference d_1 or d_2, and there exist three distinct elements $x_1, x_2, x_3 \in \mathbb{Z}_q$ such that

$$\bigcup_{i=1}^{3} (A + x_i) = (A + x_a) \cup (A + x_b)$$

for any choice of distinct $a, b \in \{1, 2, 3\}$.

We are thus looking for an answer to the question: if $\xi_A(2) = |A| + k$, is there a unique d, up to a sign, such that A can be written as a union of k arithmetic progressions with difference d?

In other words, can there be two proper decompositions of A as

$$A = \cup_{i=1}^{k} P_i = \cup_{i=1}^{k} Q_i,$$

$$P_i = \{a_i, a_i + d_1, \ldots, a_i + k_i d_1\}, \quad Q_i = \{a_i', a_i' + d_2, \ldots, a_i' + k_i' d_2\}$$

with $d_1 \neq \pm d_2$, $d_1, d_2 \in (-q/2, q/2]$?

Note here that the existence of such a double decomposition is implied by the condition $\xi_A(2) = \xi_A(3)$ but it is not equivalent to it. For example, Theorem 3 below characterizes sets A which are union of 2 arithmetic progressions with distinct differences, and they do not satisfy $\xi_A(2) = \xi_A(3)$ unless they are very large.

If A is an arithmetic progression of difference d itself, so that $k = 1$, since A does not contain full cosets, the only possibility is clearly $d_1 = \pm d_2$.

Suppose now $k = 2$. Very small (or, by taking their complement in the right cosets, very large) sets A with $|A| \leq 4$ may have multiple representation as union of two arithmetic progressions, as happens for sets of the form $A = \{a, a + d, b, b + d\}$. On the other hand, we can easily provide examples of different arithmetic progression decompositions if the differences are "small", as happens for sets of the form $A = [a, b] \cup \{b + 2\}$ or $A = \{a - 2\} \cup [a, b]$, which are unions of two intervals as well as two arithmetic progressions of difference 2.

The following theorem states that these are the only kinds of sets having multiple decompositions as union of two arithmetic progressions.

Theorem 3. *Let $A \subseteq \mathbb{Z}_q$, $4 < |A| < q - 4$. Assume that $q > 100$ and A is not contained in a coset of any nontrivial subgroup of $\mathbb{Z}_q$. If $\xi_A(2) = |A + \{0, d\}| = |A| + 2$, then the only elements $x \in \mathbb{Z}_q$ with $|A + \{0, x\}| = |A| + 2$ are $\pm d$, unless A is a dilation of sets of the form $[a, b] \cup \{b + 2\}$ or $\{a - 2\} \cup [a, b]$ for suitable $a, b \in \mathbb{Z}_q$, or, only if q is even, A is a dilation of two intervals as well as two arithmetic progressions of difference $\frac{q}{2} \pm 1$.*

Proof. Let d_1, d_2 be such that $|A + \{0, d_i\}| = |A| + 2$.

`Case 1`: $(d_1, q) = (d_2, q) = 1$.

We will assume that q is odd. The proof for even q is almost identical and can be easily reconstructed from the argument in the odd case.

Dilating A by d_2^{-1} we can assume that A is the union of two disjoint intervals in $\mathbb{Z}_q$. Also, by taking the complementary of A, we can assume $|A| < q/2$. (This may fail if the differences are not coprime to q; then possibly the complement is the union of the same number of arithmetic progressions and some cosets of the subgroup generated by the difference.)

Let $A = I_1 \cup I_2 = P_1 \cup P_2$ where P_i are arithmetic progressions with common difference $1 < d < q/2$, $I_i = [a_i, b_i]$ and $(d, q) = 1$.

Let $d = \frac{q+1}{2} - x$ for a positive integer $x < \frac{q-1}{2}$. Either d^{-1} or $-d^{-1}$ must be congruent to $\frac{q+1}{2} - y$ for a positive integer $y < \frac{q-1}{2}$. Then

$$\pm 4 \equiv 2d(\pm 2d^{-1}) \equiv (2x - 1)(2y - 1) \mod q,$$

which implies that either x or y must be greater than $\frac{\sqrt{q-4}+1}{2} \geq \frac{\sqrt{q}}{2}$.

Hence we can also assume $1 < d \leq (q - \sqrt{q})/2$.

We say that a progression $P_i = \{a + kd : k = 0, \ldots, N\}$ jumps from I_1 to I_2 at $l \in [1, N]$ if $a + (l - 1)d \in I_1 \cap P_i$ and $a + ld \in I_2 \cap P_i$.

We now split the proof into two subcases.

Subcase 1: $d = 2$.

Since $|A| < q/2$, neither P_1 nor P_2 can jump from I_1 to I_2 or vice versa more than once. Each interval I_i has to be covered by both P_i's since $|I_i| < |A| < q/2$, and so we can assume, without loss of generality, that $a_2 = b_1 + 2$. Then one of the two arithmetic progressions of difference $d = 2$ jumps from b_1 to a_2, and the other has to be contained entirely in one interval since $b_2 + 1 \notin A$. Then the only possibility for this to happen is that $a_1 = b_1$ or $a_2 = b_2$, which are the two exceptional sets in the statement of the theorem.

Subcase 2: $d > 2$.

Since $A < q/2$, there must be a gap between the intervals I_1 and I_2 of length $g > q/4$. Let $|I_1| \leq |I_2|$ so that $|I_2| > 2$ and I_2 contains three consecutive elements, and, considering $-A$ instead of A if necessary, let $a_1 - b_2 - 1 \equiv g \bmod q$. Then at least one of the P_i's must jump from I_2 to I_1 and then to I_2 again, implying that $d > g > q/4 > |I_1|$, and that at least one element x' in I_1 satisfies $x' \pm d \in A$.

There are at most four elements $x \in A$, the starting and ending points of the P_i's, such that $\{x+d, x-d\} \not\subseteq A$. So we can find an element $y \in [a_1, a_1+4] \cap A \subseteq I_1$ such that $y \pm d \in A$, either by taking $y = x'$ if $|I_1| < 5$ or y as a point in the middle of an arithmetic progression if $|I_1| \geq 5$.

Since $|I_1| < d$ we have $y \pm d \in I_2$, and so the interval $[y + d, y - d]$ must be contained in I_2.

Take now an element $z \in [y - d - 7, y - d - 5] \subseteq [y + d, y - d]$ which is not the ending element of P_1 or P_2, so that $z + d \in A$, to obtain a contradiction since $z + d \in [y - 7, y - 5] \subseteq [a_1 - 7, a_1 - 1] \subseteq A^c$. (Here we need that $2d + 7 \leq q$, which follows from the assumption on the size of q and the above inequality for d.)

To proceed to the case of not coprime differences we need a simple lemma which allows us to normalize the differences of the arithmetic progressions.

Lemma 2. *Given integers a, q there exists an integer a', $a' \equiv a \bmod q$ and $a' = a_1 a_2$, with $a_1 | q$ and $(a_2, q) = 1$*

Proof. Let $I = \{p : p \text{ prime}, v_p(a) = v_p(q) > 0\}$, where $v_p(x)$ is the usual p-adic valuation of x. Define $a' := q \prod_{p \in I} p + a$, with the usual notation that if $I = \emptyset$, then $\prod_{p \in I} p = 1$. Then $a' \equiv a \bmod q$, $v_p(a') = v_p(q)$ for all primes $p \in I$ and $v_p(a') = \min(v_p(a), v_p(q)) \leq v_p(q)$ for all primes $p \notin I$, $p | q$. □

Let $A = P_1 \cup P_2 = Q_1 \cup Q_2$, with P_i's arithmetic progressions of difference d_1 and Q_i's of difference d_2, with $P_i \setminus (P_i + d_1) = \alpha_i$ for $i = 1, 2$.

Case 2: $(d_2, q) = 1 < (d_1, q)$.

After a dilation we can assume $d_2 = 1$, and so there are three consecutive elements $\{\gamma, \gamma + 1, \gamma + 2\}$ contained in A. If $(d_1, q) > 2$ we have that the union of P_1 and P_2

can cover at most two elements of $\{\gamma, \gamma+1, \gamma+2\}$, which is a contradiction.

Assume now $(d_1, q) = 2$, so that q must be even.

Since at least one of the intervals I_i's contains an element $x_1 \equiv 1 \bmod 2$ and an element $x_2 \equiv 0 \bmod 2$, the two arithmetic progressions Q_1 and Q_2 cannot lie in the same coset of $2\mathbb{Z}_q$. Suppose $Q_1 \subseteq 2\mathbb{Z}_q$.

Let $A_1' = \frac{A \cap 2\mathbb{Z}_q}{2} = \frac{Q_1}{2} \subseteq \mathbb{Z}_{q/2}$. We can assume without loss of generality that $|A_1'| < q/2 - 2$.

Then A_1' is a single arithmetic progression of difference $d_1/2$ (the image of Q_1 under the projection on $\mathbb{Z}_{q/2}$ and up to two distinct intervals I_1' and possibly I_2' (the images of $I_i \cap 2\mathbb{Z}_q$ under the same projection).

Then two things can happen. The first one is that $d_1/2 = 1$, so that the set $I_1' \cup I_2'$ is a single interval, $d_1 = 2$ and we can argue as in Subcase 1 above to get the desired conclusion. The second possibility is that $d_1/2 > 1$ and then $A_1' = I_1' \cup I_2'$ cannot be a single interval, for a single arithmetic progression has a unique difference, up to a sign. Then A_1' is a single arithmetic progression which is the union of two intervals. A simple analysis can show that this can happen only if $q/2$ is odd and $\frac{d_2}{2} = \frac{q/2 \pm 1}{2}$, so that $d_2 = q/2 \pm 1$ and we recover the other exceptional sets in the statement of the theorem.

Case 3: $(d_1, q), (d_2, q) > 1$.

After a dilation, thanks to Lemma 2, we can assume $d_1 | q$.

If $\alpha_1 \equiv \alpha_2 \bmod d_1$ then A is contained in a single coset of the subgroup generated by d_1, contrary to the assumption.

If $\alpha_1 \not\equiv \alpha_2 \bmod d_1$ then $P_i = \{x \in A : x \equiv \alpha_i \bmod d_1\}$.

If $d_1 | d_2$ then we also get $Q_i = \{x \in A : x \equiv \alpha_{\varphi(i)} \bmod d_1\}$ for a permutation $\varphi : \{1, 2\} \to \{1, 2\}$, and the result follows immediately since $A \cap \alpha_i + \mathbb{Z}_q$ is a single arithmetic progression and hence it has a unique, up to a sign, difference.

If $d_1 \nmid d_2$ then, letting $\{q_1, q_2 = q_1 + d_2, q_3 = q_2 + d_2\} \subseteq Q_1$ be elements in an arithmetic progression with at least three elements, we have $q_1 + d_2 \not\equiv q_1 \bmod d_1$ and so $q_1 + 2d_2 \equiv q_1 \bmod d_1$, which leads to a contradiction if q is odd, since then $2|q$, or to $\frac{d_1}{2} | d_2$ if q is even.

Then, if $d_1 = 2$, we can argue as in Case 2 to get the desired conclusion.

If $d_1 > 2$, by our assumptions on A we have that A is not contained in a single coset generated by $d_1/2$, and hence $A_1' = \frac{A \cap \alpha_1 + \frac{d_1}{2}\mathbb{Z}_q}{2} = \frac{P_1}{2} \subseteq \mathbb{Z}_{2q/d_1}$ is an interval (the image of P_1 under the projection) and the union of up to two arithmetic progressions of difference $2d_2/d_1$. Once more, the same argument as Case 2 leads to the desired conclusion. □

Trying to prove results similar to Theorem 3, for larger k, even for prime modulus, is a harder task, since new families of exceptions have to be considered.

For $k > 2$ we still find the same families of sets having more than one decomposition which we found for $k = 2$: small sets or unions of k arithmetic progressions

of small difference.

If $|A| \leq k^2$, there exists an arithmetic progression of difference d in its decomposition having cardinality less or equal than k, so after removing its points from A we obtain a set $\widetilde{A}$ with $|\widetilde{A}| \geq |A| - k$ and $|(\widetilde{A}+d) \setminus \widetilde{A}| \leq k-1$.

On the other hand, if $A = I_1 \cup \cdots \cup I_k = P_1 \cup \cdots \cup P_k$ for intervals I_i's and arithmetic progressions P_i's of difference $d \leq k$, since at least one of these arithmetic progressions must jump from one interval to another, there exists a gap between two intervals of length less or equal than k, and so, by adding those points to A we obtain a set $\widetilde{A}$ with $|\widetilde{A}| \leq |A| + k$ and $|(\widetilde{A}+d) \setminus \widetilde{A}| \leq k-1$.

The common point between these two kinds of sets and the multitude of other types of examples one can produce as k grows, is that even though they both are the union of k d-arithmetic progression, they are actually obtained by sets $\widetilde{A}$ which are the union of $k-1$ d-arithmetic progressions by removing or adding up to k elements. To exclude these sets, we give the following definition.

Definition 1. A set $A \subseteq \mathbb{Z}_q$ has k stable d-components if $|A + \{0,d\}| = |A| + k$, and any set $\widetilde{A}$ obtained by A by removing or adding up to k elements satisfies $|(\widetilde{A}+d) \setminus \widetilde{A}| \geq k$.

Moreover, if we work in the composite number modulus case, new sets having multiple representation as union of a minimal number of arithmetic progressions can be found because of the presence of nontrivial cosets. Of course, the union of k disjoint cosets, each missing one element, has a lot of representations as the union of k arithmetic progressions, but it is not hard to find other less trivial sets which satisfy this property. For example, for suitable k, q, $k \mid q$ and $d = q/k + 1$,

$$A = [0, 2k-1] \bigcup_{i=1}^{k-1} \left[\frac{iq}{k} + i, \frac{iq}{k} + (k+1) + i \right] \subseteq \mathbb{Z}_q$$

is a set of k 1- and d-stable components which is not the union of cosets but still is the union of either k intervals or k arithmetic progressions of difference d. Nevertheless, this set A has high density in some coset of $\mathbb{Z}_q$, namely $\langle q/k \rangle$.

In the following theorem we show that the essential uniqueness of the decomposition of a set into k arithmetic progressions still holds for sets of k stable components and with low density into any coset of $\mathbb{Z}_q$.

Theorem 4. *Let $A \subseteq \mathbb{Z}_q$ be the union of k arithmetic progressions of difference d_1 and d_2, $|A \cap (H+t)| < |H|/2$ for any nonzero coset $H+t$ of $\mathbb{Z}_q$, and A has k stable d_1- and d_2-components. Then $d_1 = \pm d_2$.*

Proof. Let $A = P_1 \cup \cdots \cup P_k = Q_1 \cup \cdots \cup Q_k$ with P_i's being arithmetic progressions of difference d_1 and Q_i's of difference d_2.

Since we are going to prove $d_1 = \pm d_2$, and since every arithmetic progression of difference d is also an arithmetic progression of difference $-d$, during the course of the proof we choose suitable signs for d_i in order to simplify the notations.

We denote by S_i and E_i, $i = 1, 2$ the starting and ending points of the arithmetic progressions of difference d_i forming A, i.e.,

$$S_i = \{x \in A : x - d_i \notin A\}, \qquad E_i = \{x \in A : x + d_i \notin A\},$$

with $|S_i| = |E_i| = k$.

Given x, y, we will write $x \sim_i y$ for $i = 1, 2$ if $x, y \in A$ and they both belong to the same arithmetic progression of difference d_i.

Since A has k stable d_1- and d_2-components, the following properties hold:

(i) $|P_i|, |Q_i| \geq k + 1$ for all $i = 1, \ldots, k$, for if otherwise, by removing a short arithmetic progression, we would obtain a contradiction with Definition 1.

(ii) If $P_i = \{a + ld_1 : l = 0, \ldots, M_i - 1\}, P_j = \{a + (M_i + l)d_1 : l = N, \ldots, N + M_j - 1\}, N > 0$, are two different components contained in the same coset $a + \langle d_1 \rangle$, then $N \geq k + 1$, for otherwise, by adding the elements $\{a + ld_1 : l = M_i, \ldots, M_i + N - 1\}$ to A we would obtain a contradiction to Definition 1. A similar statement holds for Q_i, Q_j and d_2 in place of P_i, P_j and d_1.

(iii) for all i there exists $j : (P_i + d_2) \cap A \subseteq P_j$. In fact, if $P_i \subseteq a + \langle d_1 \rangle$ and $(P_i + d_2) \cap P_{k_l} \neq \emptyset$ for two different components P_{k_1} and P_{k_2}, then we have $P_i + d_2 \subseteq a + d_2 + \langle d_1 \rangle$, which implies that both P_{k_1} and P_{k_2} are contained in the same coset of $\langle d_1 \rangle$. Then, because of (ii), the set $P_i + d_2$ contains at least $k + 1$ elements not belonging to A, and hence $|E_2| \geq k + 1$, a contradiction. A similar statement holds for Q_i and d_1 in place of P_i and d_2.

(iv) for all i there exists $j : (P_i - d_2) \cap A \subseteq P_j$ and for all i there exists $j : (Q_i - d_1) \cap A \subseteq Q_j$, by an argument similar to (iii).

Thanks to Lemma 2 we can assume, after a dilation, that $d_1, d_2 \in [0, q - 1]$, $d_2 \mid q$.

Let $d = (d_1, d_2)$, $d_i = d_i' d$ for $i = 1, 2$, $q = dq'$ and $\mathcal{A}_i = \{x \in A : x \equiv i \bmod d\}$. Clearly, if $P_j \cap \mathcal{A}_i \neq \emptyset$, then $P_j \subseteq \mathcal{A}_i$, and the same holds for the Q_j's, so that every $\mathcal{A}_i$ is the union of $r_{1,i}$ d_1-arithmetic progressions and $r_{2,i}$ d_2-arithmetic progressions.

We are going to show that the ratio $r_{1,i}/r_{2,i}$ is constant for every i such that $\mathcal{A}_i \neq \emptyset$.

Let $A_i = \frac{\mathcal{A}_i - i}{d} \subseteq \mathbb{Z}_{q'}$. Clearly every set A_i inherits from A the same stability properties (relative to k) and the condition of density into cosets.

We use the same notation above for subsets of $\mathbb{Z}_{q'}$, and fix $i \in [0, d - 1]$.

Claim. $r_{2,i} \geq d_2'$.

Proof of claim. Since $d_2'|q'$, $x \sim_2 y$ implies $x \equiv y \bmod d_2'$.

Given $s \in S_1'$, if by contradiction $q' > d_2' > r_{2,i}$ then the set $B = \{s, s+d_1', \ldots, s+r_{2,i}d_1'\}$, which has cardinality $r_{2,i}+1$, is contained in A_i since $r_{2,i} \leq k$.

For $j \in [0, r_{2,i}] \subseteq [0, d_2'-1]$, $jd_1' \equiv 0 \bmod d_2'$ can only happen for $j = 0$ by the coprimality of d_1' and d_2'. Hence B intersects $r_{2,i}+1$ distinct d_2'-arithmetic progressions, which is a contradiction. □

Let now $X = \{x \in [k] : xd_1' \equiv 0 \bmod d_2'\}$. From $d_2' \leq r_{2,i} \leq k$ we get $d_2' \in X$ and hence $X \neq \emptyset$.

For every $x \in X$ let $\beta_+(x)$ be the minimal positive integer such that $xd_1' \equiv \beta_+(x)d_2' \bmod q'$, and $\beta_-(x)$ be the minimal positive integer such that $-xd_1' \equiv \beta_-(x)d_2' \bmod q'$. Let $\beta(x) = \min(\beta_+(x), \beta_-(x))$ and $\min_{x\in X} \beta(x) = \beta(\alpha)$ for some $\alpha \in [k]$.

Since $(d_1, d_2) = (q - d_1, d_2)$ if $d_2|q$, replacing d_1 with $-d_1$ if necessary we can assume $\beta(\alpha) = \beta_+(\alpha)$.

Let $S_1' = \{s_1, \ldots, s_{r_{2,i}}\}$. For every $j \in [0, r_{2,i}]$ define l_j to be the minimal integer such that $s_j + l_jd_1' \sim_2 s_j$. Clearly, by property (iv) and since $l_jd_1' \equiv 0 \bmod d_2'$, we have $l_j \in X$, and one of the following must happen

(i) $s_j + ld_2' \in A_i$ for $l \in [0, \beta_+(l_j)]$

(ii) $s_j - ld_2' \in A_i$ for $l \in [0, \beta_-(l_j)]$

Remark. Because of property (iii) all the elements x such that $x \sim_{1,2} s_j$ are of the form $s_j + ll_jd_1'$ for some $l \geq 0$. In particular, fr $l > 0$, $\beta(ll_j) > \beta(l_j)$, otherwise $|A_i \cap (s_j + \langle d_2' \rangle)| > \frac{|\langle d_2' \rangle|}{2}$.
Moreover, all those elements x belong to the same semicircle $[s_j, s_j + m'/2)$ or $(s_j - m'/2, s_j]$.

Suppose $\beta(l_j) > k$ for all j and $\beta(l_1) = \beta_+(l_1)$, $\beta(l_1) = \min_{j=1,\ldots,r_{2,i}}(\beta(l_j))$. Then the set $\{s_1, s_1 + d_2', \ldots, s_1 + \beta(l_1)d_2' = s_1 + l_1d_1'\} \subseteq A_i$ intersects at least $k+1$ different d_1'-arithmetic progression, leading to a contradiction. A similar argument leads to a contradiction if $\beta(l_1) = \beta_-(l_1)$. Then, since $\beta(l_1), l_1 \leq k$, we get that for every j, $s_j + l_1d_1' = s_j + \beta(l_1)d_2' \sim_{1,2} s_j$. Moreover, since this also implies $\beta(\alpha) \leq k$, Remark 3 tells us that $l_1 = l_j = \alpha$ for all j.

Split the set A_i into M equivalence classes under the relation $P_{j_1} \sim P_{j_2}$ if there are $p_1 \in P_{j_1}$, $p_2 \in P_{j_2}$, with $p_1 \sim_2 p_2$. This is well defined by (iii). Each equivalence class is composed by α d_2'-arithmetic progressions, so that $r_{2,i} = M\alpha$.

If $x, x + \alpha d_1' \in A_i$, there does not exist a $y \in \{x + ld_2', l \in (0, \beta(\alpha))\}$ with $y \sim_1 x$, and hence $k \geq r_{1,i} \geq M\beta(\alpha)$. On the other hand, we already know that $x \sim_1 x + \alpha d_1'$, and so $r_{1,i} = M\beta(\alpha)$. Hence the ratio $r_{1,i}/r_{2,i} = \beta(\alpha)/\alpha$, a constant not depending on i.

Since A is the union of k d_1-arithmetic progressions and k d_2-arithmetic progressions, we must have $\beta(\alpha) = \alpha$.

We now show that this leads to $d_1' = d_2'$, which concludes the proof since, after dilating the set A so that $d_2 \mid q$, we have already chosen between d_1 and $-d_1$ in order to simplify the notation.

Going back to A_i we have $\alpha d_1' \equiv \alpha d_2' \bmod q'$, and so, for $D = (\alpha, q')$ we get $\frac{q'}{D} \mid \frac{\alpha}{D}(d_1' - d_2')$ and so $d_1' = d_2' + j\frac{q'}{D}$ for some $j \geq 0$.

Assume by contradiction that $D > j > 0$. We already know that $B = \{s_1, s_1 + d_2', \ldots, s_1 + \alpha d_2' = s_1 + \alpha d_1'\} \subseteq A_i$. Let D' be the additive order of $j\frac{q'}{D}$ in $\mathbb{Z}_{q'}$, $D' \leq D \leq \alpha \leq k$. Then $s_1 + D'd_1' = s_1 + D'd_2' \in B$ and $s_1 + D'd_1' \sim_2 s_1$, so that $D' = \alpha$. Moreover, $s_1 + ld_1' \in A_i$ for $0 \leq l \leq \alpha$.
By property (i) and $\alpha \leq k$ we have that at least one between

$$s_1 + ld_1' - ld_2' = s_1 + lj\frac{q'}{D} \quad \text{or} \quad s_1 + ld_1' + (\alpha - l)d_2' = s_1 + \alpha d_2' + lj\frac{q}{D}$$

belongs to A_i, and so at least one of the two cosets $s_1 + \langle j\frac{q'}{D}\rangle$ and $s_1 + \alpha d_2' + \langle j\frac{q'}{D}\rangle$, both having cardinality $D' = \alpha$, intersects A_i in more than half of its elements, which leads to a contradiction with our hypothesis of low density in cosets.

Hence $j = 0$ and $d_1' = d_2'$.

□

4. Sets A with $\xi_A(2) = \xi_A(3)$

Let $A \subseteq \mathbb{Z}_q$ be a set containing no nontrivial cosets, with $|A| = m$, $\xi_A(2) = \xi_A(3)$. Then there are $d_1 \neq d_2$ such that

$$A + \{0, d_1, d_2\} = A + \{0, d_1\} = A + \{0, d_2\} = A + \{d_1, d_2\}, \tag{12}$$

After a dilation, applying Lemma 2, we can assume $d_1, d_2 \in [0, q-1]$ and $d_1 | q$. Let $H = \langle d_1 \rangle$ be the subgroup generated by d_1, so that $|H| = q/d_1$.

As usual, write $A = P_1 \cup \cdots \cup P_k = Q_1 \cup \cdots \cup Q_k$ as the union of k d_1-arithmetic progressions P_i's as well as k d_2-arithmetic progressions Q_i's, with

$$P_i = \{a_i + jd_1; j = 0, \ldots, j_i\}, \quad a_i + j_i d_1 = b_i,$$

$$Q_i = \{\alpha_i + ld_2; l = 0, \ldots, l_i\}, \quad \alpha_i + l_i d_2 = \beta_i$$

Since

$$A + \{0, d_1\} = A \amalg \{b_i + d_1\}_{i=1,\ldots,k}$$

$$A + \{0, d_2\} = A \amalg \{\beta_i + d_2\}_{i=1,\ldots,k}$$

we have

$$\{b_i + d_1\}_{i=1,\dots,k} = \{\beta_i + d_2\}_{i=1,\dots,k}. \tag{13}$$

Suppose that set A has nonempty intersection with z cosets of H.

Let $\{G_i\}_{i=1,\dots,k}$ be the set of maximal d_1-arithmetic progressions contained in those z cosets of H such that $G_i \subseteq A^c$. In particular, after a reordering, we can assume $G_i = \{x_i + hd_1, h = 0, \dots, h_i\}$, with $x_i = b_i + d_1$ and $x_i + h_i d_1 = a_{\varphi(i)} - d_1$ for a permutation $\varphi : [k] \to [k]$.

Note that $a_i \in A + \{d_1, d_2\} \setminus A + d_1$, for otherwise A would contain a full coset of H.

Hence

$$a_i - d_2 \in A \tag{14}$$

and from (13) and (14) we deduce that

$$(G_i - d_2) \cap A = \{\beta_{\tau(i)}\}$$

for a permutation $\tau : [k] \to [k]$. Moreover, either $|G_i| = 1$ or $(G_i - d_2) \cap A^c = G_j$ for another G_j with $|G_j| = |G_i| - 1$.

We can then define a partial order $\leq$ on the G_i's by $G_a \leq G_b$ if and only if there exists $i \geq 0$ such that

$$G_a = (G_b - id_2) \cap G_b - i(d_2 - d_1).$$

A G_i which is maximal for this partial order satisfies $G_i + d_2 \subseteq \{\alpha_i\}_{i=1,\dots,k} \subseteq A$, and so $|G_i| \leq k$, leading to

$$|A| \geq z|H| - \frac{k(k+1)}{2}. \tag{15}$$

We have then proved the following:

Theorem 5. *Let $A \subseteq \mathbb{Z}_q$ be a set not containing any nontrivial cosets and which satisfies*

$$\xi_A(2) = \xi_A(3).$$

Then there exists a $d_1|q$ such that A intersects z cosets of $H = \langle d_1 \rangle$ and, after a dilation, A is of the form

$$\mathbb{Z}_q \setminus \left(\coprod_i \mathcal{G}_i \coprod \coprod_{j=1}^{d_1 - z} (t_j + H) \right),$$

where $\mathcal{G}_i$ are chains $\mathcal{G}_i = \{\{g_i\} = G_{i,1} \leq \cdots \leq G_{i,j_i}\}$ with

(i) $|G_{i,j_i}| \leq \xi_A(3) - |A|$,

(ii) $|G_{i,j-1}| = |G_{i,j}| - 1$,

(iii) $g_i - d_2 \in A$,

(iv) $(G_{x,y} + \{0, d_1\}) \cap (G_{w,z} + \{0, d_1\}) = \emptyset$ *for* $(x, y) \neq (w, z)$.

Restricting ourselves to the case $q = p$ prime, it is an interesting question to study the minimal cardinality of A in order to have $\xi_A(2) = \xi_A(3)$.

A rectification argument shows that $|A| > \log_4(p)$. In fact, it is shown in [3] and [7] that sets $A \subseteq \mathbb{Z}_p, |A| \leq \log_4(p)$ are isomorphic to subsets of the integers, and equality (15) cannot hold in this setting, for, if $d_1 > d_2$, then $\max(A) + d_1 \notin A + \{0, d_2\}$.

Since every element $a \in A + \{0, d_1, d_2\}$ must belong to at least two sets $A + x$, $x \in \{0, d_1, d_2\}$, as long as $|A| < 2/3p$ we have

$$k = |A + \{0, d_1, d_2\}| - |A| \leq \frac{|A|}{2}.$$

This, combined with the bound in (15), gives

$$|A| \geq \sqrt{8p + 25} - 5.$$

Let $\mu(p) = \min(|A| : A \subseteq \mathbb{Z}_p$ and A satisfies $\xi_A(2) = \xi_A(3)$). We conjecture the following:

Conjecture 1.

$$\lim_{p\to\infty} \frac{\mu(p)}{p} > 0.$$

In [10] the authors provide an example of a set A with roughly $p/2$ elements and such that $\xi_A(2) = \xi_A(3)$, thus proving that $\liminf_{p\to\infty} \frac{\mu(p)}{p} \leq \frac{1}{2}$.

In the following we will show that $\liminf_{p\to\infty} \frac{\mu(p)}{p} \leq \frac{5}{18}$.

To do this we construct sets $B \subseteq [0, 2^{2m}]$ of cardinality $|B| = \frac{13}{18}2^{2m} + o(2^{2m})$ which is the union of disjoint chains satisfying conditions (i)-(iv) in Theorem 5.

Since by [2] there exists a prime p in $[2^{2m}, 2^{2m} + 2^{21m/20}]$, the complement of the image of the canonical projection of B into $\mathbb{Z}_p$ will have density asymptotic to $5/18$ as required.

Let $d = 2^m$, $\mathcal{G}_l = \{\{0\} \leq [d - 1, d] \leq \cdots \leq [d(l - 1) - (l - 1), d(l - 1)]\}$ for $l \leq d$ and $H_i = (id - d, id]$. Let $\varphi(\mathcal{G}_l) = d + \mathcal{G}_{l-1}$ be the chain of intervals obtained from $\mathcal{G}_l$ by removing the first element in each of its intervals.

If $C = \cup_{i\in I}\mathcal{G}_{l_i} + x_i$ and $\mathcal{G}_a \cap \mathcal{G}_b = \emptyset$ for all $a, b \in I$, then the set $B = \cup_{i\in I}\varphi(\mathcal{G}_{l_i}) + x_i$ satisfies the conditions of Theorem 5.

Let

$$C = C_0 \coprod_{l=1}^{m-1} \coprod_{i=1}^{m-l} B_i^{(l)},$$

where

$$\begin{aligned} C_0 &= \mathcal{G}_{2^m}, \\ B_i^{(l)} &= 2^m(2^{m+1-l} - 2^{m+2-l-i} - 1) + 2^{m+1-l-i} + \mathcal{G}_{2^{m+1-l-i}}. \end{aligned}$$

If we denote by $B_{i,k}^{(l)}$ the k-th interval of the chain, $0 \leq k \leq 2^{m+1-l-i} - 1$, we have that

$$B_{i,k}^{l} = [2^m(2^{m+1-l} - 2^{m+2-l-i} - 1 + k) + 2^{m+1-l-i} - k, \\ 2^m(2^{m+1-l} - 2^{m+2-l-i} - 1 + k) + 2^{m+1-l-i}]$$

Suppose now that $B_{i,k}^{(l)} \cap B_{i',k'}^{(l')} \neq \emptyset$. Then, since $B_{i,k}^{(l)} \subseteq H_{2^{m+1-l}-2^{m+2-l-i}+k}$, for $\alpha(l,i,k) = 2^{m+1-l} - 2^{m+2-l-i} + k$, we must have $\alpha(l,i,k) = \alpha(l',i',k')$.

`Case 1:` $i, i' \geq 2$.

In this case we have $\alpha(l,i,k) \in [2^{m-l}, 2^{m+1-l})$ and since any two of these intervals are disjoint, we must have $l = l'$, which implies that

$$k - 2^{m+2-l-i} = k' - 2^{m+2-l'-i'} \in [-2^{m+2-l-i'}, -2^{m+1-l-i'}].$$

Again, since any two of these intervals are disjoint, we must have $i = i'$, which immediately gives $k = k'$.

`Case 2:` $i = 1$.

In this case from the equality $\alpha(l,i,k) = \alpha(l',i',k')$ we have

$$k = 2^{m+1-l'} - 2^{m+2-l'-i'} + k'.$$

If $i' \geq 2$, then the left hand side is in $[0, 2^{m-l})$, while the right hand side belongs to $[2^{m-l'}, 2^{m+1-l'})$. From this we get that $m-l' < m-l$ and so $\max(B_{i,k}^{l}) > \max B_{i',k'}^{l'}$. Moreover, we have

$$2^{m-l} - k = 2^{m-l} - 2^{m+1-l'} + 2^{m+2-l'-i'} - k' > 2^{m+1-l'-i'}$$

since $k' < 2^{m+1-l'-i'}$, so that $\max B_{i',k'}^{l'} < \min(B_{i,k}^{l})$ and $B_{i,k}^{(l)} \cap B_{i,k}^{(l')} = \emptyset$.

If also $i' = 1$, then $k = k'$ and, if $l < l'$, we have $k \leq 2^{m-l'} - 1 \leq 2^{m-l-1} - 1$, so that $2^{m-l} - k \geq 2^{m-l-1} + 1 \geq 2^{m-l'} + 1$, and so $B_{i,k}^{(l)} \cap B_{i,k}^{(l')} = \emptyset$.

Since $|\varphi(\mathcal{G}_l)| = \frac{l(l-1)}{2}$, for $B = \varphi(C_0) \coprod_{l=1}^{m-1} \coprod_{i=1}^{m-l} \varphi(B_i^{(l)})$, we have

$$|B| = \frac{2^m(2^m-1)}{2} + \sum_{l=1}^{m-1}\sum_{i=1}^{m-l} \frac{2^{m+1-l-i}(2^{m+1-l-i}-1)}{2} = \frac{13}{18}2^{2m} + o(2^{2m})$$

as required.

An analogue of Conjecture 1 can not hold for composite modulus $q = q'q''$, as in this case we can just take a set $A' \subseteq \mathbb{Z}_{q'}$ with $\xi_{A'}(2) = \xi_{A'}(3)$ and consider the set $A = A' \times \{0\} \subseteq \mathbb{Z}_{q'} \times \mathbb{Z}_{q''} = \mathbb{Z}_q$ for any coprime q', q'' with $q = q'q''$.

We can now finish the proof of Theorem 1 and Corollary 1.

Proof of Theorem 1. If A is a digital set with $\xi_A(2) = m+3 = \xi_A(3) = |A + \{0, d_1, d_2\}|$ as in Theorem 5, we have by Lemma 1 and (15) that

$$|A| \geq z|H| - 6,$$

with $z \in \{2, 3\}$.

Therefore there exists a coset $t + H$ of $H = \langle d_1 \rangle$ such that

$$\frac{|H|}{2} \geq |A \cap (t + H)| \geq |H| - 3.$$

This means that $q/d_1 = |H| \leq 6$, and so $ld_1 \equiv 0 \bmod q$ for some $1 \leq l \leq 6$, and any arithmetic progression of difference d_1 forming A could not have more that 5 elements, implying that $m \leq 15$. □

Proof of Corollary 1. To prove Corollary 1, thanks to Theorem 1 we are left to consider the case of $A = P_1 \cup P_2$ a proper union of two arithmetic progressions of common difference d, and $2A \subseteq \{x, y\} + A$.

Once we establish that such a set cannot be a digital set, we are done since the only possibilities for a single arithmetic progression to be a digital set with minimal number of distinct carries is clearly the one stated in the corollary.

Consider at first the case $(d, q) > 1$. After a dilation, thanks to Lemma 2, we can assume $d|q$. Since A is a digital set, we must have $d = 2$ and hence $2|q$.

Moreover, by 2 we have $|P_1| = |P_2| = m/2$, and $P_i = \alpha_i + 2 \cdot [0, m/2 - 1]$, $i = 1, 2$, where $\alpha_1 \not\equiv \alpha_2 \bmod 2$.

Then

$$2A = (2\alpha_1 + 2 \cdot [0, m-1]) \cup (\alpha_1 + \alpha_2 + 2 \cdot [0, m-1]) \cup (2\alpha_2 + 2 \cdot [0, m-1]).$$

By the parity of α_1 and α_2, we must have

$$|(2\alpha_1 + 2 \cdot [0, m-1]) \cup (2\alpha_2 + 2 \cdot [0, m-1])| \leq m + 1,$$

which implies without loss of generality, since $2m \leq q$, that $2\alpha_1 \in \{2\alpha_2, 2\alpha_2 + 2, 2\alpha_2 + 4\}$.

Once again, since $\alpha_1 \not\equiv \alpha_2 \bmod 2$, and A is not an arithmetic progression, this leaves us with the only choice $\alpha_1 = \alpha_2 + 1 + q/2$, and so, up to translation,

$$A = 2 \cdot \left[0, \frac{m}{2} - 1\right] \cup \left(\frac{q}{2} + 1 + 2 \cdot \left[0, \frac{m}{2} - 1\right]\right),$$

which is a single arithmetic progression of difference $q/2 + 1$.

Assume now $(d, q) = 1$, so that, after a dilation and a translation, we can assume that A is of the form

$$A = [0, a-1] \cup [bm + a, (b+1)m - 1],$$

with $a \geq m-a$, $1 \leq b \leq q/m-2$.

Then $2A = B_1 \cup B_2 \cup B_3$, where

$$B_1 = [0, 2a-2], \quad B_2 = [bm+a, (b+1)m+a-2], \quad B_3 = [2bm+2a, 2(b+1)m-2]$$

are all nonempty sets.

A routine check shows that $B_1 \cap B_2 = \emptyset$, and $|B_1| + |B_2| = 2a+m-2 \leq 2m$ implies $m/2 \leq a \leq (m+2)/2$ and $|B_3 \cap (B_1 \cup B_2)^c| \leq 2$.

For these possible values of a, we must have $B_3 \subseteq B_1$, so that $m(2b+1) \equiv 0 \mod q$, and since all primes dividing m must divide q/m, we have $2 \nmid q$ and so

$$a = \frac{m+1}{2}, bm = \frac{q-m}{2} \text{ implies } A = \left[0, \frac{m-1}{2}\right] \cup \left[\frac{q+1}{2}, \frac{q+m-2}{2}\right].$$

Once again, this is a single arithmetic progression of difference $(q+1)/2$. □

Acknowledgements. We would like to thank the anonymous referee for detecting some inaccuracies and suggesting improvements in many points of the paper.

References

[1] N. Alon, Minimizing the number of carries in addition, *SIAM J. Discrete Math* **27** (2013), no. 1, 562-566.

[2] R. C. Baker, G. Harman, and J. Pintz, The difference between consecutive primes. II, *Proc. Lond. Math. Soc. (3)* **83** (2001), no. 3, 532-562.

[3] Y. F. Bilu, V. F. Lev, and I. Z. Ruzsa, Rectification principles in additive number theory, *Discrete Comput. Geom.* **19** (1998), no. 3, Special Issue, 343-353, Dedicated to the memory of Paul Erdős.

[4] P. Diaconis, X. Shao, and K. Soundararajan, Carries, group theory, and additive combinatorics, *Amer. Math. Monthly* **121** (2014), no. 8, 674-688.

[5] D. J. Grynkiewicz, A step beyond Kemperman's structure theorem, *Mathematika* **55** (2009), no. 1-2, 67-114.

[6] Y. O. Hamidoune, O. Serra, and G. Zémor, On the critical pair theory in abelian groups: beyond Chowla's theorem, *Combinatorica* **28** (2008), no. 4, 441-467.

[7] V. F. Lev, The rectifiability threshold in abelian groups, *Combinatorica* **28** (2008), no. 4, 491-497.

[8] I. Z. Ruzsa, An application of graph theory to additive number theory, *Sci. Ser. A Math. Sci. (N.S.)* **3** (1989), 97-109.

[9] I. Z. Ruzsa, Solving a linear equation in a set of integers. I, *Acta Arith.* **65** (1993), no. 3, 259-282.

[10] O. Serra and G. Zémor, On a generalization of a theorem by Vosper, *Integers* **0** (2000), Article A10.