Rainbow Solutions of Linear Equations over $\mathbb{Z}_p$

David Conlon[*]

Abstract

We prove that if the group $\mathbb{Z}_p$, with p a prime, is coloured with $k \geq 4$ different colours such that each colour appears at least k times, then for any $a_1, \cdots, a_k, b$ in $\mathbb{Z}_p$ with not all the a_i being equal, we may solve the equation $a_1x_1 + \cdots + a_kx_k = b$ so that each of the variables is chosen in a different colour class. This generalises a similar result concerning three colour classes due to Jungić, Licht, Mahdian, Nešetřil and Radoičić.

In the course of our proof we classify, with some size caveats, the sets in $\mathbb{Z}_p$ which satisfy the inequality $|A_1 + \cdots + A_n| \leq |A_1| + \cdots + |A_n|$. This is a generalisation of an inverse theorem due to Hamidoune and Rødseth concerning the case $n = 2$.

1 Introduction

Throughout this paper it is assumed that p is a prime number and that $\mathbb{Z}_p$ is the corresponding cyclic group.

Definition: Let A be a subset of a group G, and let $A = C_1 \cup C_2 \cup \cdots \cup C_k$ be a partition (colouring) of A. The equation $a_1x_1 + \cdots + a_kx_k = b$ with $a_1, \cdots, a_k \in \mathbb{Z}$ and $b \in G$ is said to have a rainbow solution with respect to this colouring if the equation can be solved in such a way that each of the variables is chosen within a different colour class.

When $A = G = \mathbb{Z}_p$ it is possible to say quite a bit about when linear equations have rainbow solutions, as is evidenced by the following result, due to Jungić, Licht, Mahdian, Nešetřil and Radoičić [3]:

Theorem 1 *(Jungić, Licht, Mahdian, Nešetřil, Radoičić [3]) Let $a_1, a_2, a_3, b \in \mathbb{Z}_p$ be such that $a_1a_2a_3 \neq 0$ and, for some i and j, $a_i \neq a_j$. Then every colouring of $\mathbb{Z}_p = C_1 \cup C_2 \cup C_3$ with $|C_1|, |C_2|, |C_3| \geq 4$ contains a rainbow solution of $a_1x_1 + a_2x_2 + a_3x_3 = b$.*

The main result of this paper will be a generalisation of this result to more than three variables. Qualitatively, the result says that given a natural number $k \geq 4$, if we divide $\mathbb{Z}_p$, for p a prime, into k large colour classes then for nearly all linear equations in k variables we are guaranteed a rainbow solution. More precisely our result states:

[*] The author is kindly supported by a grant from St John's College, Cambridge.

Theorem 2 *Fix k as a natural number with $k \geq 4$. Let $a_1, \cdots, a_k, b \in \mathbb{Z}_p$ be such that $a_1 \cdots a_k \neq 0$ and, for some i and j, $a_i \neq a_j$. Then every colouring of $\mathbb{Z}_p = C_1 \cup \cdots \cup C_k$ with $|C_1|, |C_2|, \cdots, |C_k| \geq k$ contains a rainbow solution of $a_1 x_1 + \cdots + a_k x_k = b$.*

The restriction that not all the a_i be equal is necessary as well as sufficient, for it is easy to construct counterexamples in this case, as we shall see in Section 4.

Jungić et al proved their result by applying the following inverse theorem of Hamidoune and Rødseth [2]:

Theorem 3 *(Hamidoune-Rødseth [2]) Let S and T be subsets of $\mathbb{Z}_p$ such that $|S| \geq 3, |T| \geq 3$ and $7 \leq |S+T| \leq p-4$. Then either $|S+T| \geq |S|+|T|+1$ or S and T are subsets of arithmetic progressions with the same common difference and with lengths at most $|S|+1$ and $|T|+1$ respectively.*

Our approach will be along similar lines to that used in [3]. We begin (Lemma 1) by proving some quantitative bounds on when a set A cannot be a large subset of two arithmetic progressions, both of length at most $|A|+r$, but with different common differences. We will then use this result to prove the following generalisation of the Hamidoune-Rødseth Theorem to more than two summands, which in turn will be used to prove our result about rainbow solutions to linear equations.

Theorem 4 *Let l be a fixed natural number with $l \geq 3$. Let $A_1, A_2, \cdots, A_l$ be subsets of $\mathbb{Z}_p$ satisfying $|A_i| \geq l+1$ for all $1 \leq i \leq l$ and $|A_1 + A_2 + \cdots + A_l| \leq p-2$. Then either $|A_1 + A_2 + \cdots + A_l| \geq |A_1| + |A_2| + \cdots + |A_l| + 1$ or all of the A_i are contained in arithmetic progressions with the same common difference and lengths at most $|A_i| + (l-1)$.*

With this theorem in place the proof of Theorem 2 becomes relatively straightforward. The main trick of the argument is to use Theorem 4 to show that for any colour class C and any coefficient a involved in the specific equation that we are considering we must have that aC, by which we mean the set $\{ac : c \in C\}$, is a large subset of an arithmetic progression. With the size caveats that we have given this is then seen, by Lemma 1, to be an impossibility provided our equation has two coefficients a_i and a_j such that $a_i \neq \pm a_j$. The case that remains, where $a_i = \pm a_j$ for all coefficients a_i and a_j, but where they are not all equal, may then be ruled out by a further argument.

We conclude by making some suggestions for future research regarding rainbow solutions to sets of equations.

2 A Preliminary Lemma

To begin we have the following lemma (which extends Lemma 4.3 in [3]), which we shall need in the proofs of both Theorem 2 and Theorem 4:

Lemma 1 *Let $r \in \mathbb{N}_0$ and let $A \subset \mathbb{Z}_p$ with $r+2 \leq |A| \leq p-(r^2+3r+2)$, be contained in an arithmetic progression of length $|A|+r$ with common difference d. Then, except for the examples where $r=2$, $p=17$ and $A = \{a, a+d, a+4d, a+5d\}$, every arithmetic progression of length $|A|+r$ containing A has common difference equal to either d or $p-d$.*

Proof: Suppose otherwise. Then A is contained within two arithmetic progressions of length $|A|+r$, say S and S', which have genuinely different common differences. Without loss of generality it may be assumed that $S=\{i\}_{i=0}^{|A|+r-1}$, and that S' has common difference d with $\frac{p}{2} \geq d > 1$. We split our considerations into three cases:

Case 1: $d > |S|$.
Consider the set $U=\{d+i\}_{i=0}^{2r+1}$. Then no element of U is in S, since $d>|S|$ and $d+2r+1 \leq \frac{p}{2}+(2r+1) < p$ (as $p > 4r+2$). On the other hand, every element of $U-d$ is in S, since $2r+1 \leq |A|+r-1$. But now this implies that there are at least $r+2$ elements a of A such that a is in A, but $a+d$ is not. But it is easily seen that, by assumption, since A is contained in an arithmetic progression of length $|A|+r$ and common difference d, that there can be at most $r+1$ such points, and therefore we have a contradiction.

Case 2: $2r+2 \leq d \leq |S|$.
Consider the set $V=\{|A|+r+i\}_{i=0}^{2r+1}$. Then, once again, no element of V is in S, since $|A|+r+2r+1<p$. But, again, every element of $V-d$ is in S, since $|A|+r-d \geq 0$ and $|A|+3r+1-d \leq |A|+r-1$. Therefore, once again there are at least $r+2$ elements a of A with $a+d$ not in A, and as above, this is a contradiction.

Case 3: $d \leq 2r+1$.
Note that we only need to consider $r \geq 1$, since the $r=0$ case is completely covered by the other two cases.
Consider the process of looping around through the elements of S' in steps of size d starting at the first element thereof. Let j be the number of complete loops around $\mathbb{Z}_p$ undertaken before all the elements of S' have been visited. Note that on each complete loop we visit at least $\left\lfloor \frac{p-|S|}{d} \right\rfloor$ elements of S' which are not in S.
Since S and S' have at least $|A|$ elements in common, the maximum number of elements of S', but not in S, which can be visited is r. Therefore, if we can find conditions under which we visit more than r elements, we will be done. To do this, we need to estimate the number of complete loops j. But we have that on each complete loop at most $\left\lceil \frac{|S|}{d} \right\rceil$ elements of $|A|$ are visited, and therefore $j \geq \frac{|A|}{\left\lceil \frac{|S|}{d} \right\rceil}-1$, the -1 arising from the fact that the last loop may not be a complete one. Putting things together we see then that we just need to verify that the quantity

$$\left(\frac{|A|}{\left\lceil \frac{|S|}{d} \right\rceil}-1\right)\left(\left\lfloor \frac{p-|S|}{d} \right\rfloor\right)$$

is greater than r.
But we have

$$\begin{aligned}\left(\frac{|A|}{\left\lceil \frac{|S|}{d} \right\rceil}-1\right)\left(\left\lfloor \frac{p-|S|}{d} \right\rfloor\right) &\geq \left(\frac{(d-1)|A|-r-d+1}{|A|+r+d-1}\right)\left(\frac{p-|A|-r-d+1}{d}\right)\\ &\geq \left(\frac{rd-2r+d-1}{2r+1+d}\right)\left(\frac{r^2+2r+3-d}{d}\right)\end{aligned}$$

Let us suppose that r is fixed in the latter function, which we call $f_r(d)$. Then it is straightforward to verify that this is continuous with no local minima between $d = 3$ and $d = 2r + 1$, so it is minimised at the endpoints of this range. It is then easy to verify that for $3 \leq d \leq 2r+1$ and $r \geq 5$ we have $f_r(d) > r$.

To check the remaining cases note that we must in fact always have $j \geq 1$ and that for $d \geq 5$ and $r \geq 3$, we must have $j \geq 2$. (This follows easily from the inequality $j \geq \frac{rd-2r+d-1}{2r+1+d}$.) Therefore we have that the number of points of S' which are not in S that are visited is at least

$$j.\frac{r^2+2r+3-d}{d},$$

with $j = 1$ for $2 \leq d \leq 4$ and $j = 2$ for $d \geq 5$ and $r \geq 3$. Now we just run through the remaining cases:
$d = 2$: trivially $\frac{r^2+2r+1}{2} > r$.
$r = 2$: $\frac{11-d}{d} > 2$ for $d = 3$.
$r = 3$: $\frac{18-d}{d} > 3$ for $d = 3, 4$, and $2.\frac{18-d}{d} > 3$ for $d = 5, 6, 7$.
$r = 4$: $\frac{27-d}{d} > 4$ for $d = 3, 4$, and $2.\frac{27-d}{d} > 4$ for $d = 5, 6, 7, 8$.

This still leaves 4 cases to check, viz. $(r, d) = (1, 3), (2, 4), (2, 5)$ and $(4, 9)$. We simply use our inequality for j to show that $|A|$ can only have certain specific sizes in each case, and then consider each in turn to see that they do not work:
$(r, d) = (1, 3)$: we must have $|A| = 3$ or 4, for otherwise $j > 1$ and we're done. In both cases it is straightforward to see that the only possible counterexamples could be when $p = 9$ or $p = 10$, both of which are of course not prime.
$(r, d) = (2, 4)$: we must have $|A| = 4$, for otherwise $j > 1$ and we would be done. This yields exactly one counterexample, when $p = 17$ and $A = \{0, 1, 4, 5\}$, for then we may take $S' = \{1, 5, 9, 13, 0, 4\}$.
$(r, d) = (2, 5)$: we must have $|A| = 4$ similarly, and the only resulting configurations must yield $j \geq 2$, which is a contradiction.
$(r, d) = (4, 9)$: we must have $|A| = 6$ for otherwise $j > 2$, and we would be done. But in this case, it is easy to see that for any resulting configurations we must in actual fact have $j \geq 4$, which is also a contradiction. □

The lower bound on the size of $|A|$ in the above lemma is sharp. This follows from considering the simple example of $A = \{0, 1, \cdots, r\}$ and $S' = \{0, 1, \cdots, r, (p+1)/2, \cdots, (p+1)/2 + (r-1)\}$.
The upper bound on the other hand was chosen so as to meet the demands of proving Theorems 2 and 4, and is almost certainly not sharp, but it is quite sufficient for our purposes.

3 Two Inverse Theorems

Before we get started we need to state a couple of theorems from additive number theory that we will need in the course of the next few sections. The first is the Cauchy-Davenport Theorem, a standard result about the addition of two sets in $\mathbb{Z}_p$:

Cauchy-Davenport Theorem. *Let A and B be subsets of $\mathbb{Z}_p$ with $1 \leq |A|, |B|$ and $|A + B| \leq p - 1$. Then $|A + B| \geq |A| + |B| - 1$.*

We will also need Vosper's Theorem, which characterises the examples for which this theorem is sharp:

Vosper's Theorem. *Let A and B be subsets of $\mathbb{Z}_p$ with $2 \leq |A|, |B|$ and $|A+B| \leq p-2$. Then, if $|A+B| = |A|+|B|-1$, A and B are both arithmetic progressions with the same common difference.*

With these in hand, we will begin by proving a lemma, which we will need in proving our generalisation of the Hamidoune-Rødseth Theorem, about how arithmetic progressions add to other sets:

Lemma 2 *Let U and V be non-empty subsets of $\mathbb{Z}_p$ with U an arithmetic progression of common difference d. Then, if $|U+V| \leq |U|+|V|+t$, $|U| \geq t+3$ and $|U+V| \leq p-1$, $U+V$ is an arithmetic progression with common difference d, and V is contained in an arithmetic progression of common difference d and with length at most $|V|+t+1$.*

Proof: If the set $U+V$ is not an arithmetic progression of common difference d, then it can be written as the union of separated arithmetic progressions of common difference d, say $U+V = P_1 \cup \cdots \cup P_m$. Now for $i = 1, \cdots, m$, let $V_i = \{v \in V : U+v \subset P_i\}$. Plainly these sets form a partition of V, and also $P_i = U + V_i$. Therefore we have, by the Cauchy-Davenport Theorem:

$$\begin{aligned} |U+V| &= |P_1| + \cdots + |P_m| \\ &= |U+V_1| + \cdots + |U+V_m| \\ &\geq m|U| + |V_1| + \cdots + |V_m| - m \\ &= m|U| + |V| - m \end{aligned}$$

But now $|U+V| \leq |U|+|V|+t$, and so we have $|U| \leq \frac{m+t}{m-1} \leq t+2$, for $m \geq 2$. But, $|U|$ was specifically chosen to be greater than $t+3$, so this cannot happen. Therefore $U+V$ is an arithmetic progression with common difference d.

To prove our result about the structure of V, let us suppose, without loss of generality, that in fact $|U+V| = |U|+|V|+t$. Let $W = \{x \in \mathbb{Z}_p : U+x \subset U+V\}$. Then it is easily seen that W contains an arithmetic progression P of length $|V|+t+1$. But now, we have $|U+P| = |U|+|V|+t \leq p-1$. Therefore $W = P$, for adding another point would imply, by the Cauchy-Davenport Theorem that $|U+W| > |U+V|$, which is impossible. □

Note that this lemma is sharp. For let $U = \{0, 1, \cdots, t+1\}$ and let $V = \{0, \cdots, |V|-2, |V|+t+1\}$ with $|V|+2t+2 < p$. Then $|U+V| = |V|+2t+2 = |U|+|V|+t$, since $U+V = \{0, 1, \cdots, |V|+t-1, |V|+t+1, \cdots, |V|+2t+2\}$. But neither is $U+V$ an arithmetic progression nor is V contained in an arithmetic progression of length $|V|+t+1$.

We now prove our generalisation of the Hamidoune-Rødseth Theorem (Theorem 4):

Proof: By induction. Assume that the result holds for $l-1$ (the base case will itself emerge from the ordinary Hamidoune-Rødseth Theorem in the course of the proof). Now, for l summands, assume that

$$|A_1 + A_2 + \cdots + A_l| \leq |A_1| + |A_2| + \cdots + |A_l|.$$

For all $1 \leq i \leq l$, define ϵ_{i1} and ϵ_{i2} by

$$|\sum_{j=1}^{l} A_j| = |\sum_{j \neq i} A_j| + |A_i| + \epsilon_{i1},$$

$$|\sum_{j\neq i} A_j| = \sum_{j\neq i} |A_j| + \epsilon_{i2}.$$

By assumption $\epsilon_{i1} + \epsilon_{i2} \leq 0$, for each i, and, by the Cauchy-Davenport Theorem, $\epsilon_{i1} \geq -1$, for each i. We split our considerations into two cases, depending on whether two or more of the ϵ_{i1} are greater than or equal to 0 or not.

Case 1: $\epsilon_{i1} \geq 0$ for at least two i.
Without loss of generality assume that $\epsilon_{i1} \geq 0$ for $i = 1, 2$. Then, since $\epsilon_{i2} \leq 0$ for $i = 1, 2$, the following inequalities hold:

$$|A_2 + A_3 + \cdots + A_l| \leq |A_2| + |A_3| + \cdots + |A_l|,$$

$$|A_1 + A_3 + \cdots + A_l| \leq |A_1| + |A_3| + \cdots + |A_l|.$$

By the inductive hypothesis, $A_2, A_3, \cdots A_l$ are all contained in arithmetic progressions with the same common difference d, with $d \leq \frac{p}{2}$, and with lengths at most $|A_i| + (l-2)$. (Note that when $l = 3$, this is implied by the ordinary Hamidoune-Rødseth Theorem, since $|A_i| \geq 3 + 1 \geq 4$, and therefore $|A_2 + A_3| \geq |A_2| + |A_3| - 1 \geq 7$ and by the Cauchy-Davenport Theorem $|A_2 + A_3| \leq |A_1 + A_2 + A_3| - |A_1| + 1 \leq p - 2 - 4 + 1 = p - 5$. This is how we get our induction started.)
Similarly, $A_1, A_3, \cdots, A_l$ are all contained in arithmetic progressions with the same common difference d', with $d' \leq \frac{p}{2}$. Now if $d \neq d'$, it must be that A_3 is contained in two arithmetic progressions of length $|A_3| + (l-2)$ but with different common differences. But we have $(l-2) + 2 < |A_3|$ and

$$\begin{aligned}
|A_3| &\leq |A_1 + \cdots + A_l| - |A_1| - |A_2| - |A_4| - \cdots - |A_l| + (l-1) \\
&\leq p - 2 - (l-1)(l+1) + (l-1) \\
&= p - (l^2 - l + 2) \\
&< p - ((l-2)^2 + 3(l-2) + 2),
\end{aligned}$$

and therefore we may apply Lemma 1 to A_3 to conclude that $d = d'$. The only possible trouble might be when $l = 4$, but in this case, our only counterexamples are with sets of size 4, while the requirements of the theorem stipulate that we only need to consider sets of size greater than or equal to 5.

Case 2: $\epsilon_{i1} = -1$ for all but at most one i.
Without loss of generality assume that for all i except perhaps l, we have $\epsilon_{i1} = -1$. Then it follows from Vosper's Theorem (this is why we take $|A_1 + \cdots + A_l| \leq p - 2$ in the theorem) that A_i and $A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_l$ are arithmetic progressions with the same common difference d_i for all $i < l$.
Now the condition

$$|\sum_{j\neq i} A_j| \leq \sum_{j\neq i} |A_j| + 1$$

(which holds for all i) implies, using the Cauchy-Davenport Theorem, that

$$|\sum_{j\neq i} A_j| \leq |A_1| + |\sum_{j\neq 1,i} A_j| + (l-2).$$

But A_1 is an arithmetic progression with common difference d_1, and therefore it follows from Lemma 4, since $|A_1| \geq l+1$, that $A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_l$ is an arithmetic progression with common

difference d_1. But we already know that it is an arithmetic progression with common difference d_i, and therefore, by the $r = 0$ case of Lemma 1, it follows that $d_1 = d_i$ for all $i < l$.
Finally, note that $A_1 + A_2 + \cdots + A_{l-1}$ is an arithmetic progression with common difference d_1, and since

$$\begin{aligned} |A_1 + \cdots + A_l| &\leq |A_1| + \cdots + |A_l| \\ &\leq |A_1 + \cdots + A_{l-1}| + |A_l| + (l-2) \end{aligned}$$

and $|A_1 + A_2 + \cdots + A_{l-1}| \geq |A_1| \geq l + 1$, an application of Lemma 2 implies that A_l is a subset of an arithmetic progression of length $|A_l| + (l-1)$ and with common difference d_1. □

Note that with a little more care in the previous proof we could be more specific about what kind of sets $A_1, \cdots, A_l$ are admissible as sets with $|A_1 + \cdots + A_l| \leq |A_1| + \cdots + |A_l|$ under the conditions of the theorem. Following through with such an argument tells us that in fact we must have either $A_i \subset S_i$, where the S_i are arithmetic progressions of the same common difference, with $|S_i| = |A_i| + t_i$ and $\sum_{i=1}^{l} t_i \leq l - 1$, or $A_i = \{a_i, a_i + 2d, a_i + 3d, \cdots, a_i + |A_i|d\}$ for all i, and some fixed d.

4 Concluding the Proof

We are now ready to prove Theorem 2 (this is an extension of Theorem 4.1 in [3]):

Proof: To begin note that if for some permutation of the coefficients $a_1, \cdots, a_k$, say $a'_1, \cdots a'_k$,

$$|a'_1 C_1 + \cdots + a'_{k-1} C_{k-1}| \geq |C_1| + \cdots + |C_{k-1}| + 1,$$

then the Cauchy-Davenport Theorem implies that $|a'_1 C_1 + \cdots + a'_k C_k| \geq p$, and the theorem would follow trivially. Therefore assume that for any permutation $a'_1, \cdots, a'_k$ we have

$$|a'_1 C_1 + \cdots + a'_{k-1} C_{k-1}| \leq |C_1| + \cdots + |C_{k-1}|.$$

Now note that, by assumption, $|C_i| \geq (k-1) + 1$ and plainly we have that $|a'_1 C_1 + \cdots + a'_{k-1} C_{k-1}| \leq p - 2$. Therefore Theorem 4 applies and so, for all a_i and all sets C_j, the set $a_i C_j$ are contained in arithmetic progressions of length at most $|C_j| + (k-2)$ with the same common difference. We consider two cases: firstly that in which there are two coefficients a_i and a_j with $a_i \neq \pm a_j$, and secondly that where $a_i = \pm a_j$ for all i and j, but at least two coefficients are of opposite sign.

Case 1: $a_i \neq \pm a_j$ for some i and j.
Let us assume, without loss of generality, that $a_1 \neq \pm a_2$. Letting $a'_1 = a_1, a'_2 = a_3$, we see that $a_1 C_1$ and $a_3 C_2$ are both large subsets of arithmetic progressions with the same common difference. Moreover, letting $a'_1 = a_2, a'_2 = a_3$, we see also that $a_2 C_1$ and $a_3 C_2$ are large subsets of arithmetic progressions with the same common difference. Therefore, we conclude that $a_1 C_1$ and $a_2 C_1$ are both contained in arithmetic progressions of length $|C_1| + (k-2)$ with the same common difference, and so C_1 must be a large subset of two arithmetic progressions with genuinely different common differences. But since $|C_1| \geq k = (k-2) + 2$ and

$$\begin{aligned} |C_1| &= p - |C_2| - \cdots - |C_k| \\ &\leq p - (k^2 - k) \\ &= p - ((k-2)^2 + 3(k-2) + 2), \end{aligned}$$

an application of Lemma 1 tells us that this cannot be so. Again, our one set of counterexamples is easily ruled out as a possibility, because at least one of the sets into which we partition $\mathbb{Z}_{17}$ must have other than four elements.

Case 2: $a_i = \pm a_j$ for all i and j, but at least two coefficients have opposite sign.
For a fixed permutation $a'_1, \cdots, a'_k$ of $a_1, \cdots, a_k$, we see from

$$|a'_1 C_1 + a'_2 C_2 + \cdots + a'_{k-1} C_{k-1}| \leq |C_1| + \cdots + |C_{k-1}|,$$

and the remark after the proof of Theorem 4, that the $a'_i C_i$, for $1 \leq i \leq k-1$, are either all of the form $a'_i C_i = \{c_i, c_i + 2d, c_i + 3d, \cdots, c_i + |C_i|d\}$, for some fixed d, or each $a'_i C_i$ is a subset of an arithmetic progression S_i with $|S_i| = |C_i| + t_i$ and $\sum_{i=1}^{k-1} t_i \leq k-2$, where all the S_i have the same common difference d.
But now, if the first case occurs, and $a'_1 = -a'_2$, say, then we have that $C_1 = \{c_1, c_1 + 2d, \cdots, c_1 + |C_1|d\}$ and $C_2 = \{c_2, c_2 + d, \cdots, c_2 + (|C_2| - 2)d, c_2 + |C_2|d\}$, for some fixed d. But now choosing a different permutation such that $a''_1 = a''_2$ we have $|a''_1 C_1 + a''_2 C_2| = |C_1| + |C_2| + 1$, with $a''_1 C_1 + a''_2 C_2$ an arithmetic progression (provided the sizes of the colour classes are all greater than or equal to 3). Adding on successive $a''_i C_i$s, it is easy to see that for $i \leq k-1$,

$$|a''_1 C_1 + \cdots + a''_i C_i| = |C_1| + \cdots + |C_i| + 1,$$

with $a''_1 C_1 + \cdots + a''_i C_i$ an arithmetic progression, and therefore that $a''_1 C_1 + \cdots + a''_k C_k = \mathbb{Z}_p$.
For the second case, at least one of the C_i, say C_1 is an arithmetic progression. Because this has size at least k, adding it to other classes has the effect of closing off the gaps in the other classes (since the gaps have size smaller than k) and the resultant sum is also an arithmetic progression. Therefore, we see that for all possible permutations $a'_1, \cdots, a'_k$ of the coefficients $a_1, \cdots, a_k$, the set $a'_1 C_1 + \cdots + a'_k C_k$ is an arithmetic progression of length at least $p - (k-1)$. If we can show that these arithmetic progressions form a cover of $\mathbb{Z}_p$, we will be done.
Let C_1 be $\{c_1, \cdots, c_1 + (|C_1| - 1)d\}$. Write out the elements of $\mathbb{Z}_p$ by starting at c_1 and writing down every dth term thereafter, where d is the common difference of all the S_i. Denote the first term and last terms of $C_i, 1 \leq i \leq k$, encountered on this path by $c_1 + e_i d$ and $c_1 + f_i d$ respectively. Let us now suppose, without any loss of generality, that we have exactly l coefficients amongst $a_1, \cdots, a_k$ which are between 1 and $\frac{p}{2}$. Now if we do not have a cover of $\mathbb{Z}_p$ then we necessarily have for all $A, B \subset [k]^{(l)}$ that

$$(\sum_{a \in A} e_a - \sum_{a' \in A^c} f_{a'}) - (\sum_{b \in B} e_b - \sum_{b' \in B^c} f_{b'}) \in \{-(k-2), \cdots, k-2\},$$

that is, that the first terms in the arithmetic progressions $\sum_{a \in A} C_a - \sum_{a' \in A^c} C_{a'}$ and $\sum_{b \in B} C_b - \sum_{b' \in B^c} C_{b'}$ differ by at most $k-2$.
In particular, for any r and $s \in [k]$, choose A containing r but not s, and $B = (A - \{r\}) \cup \{s\}$, so we have

$$(e_r + f_r) - (e_s + f_s) \in \{-(k-2), \cdots, k-2\}.$$

Now let us consider what this implies for $r = 2$ and $s = 1$, where we take C_2 to be the colour class containing $c_1 + |C_1|d$. In this case, we know that $e_1 = 0, f_1 = |C_1| - 1$, and $e_2 = |C_1|$. Therefore, from the above deduction, we see that f_2 must lie within the set $\{-(k-1), \cdots, k-3\}$. But f_2 cannot possibly lie within $\{0, \cdots, k-3\}$, since all these points are in C_1. If it lies amongst the points $\{-(k-1), \cdots, -1\}$, then the set S_2 must have size at least $p - |C_1| - (k-1)$, and so C_2 has size at least $p - |C_1| - (2k-3)$. But this then implies that

$$|C_3| + \cdots + |C_k| \leq 2k - 3,$$

which is plainly false for $k \geq 4$. □

The remaining case which is not dealt with is when all of the a_i are in fact congruent. But it is straightforward to see that in this case there are colourings such that an equation of this form does not necessarily have a solution. For example, partitioning $\mathbb{Z}_p$ into k consecutive segments (arithmetic progressions of length 1), it is easy to see that the size of $C_1 + \cdots + C_k$ is then only $p - (k-1)$, so we cannot possibly have solutions to all equations of the form $x_1 + \cdots + x_k = b$. There are of course many more similar examples which work, where each of the C_i is chosen so as to be a large subset of an arithmetic progression with some fixed common difference.

5 Further Research

We have no evidence to suggest that the lower bounds on the sizes of the sets in Theorems 2 and 4 are sharp, and in fact it seems quite unlikely that they are. On the other hand, it seems unlikely that our method can do much better than the bounds we have given, since the proofs have a strong dependency upon certain lemmas which require that the relevant sets are large.

If, however, one could find an approach to generalising the Hamidoune-Rødseth Theorem which avoided the use of these lemmas, and thus improved the bounds, it would be straightforward to improve the bounds on Theorem 2. For, if we could impose structure on all the sets in the partition, then we could use the obvious fact that one of these sets must be large (for p large), and apply our lemmas to that particular set. So we have the following problem:

Problem 5. *What are the optimal bounds for the generalised Hamidoune-Rødseth Theorem, i.e. Theorem 4?*

The question also arises as to whether or not anything can be said about systems of linear equations in $\mathbb{Z}_p$. In $\mathbb{Z}_n$, for n not a prime, this question has been looked at (see for example [1] and [4]), and numerous examples have been found showing that there are equinumerous configurations in $k = 4, 5, 6$ and $k \geq 10$ colours (i.e. colourings of $\mathbb{Z}_{km}$ for some m such that each colour occurs m times) within which we cannot find rainbow arithmetic progressions of length k, that is an arithmetic progression with each colour in a different class. This being a typical example of a system of linear equations, our hopes of saying anything about solving such systems would appear to be shattered.

However, there have as yet been no examples of k-colourings of $\mathbb{Z}_p$ for p a prime and with the colour classes all of nearly equal (and large) sizes containing no rainbow arithmetic progression of length k. This is not to say that such colourings won't be found, but the problem of finding such colourings, or indeed proving that they do not exist, remains open. More specifically, we have the following open question:

Problem 6. *Do 4-colourings of $\mathbb{Z}_p$, for p a large prime, always contain a rainbow AP(4) if each of the colour classes is of size either $\lfloor \frac{p}{4} \rfloor$ or $\lceil \frac{p}{4} \rceil$?*

Acknowledgements I would like to thank both Tim Gowers and Imre Leader for their comments

and observations.

References

[1] D. Conlon, V. Jungić, R. Radoičić - On the Existence of Rainbow 4-term Arithmetic Progressions, preprint.

[2] Y.O. Hamidoune, O. J. Rødseth - An Inverse Theorem mod p, in Acta Arithmetica 92, 2000, p. 251-262.

[3] V. Jungić, J. Licht (Fox), M. Mahdian, J. Nešetřil, R. Radoičić - Rainbow Arithmetic Progressions and Anti-Ramsey Results, in Combinatorics, Probability and Computing 12, 2003, p. 599-620.

[4] V. Jungić, J. Nešetřil, R. Radoičić - Rainbow Ramsey Theory, in Integers, the Electronic Journal of Combinatorial Number Theory, Proceedings of the Integers conference in honour of Tom Brown, to appear in Special Issue 5(2), 2005.