AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **78(1)** (2020), Pages 118–132

On the number of rainbow solutions of linear equations in $\mathbb{Z}/p\mathbb{Z}$

Mario Huicochea

CONACyT/UAZ
Zacatecas
Mexico
dym@cimat.mx

Abstract

Let $n_1, n_2, n_3, m \in \mathbb{Z}$ and p be a prime, and write $b := m + p\mathbb{Z}$ and $a_i := n_i + p\mathbb{Z}$ for each $i \in \{1, 2, 3\}$. Given a partition of $\mathbb{Z}/p\mathbb{Z}$ into nonempty subsets $\mathbb{Z}/p\mathbb{Z} = A_1 \cup A_2 \cup A_3$, we say that (s_1, s_2, s_3) is a rainbow solution of $a_1x_1 + a_2x_2 + a_3x_3 - b = 0$ if it is a solution of this equation and $A_i \cap \{s_1, s_2, s_3\} \neq \emptyset$ for each $i \in \{1, 2, 3\}$; we denote by R the family of rainbow solutions of $a_1x_1 + a_2x_2 + a_3x_3 - b = 0$. The first result of this paper is that if $a_1a_2a_3 \neq 0+p\mathbb{Z}$ and the coefficients a_1, a_2, a_3 are not equal, then $|R| = \Omega(\min\{|A_1|, |A_2|, |A_3|\})$ where the constants are absolute. The second result of this paper is that if $|A_1|, |A_2|, |A_3|$ are almost equal, $n_1n_2n_3 \neq 0 = m$ and $p \gg 0$, then $|R| = \Omega(\min\{|A_1|, |A_2|, |A_3|\}^2)$ where the constants depend only on n_1, n_2, n_3.

1 Introduction

In this paper $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Z}^+$, $\mathbb{Z}_0^+$ denote the set of real numbers, integers, positive integers and nonnegative integers, respectively. Let X be a set and $n \in \mathbb{Z}^+$. An *n-colouring* of X is a surjective function $\chi : X \to \{1, 2, \ldots, n\}$; thus an n-colouring is identified with the partition into n nonempty subsets $X = \bigcup_{i=1}^{n} \chi^{-1}(i)$. The sets $\chi^{-1}(1), \chi^{-1}(2), \ldots, \chi^{-1}(n)$ are known as *chromatic classes.* A subset Y of X is *rainbow* with respect to χ if it intersects each chromatic class. If it is clear with respect to which colouring we are talking about, then we simply say that Y is rainbow. We say that a subset Y of X is *monochromatic* with respect to χ if Y is contained in a chromatic class.

The study of rainbow objects has had a very long history. However, the study of rainbow solutions of linear equations $\sum_{i=1}^{n} a_ix_i = b$ given an n-colouring of a commutative group $\chi : G \to \{1, 2, \ldots, n\}$ is more recent, see [1–6, 8, 9, 11–13, 15–17]. In this paper, we will work with $\mathbb{Z}/p\mathbb{Z}$ which is the set of congruence classes modulo a prime p with its usual field structure; we write $(\mathbb{Z}/p\mathbb{Z})^* := \mathbb{Z}/p\mathbb{Z} \setminus \{0 + p\mathbb{Z}\}$. For any

ISSN: 2202-3518

$a_1, a_2, a_3 \in (\mathbb{Z}/p\mathbb{Z})^*$ and $b \in \mathbb{Z}/p\mathbb{Z}$, we denote the equation $a_1x_1 + a_2x_2 + a_3x_3 - b = 0$ (where the variables are x_1, x_2, x_3) by $\mathrm{eq}(a_1, a_2, a_3, b)$. For any colouring $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$, we say that a solution (s_1, s_2, s_3) of $\mathrm{eq}(a_1, a_2, a_3, b)$ is rainbow (respectively, monochromatic) with respect to χ, if the set $\{s_1, s_2, s_3\}$ is rainbow (respectively, monochromatic) with respect to χ. The family of rainbow (respectively, monochromatic) solutions (s_1, s_2, s_3) (with respect to χ) of the equation $\mathrm{eq}(a_1, a_2, a_3, b)$ will be denoted by $R(\mathrm{eq}(a_1, a_2, a_3, b), \chi)$ (respectively, $M(\mathrm{eq}(a_1, a_2, a_3, b), \chi)$). The study of which $a_1, a_2, a_3 \in (\mathbb{Z}/p\mathbb{Z})^*$, $b \in \mathbb{Z}/p\mathbb{Z}$ and colourings $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$ satisfy $R(\mathrm{eq}(a_1, a_2, a_3, b), \chi) \neq \emptyset$ can be found in [8], [11], [15]. In particular, it is proven in [8, Thma6] that if a_1, a_2, a_3 are not equal and $\min_{1 \leq i \leq 3} |\chi^{-1}(i)| > 1$, then $R(\mathrm{eq}(a_1, a_2, a_3, b), \chi) \neq \emptyset$. Another step in the study of the set of rainbow solutions of a given linear equation $\mathrm{eq}(a_1, a_2, a_3, b)$ was to bound its size. Nonetheless, there are very few results about $|R(\mathrm{eq}(a_1, a_2, a_3, b), \chi)|$. More specifically, Balandraud in [2, Prop. 1] and Montejano and Serra in [17, Prop. 11] found lower bounds of $|R(\mathrm{eq}(1 + p\mathbb{Z}, 1 + p\mathbb{Z}, -2 + p\mathbb{Z}, 0 + p\mathbb{Z}), \chi)|$ for some colourings χ; also, some relations between $M(\mathrm{eq}(a_1, a_2, a_3, b), \chi)$ and $R(\mathrm{eq}(a_1, a_2, a_3, b), \chi)$ were found by Cameron, Cilleruelo and Serra in [3].

The first result of this paper provides a nontrivial lower bound of $|R(\mathrm{eq}(a_1, a_2, a_3, b), \chi)|$ whenever a_1, a_2, a_3 are not equal.

Theorem 1.1. *Let p be a prime, $c_1 := 31 \cdot 10^{-1550}$, $a_1, a_2, a_3 \in (\mathbb{Z}/p\mathbb{Z})^*$ and $b \in \mathbb{Z}/p\mathbb{Z}$. Assume that a_1, a_2, a_3 are not equal. Then, for any colouring $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$, we have*

$$|R(\mathrm{eq}(a_1, a_2, a_3, b), \chi)| \geq \min\left\{c_1 p - \frac{6}{5}, \frac{1}{13} \cdot \min_{1 \leq i \leq 3} |\chi^{-1}(i)| - 3\right\}.$$

In particular, since $\min_{1 \leq i \leq 3} |\chi^{-1}(i)| \leq \frac{p}{3}$,

$$|R(\mathrm{eq}(a_1, a_2, a_3, b), \chi)| \geq 3c_1 \min_{1 \leq i \leq 3} |\chi^{-1}(i)| - \frac{6}{5}.$$

To explain the exclusion of the case $a_1 = a_2 = a_3$ from Theorem 1.1, we give an example that shows that the conclusion of Theorem 1.1 is not always true in this case. Take a prime $p > \frac{6}{5c_1}$ and set $n := \lfloor \frac{p}{3} \rfloor$ and $m := 2\lfloor \frac{p}{3} \rfloor$. Define the colouring $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$ with

$$\chi(l + p\mathbb{Z}) := \begin{cases} 1 & \text{if } 0 \leq l < n; \\ 2 & \text{if } n \leq l < m; \\ 3 & \text{if } m \leq l < p. \end{cases}$$

Then the equation $x_1 + x_2 + x_3 - b = 0$ has no rainbow solutions so

$$|R(\mathrm{eq}(1 + p\mathbb{Z}, 1 + p\mathbb{Z}, 1 + p\mathbb{Z}, b), \chi)| = 0,$$

while

$$\min_{1 \leq i \leq 3} |\chi^{-1}(i)| = \min\{n, m - n, p - m\} = \left\lfloor \frac{p}{3} \right\rfloor,$$

and then the conclusion of Theorem 1.1 does not hold in this case.

For any $n, m \in \mathbb{Z}$, we write $n \nmid m$ if n does not divide m. Let $n_1, n_2, n_3, m \in \mathbb{Z}$. Theorem 1.1 implies that for all p prime satisfying $p \nmid n_i$ for all $i \in \{1, 2, 3\}$ and for any colouring $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$, we have

$$|R(\mathrm{eq}(n_1 + p\mathbb{Z}, n_2 + p\mathbb{Z}, n_3 + p\mathbb{Z}, m + p\mathbb{Z}), \chi)| \geq 3c_1 \min_{1\leq i\leq 3} |\chi^{-1}(i)| - \frac{6}{5}. \tag{1}$$

Nevertheless, we think that the term $\min_{1\leq i\leq 3} |\chi^{-1}(i)|$ can be improved to $(\min_{1\leq i\leq 3} |\chi^{-1}(i)|)^2$ in (1). First we show that if this can be done, this is the best possible. Let p be a prime, $a_1, a_2, a_3 \in (\mathbb{Z}/p\mathbb{Z})^*, b \in \mathbb{Z}/p\mathbb{Z}$ and $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$ a colouring such that

$$|\chi^{-1}(1)| = |\chi^{-1}(2)| \leq |\chi^{-1}(3)|.$$

For each $i, j \in \{1, 2, 3\}$ with $i \neq j$, the number of rainbow solutions (s_1, s_2, s_3) with $s_i \in \chi^{-1}(1)$ and $s_j \in \chi^{-1}(2)$ is at most $|\chi^{-1}(1)| \cdot |\chi^{-1}(2)|$ (since the term $s_k \in \{s_1, s_2, s_3\} \setminus \{s_i, s_j\}$ is determined by s_i and s_j); hence there are at most $6|\chi^{-1}(1)| \cdot |\chi^{-1}(2)|$ rainbow solutions so

$$|R(\mathrm{eq}(a_1, a_2, a_3, b), \chi)| \leq 6|\chi^{-1}(1)|^2 = 6 \left(\min_{1\leq i\leq 3} |\chi^{-1}(i)| \right)^2.$$

Thus nothing better than $(\min_{1\leq i\leq 3} |\chi^{-1}(i)|)^2$ can be expected in (1) but we conjecture that this is the correct term.

Conjecture 1.2. *Let $n_1, n_2, n_3, m \in \mathbb{Z}$. There exist $c_2 = c_2(n_1, n_2, n_3, m), c_3 = c_3(n_1, n_2, n_3, m)$ with the following property. Take p a prime satisfying $p \nmid n_i$ for all $i \in \{1, 2, 3\}$, and $p \nmid (n_j - n_k)$ for some $j, k \in \{1, 2, 3\}$. For any colouring $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$, we have that*

$$|R(\mathrm{eq}(n_1 + p\mathbb{Z}, n_2 + p\mathbb{Z}, n_3 + p\mathbb{Z}, m + p\mathbb{Z}), \chi)| \geq c_2 \left(\min_{1\leq i\leq 3} |\chi^{-1}(i)| \right)^2 - c_3.$$

For any $n, m \in \mathbb{Z}^+$, the *van der Waerden number* $w(n, m)$ is the smallest positive number w with the property that for any colouring $\chi : \{1, 2, \ldots, w\} \to \{1, 2, \ldots, n\}$, there is a monochromatic arithmetic progressions with length m.

For any prime p and $m \in \mathbb{Z}^+$, we say that a colouring $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$ is *m-almost equinumerous* if

$$3 \left(\sum_{i=1}^{3} |\chi^{-1}(i)|^2 \right) - p^2 \leq \frac{p^2 - p}{6w(3, m)^2}.$$

The second result of this paper gives some evidence that Conjecture 1.2 is true.

Theorem 1.3. *Let $n_1, n_2, n_3 \in \mathbb{Z} \setminus \{0\}$ be such that $n_1 + n_2 + n_3 = 0$. Set $m := 1 + \max_{1\leq i\leq 3} |n_i|$ and $w := w(3, m)$. For any prime $p > w$ and for any m-almost equinumerous colouring $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$, we have that*

$$|R(\mathrm{eq}(n_1 + p\mathbb{Z}, n_2 + p\mathbb{Z}, n_3 + p\mathbb{Z}, 0 + p\mathbb{Z}), \chi)| \geq \frac{p^2 - p}{6w^2}$$

In particular, since $\min_{1\leq i\leq 3}|\chi^{-1}(i)| \leq \frac{p}{3}$ *and* $p \geq 3$*,*

$$|R(\mathrm{eq}(n_1 + p\mathbb{Z}, n_2 + p\mathbb{Z}, n_3 + p\mathbb{Z}, 0 + p\mathbb{Z}), \chi)| \geq \frac{1}{w^2}\left(\min_{1\leq i\leq 3}|\chi^{-1}(i)|\right)^2.$$

We sketch the proofs of the main results of this paper.

- The proof of Theorem 1.1 is divided into two cases: when there are $i, j \in \{1, 2, 3\}$ such that $a_i \notin \{\pm a_j\}$ (see Theorem 3.1), and when $a_i \in \{\pm a_j\}$ for all $i, j \in \{1, 2, 3\}$ (see Theorem 3.2). In the proof of Theorem 3.1, first it is shown that if A_1, A_2, A_3 are the chromatic classes with $|A_1| \leq |A_2| \leq |A_3|$ and $a_i \notin \{\pm a_j\}$, then $|(a_iA_1 + a_jA_2) \cup (a_jA_1 + a_iA_2)| - |A_1| - |A_2|$ is not very small; this is done by contradiction using the structural statements Theorem 2.1 and Theorem 2.3 (which are the main features in the proof and are not used previously in the area for this application). After this is done, it is seen that the number of rainbow solutions of the given equation is at least $|(a_iA_1 + a_jA_2) \cup (a_jA_1 + a_iA_2)| - |A_1| - |A_2|$, and this provides the desired conclusion. The proof of Theorem 3.2 is similar but, instead of using Theorem 2.3, the pairwise disjointedness of the chromatic classes is crucial in the proof of this statement.

- The proof of Theorem 1.3 is done in two stages. First we bound the number of monochromatic solutions of $\mathrm{eq}(n_1 + p\mathbb{Z}, n_2 + p\mathbb{Z}, n_3 + p\mathbb{Z}, 0 + p\mathbb{Z})$; this is done using the fact that if $A \subseteq \mathbb{Z}/p\mathbb{Z}$ is a sufficiently long arithmetic progression, then it has a monochromatic solution of the equation. Each solution cannot be in many arithmetic progressions so there are many monochromatic solutions of the equation; this is Theorem 4.1. The second stage is to use Theorem 2.6 which relates the number of rainbow and monochromatic solutions of 3-variables linear equations.

This paper is organized as follows. In Section 2 we state the auxiliary results that will be needed in the proofs of the main results. The proof of Theorem 1.1 will be a direct consequence of Theorems 3.1 and 3.2; they will be stated and proven in Section 3. The proof of Theorem 1.3 will rely on Theorem 4.1 and the proofs of these statements can be found in Section 4.

2 Preliminaries

In this section we state some auxiliary results needed in the proofs of Theorem 1.1 and Theorem 1.3.

Let p be a prime, A, B nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ and $c \in \mathbb{Z}/p\mathbb{Z}$. We write

$$\begin{aligned} A + B &:= \{a + b : a \in A, b \in B\} \\ -A &:= \{-a : a \in A\} \\ cA &:= \{ca : a \in A\} \\ A + c &:= A + \{c\}. \end{aligned}$$

For any $d \in (\mathbb{Z}/p\mathbb{Z})^*$ and $l \in \mathbb{Z}_0^+$, an *arithmetic progression with difference d and length l* in $\mathbb{Z}/p\mathbb{Z}$ is a subset of the form $\{a+(i+p\mathbb{Z})d \in \mathbb{Z}/p\mathbb{Z} : \ i \in \{0,1,2,\dots,l-1\}\}$ for some $a \in \mathbb{Z}/p\mathbb{Z}$. For any nonempty subset A of $\mathbb{Z}/p\mathbb{Z}$, denote by $\mathcal{A}_d(A)$ the family of arithmetic progressions with difference d which contain A; the length of the smallest element of $\mathcal{A}_d(A)$ (with respect to $\subseteq$) will be denoted by $l_d(A)$. The first result of this section is a weak version of a result of Grynkiewicz.

Theorem 2.1. *Let p be a prime, $r \in \mathbb{Z}_0^+$ and A, B subsets of $\mathbb{Z}/p\mathbb{Z}$. Write $C := \mathbb{Z}/p\mathbb{Z} \setminus -(A+B)$. Assume that*

- $r \le c_1 p - \frac{6}{5}$
- $|A|, |B|, |C| \ge r+3$
- $|A+B| = |A|+|B|+r-1.$

Then there is $d \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $l_d(A) \le |A|+r, l_d(B) \le |B|+r$ and $l_d(C) \le |C|+r$.

Proof. See [7, Thm. 21.8]. □

We will use the following consequence of Theorem 2.1.

Corollary 2.2. *Let p be a prime, $r \in \mathbb{Z}_0^+$ and A, B subsets of $\mathbb{Z}/p\mathbb{Z}$. Assume that*

- $r \le c_1 p - \frac{6}{5}$
- $|A|, |B| \ge r+3$
- $|A+B| \le p-r-3$
- $|A+B| \le |A|+|B|+r-1.$

Then there is $d \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $l_d(A) \le |A|+r$ and $l_d(B) \le |B|+r$.

Proof. Set $r' := |A+B|-|A|-|B|+1$ and $C := \mathbb{Z}/p\mathbb{Z} \setminus -(A+B)$. Then $r' \le r$ and $|C| = |\mathbb{Z}/p\mathbb{Z} \setminus -(A+B)| = p-|A+B|$. Note that the assumption gives

- $r' \le r \le c_1 p - \frac{6}{5}$
- $|A|, |B|, |C| \ge r+3 \ge r'+3$
- $|A+B| = |A|+|B|+r'-1.$

Hence Theorem 2.1 yields the existence of $d \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $l_d(A) \le |A|+r'$ and $l_d(B) \le |B|+r'$. Finally, since $r' \le r$, we get that $l_d(A) \le |A|+r$ and $l_d(B) \le |B|+r$ and we are done. □

We will need also the following statement.

Theorem 2.3. *Let p be a prime, $d_1, d_2 \in (\mathbb{Z}/p\mathbb{Z})^*$, $r \in \mathbb{Z}_0^+$ and A a subset of $\mathbb{Z}/p\mathbb{Z}$. Assume that*

- $l_{d_1}(A) \leq |A| + r$
- $l_{d_2}(A) \leq |A| + r$
- $r + 3 \leq |A| \leq p - 4r - 10$.

Then $d_1 \in \{\pm d_2\}$.

Proof. See [10, Thm. 1.1]. □

We will also need the well-known Cauchy-Davenport Theorem.

Theorem 2.4. *Let p be a prime, and A, B nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof. See [18, Thm. 5.4]. □

In Section 1 we already saw the definition of the van der Waerden numbers; their existence is warranted by van der Waerden's Theorem.

Theorem 2.5. *Let $m, n \in \mathbb{Z}^+$. There exists $w(n, m) \in \mathbb{Z}^+$ with the following property. For all $w \in \mathbb{Z}^+$ with $w \geq w(n, m)$ and for any n-colouring of $\{1, 2, \ldots, w\}$, there exists a monochromatic arithmetic progression of length m.*

Proof. See [14, Thm. 2.1]. □

The last result of this section is a particular case of a more general statement of Cameron, Cilleruelo and Serra.

Theorem 2.6. *Let p be a prime, $a_1, a_2, a_3 \in (\mathbb{Z}/p\mathbb{Z})^*$, $b \in \mathbb{Z}/p\mathbb{Z}$ and $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$ a colouring. Write $R := R(\mathrm{eq}(a_1, a_2, a_3, b), \chi)$ and $M := M(\mathrm{eq}(a_1, a_2, a_3, b), \chi)$. Then*

$$2|M| - |R| = 3\left(\sum_{i=1}^{3} |\chi^{-1}(i)|^2\right) - p^2.$$

Proof. See [3, Thm. 4.2]. □

3 Proof of Theorem 1.1

In this section we prove Theorem 1.1. This will be an immediate consequence of Theorems 3.1 and 3.2. The main ideas in both proofs are similar but there are some technical differences; therefore, for the sake of comprehension, we decided to split Theorem 1.1 into these statements.

Theorem 3.1. *Let p be a prime, $a_1, a_2, a_3 \in (\mathbb{Z}/p\mathbb{Z})^*$ and $b \in \mathbb{Z}/p\mathbb{Z}$. Assume that there are $i, j \in \{1, 2, 3\}$ such that $a_i \notin \{\pm a_j\}$. Then, for any colouring $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$, we have that*

$$|R(\mathrm{eq}(a_1, a_2, a_3, b), \chi)| \geq \min\left\{c_1 p - \frac{6}{5}, \frac{1}{13} \cdot \min_{1\leq i\leq 3} |\chi^{-1}(i)| - 3\right\}.$$

Proof. For each $i \in \{1, 2, 3\}$, set $A_i := \chi^{-1}(i)$, and assume without loss of generality that $|A_1| \leq |A_2| \leq |A_3|$. Also we assume without loss of generality that $a_1 \notin \{\pm a_2\}$. Write

$$\begin{aligned} r &:= \min\left\{c_1 p - \frac{6}{5}, \frac{1}{13} \cdot |A_1| - 3\right\} \\ B_1 &:= a_1 A_1 + a_2 A_2 \\ B_2 &:= a_2 A_1 + a_1 A_2. \end{aligned}$$

The first step in the proof is to show that

$$|B_1 \cup B_2| \geq |A_1| + |A_2| + r, \tag{2}$$

and this will be done by contradiction. If (2) is false, then

$$\max\{|B_1|, |B_2|\} \leq |A_1| + |A_2| + r - 1. \tag{3}$$

In so far as

$$\begin{aligned} r &\leq c_1 p - \frac{6}{5} \\ r + 3 &\leq \frac{|A_1|}{13} \leq |A_1| \leq |A_2| \\ r + 3 &\leq |A_1| - 12r \leq |A_3| - 12r \leq p - |A_1| - |A_2| - r + 1 \leq p - \max\{|B_1|, |B_2|\}, \end{aligned}$$

we have by (3) that we can apply Corollary 2.2 to the pairs (a_1A_1, a_2A_2) and (a_2A_1, a_1A_2), and therefore there exist $d_1, d_2 \in (\mathbb{Z}/p\mathbb{Z})^*$ such that

$$l_{d_1}(a_1A_1) \leq |A_1| + r, \qquad l_{d_1}(a_2A_2) \leq |A_2| + r \tag{4}$$

and

$$l_{d_2}(a_2A_1) \leq |A_1| + r, \qquad l_{d_2}(a_1A_2) \leq |A_2| + r. \tag{5}$$

Multiplying a_1A_1 by $a_2a_1^{-1}$, we get from (4) that

$$l_{a_2a_1^{-1}d_1}(a_2A_1) \leq |A_1| + r. \tag{6}$$

Insomuch as

$$r+3 \leq \frac{|A_1|}{13} \leq |A_1|$$
$$|A_1| = p - |A_2| - |A_3| \leq p - 2|A_1| \leq p - 4r - 10,$$

we can apply Theorem 2.3 to a_2A_1 by (5) and (6). Thus $a_2a_1^{-1}d_1 \in \{\pm d_2\}$, and we assume without loss of generality that

$$a_2a_1^{-1}d_1 = d_2. \tag{7}$$

On the one hand, since we are assuming that (2) is false,

$$|B_1 \cup B_2| \leq |A_1| + |A_2| + r - 1.$$

On the other hand,

$$|B_1 \cup B_2| + |B_1 \cap B_2| = |B_1| + |B_2|.$$

We have

$$|B_1 \cap B_2| = |B_1| + |B_2| - |B_1 \cup B_2| \geq |B_1| + |B_2| - |A_1| - |A_2| - r + 1. \tag{8}$$

From Theorem 2.4, we have that for $i \in \{1, 2\}$,

$$|B_i| \geq |A_1| + |A_2| - 1. \tag{9}$$

Then (8) and (9) lead to

$$|B_1 \cap B_2| \geq |A_1| + |A_2| - r - 1. \tag{10}$$

From (4), there are arithmetic progressions C_1, C_2 of difference d_1 such that $a_1A_1 \subseteq C_1, a_2A_2 \subseteq C_2, |C_1| \leq |A_1|+r$ and $|C_2| \leq |A_2|+r$. Note that C_1+C_2 is an arithmetic progression of difference d_1 such that

$$|C_1 + C_2| = |C_1| + |C_2| - 1 \leq |A_1| + |A_2| + 2r - 1. \tag{11}$$

Notice that $B_1 \cap B_2 \subseteq B_1 \subseteq C_1 + C_2$. Hence (10) and (11) yield that

$$l_{d_1}(B_1 \cap B_2) \leq |B_1 \cap B_2| + 3r. \tag{12}$$

Likewise,

$$l_{d_2}(B_1 \cap B_2) \leq |B_1 \cap B_2| + 3r. \tag{13}$$

Since

$$3r + 3 \leq 2|A_1| - r - 1 \leq |A_1| + |A_2| - r - 1 \leq |B_1 \cap B_2|$$
$$|B_1 \cap B_2| \leq |B_1| \leq |A_1| + |A_2| + r - 1 = p - |A_3| + r - 1 \leq p - 12r - 10,$$

we can apply Theorem 2.3 to $B_1 \cap B_2$ by (12) and (13). Hence we get from Theorem 2.3 that $d_1 \in \{\pm d_2\}$. However, this inclusion and (7) imply that $a_1 \in \{\pm a_2\}$ which contradicts the assumption, and therefore (2) is true.

Insomuch as

$$|(B_1 \cup B_2) \cup (-a_3A_3 + b)| \leq |\mathbb{Z}/p\mathbb{Z}| = p = |A_1| + |A_2| + |A_3|,$$

we get from (2) that

$$\begin{aligned} |(B_1 \cup B_2) \cap (-a_3A_3 + b)| &\geq |B_1 \cup B_2| + |a_3A_3 + b| - p \\ &\geq |A_1| + |A_2| + r + |a_3A_3 + b| - p \\ &= |A_1| + |A_2| + |A_3| - p + r \\ &= r. \end{aligned} \tag{14}$$

Finally, for any $s_3 \in A_3$ such that $-a_3s_3+b \in B_1 \cup B_2 = (a_1A_1+a_2A_2) \cup (a_2A_1+a_1A_2)$, we have that there are s_1, s_2 such that $(s_1, s_2, s_3) \in R(\text{eq}(a_1, a_2, a_3, b), \chi)$. Then, by (14), there are at least r of these elements and the proof is completed. ☐

Theorem 3.2. *Let p be a prime, $a_1, a_2, a_3 \in (\mathbb{Z}/p\mathbb{Z})^*$ and $b \in \mathbb{Z}/p\mathbb{Z}$. Assume that a_1, a_2, a_3 are not equal but $a_i \in \{\pm a_j\}$ for all $i, j \in \{1, 2, 3\}$. Then, for any colouring $\chi : \mathbb{Z}/p\mathbb{Z} \to \{1, 2, 3\}$, we have that*

$$|R(\text{eq}(a_1, a_2, a_3, b), \chi)| \geq \min\left\{c_1p - \frac{6}{5}, \frac{1}{5} \cdot \min_{1\leq i\leq 3} |\chi^{-1}(i)| - 3\right\}.$$

Proof. Applying a dilation if necessary, we may assume that $a_1 = a_3 = -a_2 = 1+p\mathbb{Z}$. For each $i \in \{1, 2, 3\}$, set $A_i := \chi^{-1}(i)$, and assume without loss of generality that $|A_1| \leq |A_2| \leq |A_3|$. Write

$$\begin{aligned} r &:= \min\left\{c_1p - \frac{6}{5}, \frac{1}{5} \cdot |A_1| - 3\right\} \\ B_2 &:= A_1 - A_2 \\ B_3 &:= A_1 - A_3. \end{aligned}$$

We will show that

$$|B_2 \cup (-B_2)| \geq |A_1| + |A_2| + r \tag{15}$$

or

$$|B_3 \cup (-B_3)| \geq |A_1| + |A_3| + r, \tag{16}$$

and this shall be done by contradiction. Thus we assume that (15) and (16) are false so

$$|B_2| \leq |B_2 \cup (-B_2)| \leq |A_1| + |A_2| + r - 1 \tag{17}$$

and

$$|B_3| \leq |B_3 \cup (-B_3)| \leq |A_1| + |A_3| + r - 1. \tag{18}$$

In so far as

$$\begin{aligned} &r \leq c_1p - \frac{6}{5} \\ &r + 3 \leq \frac{|A_1|}{5} \leq |A_1| \leq |A_2| \leq |A_3| \\ &r + 3 \leq |A_2| - r + 1 = p - |A_1| - |A_3| - r + 1 \leq p - \max\{|B_2|, |B_3|\}, \end{aligned}$$

we have by (17) and (18) that we can apply Corollary 2.2 to the pairs $(A_1, -A_2)$ and $(A_1, -A_3)$, respectively. Hence there are $d_2, d_3 \in (\mathbb{Z}/p\mathbb{Z})^*$ such that for $i \in \{2, 3\}$,

$$l_{d_i}(A_1) \leq |A_1| + r, \qquad l_{d_i}(A_i) = l_{d_i}(-A_i) \leq |A_i| + r. \tag{19}$$

Insomuch as

$$\begin{aligned} r + 3 &\leq \frac{|A_1|}{5} \leq |A_1| \\ |A_1| &= p - |A_2| - |A_3| \leq p - 2|A_1| \leq p - 4r - 10, \end{aligned}$$

we can apply Theorem 2.3 to A_1 by (19). Then $d_2 \in \{\pm d_3\}$, and we assume without loss of generality that $d_2 = d_3$. Applying a dilation if necessary, we assume that

$$d_2 = d_3 = 1 + p\mathbb{Z}. \tag{20}$$

We need some notation. For any $c, d \in \mathbb{Z}/p\mathbb{Z}$, let $n \in \{0, 1, \ldots, p-1\}$ be the element satisfying that $d - c = n + p\mathbb{Z}$; then we write

$$[c, d] := \{c + (i + p\mathbb{Z}) : \ i \in \{0, 1, \ldots, n\}\}.$$

From (19) and (20), there are $b_1, b_2, b_3, c_1, c_2, c_3 \in \mathbb{Z}/p\mathbb{Z}$ such that $A_i \subseteq [b_i, c_i]$ and $|[b_i, c_i] \setminus A_i| \leq r$ for each $i \in \{1, 2, 3\}$. Call $C_i := [b_i, c_i] \setminus A_i$ for each $i \in \{1, 2, 3\}$. Then, for any $i, j \in \{1, 2, 3\}$ with $i \neq j$,

$$\begin{aligned} |[b_i, c_i] \cap [b_j, c_j]| &= |(A_i \cup C_i) \cap (A_j \cup C_j)| \\ &\leq |A_i \cap (A_j \cup C_j)| + |C_i \cap (A_j \cup C_j)| \\ &= |A_i \cap C_j| + |C_i \cap (A_j \cup C_j)| && \Big(\text{since } A_i \cap A_j = \emptyset\Big) \\ &\leq |C_j| + |C_i| \\ &\leq 2r. \end{aligned} \tag{21}$$

Thus, by (21), the intervals $[b_1, c_1], [b_2, c_2]$ and $[b_3, c_3]$ can overlap but in very small segments. Assume that $c_1 = b_2 + (n_1 + p\mathbb{Z}), c_2 = b_3 + (n_2 + p\mathbb{Z})$ and $c_3 = b_1 + (n_3 + p\mathbb{Z})$ with $n_1, n_2, n_3 \in \{0, 1, \ldots, 2r - 1\}$ (the other cases are done in the same way). For each $i \in \{1, 2, 3\}$ (considering $i \mod 3$), we have that $A_i \subseteq [b_i, c_i] = [b_i, b_{i+1} + (n_i + p\mathbb{Z})]$ so

$$\begin{aligned} &[b_{i+2} + (n_{i+1} + 1 + p\mathbb{Z}), b_i - (1 + p\mathbb{Z})] \\ =&\mathbb{Z}/p\mathbb{Z} \setminus [b_i, b_{i+2} + (n_{i+1} + p\mathbb{Z})] \\ =&\mathbb{Z}/p\mathbb{Z} \setminus ([b_i, b_{i+1} + (n_i + p\mathbb{Z})] \cup [b_{i+1}, b_{i+2} + (n_{i+1} + p\mathbb{Z})]) \\ \subseteq&\mathbb{Z}/p\mathbb{Z} \setminus (A_i \cup A_{i+1}) \\ =&A_{i+2}; \end{aligned} \tag{22}$$

furthermore, note that

$$\begin{aligned} |[b_{i+2} + (n_{i+1} + 1 + p\mathbb{Z}), b_i - (1 + p\mathbb{Z})]| &\geq |[b_{i+2}, b_i + (n_{i+2} + p\mathbb{Z})]| - n_{i+1} - 2 \\ &= |[b_{i+2}, c_{i+2}]| - n_{i+1} - 2 \\ &\geq |[b_{i+2}, c_{i+2}]| - 2r - 1 \\ &\geq |A_{i+2}| - 2r - 1. \end{aligned} \tag{23}$$

Write

$$D := [(b_1 - b_3) + (n_3 + 2 + p\mathbb{Z}), -n_1 - 2 + p\mathbb{Z}]$$

From (22), we conclude that

$$\begin{aligned} B_2 &= A_1 - A_2 \\ &\supseteq [b_1 + (n_3 + 1 + p\mathbb{Z}), b_2 - (1 + p\mathbb{Z})] - [b_2 + (n_1 + 1 + p\mathbb{Z}), b_3 - (1 + p\mathbb{Z})] \\ &= D, \end{aligned} \tag{24}$$

and likewise

$$-B_2 \supseteq -D. \tag{25}$$

We find a contradiction depending on whether or not D and $-D$ are disjoint.

- Assume that $D \cap (-D) \neq \emptyset$. Then $D \cup (-D) = [n_1 + 2 + p\mathbb{Z}, -n_1 - 2 + p\mathbb{Z}]$ or $D \cup (-D) = [(b_1 - b_3) + (n_3 + 2 + p\mathbb{Z}), (b_3 - b_1) - (n_3 + 2 + p\mathbb{Z})]$. If $D \cup (-D) = [(b_1 - b_3) + (n_3 + 2 + p\mathbb{Z}), (b_3 - b_1) - (n_3 + 2 + p\mathbb{Z})]$, then $D \cap (-D) = [n_1 + 2 + p\mathbb{Z}, -n_1 - 2 + p]$. Thus, in any case,

  $$D \cup (-D) \supseteq [n_1 + 2 + p\mathbb{Z}, -n_1 - 2 + p\mathbb{Z}].$$

  Hence, since $n_1 \leq 2r - 1$,

  $$|D \cup (-D)| \geq |[n_1 + 2 + p\mathbb{Z}, -n_1 - 2 + p\mathbb{Z}]| = p - 2(n_1 + 2) + 1 \geq p - 4r - 1. \tag{26}$$

  Thus

  $$\begin{aligned} |A_1| + |A_2| + r &\geq |B_2 \cup (-B_2)| && \text{by (17)} \\ &\geq |D \cup (-D)| && \text{by (24), (25)} \\ &\geq p - 4r - 1 && \text{by (26)} \\ &= |A_1| + |A_2| + |A_3| - 4r - 1 \\ &= (|A_1| + |A_2| + r) + (|A_3| - 5r - 1), \end{aligned}$$

  which is impossible since $|A_3| \geq |A_1| > 5r + 1$.

- Assume that $D \cap (-D) = \emptyset$. Then

  $$|D \cup (-D)| = |D| + |-D| = 2|D|. \tag{27}$$

  Also

  $$\begin{aligned} |D| =& |[(b_1 - b_3) + (n_3 + 1 + p\mathbb{Z}), -(n_1 + 2) + p\mathbb{Z}]| \\ =& |[b_1 + (n_3 + 1 + p\mathbb{Z}), b_2 - (1 + p\mathbb{Z})] \\ &- [b_2 + (n_1 + 1 + p\mathbb{Z}), b_3 - (1 + p\mathbb{Z})]| \\ =& |[b_1 + (n_3 + 1 + p\mathbb{Z}), b_2 - (1 + p\mathbb{Z})]| \\ &+ |[b_2 + (n_1 + 1 + p\mathbb{Z}), b_3 - (1 + p\mathbb{Z})]| - 1 \\ \geq& |A_1| + |A_2| - 4r - 3 && \text{by (23)} \end{aligned} \tag{28}$$

Hence

$$\begin{aligned}
|A_1|+|A_2|+r &\geq |B_2\cup(-B_2)| && \text{by (17)}\\
&\geq |D\cup(-D)| && \text{by (24), (25)}\\
&= 2|D| && \text{by (27)}\\
&\geq (|A_1|+|A_2|+r)+(|A_1|+|A_2|-9r-6); && \text{by (28)}
\end{aligned}$$

however, this is impossible since $|A_2|\geq|A_1|>5r+3$.

In any case, we have found a contradiction and hence (15) or (16) holds. Assume without loss of generality that (15) is true. In so far as

$$|(B_2\cup(-B_2))\cup(-A_3+b)|\leq|\mathbb{Z}/p\mathbb{Z}|=p=|A_1|+|A_2|+|A_3|,$$

we get from (15) that

$$\begin{aligned}
|(B_2\cup(-B_2))\cap(-A_3+b)| &\geq |B_2\cup(-B_2)|+|A_3+b|-p\\
&\geq |A_1|+|A_2|+r+|-A_3+b|-p\\
&= |A_1|+|A_2|+|A_3|-p+r\\
&= r. \qquad (29)
\end{aligned}$$

For any $s_3\in A_3$ such that $-s_3+b\in(A_1-A_2)\cup(A_2-A_1)$, we have that there s_1,s_2 such that (s_1,s_2,s_3) is a rainbow solution of $x_1-x_2+x_3-b=0$. Thus, from (29), we conclude that there are at least r of these rainbow solutions and we are done. □

In Theorems 3.1 and 3.2, when the two smallest chromatic classes have almost the same size, the constant c_1 can be substituted by a much bigger constant c_1' using the structural results of [7, Ch. 19] instead of Theorem 2.1.

4 Proof of Theorem 1.3

In this section we show Theorem 1.3. It will be a consequence of Theorems 2.6 and 4.1.

Theorem 4.1. *Let $n_1,n_2,n_3\in\mathbb{Z}\setminus\{0\}$ be such that $n_1+n_2+n_3=0$. Set $m:=1+\max_{1\leq i\leq 3}|n_i|$ and $w:=w(3,m)$. For any prime $p>w$ and for any colouring $\chi:\mathbb{Z}/p\mathbb{Z}\to\{1,2,3\}$, we have that*

$$|M(\mathrm{eq}(n_1+p\mathbb{Z},n_2+p\mathbb{Z},n_3+p\mathbb{Z},0+p\mathbb{Z}),\chi)|\geq\frac{p^2-p}{6w^2}.$$

Proof. Set $M:=M(\mathrm{eq}(n_1+p\mathbb{Z},n_2+p\mathbb{Z},n_3+p\mathbb{Z},0+p\mathbb{Z}),\chi)$. In so far as $n_1+n_2+n_3=0$, we assume without loss of generality that $n_3<0<n_1\leq n_2$ so $m=1-n_3$ and $n_2<n_1+n_2=-n_3$. For each $a\in\mathbb{Z}/p\mathbb{Z}$ and $d\in(\mathbb{Z}/p\mathbb{Z})^*$, write

$$A_{a,d}:=\{a+(i+p\mathbb{Z})d\in\mathbb{Z}/p\mathbb{Z}:\ i\in\{0,1,\ldots,w-1\}\}.$$

We claim that for each $a \in \mathbb{Z}/p\mathbb{Z}$ and $d \in (\mathbb{Z}/p\mathbb{Z})^*$, there is a monochromatic solution (with respect to χ) $(s_1, s_2, s_3) \in M$ such that $\{s_1, s_2, s_3\} \subseteq A_{a,d}$ and s_1, s_2, s_3 are pairwise distinct. Take the colouring

$$\chi_{a,d} : \{1, 2, \dots, w\} \longrightarrow \{1, 2, 3\}, \qquad \chi_{a,d}(i) = \chi(a + (i - 1 + p\mathbb{Z})d).$$

Theorem 2.5 yields that there exist $k \in \{1, 2, 3\}$ and $q, r \in \mathbb{Z}^+$ such that

$$\{q + jr : \ j \in \{0, 1, \dots, m - 1\}\} \subseteq \chi_{a,d}^{-1}(k).$$

Note that $\{a+(q-1+p\mathbb{Z})d, a+(q-n_3r-1+p\mathbb{Z})d, a+(q+n_2r-1+p\mathbb{Z})d\} \subseteq A_{a,d}$. Since $\{q, q - n_3r, q + n_2r\}$ is monochromatic with respect to $\chi_{a,d}$, the definition of $\chi_{a,d}$ implies that $\{a+(q-1+p\mathbb{Z})d, a+(q-n_3r-1+p\mathbb{Z})d, a+(q+n_2r-1+p\mathbb{Z})d\}$ is monochromatic with respect to χ. Also notice that

$$\begin{aligned}(n_1 + p\mathbb{Z})(a + (q - 1 + p\mathbb{Z})d) + (n_2 + p\mathbb{Z})(a + (q - n_3r - 1 + p\mathbb{Z})d)\\ +(n_3 + p\mathbb{Z})(a + (q + n_2r - 1 + p\mathbb{Z})d) = 0 + p\mathbb{Z}\end{aligned}$$

so $(a + (q - 1 + p\mathbb{Z})d, a + (q - n_3r - 1 + p\mathbb{Z})d, a + (q + n_2r - 1 + p\mathbb{Z})d)$ is a solution and therefore

$$(a + (q - 1 + p\mathbb{Z})d, a + (q - n_3r - 1 + p\mathbb{Z})d, a + (q + n_2r - 1 + p\mathbb{Z})d) \in M$$

Furthermore, since $0 < n_2r < -n_3r \le w < p$, the elements $a + (q - 1 + p\mathbb{Z})d, a + (q - n_3r - 1 + p\mathbb{Z})d$ and $a + (q + n_2r - 1 + p\mathbb{Z})d$ are pairwise distinct and the claim is proven.

Note that for each $(s_1, s_2, s_3) \in M$ with the elements pairwise distinct, $\{s_1, s_2, s_3\}$ can be contained in at most $6w^2$ arithmetic progressions $A_{a,d}$. Indeed, assume that $\{s_1, s_2, s_3\}$ is in at least $6w^2 + 1$ arithmetic progressions $A_{a,d}$. i Then, since there are six ordered pairs in $\{1, 2, 3\}$ and the length of the arithmetic progressions $A_{a,d}$ is w, the Pigeonhole Principle yields a pair $i, j \in \{1, 2, 3\}$ with $i \neq j$, arithmetic progressions A_{a_1,d_1}, A_{a_2,d_2} with $(a_1, d_1) \neq (a_2, d_2)$, and $k_i, k_j \in \{0, 1, \dots, w - 1\}$ with $k_i \neq k_j$ such that

$$\begin{aligned}s_i &= a_1 + k_id_1 = a_2 + k_id_2\\ s_j &= a_1 + k_jd_1 = a_2 + k_jd_2;\end{aligned}$$

however, the previous equalities imply that $(a_1, d_1) = (a_2, d_2)$, and this contradiction proves our claim. Hence, insomuch as $a \in \mathbb{Z}/p\mathbb{Z}$, $d \in (\mathbb{Z}/p\mathbb{Z})^*$ are arbitrary, we obtain that M has at least $\frac{|\mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^*|}{6w^2} = \frac{p^2-p}{6w^2}$ elements. ☐

We conclude the proof of Theorem 1.3.

Proof. (Theorem 1.3) Set $R := R(\mathrm{eq}(n_1 + p\mathbb{Z}, n_2 + p\mathbb{Z}, n_3 + p\mathbb{Z}, 0 + p\mathbb{Z}), \chi)$ and $M := M(\mathrm{eq}(n_1 + p\mathbb{Z}, n_2 + p\mathbb{Z}, n_3 + p\mathbb{Z}, 0 + p\mathbb{Z}), \chi)$. Theorem 2.6 gives us

$$|R| = 2|M| - 3\left(\sum_{i=1}^{3} |\chi^{-1}(i)|^2\right) + p^2. \tag{30}$$

Applying Theorem 4.1,

$$2|M| \geq \frac{p^2 - p}{3w^2}. \tag{31}$$

Also, insomuch as χ is m-almost equinumerous,

$$3\left(\sum_{i=1}^{3} |\chi^{-1}(i)|^2\right) - p^2 \leq \frac{p^2 - p}{6w^2}. \tag{32}$$

Finally (30), (31) and (32) let us conclude that

$$|R| \geq \frac{p^2 - p}{6w^2}.$$

$\square$

Acknowledgements

We would like to thank the referees for their positive and insightful comments and advice to improve this paper.

References

[1] M. Axenovich and D. Fon Der Flaass, On rainbow arithmetic progressions, *Electron. J. Combin.* 11 (2004), R1.

[2] E. Balandraud, Coloured solutions of equations in finite groups, *J. Combin. Theory Ser. A* 114 (5) (2007), 854–866.

[3] P. J. Cameron, J. Cilleruelo and O. Serra, On monochromatic solutions of equations in groups, *Rev. Mat. Iberoam.* 23 (1) (2007), 385–395.

[4] D. Conlon, Rainbow solutions of linear equations over $\mathbb{Z}_p$, *Discrete Math.* 306 (2006), 2056–2063.

[5] D. Conlon, V. Jungić and R. Radoičić, On the existence of rainbow 4-term arithmetic progressions, *Graphs Combin.* 23 (2007), 249–254.

[6] J. Fox, M. Mahdian and R. Radoičić, Rainbow Solutions to the Sidon Equation, *Discrete Math.* 308 (2008), 4773–4778.

[7] D. J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics 30 Springer (2013).

[8] M. Huicochea and A. Montejano, The structure of rainbow-free colorings for linear equations on three variables in $\mathbb{Z}_p$, *Integers* 15A (2015), A8.

[9] M. Huicochea, An inverse theorem in $\mathbb{F}_p$ and rainbow-free colorings, *Mosc. J. Comb. Number Theory* 7 (2) (2017), 22–58.

[10] M. Huicochea, Almost arithmetic progressions in $\mathbb{F}_p$, *Notes Number Theory Discrete Math.* 24 (1) (2018) 61–75.

[11] V. Jungić, J. Licht, M. Mahdian, J. Nešetřil and R. Radoičić, Rainbow Ramsey Theory and Anti-Ramsey results, *Combin. Probab. Comput.* 12 (2005), 599–620.

[12] V. Jungić, J. Nešetřil and R. Radoičić, Rainbow Ramsey Theory, *Integers* 5 (2) (2005), A9.

[13] V. Jungić and R. Radoičić, Rainbow 3-term Arithmetic Progressions, *Integers* 3 (2003), A18.

[14] B. Landman and A. Robertson, *Ramsey Theory on the Integers*, Student Mathematical Library Vol. 73 AMS (2015).

[15] B. Llano and A. Montejano, Rainbow-free colorings for $x+y=cz$ in Z_p, *Discrete Math.* 312 (2012), 2566–2573.

[16] A. Montejano and O. Serra, Rainbow-free three colorings in abelian groups, *Electron. J. Combin.* 19 (2012), P45.

[17] A. Montejano and O. Serra, Counting patterns in colored orthogonal arrays, *Discrete Math.* 317 (2014), 44–52.

[18] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics 105 Cambridge University Press (2006).

(Received 27 Oct 2019; revised 26 May 2020)