RESTRICTED SUMSETS IN FINITE VECTOR SPACES: THE CASE p = 3

Shalom Eliahou
Département de Mathématiques, Université du Littoral Côte d'Opale, B.P. 699, 62228 Calais, France
eliahou@lmpa.univ-littoral.fr

Michel Kervaire
Département de Mathématiques, Université de Genève, B.P. 240, 1211 Genève 24, Suisse

Received: 3/31/2000, Revised: 1/2/01, Accepted: 2/27/01, Published: 3/9/01

Abstract

We determine the sharp lower bound for the cardinality of the restricted sumset $A +' B = \{a + b \mid a \in A, b \in B, a \neq b\}$, where A, B run over all subsets of size $r = s = 1 + 3^h$ in a vector space over $\mathbf{F}_3$. This solves a conjecture stated in an earlier paper of ours on sumsets and restricted sumsets in finite vector spaces.

The analogous problem for an arbitrary prime p remains open. However, we do prove some partial results concerning more generally special pairs of the form $r = s = 1 + ap^h$.

We also provide alternate proofs for the formulas satisfied by our general lower bounds $\beta_p(r, s)$ and $\gamma_p(r, s)$ for the cardinality of the ordinary sum and restricted sum of sets of size r, s in a vector space over $\mathbf{F}_p$.

1. Introduction

Let V be a vector space over the finite field $\mathbf{F}_p$. If $A, B \subset V$ are two non-empty subsets of V, we define their restricted sumset $A +' B$ by

$$A +' B \;=\; \{a + b \mid a \in A, b \in B, a \neq b\}.$$

If $r, s \leq |V|$, we define

$$\mu'_V(r, s) \;=\; \min |A +' B|,$$

where A, B run over all subsets of V of cardinality r, s respectively.

Erdős and Heilbronn conjectured in 1964 that if A is a subset of cardinality r in $V = \mathbf{F}_p$, then $|A +' A| \geq \min\{p, 2r - 3\}$. This conjecture was solved 30 years later by

Dias da Silva and Hamidoune in [**DH**]. Using a different method, Alon, Nathanson and Ruzsa subsequently strengthened this result by establishing the equality

$$\mu'_{\mathbf{F}_p}(r,s) = \begin{cases} \min\{p, 2r-3\} & \text{if } r = s, \\ \min\{p, r+s-2\} & \text{if } r \neq s. \end{cases}$$

(See [**ANR**1, **ANR**2].)

The determination of $\mu'_V(r,s)$ for an arbitrary vector space V over $\mathbf{F}_p$ was taken up and completed for most pairs r, s in [**EK**1]. In summary, we have determined the value of $\mu'_V(r,s)$ for all r, s if $p = 2$, and for all non-special pairs (r,s) is p an odd prime. (See Section 2.) The problem of determining $\mu'_V(r,s)$ remains open for special pairs (r,s).

A pair of natural numbers (r,s) is said to be **special** for the odd prime p if r and s have p-adic expansions of the form

$$\begin{cases} r &= 1 + ap^h + \sum_{i=h+1}^{n} r_i p^i, \\ s &= 1 + ap^h + \sum_{i=h+1}^{n} s_i p^i, \end{cases} \tag{1}$$

with $h \geq 1$ and coefficients a, r_i, s_i satisfying the conditions

$$\begin{cases} 1 \leq a \leq \frac{p-1}{2}, \text{ and} \\ r_i + s_i \leq p-1 \text{ for } h+1 \leq i \leq n. \end{cases} \tag{2}$$

We do know that for a special pair (r,s), we have either $\mu'_V(r,s) = r+s-3$ or else $\mu'_V(r,s) = r+s-2$. (See Corollary (7.5) in [**EK**1].) However resolving this alternative seems to be quite difficult.

The case $r = s = 1+p$ has been treated in our previous paper [**EK**2]. With the notation $\mu'_p(r,s) = \min_V\{\mu'_V(r,s)\}$, we proved that

$$\mu'_p(1+p, 1+p) = 2(1+p) - 2 = 2p,$$

for $p \geq 5$. (See [**EK**2], Theorem (1.1).)

Although we have some partial results for certain special pairs with an arbitrary prime p, we do not have any complete treatment beyond the case $r = s = 1+p$, at least for $p \geq 5$.

For $p = 3$, there is the example $A = B = \{0,\ e_1,\ e_2,\ e_1+e_2\}$ in the plane $V = \mathbf{F}_3 e_1 \oplus \mathbf{F}_3 e_2$ with $|A| = |B| = 4$ and $|A +' B| = |\{e_1,\ e_2,\ e_1+e_2,\ 2e_1+e_2,\ e_1+2e_2\}| = 5$ realizing the lower bound $\mu'_3(4,4) = 5 = r+s-3$ for $r = s = 4$.

We know from Theorem (7.10) in [**EK**1] that the existence of this simple example implies that if r, s have 3-adic expansions of the form

$$\begin{cases} r &= 1 + 3 + \sum_{i \geq 2} r_i 3^i, \\ s &= 1 + 3 + \sum_{i \geq 2} s_i 3^i, \end{cases}$$

where $r_i + s_i \leq 2$ for all $i \geq 2$, then $\mu_3'(r,s) = r + s - 3$.

In the present paper, we solve the question of determining the value of $\mu_V'(r,s)$ at $p = 3$ for the particular special pairs (r,s) of the form

$$r \;=\; s \;=\; 1 + 3^h,$$

where $h \geq 2$. The corresponding problem for $p \geq 5$ remains open.

Our main result, which was conjectured in [**EK**1] at least for $h = 2$, is :

Theorem. *Let $A, B \subset V$ be subsets of cardinality $1 + 3^h$ with $h \geq 2$ in a vector space V over $\mathbf{F}_3$. Then,*

$$|A +' B| \;\geq\; 2 \cdot 3^h.$$

This lower bound $2 \cdot 3^h$ is sharp, i.e.*, $\mu_3'(1 + 3^h, 1 + 3^h) = 2 \cdot 3^h$.*

The above examples of special pairs (r,s) with $r \equiv s \equiv 4 \bmod 3^2$ happen in fact to be the only examples we know of special pairs (r,s) for which $\mu_p'(r,s)$ attains the lower bound $r + s - 3$.

Although $(1 + 3^h, 1 + 3^h)$ is a special pair (for the prime 3), the proof of the above result requires lower bounds for the cardinalities of sumsets and restricted sumsets for sets $X, Y \subset V$ whose cardinalities do not necessarily form a special pair.

Formulas for these lower bounds $\beta_p(r,s)$ and $\gamma_p(r,s)$, for arbitrary odd prime p, were given in [**EK**1]. In the next section we provide a somewhat different treatment of their proof and recall some needed basic facts.

Also, our proof of the Theorem (stated as Theorem (5.1) in Section 5) requires auxiliary statements which may as well be stated and proved for an arbitrary odd prime p. These will be discussed in Sections 3 and 4.

It does not seem unreasonable to conjecture that, except for the case $p = 3$ and $|A| \equiv |B| \equiv 4 \bmod 9$ we have mentioned above, the cardinality of a restricted sumset $A +' B$, with $(|A|, |B|) = (r,s)$ forming a special pair, is bounded below by $r + s - 2$. We have no clue of a method strong enough to prove this statement for an arbitrary special pair.

Right from the start of the proof (see Proposition (3.1) in Section 3 below), we need the assumption that A and B have cardinality $|A| = |B| = 1 + ap^h$. This assumption is maintained throughout Section 4.

The case $p = 3$ proper is dealt with in Section 5.

2. Basic results and explicit formulas for $\beta_p(r,s)$ and $\gamma_p(r,s)$

Given an odd prime p and positive integers r, s, let

$$\beta_p(r,s) \;=\; \min\,\{n \in \mathbf{N} \mid (x+y)^n \in (x^r, y^s)\mathbf{F}_p[x,y]\}$$

be the smallest natural number n such that $(x+y)^n$ belongs to the ideal $I(r,s) = (x^r, y^s)$ generated by x^r, y^s in the polynomial ring $\mathbf{F}_p[x,y]$.

We have proved in [**EK**1] that for any $A, B \subset V$ of cardinalities $|A| = r$ and $|B| = s$, one has the inequality

$$|A+B| \geq \beta_p(r,s), \tag{3}$$

using the usual notation $A + B = \{a + b \mid a \in A, b \in B\}$.

Moreover, this lower bound is sharp, *i.e.*, if $\mu_V(r,s)$ denotes the smallest possible value of $|A+B|$ for all $A, B \subset V$ of cardinalities $|A| = r$, $|B| = s$ then $\mu_V(r,s) = \beta_p(r,s)$, provided $r, s \leq |V|$.

We also obtained in [**EK**1], by a similar method, a lower bound $\gamma_p(r,s)$ for the size of the *restricted* sumset $A +' B = \{a + b \mid a \in A, b \in B, a \neq b\}$. More precisely, let

$$\gamma_p(r,s) \;=\; \min\{n \in \mathbf{N} \mid (x-y)(x+y)^n \in (x^r, y^s)\mathbf{F}_p[x,y]\},$$

then we have

$$|A +' B| \geq \gamma_p(r,s). \tag{4}$$

However, the lower bound $\gamma_p(r,s)$ need not be sharp if (r,s) is a special pair for the odd prime p. It is indeed sharp, *i.e.*, $\mu'_p(r,s) = \gamma_p(r,s)$ if (r,s) is *not* a special pair.

We now produce explicit formulas for these lower bounds $\beta_p(r,s)$ and $\gamma_p(r,s)$.

Given positive integers r and s, let $r-1 = \sum_{i=0}^{n} r_i p^i$, $s-1 = \sum_{i=0}^{n} s_i p^i$ be the p-adic expansions of $r-1$ and $s-1$, *i.e.*, $0 \leq r_i \leq p-1$ and $0 \leq s_i \leq p-1$ for all $i \in [0,n]$.

Define the integer $m \in \mathbf{Z}$ by the formula

$$m \;=\; \max(\{-1\} \cup \{i \in [0,n] \mid\; r_i + s_i \geq p\}).$$

In other words, $m = -1$ if for all $i \in [0,n]$ we have $r_i + s_i \leq p-1$. Else, m is characterized by the inequalities $r_m + s_m \geq p$ and $r_i + s_i \leq p-1$ for $i \in [m+1, n]$. (This last interval being of course empty if $m = n$, *i.e.*, if $r_n + s_n \geq p$.)

With this notation, the function $\beta_p(r,s)$ is given by

$$\begin{aligned} \beta_p(r,s) &= p^{m+1} + \textstyle\sum_{i=m+1}^{n}(r_i+s_i)p^i \\ &= s + \textstyle\sum_{i=m+1}^{n} r_i p^i + (p^{m+1} - 1 - \sum_{i=0}^{m} s_i p^i). \end{aligned} \tag{5}$$

Note that $\beta_p(r,s) = r+s-1$ if $m = -1$, *i.e.*, if $r_i + s_i \leq p-1$ for all $i \in [0,n]$.

The formula for $\gamma_p(r,s)$ involves a somewhat more complicated case distinction.

If $r=s=1$, then $\gamma_p(1,1)=0$. If $r+s\geq 3$, then

$$\gamma_p(r,s)=\begin{cases}\beta_p(r,s) & \text{if } \binom{r+s-2}{r-1}\equiv 0 \mod p,\\ r+s-3 & \text{if } \binom{r+s-2}{r-1}\not\equiv 0 \text{ and } \binom{r+s-3}{r-1}\equiv\binom{r+s-3}{s-1} \mod p,\\ r+s-2 & \text{if } \binom{r+s-2}{r-1}\not\equiv 0 \text{ and } \binom{r+s-3}{r-1}\not\equiv\binom{r+s-3}{s-1} \mod p.\end{cases} \tag{6}$$

The conditions on binomial coefficients in formula (6) can equivalently be formulated in terms of the respective p-adic expansions $r-1=\sum_{i\geq 0} r_i p^i$ and $s-1=\sum_{i\geq 0} s_i p^i$ of $r-1$ and $s-1$, as follows :

If $r+s\geq 3$ as above, then

$$\gamma_p(r,s)=\begin{cases}\beta_p(r,s) & \text{if there exists an index } j\\ & \text{such that } r_j+s_j\geq p,\\ r+s-3 & \text{if } r_i+s_i\leq p-1 \text{ for all } i, \text{ and}\\ & \nu_p(r-1)=\nu_p(s-1)=v, \text{ say,}\\ & \text{with } r_v=s_v,\\ r+s-2 & \text{otherwise, } i.e., \text{ still with } r_i+s_i\leq p-1\\ & \text{for all } i, \text{ but either } \nu_p(r-1)\neq\nu_p(s-1)\\ & \text{or, with } v \text{ as above, } r_v\neq s_v,\end{cases} \tag{7}$$

where $\nu_p(r-1)$ is the p-valuation of $r-1$, *i.e.*, $\nu_p(r-1)=v$ if the p-adic expansion of $r-1$ has the form $r-1=r_v p^v+\sum_{i>v} r_i p^i$ with $r_v\neq 0$.

Note that the definition of a special pair (given in the Introduction) corresponds exactly to the second case in formula (7), with the further condition $\nu_p(r-1)=\nu_p(s-1)\geq 1$.

Hence, the statement "$\mu'_V(r,s)=r+s-3$ or else $\mu'_V(r,s)=r+s-2$" in the Introduction amounts for special pairs to the inequalities

$$\gamma_p(r,s)\leq\mu'_V(r,s)\leq\gamma_p(r,s)+1$$

which are true in general. (Compare also the version of the definition of a special pair given in [**EK**1], Definition (7.8).) It is a theorem in [**EK**1] (see Theorem (7.9)) that $\mu'_V(r,s)=\gamma_p(r,s)$ for non-special pairs.

The proof of the equivalence of (6) and (7) is easy and left to the reader. Part of it is reproduced below and the rest is an immediate consequence of Lemma (7.7) in [**EK**1].

In this section, we provide a direct proof of the formulas (5) and (6) which is partially independent of [**EK**1]. However, we use but do not reprove a couple of easy lemmas from our previous paper.

We begin with a remark on the binomial coefficient $\binom{r+s-2}{r-1}$ which is the content of Lemma (7.2) in [**EK**1].

Let $r-1=\sum_{i\geq 0} r_i p^i$ and $s-1=\sum_{i\geq 0} s_i p^i$ be the p-adic expansions of $r-1$ and $s-1$. If $r+s-2=\sum_{i\geq 0} t_i p^i$ is the p-adic expansion of $r+s-2$, the well known Lucas formula for binomial coefficients modulo p, namely here,

$$\binom{r+s-2}{r-1} \equiv \prod_{i\geq 0} \binom{t_i}{r_i} \mod p,$$

shows easily that $\binom{r+s-2}{r-1} \not\equiv 0 \mod p$ if and only if $0 \leq r_i + s_i \leq p-1$ for all i.

By definition, $\beta_p(r,s) = \min\{n \in \mathbf{N} \mid (x+y)^n \in I(r,s)\}$, where $I(r,s)$ is the ideal (x^r, y^s) generated by x^r and y^s in the polynomial ring $\mathbf{F}_p[x,y]$.

Since $(x+y)^{r+s-1} = \sum_{i=0}^{r+s-1} \binom{r+s-1}{i} x^i y^{r+s-1-i}$, and either $i \geq r$, or if $i \leq r-1$, then $r+s-1-i \geq s$, it follows that $(x+y)^{r+s-1} \in I(r,s)$ and $\beta_p(r,s) \leq r+s-1$.

Furthermore, the congruence $(x+y)^{r+s-2} \equiv \binom{r+s-2}{r-1} x^{r-1} y^{s-1} \bmod I(r,s)$ gives $\beta_p(r,s) = r+s-1$ if $\binom{r+s-2}{r-1} \not\equiv 0 \bmod p$.

Thus,

$$\beta_p(r,s) \;=\; r+s-1, \; \textit{if } r_i + s_i \leq p-1 \;\; \textit{for all } i \geq 0.$$

If, on the other hand, there exists an index m such that $r_m + s_m \geq p$ and $r_i + s_i \leq p-1$ for $i \geq m+1$, then we write

$$\begin{cases} r-1 &= a_0 + a_1 p^{m+1}, \\ s-1 &= b_0 + b_1 p^{m+1}, \end{cases}$$

where $a_0 = \sum_{i=0}^{m} r_i p^i$, and $b_0 = \sum_{i=0}^{m} s_i p^i$, and of course, a_1, b_1 are non-negative integers.

Note for further use that $p^{m+1} = p \cdot p^m \leq (r_m + s_m) p^m \leq a_0 + b_0$.

We claim that, using the above notation, $\beta_p(r,s)$ is given by

$$\beta_p(r,s) \;=\; p^{m+1} + \sum_{i \geq m+1} (r_i + s_i) p^i \;=\; p^{m+1}(1 + a_1 + b_1).$$

In order to prove this, we calculate

$$\begin{aligned} (x+y)^{p^{m+1}(a_1+b_1+1)} &\equiv (x^{p^{m+1}} + y^{p^{m+1}})^{a_1+b_1+1} \bmod p \\ &= \sum_{i=0}^{a_1+b_1+1} \binom{a_1+b_1+1}{i} x^{p^{m+1} i} y^{p^{m+1} j}, \end{aligned}$$

where $i + j = a_1 + b_1 + 1$.

For $i \le a_1$, we have $j \ge b_1 + 1$ and since

$$s - 1 = b_0 + p^{m+1}b_1 \le p^{m+1} - 1 + p^{m+1}b_1 \le p^{m+1}j - 1$$

it follows that $p^{m+1}j > s$ and $y^{p^{m+1}j} \in (x^r, y^s)$.

Similarly, if $i \ge a_1 + 1$, then $j \le b_1$. As above, we have $p^{m+1}i > r$ and $x^{p^{m+1}i} \in I(r,s) = (x^r, y^s)$.

Therefore $(x+y)^{p^{m+1}(1+a_1+b_1)} \in I(r,s)$, and $\beta_p(r,s) \ge p^{m+1}(1+a_1+b_1)$ by definition.

We now calculate

$$\begin{aligned}(x+y)^{p^{m+1}(a_1+b_1+1)-1} &\equiv (x^{p^{m+1}} + y^{p^{m+1}})^{a_1+b_1} \cdot (\tfrac{x^{p^{m+1}}+y^{p^{m+1}}}{x+y}) \bmod p \\ &\equiv \textstyle\sum_{i=0}^{a_1+b_1} \binom{a_1+b_1}{i} x^{p^{m+1}i} y^{p^{m+1}j} \cdot \sum_{k=0}^{p^{m+1}-1} (-1)^k x^k y^\ell \bmod p,\end{aligned}$$

where $i + j = a_1 + b_1$ and $k + \ell = p^{m+1} - 1$.

For $i > a_1$, we have $p^{m+1}i > p^{m+1} - 1 + p^{m+1}a_1 \ge r - 1$. It follows that $x^{p^{m+1}i} \in I(r,s)$. Similarly, $y^{p^{m+1}j} \in I(r,s)$ for $j > b_1$. Hence,

$$(x+y)^{p^{m+1}(a_1+b_1+1)-1} \equiv \binom{a_1+b_1}{a_1} x^{p^{m+1}a_1} y^{p^{m+1}b_1} \cdot \sum_{k=0}^{p^{m+1}-1} (-1)^k x^k y^\ell,$$

modulo $I(r,s)$, with $\ell = p^{m+1} - k - 1$.

As noted above, $a_0 + b_0 \ge (r_m + s_m)p^m \ge p^{m+1}$. For k in the interval $p^{m+1} - b_0 - 1 \le k \le a_0$, we have $\ell = p^{m+1} - k - 1 \le b_0$. Therefore, still modulo $I(r,s)$, we have

$$(x+y)^{p^{m+1}(a_1+b_1+1)-1} \equiv \sum_{p^{m+1}-b_0-1 \le k \le a_0} (-1)^k \binom{a_1+b_1}{a_1} x^{k+p^{m+1}a_1} y^{\ell+p^{m+1}b_1},$$

and the monomials $x^{k+p^{m+1}a_1} y^{\ell+p^{m+1}b_1}$, for the indicated interval of values of k and ℓ are part of an $\mathbf{F}_p$-basis of $\mathbf{F}_p[x,y]/I(r,s)$.

Now, certainly, $(-1)^k \not\equiv 0 \bmod p$, and using again the Lucas formula and the inequalities $r_i + s_i \le p - 1$ for $i \ge m + 1$, we have

$$\binom{a_1+b_1}{a_1} \equiv \prod_{i \ge m+1} \binom{r_i+s_i}{r_i} \not\equiv 0 \mod p.$$

Hence,

$$(x+y)^{p^{m+1}(a_1+b_1+1)-1} \notin I(r,s).$$

It follows that $\beta_p(r,s) = p^{m+1}(1 + a_1 + b_1)$ as asserted.

We now prove the formula (6) for $\gamma_p(r,s)$. Let $\gamma = \gamma_p(r,s)$, $\beta = \beta_p(r,s)$, to simplify notation.

Suppose first that there exists an index n for which $r_n + s_n \geq p$ in the p-adic expansions $r-1 = \sum_{i\geq 0} r_i p^i$ and $s-1 = \sum_{i\geq 0} s_i p^i$ of $r-1$ and $s-1$, then $\binom{r+s-2}{r-1} \equiv 0 \bmod p$. Indeed, taking n such that $r_i + s_i \leq p-1$ for $i < n$, we have the p-adic expansion $r+s-2 = \sum_{i\geq 0} t_i p^i$ with $t_n = r_n + s_n - p < r_n$, and by the Lucas formula

$$\binom{r+s-2}{r-1} \equiv \prod_{k\geq 0} \binom{t_k}{r_k} \equiv 0 \mod p,$$

because the factor $\binom{t_n}{r_n}$, where $t_n < r_n$, is congruent to 0 mod p.

It follows from

$$(x+y)^\beta = \sum_i \binom{\beta}{i} x^i y^{\beta-i} \equiv \sum_{i=\beta-s+1}^{r-1} \binom{\beta}{i} x^i y^{\beta-i} \equiv 0 \mod I(r,s) = (x^r, y^s),$$

that $\binom{\beta}{i} \equiv 0 \bmod p$ in the range $i = \beta - s + 1, \ldots, r-1$.

Now, $\binom{\beta}{i} = \binom{\beta-1}{i-1} + \binom{\beta-1}{i}$ implies that all coefficients $\binom{\beta-1}{i}$ for $i = \beta - s, \ldots, r-1$ are mutually congruent modulo p, up to sign, and thus are simultaneously $\equiv 0$ or $\not\equiv 0$ mod p.

We must have $\binom{\beta-1}{i} \not\equiv 0 \mod p$, for $i = \beta - s, \ldots, r-1$ since $(x+y)^{\beta-1} \notin I(r,s)$.

It follows that

$$\begin{aligned}(x-y)(x+y)^{\beta-1} &= (x+y)^\beta - 2y(x+y)^{\beta-1} \\ &\equiv -2\textstyle\sum_{i=\beta-s+1}^{r-1} \binom{\beta-1}{i} x^i y^{\beta-i} \not\equiv 0 \bmod (x^r, y^s),\end{aligned}$$

and thus $\gamma_p(r,s) = \beta_p(r,s)$ in the case $\binom{r+s-2}{r-1} \equiv 0 \bmod p$.

Suppose now that $r_i + s_i \leq p-1$ for all $i \geq 0$ in the p-adic expansions $r-1 = \sum_{i\geq 0} r_i p^i$ and $s-1 = \sum_{i\geq 0} s_i p^i$ of $r-1$ and $s-1$.

An easy calculation shows that, modulo $I(r,s) = (x^r, y^s)\mathbf{F}_p[x,y]$, and for $r+s \geq 3$, $r \geq s$, we have the congruence

$$(x-y)(x+y)^{r+s-3} \equiv \{\binom{r+s-3}{r-2} - \binom{r+s-3}{r-1}\} x^{r-1} y^{s-1}.$$

It follows easily that $\gamma_p(r,s) = r+s-2$ if $\binom{r+s-2}{r-1} \not\equiv 0 \bmod p$ and $\binom{r+s-3}{s-1} \not\equiv \binom{r+s-3}{r-1} \bmod p$.

Moreover, we see that $\gamma_p(r,s) \leq r+s-3$ if $\binom{r+s-2}{r-1} \not\equiv 0 \bmod p$ and $\binom{r+s-3}{s-1} \equiv \binom{r+s-3}{r-1} \bmod p$.

To prove that in this last case we have $\gamma_p(r,s) = r+s-3$, it suffices to show that $(x-y)(x+y)^{r+s-4} \not\equiv 0$ modulo the ideal $I(r,s) = (x^r, y^s)\mathbf{F}_p[x,y]$.

This is obvious for $r = s = 2$, and for $r \geq 3, s \geq 2$ an easy calculation shows that $(x-y)(x+y)^{r+s-4}$ is congruent modulo $I(r,s)$ to

$$\{\binom{r+s-4}{r-3} - \binom{r+s-4}{r-2}\}x^{r-2}y^{s-1} + \{\binom{r+s-4}{r-2} - \binom{r+s-4}{r-1}\}x^{r-1}y^{s-2}.$$

By a simple lemma on binomial coefficients, Lemma (6.5) of [**EK**2], the two coefficients in this expression could only both vanish if we had

$$\binom{r+s-4}{r-3} \equiv \binom{r+s-4}{r-2} \equiv \binom{r+s-4}{r-1} \equiv 0 \bmod p.$$

This would imply $\binom{r+s-2}{r-1} \equiv 0 \bmod p$, contrary to the hypothesis. This finishes our discussion of formulas (5) and (6).

As an application of the formulas, note that

$$\gamma_p(1+ap^h, 1+ap^h) = 2ap^h - 1, \quad \beta_p(1+ap^h, 1+ap^h) = 2ap^h + 1$$

if $1 \leq a \leq \frac{p-1}{2}$. We shall use these values in the next section.

3. The case of unequal sets

Let $A, B \subset V$ be subsets of a vector space V over $\mathbf{F}_p$, of cardinality $|A| = |B| = 1 + ap^h$.

The first step in our study of $\mu'_p(1+ap^h, 1+ap^h)$ is to show that it suffices to consider the instance in which $A = B$.

Indeed, we prove

Proposition (3.1) *Let the subsets $A, B \subset V$ both have cardinality $1 + ap^h$, where $h \geq 1$ and $1 \leq a \leq \frac{p-1}{2}$. If $A \neq B$ then*

$$|A +' B| \geq \gamma_p(1+ap^h, 1+ap^h) + 1 = 2ap^h.$$

Proof. Let $X = A \cap B$ and $Y = A \cup B$. If $X = \emptyset$, then $A +' B = A + B$ and

$$|A +' B| = |A + B| \geq \beta_p(1+ap^h, 1+ap^h) = 2ap^h + 1.$$

Assume now that $X \neq \emptyset$. Set $r = |X| \geq 1$, and thus $|Y| = 2ap^h + 2 - r$. We have $X +' Y \subset A +' B$. Therefore $|A +' B| \geq |X +' Y| \geq \gamma_p(r, 2ap^h + 2 - r)$.

We claim that for $1 \leq r \leq ap^h$ we have $\gamma_p(r, 2ap^h + 2 - r) = 2ap^h$.

We set

$$R = r \quad , \quad S = 2ap^h + 2 - r$$

and write the p-adic expansions

$$\begin{cases} R+S-2 &= & 2ap^h, \\ R-1 &= & r_0 + r_1 p + \ldots + r_{h-1}p^{h-1} + r_h p^h, \end{cases}$$

where $r_h < a$, since $X = A \cap B \subset A$ and $A \cap B \neq A$.

We have

$$\binom{R+S-2}{R-1} = \binom{2ap^h}{r-1} \equiv \binom{0}{r_0} \cdots \binom{0}{r_{h-1}} \cdot \binom{2a}{r_h} \mod p.$$

The only case where this number is $\not\equiv 0 \bmod p$ is when $r_0 = r_1 = \ldots = r_{h-1} = 0$, and thus $r = 1 + cp^h$, with $0 \leq c \leq a-1$.

Let us begin with this case. If $r = 1 + cp^h$, with $0 \leq c \leq a-1$, then, by formula (6), the value of $\gamma_p(R,S) = \gamma_p(r, 2ap^h + 2 - r)$ depends on whether the binomial coefficients $\binom{R+S-3}{R-1}$ and $\binom{R+S-3}{S-1}$ are congruent mod p or not.

We examine the p-adic expansions of $R+S-3$, $R-1$ and $S-1$.

$$\begin{cases} R+S-3 &= & \sum_{i=0}^{h-1}(p-1)p^i + (2a-1)p^h, \\ R-1 &= & cp^h, \\ S-1 &= & (2a-c)p^h. \end{cases}$$

By the formula of Lucas,

$$\binom{R+S-3}{R-1} \equiv \binom{2a-1}{c} \text{ and } \binom{R+S-3}{S-1} \equiv \binom{2a-1}{2a-c} \mod p.$$

Now, since $c < a \leq \frac{p-1}{2}$, we have $c \not\equiv a \bmod p$, and therefore

$$\gamma_p(r, 2ap^h + 2 - r) = r + (2ap^h + 2 - r) - 2 = 2ap^h,$$

in accordance with the claim.

There remains to examine the case where

$$r - 1 = r_0 + r_1 p + \ldots + r_{h-1}p^{h-1} + r_h p^h,$$

with $0 \leq r_h \leq a-1$ and $(r_0, r_1, \ldots, r_{h-1}) \neq (0, 0, \ldots, 0)$. We then have

$$\binom{R+S-2}{R-1} = \binom{2ap^h}{r-1} \equiv 0 \bmod p.$$

Hence $\gamma_p(r, 2ap^h + 2 - r) = \beta_p(r, 2ap^h + 2 - r)$.

We claim that $\beta_p(r, 2ap^h + 2 - r) = 2ap^h$.

Let $0 \leq m \leq h-1$ be the index defined by $r_0 = \ldots = r_{m-1} = 0$ and $r_m \neq 0$.

The p-adic expansions of $R-1$ and $S-1$ have the form

$$\begin{cases} R-1 &= & r_m p^m + & \sum_{i=m+1}^{h-1} r_i p^i + & r_h p^h, \\ S-1 &= & (p-r_m)p^m + & \sum_{i=m+1}^{h-1} (p-1-r_i)p^i + & (2a-1-r_h)p^h. \end{cases}$$

Therefore, we have $\beta_p(R,S) = (1 + [\frac{R-1}{p^{k+1}}] + [\frac{S-1}{p^{k+1}}])p^{k+1}$, where k is the largest index for which the sum of the coefficients of the p-adic expansions is larger than or equal to p.

It is easy to see that $k = m$. It follows that

$$\beta_p(R,S) \;=\; p^{m+1} + (p-1)p^{m+1} + \ldots + (p-1)p^{h-1} + (2a-1)p^h \;=\; 2ap^h.$$

This finishes the proof of the proposition. □

Henceforth, we shall be dealing with the restricted sumset of a single subset $A \subset V$ with itself, *i.e.*, $A +' A$.

4. Slicing the set A by hyperplanes

Our approach in order to get the sharp lower bound for $|A +' A|$ will consist in keeping track of the classes of elements of A and $A +' A$ modulo a chosen hyperplane $H \subset V$ and slicing the set A by the translates of H. Let $e \neq 0$ be a vector outside H, so that $V = \mathbf{F}_p e \oplus H$. For $c \in \mathbf{F}_p$, we denote by H_c the (affine) hyperplane $c \cdot e + H$ and let $A_c = A \cap H_c$. A translation of A does not change $|A +' A|$. Hence, we may assume that the size of $A_0 = A \cap H$ is maximal in the collection of sizes $\{|A_c|, c \in \mathbf{F}_p\}$. We set $r = |A_0|$.

Let $C = \{0, c_1, \ldots, c_\ell\}$ denote the set of classes $c \in \mathbf{F}_p$ such that $A_c \neq \emptyset$. We may also assume that the classes $c_1, \ldots, c_\ell$ are ordered so that $|A_0| \geq |A_{c_1}| \geq \ldots \geq |A_{c_\ell}| \geq 1$.

We use the notation $s_i = |A_{c_i}|$ for $1 \leq i \leq \ell$ and therefore we have the inequalities $r \geq s_1 \geq \ldots \geq s_\ell \geq 1$.

Note that, changing A to a homothetic set if necessary, we may also assume that $c_1 = 1$, so that $s_1 = |A_1|$.

We call $(r, s_1, \ldots, s_\ell)$ the *partition* of $|A|$ (or of A, by abuse of language) corresponding to the choice of H.

Since we may assume that A is not contained in any hyperplane of V, we may assume $1 \leq \ell \leq p-1$.

The case where $\ell = 1$, when $|A| = 1 + ap^h$, with $1 \leq a \leq \frac{p-1}{2}, h \geq 1$, can be treated at once. This special case will be used in the next section.

Proposition (4.1) *Suppose that the subset $A \subset V$ with cardinality $|A| = 1 + ap^h$ has a partition (r, s) of length 2. Then, unless $p = 3, a = 1, h = 1$, we have*

$$|A +' A| \ \geq \ 2ap^h \ = \ \gamma_p(1 + ap^h, 1 + ap^h) + 1.$$

Proof. By hypothesis, $A = A_0 \coprod A_1$, using the notational convention specified above. Let $r = |A_0|, s = |A_1|$.

We first take care of the case where $s = 1$.

We have $A +' A = (A_0 +' A_0) \coprod (A_0 + A_1)$ and therefore $|A +' A| \geq \gamma_p(ap^h, ap^h) + \beta_p(ap^h, 1)$.

The p-adic expansion of $ap^h - 1$ is

$$ap^h - 1 \ = \ \sum_{i=0}^{h-1}(p-1)p^i + (a-1)p^h.$$

Therefore, $\gamma_p(ap^h, ap^h) = \beta_p(ap^h, ap^h) = p^h + 2(a-1)p^h$.

Since $\beta_p(ap^h, 1) = ap^h$, it follows that

$$|A +' A| \geq p^h + 2(a-1)p^h + ap^h = 2ap^h + (a-1)p^h \geq 2ap^h,$$

with equality if and only if $a = 1$.

Suppose now that $s \geq 2$. We have

$$A +' A \ = \ (A_0 +' A_0) \coprod (A_0 + A_1) \coprod (A_1 +' A_1),$$

where the sets are disjoint because they belong to distinct hyperplanes, namely H, $H_1 = e + H$ and $H_2 = 2e + H$ respectively.

We shall evaluate the right-hand side of the resulting inequality

$$|A +' A| \ \geq \ \gamma_p(r, r) + \beta_p(r, s) + \gamma_p(s, s).$$

Let $r - 1 = \sum_{i=0}^{h} r_i p^i$ be the p-adic expansion of $r - 1$. Since $1 + ap^h = r + s$, we have $s - 1 = (ap^h - 1) - (r - 1)$. This yields the p-adic expansion of $s - 1$ as follows:

$$s - 1 = \sum_{i=0}^{h} s_i p^i = \sum_{i=0}^{h-1}(p - 1 - r_i)p^i + (a - 1 - r_h)p^h,$$

where $0 \leq a - 1 - r_h$ because $r - 1 < ap^h$ and hence $r_h \leq a - 1$.

As a first consequence, we get $\beta_p(r,s) = r+s-1$ by formula (5). Indeed, $r_i+s_i = p-1$, for $i = 0, \ldots, h-1$ and $r_h + s_h = a - 1 < p - 1$. Thus $\beta_p(r,s) = ap^h$.

By the formula (6) above, we have for $t = r$ or s and $t_i = r_i$ or $t_i = s_i$, respectively,

$$\gamma_p(t,t) = \begin{cases} 2t-3 & \text{if } 2t_i \le p-1 \text{ for all } i \in [0,h] \\ p^{m+1} + 2\sum_{i=m+1}^{h} t_i p^i & \text{otherwise,} \end{cases}$$

where $m = \max(\{-1\} \cup \{i \in [0,h] \mid 2t_i \ge p\})$.

We want to evaluate $\tau = \gamma_p(r,r) + \beta_p(r,s) + \gamma_p(s,s)$.

There are 2 cases for each of r and s, and thus 4 cases altogether.

• If $2r_i \le p-1$ and $2s_i \le p-1$ for all $i \in [0,h]$, then $\gamma_p(r,r) = 2r-3$ and $\gamma_p(s,s) = 2s-3$. Note that this case occurs only if $r = 1 + \frac{p^h-1}{2} + r_h p^h$ and $s = 1 + \frac{p^h-1}{2} + (a-1-r_h)p^h$.

Then, $\tau = \gamma_p(r,r) + \beta_p(r,s) + \gamma_p(s,s) = 2r - 3 + ap^h + 2s - 3 = 2ap^h + (ap^h - 4)$.

Thus, $\tau > 2ap^h$ except for $a = 1, p = 3, h = 1$ as we already know.

• If $2r_i \le p-1$ for all $i = 0, \ldots, h$, but $r_j < \frac{p-1}{2}$ for at least one index j, then necessarily $j \le h-1$, and $2s_j = 2(p-1-r_j) \ge p$. Therefore

$$\gamma_p(s,s) \;=\; s + \textstyle\sum_{i=m+1}^{h-1}(p-1-r_i)p^i + (a-1-r_h)p^h + (p^{m+1} - 1 - \sum_{i=0}^{m} s_i p^i),$$

and so

$$\gamma_p(s,s) \;\ge\; s + (a-1-r_h)p^h.$$

Hence,

$$\begin{aligned} \tau &\ge 2r - 3 + ap^h + s + (a-1-r_h)p^h \\ &\ge (r-2) + 2ap^h + (a-1-r_h)p^h \\ &\ge 2ap^h. \end{aligned}$$

• The case where there exists an index $m \in [0, h-1]$ such that $2r_m \ge p$ and $2r_i \le p-1$ for $i \in [m+1, h]$, and where $2s_i \le p-1$ for all $i = 0, \ldots, h-1, h$ is quite symmetrical. Then, $\tau \ge r + \sum_{i=m+1}^{h} r_i p^i + ap^h + 2s - 3$. Thus, $\tau \ge 2ap^h + (s-2) + \sum_{i=m+1}^{h} r_i p^i$. This is strictly larger than $2ap^h$, even if $s = 2$.

• Finally, if there exist m and n such that $2r_m \ge p$ and $2s_n \ge p$, and m, n are the maximal indices with this property, then

$$\tau \ge r + \sum_{i=m+1}^{h} r_i p^i + ap^h + s + \sum_{i=n+1}^{h} s_i p^i.$$

Thus, clearly, $\tau \ge 2ap^h + 1$. □

5. The value of $\mu'_3(1+3^h, 1+3^h)$

In this section we take $p = 3$ and since $\mu'_3(4,4) = \gamma_3(4,4) = 5$, we assume $h \geq 2$.

Theorem (5.1) *For $h \geq 2$, we have $\mu'_3(1+3^h, 1+3^h) = 2 \cdot 3^h$.*

Proof.

Step 1. Unequal sets A and B.

Let A, B be subsets of cardinality $1+3^h$ in some vector space V over $\mathbf{F}_3$. We claim that $|A +' B| \geq 2 \cdot 3^h$. If $A \neq B$, this is just Proposition (3.1) with $p = 3$, and $a = 1$.

Thus, from now on, we assume that $B = A$.

Let (r, s, t) be the partition of $1+3^h$ associated with some decomposition $V = \mathbf{F}_3 \cdot e \oplus H$, *i.e.*, $r = |A \cap H|$, $s = |A \cap H_1|$, $t = |A \cap H_2|$, where $H_i = i \cdot e + H$. We may assume that $e \in A$ and $r \geq s \geq t$. As above, we set $A_i = A \cap H_i$. Of course $A = A_0 \coprod A_1 \coprod A_2$.

Step 2. Partitions of length 2.

If $t = 0$, it follows from Proposition (4.1) that

$$|A +' A| \geq 2 \cdot 3^h,$$

as desired.

The proof in the case where $r \geq s \geq t \geq 1$ involves an induction on h in the case of a flat partition. In this section, we call *flat partition* a partition with $r = 1 + 3^{h-1}$. Note that this is the smallest possible value of r since $r \geq s \geq t$ and $r + s + t = 1 + 3^h$. There are two flat partitions for $h = 2$, namely $(4, 4, 2)$ and $(4, 3, 3)$. They will be treated in step 4.

Step 3. Not too flat partitions of length 3.

Suppose that the partition (r, s, t) of $1 + 3^h$ satisfies

$$2 + 3^{h-1} \ \leq \ r \ \leq \ 3^h - 1,$$

and of course $r \geq s \geq t \geq 1$.

We have

$$A +' A \supset (A_0 +' A_0) \coprod (A_0 + A_1) \coprod (A_0 + A_2)$$

and therefore,

$$\begin{aligned} |A +' A| &\geq |A_0 +' A_0| + |A_0 + A_1| + |A_0 + A_2| \\ &\geq \gamma(r, r) + \beta(r, s) + \beta(r, t), \end{aligned}$$

where we write γ and β for γ_3 and β_3 respectively to simplify notation.

Assertion. *In the above range for the parameters (r, s, t), namely* $2+3^{h-1} \le r \le 3^h-1$, *and* $r \ge s \ge t \ge 1$, *we have* $\gamma(r,r)+\beta(r,s)+\beta(r,t) \ge 2\cdot 3^h+1$.

We first write the 3-adic expansions of $r-1$, $s-1$ and $t-1$:

$$\begin{aligned} r-1 &= r_0 + r_1 3 + \ldots + r_{h-2}3^{h-2} + 3^{h-1}, \\ s-1 &= s_0 + s_1 3 + \ldots + s_{h-2}3^{h-2} + s_{h-1}3^{h-1}, \\ t-1 &= t_0 + t_1 3 + \ldots + t_{h-2}3^{h-2} + t_{h-1}3^{h-1}. \end{aligned}$$

In order to calculate $\beta(r,s)$ and $\beta(r,t)$ using formula (5) in Section 2, we set $m = \max(\{-1\} \cup \{i \in [0,h-1] \mid\ r_i + s_i \ge 3\})$. Similarly, we also need $n = \max(\{-1\} \cup \{i \in [0,h-1] \mid\ r_i + t_i \ge 3\})$.

Note that $m \le h-2$ and $n \le h-2$ because $s,t \le r$.

By formulas (5) and (6) or (7), we have

$$\gamma(r,r) = \begin{cases} \text{(a)} & 2r-3, \\ & \text{if } r_i \le 1 \text{ for all } i = 0,\ldots,h-2 \\ \\ \text{(b)} & 3^{\ell+1} + 2(\sum_{i=\ell+1}^{h-2} r_i 3^i) + 2\cdot 3^{h-1}, \\ & \text{if } r_\ell = 2 \text{ and } r_i \le 1 \text{ for } i \ge \ell+1 \end{cases}$$

and

$$\beta(r,s)+\beta(r,t) \;=\; 3^{m+1} + \sum_{i=m+1}^{h-1}(r_i+s_i)3^i + 3^{n+1} + \sum_{i=n+1}^{h-1}(r_i+t_i)3^i,$$

where $r_{h-1} = 1$.

We set $\sigma = \gamma(r,r)+\beta(r,s)+\beta(r,t)$ and claim that $\sigma \ge 1 + 2\cdot 3^h$.

Suppose first that $r_i \le 1$ for all indices $i = 0,\ldots,h-1$ in the 3-adic expansion of $r-1$, so that case (a) prevails in the formula above for $\gamma(r,r)$. Then,

$$\begin{aligned} \sigma &\ge 2r-3+s+\textstyle\sum_{i=m+1}^{h-1} r_i 3^i + t + \sum_{i=n+1}^{h-1} r_i 3^i \\ &\ge (r-2) + (r+s+t-1) + 2\cdot 3^{h-1} = r-2+3^h+2\cdot 3^{h-1}. \end{aligned}$$

Since $r \ge 2+3^{h-1}$, we get $\sigma \ge 2\cdot 3^h$.

Note however that for $r = 2+3^{h-1}$, the only possibilities for the pair (s,t) are $(2+3^{h-1}, -3+3^{h-1})$ if $h \ge 3$, and $(1+3^{h-1}, -2+3^{h-1})$, $(3^{h-1}, -1+3^{h-1})$, for $h \ge 2$.

For $h = 2$, we have the partitions $(5,4,1)$ and $(5,3,2)$ which give respectively $\sigma = 20 = 2+2\cdot 3^h$ and $\sigma = 19 = 1+2\cdot 3^h$.

For $h = 3$, the three partitions $(2+3^{h-1}, 2+3^{h-1}, -3+3^{h-1})$, $(2+3^{h-1}, 1+3^{h-1}, -2+3^{h-1})$, $(2+3^{h-1}, 3^{h-1}, -1+3^{h-1})$, give respectively $\sigma = 1+2\cdot 3^h$, $2+2\cdot 3^h$, and $1+2\cdot 3^h$.

Hence, in case (a), we have indeed $\sigma \geq 2 \cdot 3^h$.

Suppose now that we are in case (b) in the formula above for $\gamma(r,r)$. Then, still with $\sigma = \gamma_p(r,r) + \beta_p(r,s) + \gamma_p(s,s)$, we have

$$\begin{aligned}\sigma &= \gamma(r,r) + \beta(r,s) + \beta(r,t) \\ &= 3^{\ell+1} + 2(\textstyle\sum_{i=\ell+1}^{h-1} r_i 3^i) + 3^{m+1} + \sum_{i=m+1}^{h-1}(r_i+s_i)3^i + 3^{n+1} + \sum_{i=n+1}^{h-1}(r_i+t_i)3^i\end{aligned}$$

where as before $r_{h-1} = 1$.

Replacing one copy of $\sum_{i=\ell+1}^{h-1} r_i 3^i$ in the first summation by the equal quantity $r-1-\sum_{i=0}^{\ell} r_i 3^i$, and similarly, $\sum_{i=m+1}^{h-1} s_i 3^i$ by $s-1-\sum_{i=0}^{m} s_i 3^i$ and $\sum_{i=n+1}^{h-1} t_i 3^i$ by $t-1-\sum_{i=0}^{n} t_i 3^i$, we get

$$\begin{aligned}\sigma &= r+s+t-3+\textstyle\sum_{i=\ell+1}^{h-1} r_i 3^i + (3^{\ell+1} - \sum_{i=0}^{\ell} r_i 3^i) \\ &\quad + \textstyle\sum_{i=m+1}^{h-1} r_i 3^i + (3^{m+1} - \sum_{i=0}^{m} s_i 3^i) \\ &\quad + \textstyle\sum_{i=n+1}^{h-1} r_i 3^i + (3^{n+1} - \sum_{i=0}^{n} t_i 3^i).\end{aligned}$$

Now, $r+s+t = 3^h+1$. Since $\ell, m, n \leq h-2$, the three summations $\sum_{i=\ell+1}^{h-1} r_i 3^i$, $\sum_{i=m+1}^{h-1} r_i 3^i$ and $\sum_{i=n+1}^{h-1} r_i 3^i$ each actually contain $r_{h-1}3^{h-1} = 3^{h-1}$, and their sum is not smaller than 3^h. Finally, all three terms of the form $3^{k+1} - \sum_{i=0}^{k} u_i 3^i$, with $(k, u_i) = (\ell, r_i)$, (m, s_i) and (n, t_i) respectively, are at least 1.

Summarizing, we get $\gamma(r,r) + \beta(r,s) + \beta(r,t) \ \geq \ 2 \cdot 3^h + 1$ also in the case encoded as (b).

Step 4. Flat partitions.

The argument will proceed by induction on h, starting with $h = 2$.

The induction step is very simple. The main difficulty will consist in the analysis of the case $h = 2$. As already noted above, for $h = 2$ there are two flat partitions, namely $(4,4,2)$ and $(4,3,3)$. Unfortunately, we do not have a more conceptual treatment of these two cases than brute force calculation.

We begin with the partition $(4,4,2)$.

Since

$$A +' A \ \supset \ (A_0 +' A_0) \coprod (A_0 + A_1) \coprod (A_0 + A_2),$$

and $\gamma_3(4,4) = 5$, $\beta_3(4,4) = 7$, $\beta_3(4,2) = 5$ with sum 17, the assertion $|A +' A| \geq 18$ follows if any of the three sets $A_0 +' A_0$, $A_0 + A_1$, $A_0 + A_2$ has a cardinality exceeding its lower bound $\gamma_3(4,4)$, $\beta_3(4,4)$, $\beta_3(4,2)$ respectively.

We will show that if $|A_0 +' A_0| = 5$, then $|A_0 + A_2| \geq \beta_3(4,2) + 1 = 6$. We express

this in a slightly more general statement :

Lemma (5.2) *Let X, Y be subsets of a vector space over $\mathbf{F}_3$. Assume $|X| = 4$, $|Y| = 2$ and $|X +' X| = 5$. Then, $|X + Y| \geq 6$.*

Proof. We may assume that $0 \in X$ by translating X if necessary. Note that X, being of cardinality 4, must contain two linearly independent vectors e_1, e_2. Thus, X has the form $X = \{0, e_1, e_2, v\}$.

We now show that by proper choice of e_1, e_2, we may assume $v = e_1 + e_2$. Indeed,

$$X +' X \ = \ \{e_1, e_2, e_1 + e_2, v, e_1 + v, e_2 + v\},$$

and $|X +' X| = 5$ implies that exactly two of these vectors must coincide, *i.e.*, one of them is redundant.

If $e_2 + v$ is redundant, we must have $e_2 + v = e_1$. Equality with any one of the other vectors leads to a contradiction with $v \neq 0, v \neq e_1, e_2 \neq 0$, or $e_1 \neq e_2$. We set $e_1' = v = e_1 - e_2$, $e_2' = e_2$. Then, $X = \{0, e_1', e_2', e_1' + e_2'\}$. Similarly, if $e_1 + v$ is redundant, *i.e.*, $e_1 + v \in \{e_1, e_2, e_1 + e_2, v, e_2 + v\}$, then $e_1 + v = e_2$ and X can be written as $X = \{0, e_1', e_2', e_1' + e_2'\}$ with $e_1' = e_1$, and $e_2' = v$. If v is redundant, we must have $v = e_1 + e_2$. In all cases we can rename the elements of X so that $X = \{0, e_1, e_2, e_1 + e_2\}$. Thus,

$$X +' X \ = \ \{e_1, e_2, e_1 + e_2, 2e_1 + e_2, e_1 + 2e_2\}.$$

Now, we may also assume $0 \in Y$, as Y may be translated independently of X.

Set $Y = \{0, y\}$. If y were linearly independent of the plane $[e_1, e_2]$, the set $X + Y$ would obviously have cardinality 8.

Without loss of generality, we may assume that $y = e_1 + \lambda e_2$, for some $\lambda \in \mathbf{F}_3$. Indeed, we may interchange e_1, e_2 and may change the sign of y by a translation of Y, since $\{0, y\} + \{-y\} = \{0, -y\}$.

But now, $X + Y$ contains the six distinct elements 0, e_1, e_2, $e_1 + e_2$, $-e_1 + \lambda e_2$, $-e_1 + (\lambda + 1)e_2$. □

This finishes the case of a partition of type (4,4,2).

Suppose now that the partition of A is of type $(4, 3, 3)$, *i.e.*, $|A_0| = 4$, $|A_1| = |A_2| = 3$. We have

$$A +' A \supset ((A_0 +' A_0) \cup (A_1 + A_2)) \coprod (A_0 + A_1) \coprod (A_0 + A_2)$$

and thus $|A +' A| \geq 18$ except perhaps if $|(A_0 +' A_0) \cup (A_1 + A_2)| = 5$, and $|A_0 + A_1| = |A_0 + A_2| = 6$.

Assuming $|A_0 +' A_0| = 5$, the same argument as in the lemma above shows that $A_0 = \{0, e_1, e_2, e_1 + e_2\}$. Furthermore, we may assume the inclusion $A_1 + A_2 \subset A_0 +' A_0$.

Keeping the same notation as above, we assume $V = \mathbf{F}_3 \cdot e \oplus H$, where $e \in A_1$.

Set $A_2 = 2e + \{x, y, z\}$ with distinct $x, y, z \in H$. Since $x, y, z \in A_1 + A_2$, e.g., $x = e + (2e + x) \in A_1 + A_2$, we must have

$$x, y, z \in A_0 +' A_0 = \{e_1, e_2, e_1 + e_2, e_1 + 2e_2, 2e_1 + e_2\}.$$

Each of the $\binom{5}{3} = 10$ choices for the triple (x, y, z) furnishes a set $A_0 + A_2$ of cardinality 8 except the 2 choices $x = e_1, y = e_1 + e_2, z = e_1 + 2e_2$ and $x = e_2, y = e_1 + e_2, z = 2e_1 + e_2$. The two choices are in fact equivalent, up to interchange of e_1 and e_2.

The choice $x = e_1, y = e_2, z = e_1 + e_2$ for example, produces

$$A_0 + A_2 \ = \ \{e_1, e_2, e_1 + e_2, 2e_1, 2e_2, 2(e_1 + e_2), e_1 + 2e_2, 2e_1 + e_2\}.$$

The exceptional choice $x = e_1, y = e_1 + e_2, z = e_1 + 2e_2$ on the other hand, yields

$$\begin{cases} A_0 &= \{0, e_1, e_2, e_1 + e_2\} \\ A_1 &= e_0 + \{0, u, v\} \\ A_2 &= 2e_0 + \{e_1, e_1 + e_2, e_1 + 2e_2\}. \end{cases}$$

We must have $A_1 + A_2 \subset A_0 +' A_0 = \{e_1, e_2, e_1 + e_2, e_1 + 2e_2, 2e_1 + e_2\}$. We see then, by examining the possible candidates for $u + e_1$ and $v + e_1$, that u and v must belong to the set $\{e_2, 2e_1 + e_2, e_1 + e_2, 2e_2\}$. In fact, neither u nor v can be equal to $2e_1 + e_2$ or $e_1 + e_2$, since then $e_1 + e_2 + u$ or $e_1 + e_2 + v$ would be equal to $2e_2$ or $2(e_1 + e_2)$, none of which belongs to $A_0 +' A_0$.

The only remaining possibility is $\{u, v\} = \{e_2, 2e_2\}$. But, since $u \neq v$, this would imply $u + v = 0$ and $2e \in A_1 +' A_1$. However, $A_0 + A_2$ does not contain $2e$.

Hence, if $A \subset V$, a vector space over $\mathbf{F}_3$, has cardinality 10 and possesses a partition of type (4, 4, 2) or (4, 3, 3), then $|A +' A| \geq 18$.

We now finish up the case of flat partitions for $h \geq 3$ by induction on h. Suppose H is a hyperplane such that $A_0 = A \cap H$ has cardinality $r = 1 + 3^{h-1}$ and $r \geq s \geq t$, where as before r, s, t are the cardinalities of the intersections of A with the various translates of H.

Claim. *Suppose by induction on $h \geq 3$ that $|A_0 +' A_0| \geq 2 \cdot 3^{h-1}$. Then, we have $|A +' A| \geq 2 \cdot 3^h$.*

Proof. Since we assume $r = 1 + 3^{h-1}$ and $|A| = 1 + 3^h$ there are only two possible partitions:

$$\begin{array}{lll} (1) & (r, s, t) &= (3^{h-1} + 1, 3^{h-1}, 3^{h-1}), \\ (2) & (r, s, t) &= (3^{h-1} + 1, 3^{h-1} + 1, 3^{h-1} - 1), \end{array}$$

and we have

$$|A +' A| \geq |A_0 +' A_0| + \beta(r, s) + \beta(r, t).$$

Using the 3-adic expansions of $r-1, s-1$, and $t-1$, we get in both cases $\beta(r,s) = r+s-1$ and $\beta(r,t) = r+t-1$.

Of course, in both cases $s+t = 2\cdot 3^{h-1}$ since $r+s+t = |A| = 1+3^h$.

Therefore, the induction assumption on $|A_0 +' A_0|$ yields

$$|A +' A| \geq 2\cdot 3^{h-1} + 4\cdot 3^{h-1} = 2\cdot 3^h.$$

This finishes the proof of the claim and of Theorem (5.1). □

Summarizing our knowledge of $\mu'_3(r,s)$, if $r = 1+3+\sum_{i\geq 2} r_i 3^i$ and $s = 1+3+\sum_{i\geq 2} s_i 3^i$ form a special pair (*i.e.*, $r_i + s_i \leq 2$ for all $i \geq 2$), we have $\mu'_3(r,s) = r+s-3$.

If (r,s) is a special pair for $p=3$ but $r \equiv s \equiv 1 \bmod 9$, then the only case for which we know $\mu'_3(r,s)$ is $r = s = 1+3^h$, namely $\mu'_3(r,s) = r+s-2$ as proved in this paper. In all other cases, $r = 1+3^h+\sum_{i\geq h+1} r_i 3^i$ and $s = 1+3^h+\sum_{i\geq h+1} s_i 3^i$ forming a special pair with $h \geq 2$ and $(r,s) \neq (1+3^h, 1+3^h)$, it remains an open problem to decide whether $\mu'_3(r,s)$ equals $r+s-3$ or $r+s-2$.

If, still with $p=3$, (r,s) is not a special pair at $p=3$, then $\mu'_3(r,s) = \gamma_3(r,s)$ as given by formula (6) or (7).

Acknowledgments

During the preparation of this paper, the first author has partly benefited from a research contract with the Fonds National Suisse pour la Recherche Scientifique.

References

[**ANR**1] N. Alon, M. B. Nathanson and I. Z. Ruzsa, Adding Distinct Congruences Classes Modulo a Prime, *American Math. Monthly* **102** (1995), 250-255.

[**ANR**2] N. Alon, M. B. Nathanson and I. Z. Ruzsa, The polynomial method and restricted sums of congruences classes, *Journal of Number Theory* **56** (1996), 404-417.

[**DH**] J. A. Dias da Silva and Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (1994), 140-146.

[**EK**1] S. Eliahou and M. Kervaire, Sumsets in vector spaces over a finite field, *Journal of Number Theory* **71** (1998), 12-39.

[**EK**2] S. Eliahou and M. Kervaire, Restricted sums of sets of cardinality $1+p$ in a vector space over $\mathbf{F}_p$, Preprint, Université du Littoral Côte d'Opale, Cahiers du LMPA Joseph Liouville No. 75 (1998). To appear in *Discrete Mathematics*.