Pré-Publicações do Departamento de Matemática
Universidade de Coimbra
Preprint Number 10–41

PAIRS OF SETS WITH SMALL SUMSET AND SMALL PERIODIC PRODUCT-SET

CRISTINA CALDEIRA

Dedicated to J.A. Dias da Silva

ABSTRACT: We characterize the pairs (A, B) of finite non-empty subsets of a field such that $|A + B| = \min\{p, |A| + |B| - 1\}$ and $|AB| = \max\{|A|, |B|\}$.

KEYWORDS: Sumset, product-set, cardinality.
AMS SUBJECT CLASSIFICATION (2010): 11P70.

1. Introduction

Let $\mathbb{F}$ be a field and p its characteristic in nonzero characteristic, $p = +\infty$ otherwise. We denote $\mathbb{F} \setminus \{0\}$ by $\mathbb{F}^*$.

Let $A \neq \{0\}$ and $B \neq \{0\}$ be two non-empty finite subsets of $\mathbb{F}$. The sumset of A and B is the set $A + B = \{a + b : a \in A \text{ and } b \in B\}$ and the product-set is $AB = \{ab : a \in A \text{ and } b \in B\}$. When $\mathbb{F} = \mathbb{Z}_p$, Cauchy-Davenport Theorem [2, 3, 4] establishes a lower bound for the cardinality of $A + B$:

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

In [5] Dias da Silva and Hamidoune proved that this result holds for any field.

For the product-set the trivial lower bound $|AB| \geq \max\{|A|, |B|\}$ is best possible. Equality holds, for instance, when A and B are cosets associated to the same subgroup of $(\mathbb{F}^*, \cdot)$.

We characterize the pairs (A, B) of finite non-empty subsets of $\mathbb{F}$ such that $|A + B| = \min\{p, |A| + |B| - 1\}$ and $|AB| = \max\{|A|, |B|\}$.

Received October 11, 2010.
This research was done within the activities of “Centro de Matemática da Universidade de Coimbra/FCT”.

2. Polynomials whose roots are arithmetic or geometric progressions

Let $u, d \in \mathbb{F}$ and $k \in \mathbb{N}$. We denote by $B^{(k)}(u,d)$ the $k \times k$ upper-triangular matrix with elements in $\mathbb{F}$, such that its (i,j)-entry is

$$b_{i,j}^{(k)} = \begin{cases} k+1-i & \text{if } \ i=j \\ (-d)^{j-i-1}\left[(u-d)\binom{j}{i} + d\binom{j+1}{i}\right] & \text{if } \ i<j \\ 0 & \text{if } \ i>j\,. \end{cases}$$

Notice that, for $k < p$, $B^{(k)}(u,d)$ is invertible.

We denote by $C^{(k)}(u,d)$ the vector in $\mathbb{F}^k$ with i-entry given by

$$c_i^{(k)} = (-d)^{k-i}\left(u\binom{k+1}{i} + d\binom{k+1}{i-1}\right)\,, \qquad \text{for } i = 1, \ldots, k\,.$$

Next we present a characterization for the coefficients of a monic polynomial whose roots are a given arithmetic progression.

Proposition 1. *Let $u, d \in \mathbb{F}$, $n \in \mathbb{N}$ be such that $d \neq 0$ and $n \leq p$. The roots of the polynomial $X^n - \sum_{i=0}^{n-1} A_i X^i \in \mathbb{F}[X]$ are $u, u+d, \ldots, u+(n-1)d$ if and only if $A_0 = (-1)^n \prod_{i=0}^{n-1}(u+id)$ and $B^{(n-1)}(u,d)[A_1 \cdots A_{n-1}]^T = C^{(n-1)}(u,d)$.*

Proof: Suppose $X^n - \sum_{i=0}^{n-1} A_i X^i = \prod_{i=0}^{n-1}(X-u-id)$. Obviously, $A_0 = (-1)^n \prod_{i=0}^{n-1}(u+id)$ and

$$\begin{aligned} \prod_{i=-1}^{n-1}(X-u-id) &= (X-u+d)\left(X^n - \sum_{i=0}^{n-1} A_i X^i\right) \\ &= X^{n+1} + \sum_{i=0}^{n}\left[(u-d)A_i - A_{i-1}\right]X^i\,, \end{aligned}$$

where $A_{-1} := 0$ and $A_n := -1$.

Consider $Y = X + d$. Then

$$\prod_{i=0}^{n}(Y-u-id) = (Y-d)^{n+1} + \sum_{i=0}^{n}\left[(u-d)A_i - A_{i-1}\right](Y-d)^i$$

$$\Leftrightarrow \quad (Y-u-nd)\sum_{j=0}^{n} -A_jY^j =$$

$$(Y-d)^{n+1} + \sum_{i=0}^{n}\left[(u-d)A_i - A_{i-1}\right](Y-d)^i \,. \qquad (1)$$

Comparing the coefficients of Y^j in both sides of (1) we obtain

$$(n-j)dA_j + \sum_{i=j+1}^{n-1}(-1)^{i-j+1}d^{i-j}\left[d\,\binom{i+1}{j} + (u-d)\,\binom{i}{j}\right]A_i =$$

$$= (-1)^{n-j+1}d^{n-j}\left[d\,\binom{n+1}{j} + (u-d)\,\binom{n}{j}\right], \qquad j = 1,\dots,n-1\,,$$

that is,

$$\sum_{i=j}^{n-1} b_{ji}^{(n-1)}A_i = c_j^{(n-1)}\,, \qquad j = 1,\dots,n-1\,.$$

Reciprocally, let $q(X) = X^n - \sum_{i=0}^{n-1} A_iX^i$, where $A_0 = (-1)^n\prod_{i=0}^{n-1}(u+id)$ and $B^{(n-1)}(u,d)[A_1\cdots A_{n-1}]^T = C^{(n-1)}(u,d)$.

Consider $t(X) = \prod_{i=0}^{n-1}(X-u-id) = X^n - \sum_{i=0}^{n-1} B_iX^i$. Of course $B_0 = A_0$ and, from what we have already proved, $[B_1B_2\cdots B_{n-1}]^T$ is a solution of the system $B^{(n-1)}(u,d)x = C^{(n-1)}(u,d)$. Since $p > n-1$, matrix $B^{(n-1)}(u,d)$ is invertible and so $A_i = B_i$, for $i = 1,\dots,n-1$. ■

In the next proposition we present an explicit characterization for the coefficients of a polynomial whose roots are a given geometric progression. As a corollary we obtain, for finite p, a result on certain subgroups of $\{1,\dots,p-1\}$ in the multiplicative group of the field $\mathbb{F}$. This corollary is used in section 4.

Proposition 2. *Let $u, r \in \mathbb{F}^*$, $n \in \mathbb{N}$ be such that $r \neq 1$. Then*

$$\prod_{i=0}^{n-1}(X-ur^i) = X^n + \sum_{i=1}^{n-1} d_i^{(n)}(u,r)X^i + (-u)^n r^{\frac{n(n-1)}{2}}\,,$$

where

$$d_i^{(n)}(u,r) = (-u)^{n-i} r^{\frac{(n-i)(n-i-1)}{2}} \prod_{j=1}^{\min\{i,n-i\}} \frac{1-r^{n-j+1}}{1-r^j}\,, \quad i=1,\ldots,n-1\,.$$

Proof: It is a matter of straight forward calculations to prove that, for $n \geq 2$, $d_1^{(n+1)}(u,r) = (-u)^n r^{\frac{n(n-1)}{2}} - ur^n d_1^{(n)}(u,r)$, $d_n^{(n+1)}(u,r) = d_{n-1}^{(n)}(u,r) - ur^n$ and

$$d_i^{(n+1)}(u,r) = d_{i-1}^{(n)}(u,r) - ur^n d_i^{(n)}(u,r)\,, \quad i=2,\ldots,n-1\,.$$

The result follows by induction on n. ∎

Corollary 1. *Suppose p is finite and $p > 2$. Let $H = < h > \neq \{1\}$ be a subgroup of $\{1,2,\ldots,p-1\}$ in the multiplicative group of the field $\mathbb{F}$. Then*

$$H = \{1\} \dot\cup \{1 + |H|\, h^j : j = 1,\ldots,|H|-1\}$$

if and only if $H = \{1, p-1\}$ or $H = \{1,2,\ldots,p-1\}$.

Proof: It is trivial to prove that $\{1, p-1\}$ and $\{1,2,\ldots,p-1\}$ satisfy the desired condition. Suppose $H = \{1\}\dot\cup\{1 + th^j : j = 1,\ldots,t-1\}$ where $t = |H| \geq 3$. Then the polynomials in $\mathbb{F}[X]$

$$f(X) = \prod_{j=1}^{t-1}(X - h^j) = \frac{X^t - 1}{X-1} = \sum_{i=0}^{t-1} X^i \qquad \text{and} \qquad g(X) = \prod_{j=1}^{t-1}(X - 1 - th^j)$$

coincide.

First we consider the case $t = 3$. The coefficients of X^0 in $f(X)$ and $g(X)$ are, respectively, 1 and $(-1-3h)(-1-3h^2)$. From $h^3 = 1$ and $h \neq 1$ we get $h^2 + h + 1 = 0$. Then, from $1 = (-1-3h)(-1-3h^2)$ it follows that $6 \equiv 0 (\text{mod } p)$, which is absurd, since $t = 3$ and $t | p-1$.

Next we suppose $t > 3$. Since

$$\begin{aligned} g(X) &= \prod_{j=1}^{t-1}[(X-1) - th^j] \\ &= (X-1)^{t-1} + \sum_{i=1}^{t-2} d_i^{(t-1)}(th,h)(X-1)^i + (-th)^{t-1} h^{\frac{(t-1)(t-2)}{2}}\,, \end{aligned}$$

the coefficient of X^{t-3} in $g(X)$ coincides with the coefficient of X^{t-3} in

$$(X-1)^{t-1} + d_{t-2}^{(t-1)}(th,h)(X-1)^{t-2} + d_{t-3}^{(t-1)}(th,h)(X-1)^{t-3}\,.$$

Hence, the coefficient of X^{t-3} in $g(X)$ is

$$\begin{cases} 8h\,\frac{1-h^3}{1-h}(2h^2+1)+3 & \text{if} \quad t=4 \\ \\ th\,\frac{1-h^{t-1}}{1-h}\left(th^2\,\frac{1-h^{t-2}}{1-h^2}+t-2\right)+\frac{(t-1)(t-2)}{2} & \text{if} \quad t\geq 5 \end{cases} . \tag{2}$$

If $t=4$ then $\operatorname{ord} h=4$ and, from $h^4=1 \Leftrightarrow (h^2-1)(h^2+1)=0$, it follows that $h^2=-1$. Then, making (2) equal to 1, we have $10\equiv 0(\bmod p)$. Hence $p=5$ and $H=\{1,2,3,4\}$.

If $t\geq 5$, since

$$h\,\frac{1-h^{t-1}}{1-h}=h+h^2+\cdots+h^{t-1}=-1$$

and

$$h^2\frac{1-h^{t-2}}{1-h^2}=\frac{h^2}{1+h}(1+h+\cdots+h^{t-3})=-\frac{h^t+h^{t+1}}{1+h}=-1\,,$$

we obtain $t(t+1)\equiv 0(\bmod p)$. From $t\mid p-1$, it follows that $t=p-1$ and $H=\{1,\ldots,p-1\}$. ■

3. Auxiliary results

In this section we begin by presenting, for the benefit of the reader, two known results on the cardinalities of $A+B$ and AB, respectively. The first one is just a generalization of Vosper's Theorem [10, 11] to the additive group of an arbitrary field. The second is a trivial corollary from Kneser's Theorem. As before, $\mathbb{F}$ is a field and p its characteristic in nonzero characteristic, $p=+\infty$ otherwise.

Proposition 3. [1, Lemma 2.6] *Let A and B be finite nonempty subsets of $\mathbb{F}$.*

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

if and only if one of the following alternatives holds:

- **(1):** $1=|A|\leq|B|\leq p$ *or* $1=|B|\leq|A|\leq p$*;*
- **(2):** *A and B are arithmetic progressions with the same difference;*
- **(3):** $|A|+|B|=p$ *and there exist* $d\in\mathbb{F}^*$, $a\in A$, $b\in B$ *and* $n\in\{1,2,...,p-1\}$ *such that* $A\subsetneq a+\{0,d,...,(p-1)d\}$, $B\subsetneq b+\{0,d,...,(p-1)d\}$ *and* $a+b+nd-A=(b+\{0,d,...,(p-1)d\})\setminus B$*;*
- **(4):** $|A|+|B|\geq p+1$ *and there exist* $d\in\mathbb{F}^*$, $a\in A$, $b\in B$ *such that* $A\subseteq a+\{0,d,...,(p-1)d\}$ *and* $B\subseteq b+\{0,d,...,(p-1)d\}$.

Remarks

(1) If (3) holds then $A+B=(a+b+\{0,d,\ldots,(p-1)d\})\setminus\{a+b+nd\}$;
(2) If (4) holds then $A+B=a+b+\{0,d,\ldots,(p-1)d\}$;
(3) If (4) holds then, for all $a\in A$, $b\in B$, $A\subseteq a+\{0,d,...,(p-1)d\}$ and $B\subseteq b+\{0,d,...,(p-1)d\}$;
(4) If (3) holds then, for all $a\in A$, $b\in B$, there exists $n\in\{1,\ldots,p-1\}$ (depending on a and b) such that $A\subsetneq a+\{0,d,...,(p-1)d\}$, $B\subsetneq b+\{0,d,...,(p-1)d\}$ and $a+b+nd-A=(b+\{0,d,...,(p-1)d\})\setminus B$.

Let G be an abelian group with multiplicative notation and let A be a non-empty subset of G. The *stabilizer* of A in G is the subgroup of G, $H(A)=\{g\in G: gA=A\}$.

Since A is the union of $H(A)$-cosets, if A is finite then $H(A)$ is a finite subgroup of G. A non-empty set A is said periodic if $H(A)\neq\{1\}$.

Theorem 1. (Kneser's Theorem) [6, 7, 9] *Let A and B be two finite non-empty subsets of an abelian group $(G,\cdot)$. Let H denote the stabilizer of AB in G. Then $|AB|\geq|A|+|B|$ or $|AB|=|AH|+|BH|-|H|$.*

From Kneser's Theorem it is easy to obtain the next corollary.

Corollary 2. *Let A and B be two finite non-empty subsets of an abelian group $(G,\cdot)$ such that $|B|\geq|A|\geq 2$. Then $|AB|=|B|$ if and only if $|H(B)|\geq 2$ and $A\subseteq aH(B)$, for all $a\in A$.*

Notice that, from the previous corollary and from $H(B)\subseteq H(AB)$, it follows that, if A and B are finite non-empty subsets of a group such that $|A|\geq 2$, $|B|\geq 2$ and $|AB|=\max\{|A|,|B|\}$ then AB is periodic.

In order to use Proposition 3 and Corollary 2 simultaneously, we need to obtain information, for finite p, on arithmetic progressions that contain a geometric progression of length at least 3. This will be done in the next lemma.

Lemma 1. *Suppose $p>2$ is finite and let $c,d\in\mathbb{F}^*$, $r\in\mathbb{F}^*\setminus\{-1,1\}$ be such that $cr,cr^2\in c+d\{0,1,\ldots,p-1\}$. Then $r\in\{1,2,\ldots,p-1\}$ and $c^{p-1}=d^{p-1}$.*

Proof: Let $k_1,k_2\in\{1,\ldots,p-1\}$ be such that $cr^j=c+dk_j$, $j=1,2$. Since $k_j^{p-1}=1$ it follows that

$$(r^j-1)^{p-1}=(dc^{-1})^{p-1}\,,\qquad j=1,2\,. \tag{3}$$

Then

$(r^2-1)^{p-1} = (r-1)^{p-1} \Leftrightarrow (r+1)^p = r+1 \Leftrightarrow r^{p-1} = 1 \Rightarrow r \in \{1, 2, \dots, p-1\}$.

Also, from $r \in \{1, 2, \dots, p-1\}$ and (3) it follows that $c^{p-1} = d^{p-1}$. ■

In the next lemma we obtain information on the stabilizer in $(\mathbb{F}^*, \cdot)$ of periodic subsets of type $C \cap \mathbb{F}^*$ when p is finite and C is a subset of an arithmetic progression.

Lemma 2. *Suppose $p > 2$ is finite and let C be a subset of $\mathbb{F}$ such that $|C| \geq 2$ and C is a subset of an arithmetic progression with difference $d \in \mathbb{F}^*$. If $|H(C \cap \mathbb{F}^*)| \geq 2$ then $H(C \cap \mathbb{F}^*) \subseteq \{1, 2, \dots, p-1\}$ and $C \subseteq d\{0, 1, \dots, p-1\}$.*

Proof: Let $C^* = C \cap \mathbb{F}^*$, $H = H(C^*)$ and $t = |H| \geq 2$. Every finite subgroup of the multiplicative group of a field is cyclic [8, Theorem 1.9, pg 177] so, there exists $r \in \mathbb{F}^*$, with ord $r = t$, such that $H = < r >$.

Let $c \in C^*$. Then $cH = c\{1, r, \dots, r^{t-1}\} \subseteq C \subseteq c + \{0, d, ..., (p-1)d\}$.

Suppose $t \geq 3$. From Lemma 1 it follows that $r \in \{1, 2, \dots, p-1\}$. Hence $H \subseteq \{1, 2, \dots, p-1\}$. Also, from Lemma 1 we have $c^{p-1} = d^{p-1}$. This is true for all $c \in C^* = C \cap \mathbb{F}^*$, therefore

$$C \cap \mathbb{F}^* \subseteq \{x \in \mathbb{F}^* : x^{p-1} = d^{p-1}\} = d\{1, 2, \dots, p-1\}.$$

If $t = 2$ then $H = \{1, p-1\}$, $r = p-1$ and, using the same arguments as in the proof of Lemma 1, we have,

$$(r-1)^{p-1} = (dc^{-1})^{p-1} \Leftrightarrow 1 = (dc^{-1})^{p-1}.$$

Therefore $c^{p-1} = d^{p-1}$, for all $c \in C \cap \mathbb{F}^*$. ■

If C is an arithmetic progression then the result in Lemma 2 may be improved.

Lemma 3. *Suppose $p > 2$ and let $C \subseteq \mathbb{F}$ be a finite arithmetic progression, with difference $d \in \mathbb{F}^*$. If $|H(C \cap \mathbb{F}^*)| \geq 2$ then one the following alternatives holds:*

- **(1):** *p is finite and $C = d\{0, 1, 2, \dots, p-1\}$;*
- **(2):** *p is finite and $C = d\{1, 2, \dots, p-1\}$;*
- **(3):** *$C = d\{-k, -k+1, \dots, -1, 0, 1, \dots, k\}$, for some $k \in \mathbb{N}$ such that $2k+1 < p$;*
- **(4):** *$C = d\{-k + 2^{-1} + i : i = 0, 1, \dots, 2k-1\}$, for some $k \in \mathbb{N}$ such that $2k+1 < p$.*

Proof: Let $H = H(C \cap \mathbb{F}^*)$ and $t = |H| \geq 2$. Then $H = \{x \in \mathbb{F}^* : x^t = 1\}$. $C \cap \mathbb{F}^*$ is an union of H-cosets, so there exist $k \in \mathbb{N}$, $c_1, \ldots c_k \in C \cap \mathbb{F}^*$ such that

$$C \cap \mathbb{F}^* = \dot{\bigcup_{i=1}^{k}} c_i\ H = \dot{\bigcup_{i=1}^{k}} \{x \in \mathbb{F}^* : x^t = c_i^t\}\,.$$

Let u be the first term of the arithmetic progression C. If p is finite then $C \subseteq u + \{0, d, \ldots, (p-1)d\}$ and, from Lemma 2, $H \subseteq \{1, 2, \ldots, p-1\}$. So, if $p = |C|$ and $0 \in C$ then (1) holds. We consider the remaining four cases:

Case I: : $p > |C|$, $0 \in C$ and $t = 2$.

In this case, $H = \{-1, 1\}$ and $C = \{0\} \dot\cup \dot{\bigcup_{i=1}^{k}} \{c_i, -c_i\}$. Then C is the set of the roots of the polynomial

$$X \prod_{i=1}^{k} (X^2 - c_i^2) = X^{2k+1} - \sum_{i=1}^{2k} A_i X^i\,,$$

where $A_i = 0$ for i even. Then $A_{2k} = 0$ and, from Proposition 1, we have

$B^{(2k)}(u, d)[A_1 A_2 \cdots A_{2k-1} 0]^T = C^{(2k)}(u, d)$. Considering the last one of these $2k$ equalities we obtain, since $2k + 1 = |C| < p$,

$$u \binom{2k+1}{2k} + d \binom{2k+1}{2k-1} = 0 \Leftrightarrow u = -dk\,.$$

Hence (3) holds.

Case II: : $0 \notin C$ and $t = 2$.

C is the set of roots of the polynomial

$$\prod_{i=1}^{k} (X^2 - c_i^2) = X^{2k} - \sum_{i=1}^{2k-1} A_i X^i\,,$$

where $A_i = 0$ for i odd. As in the previous case, from Proposition 1, we have, since $2k = |C| < p$,

$$u \binom{2k}{2k-1} + d \binom{2k}{2k-2} = 0 \Leftrightarrow u = (-k + 2^{-1})d\,.$$

Hence (4) or (2) hold, according $2k + 1 < p$ or $2k + 1 = p$.

Case III: : $p > |C|$, $0 \in C$ and $t \geq 3$.

The set C is the set of all roots of the polynomial

$$X \prod_{i=1}^{k} (X^t - c_i^t) = X^{kt+1} - \sum_{i=1}^{kt} A_i X^i ,$$

where $A_i = 0$ for $i \not\equiv 1 (\text{mod } t)$. Since $kt \not\equiv 1 (\text{mod } t)$ and $kt - 1 \not\equiv 1$ $(\text{mod } t)$ $A_{kt} = A_{kt-1} = 0$. Then, from Proposition 1, we have

$$\begin{cases} u \binom{kt+1}{kt-1} + d \binom{kt+1}{kt-2} &= 0 \\ u \binom{kt+1}{kt} + d \binom{kt+1}{kt-1} &= 0 \end{cases} .$$

From these two equalities it follows, because $p > |C| = kt + 1 > 3$, that p is finite, $kt + 2 = p$ and $u = d$. Then $C = d\{1, 2, \ldots, p-1\}$ but this is absurd, since we are assuming that $0 \in C$.

Case IV: : $0 \notin C$ and $t \geq 3$.

As in case III, from Proposition 1 we have

$$\begin{cases} u \binom{kt}{kt-2} + d \binom{kt}{kt-3} &= 0 \\ u \binom{kt}{kt-1} + d \binom{kt}{kt-2} &= 0 \end{cases} ,$$

and, since $p > kt \geq 3$, it follows that p is finite, $p = kt + 1$ and $u = d$. Then $C = d\{1, 2, \ldots, p-1\}$ and (2) holds. ■

Remarks

(1) If (1) or (2) hold then $H(C \cap \mathbb{F}^*) = \{1, 2, \ldots, p-1\}$;
(2) If (3) holds then $0 \in C$ and $H(C \setminus \{0\}) = \{-1, 1\}$;
(3) If (4) holds then $0 \notin C$ and $H(C) = \{-1, 1\}$.

4. Main Result

In order to obtain the main result we will prove three results each of which characterizing the pairs (A, B) satisfying: one of cases (2)-(4) from Proposition 3, $|B| \geq |A| \geq 2$ and $|AB| = |B|$.

Proposition 4. *Let A and B be two finite subsets of $\mathbb{F}$ such that $|B| \geq |A| \geq 2$. Then $|AB| = |B|$ and A and B are arithmetic progressions with the same difference if and only if one of the following alternatives holds:*

(1): *$A = d\{0, 1\}$ and B is an arithmetic progression with difference d that contains 0, for some $d \in \mathbb{F}^*$;*

(2): *$A = \{-d, 0, d\}$ and $B = d\{-k, \ldots, -1, 0, 1, \ldots, k\}$, for some $d \in \mathbb{F}^*$ and $k \in \mathbb{N}$ such that $p > 2k+1$;*

(3): *$A = \{-\frac{d}{2}, \frac{d}{2}\}$ and $B = d\{-k, \ldots, -1, 0, 1, \ldots, k\}$, for some $d \in \mathbb{F}^*$ and $k \in \mathbb{N}$ such that $p > 2k+1$;*

(4): *$A = \{-\frac{d}{2}, \frac{d}{2}\}$ and $B = d\{-k + 2^{-1} + i : i = 0, 1, \ldots, 2k-1\}$, for some $d \in \mathbb{F}^*$ and $k \in \mathbb{N}$ such that $p > 2k+1$;*

(5): *p is finite and $A = d(s + \{0, 1, \ldots, \ell - 1\})$, $B = d\{1, \ldots, p-1\}$, for some $d \in \mathbb{F}^*$ and $s, \ell \in \mathbb{N}$ such that $\ell \geq 2$, $s < p-1$ and $s + \ell \leq p$;*

(6): *p is finite and $A = d(s + \{0, 1, \ldots, \ell - 1\})$, $B = d\{0, 1, \ldots, p-1\}$, for some $d \in \mathbb{F}^*$ and $s, \ell \in \mathbb{N}$ such that $2 \leq \ell \leq p$ and $s \leq p-1$.*

Proof: First we consider two arithmetic progressions, A and B, with the same difference $d \in \mathbb{F}^*$, such that $|B| \geq |A| \geq 2$ and $|AB| = |B|$.

If $p = 2$ then $|AB| = |A| = |B| = 2$ and it is easy to prove that (1) holds.

Suppose $p > 2$. Let $A^* = A \cap \mathbb{F}^*$, $B^* = B \cap \mathbb{F}^*$, $H = H(B^*)$ and $t = |H|$. Notice that, from $|AB| = |B|$ it follows that if $0 \in A$ then also $0 \in B$. Hence $0 \in AB \Leftrightarrow 0 \in B$ and $|A^*B^*| = |B^*|$. Then, also, $|B^*| \geq |A^*|$. If $|A^*| = 1$ then (1) holds. Suppose $|A^*| \geq 2$. Then, from Corollary 2 it follows that $t \geq 2$ and $A^* \subseteq aH$, for all $a \in A^*$. From Lemma 3, applied to B, we have four possible cases.

- p is finite and $B = d\{0, 1, \ldots, p-1\}$:
  Suppose $A = \{a', a'+d, \ldots, a'+(\ell-1)d\}$, where $\ell = |A| \in \{2, \ldots, p\}$. From $|AB| = |B|$ it follows that $AB = a'B$. Then $(a'+d)d \in a'B$. Hence, for some $i \in \{2, \ldots, p\}$, we have
  $$a' + d = a'i \Leftrightarrow a'(i-1) = d\,.$$
  Let $s \in \{1, \ldots, p-1\}$ be the inverse, modulus p, of $i-1$. Then $a' = sd$ and $A = d(s + \{0, 1, \ldots, \ell-1\})$. Hence (6) holds.
- p is finite and $B = d\{1, \ldots, p-1\}$:
  Similarly to the previous case it can be proved that (5) holds. Notice that, in this case, $0 \notin B$. Hence $0 \notin A$ and $s + \ell \leq p$.
- $B = d\{-k, -k+1, \ldots, -1, 0, 1, \ldots, k\}$, for some $k \in \mathbb{N}$ such that $p > 2k+1$:
  In this case $H = \{-1, 1\}$. Hence, (2) or (3) hold according $0 \in A$ or $0 \notin A$.
- $B = d\{-k + 2^{-1} + i : i = 0, 1, \ldots, 2k-1\}$, for some $k \in \mathbb{N}$ such that $p > 2k+1$:

In this case $0 \notin B$ and $H = \{-1, 1\}$. Then $0 \notin A$ and $|A| = 2$. Then (4) holds.

Let A and B satisfy one of the conditions (1)-(6). It is obvious that they are arithmetic progressions with difference d. It remains to prove that $|AB| = |B|$. For the six possible cases we have:

(1): $AB = dB$.

(2): $AB = \{0\} \dot{\bigcup} \{id^2 : i = 1, 2, \dots, k\} \dot{\bigcup} \{-id^2 : i = 1, 2, \dots, k\}$. Therefore $|AB| = 2k + 1 = |B|$.

(3): $AB = \{0\} \dot{\bigcup} \{i2^{-1}d^2 : i = 1, 2, \dots, k\} \dot{\bigcup} \{-i2^{-1}d^2 : i = 1, 2, \dots, k\}$. Then $|AB| = 2k + 1 = |B|$.

(4): $AB = \{d^2\, 2^{-1}(-k + i + 2^{-1}) : i = 0, 1, \dots, 2k - 1\}$. Then $|AB| = 2k = |B|$.

(5): From Corollary 2 it is sufficient to prove that $|H(B)| \geq 2$ and $A \subseteq aH(B)$, for all $a \in A$. It is obvious that $H(B) = \{1, 2, \dots, p-1\}$. Let $a \in A$. Then $a = jd$ for some $j \in \{s, s+1, s+\ell-1\}$ and $aH(B) = jd\{1, 2, \dots, p-1\}$. Since the congruence $j\ x \equiv i (\mathrm{mod}\ p)$ has exactly one solution in $\{1, \dots, p-1\}$, for $i = 1, \dots, p-1$, then, from $A = d\{i : i = s, s+1, \dots, s+\ell-1\} \subseteq d\{1, \dots, p-1\}$, it follows that $A \subseteq aH(B)$.

(6): Since $B^* = d\{1, 2, \dots, p-1\}$ then $H(B^*) = \{1, 2, \dots, p-1\}$ and, as in case (5), we have $A^* \subseteq aH(B^*)$, for all $a \in A^*$. Then $|AB| = |A^*B^*| + 1 = |B^*| + 1 = |B|$. ■

Proposition 5. *Suppose p is finite and let A and B be two finite subsets of $\mathbb{F}$ such that $|B| \geq |A| \geq 2$. Then, the pair (A, B) satisfies*

(i): $|A| + |B| \geq p + 1$;

(ii): $|AB| = |B|$;

(iii): *There exists $d \in \mathbb{F}^*$ such that $A \subseteq a + d\{0, 1, \dots, p-1\}$, $B \subseteq b + d\{0, 1, \dots, p-1\}$, for all $a \in A$, $b \in B$;*

if and only if one of the following cases holds:

(1): $|A| = 2$, $|B| \in \{p-1, p\}$, $0 \in A \cap B$ *and* $A, B \subseteq d\{0, 1, \dots, p-1\}$, *for some* $d \in \mathbb{F}^*$;

(2): $A \subseteq B = d\{0, 1, 2, \dots, p-1\}$, *for some* $d \in \mathbb{F}^*$;

(3): *$A \subseteq B = d\{1, 2, \ldots, p-1\}$, for some $d \in \mathbb{F}^*$;*

(4): *There exist $\{1\} \neq H \subsetneq \{1, 2, \ldots, p-1\}$ subgroup of $(\mathbb{F}^*, \cdot)$, $d \in \mathbb{F}^*$, $c_1, c_2, \ldots, c_{k+1} \in \{1, 2, \ldots, p-1\}$, where $k = \frac{p-1}{|H|} - 1$, and $j \in \{1, 2, \ldots, k+1\}$ such that*

$$\{1, 2, \ldots, p-1\} = \dot{\bigcup_{i=1}^{k+1}} c_i H\,, \quad B = \{0\} \dot{\cup} \dot{\bigcup_{i=1}^{k}} dc_i H$$

and $A = \{0\} \dot{\cup} dc_j H$.

Proof: Let A and B be subsets of $\mathbb{F}$ such that (i)-(iii) hold. If $p = 2$ then (1) holds. Suppose $p > 2$. Let A^*, B^*, H and t be as in the proof of the previous proposition. Then $0 \in AB \Leftrightarrow 0 \in B$ and $|A^*B^*| = |B^*|$. Then, also, $|B^*| \geq |A^*|$.

If $|A^*| = 1$ then (1) holds. Suppose $|A^*| \geq 2$. Then, from Corollary 2 it follows that $t \geq 2$ and $A^* \subseteq aH$, for all $a \in A^*$. From Lemma 2, applied to B, we have $H \subseteq \{1, \ldots, p-1\}$ and $B^* \subseteq d\{1, \ldots, p-1\}$. Hence $p \equiv 1 (\mathrm{mod}\ t)$. Since $H = H(B^*)$, B^* is the union of H-cosets. Let k be the number of such H-cosets, that is, $k = \frac{|B^*|}{t}$. We consider four cases:

(a): $0 \notin B$

Since $kt = |B| \leq p$ and $p \equiv 1 (\mathrm{mod}\ t)$, we have $kt < p$. Then $kt < p \leq |A| + |B| - 1 \leq (k+1)t - 1$. From $p \equiv 1 (\mathrm{mod}\ t)$ it follows that $p = kt + 1$ and $|B| = p - 1$. Therefore, $B = d\{1, \ldots, p-1\}$, $H = H(B) = \{1, \ldots, p-1\}$ and $k = 1$. Also, since $A \subseteq a + d\{1, \ldots, p-1\}$ and $A \subseteq a\{1, \ldots, p-1\}$ for all $a \in A$, we have $A \subseteq d\{1, \ldots, p-1\}$ and (3) holds.

(b): $p = |B|$ and $0 \in B$

Then $B = d\{0, 1, \ldots, p-1\}$, $H = H(B^*) = \{1, \ldots, p-1\}$ and $k = 1$. Also, since $A \subseteq a + d\{0, 1, \ldots, p-1\}$ and $A^* \subseteq a\{1, \ldots, p-1\}$ for all $a \in A^*$, we have $A \subseteq d\{0, 1, \ldots, p-1\}$ and (2) holds.

(c): $p > |B|$, $0 \in B$ and $0 \notin A$

In this case we have $kt + 1 = |B| < p \leq |A| + |B| - 1 \leq (k+1)t$ and this contradicts $p \equiv 1 (\mathrm{mod}\ t)$.

(d): $p > |B|$ and $0 \in A \cap B$

Then $kt + 1 = |B| < p \leq |A| + |B| - 1 \leq (k+1)t + 1$. From $p \equiv 1$ $(\mathrm{mod}\ t)$ it follows that $p = (k+1)t + 1$. Then $k = \frac{p-1}{t} - 1$, $|B| = p - t$ and $A = \{0\} \dot{\cup} aH$, for all $a \in A^*$.

Let $c_1, c_2, \ldots, c_{k+1} \in \{1, 2, \ldots, p-1\}$ be such that $\{1, 2, \ldots, p-1\} = \dot{\bigcup}_{i=1}^{k+1} c_i H$. Since $B^* \subseteq d\{1, 2, \ldots, p-1\}$ and B^* is an union of k H-cosets we may assume that $B = \{0\} \dot{\cup} \dot{\bigcup}_{i=1}^{k} dc_i H$. From (iii) it follows that $A \subseteq d\{0, 1, \ldots, p-1\} = \{0\} \dot{\cup} \dot{\bigcup}_{i=1}^{k+1} dc_i H$. Hence, because A^* is an H-coset, $A = \{0\} \dot{\cup} dc_j H$, for some $j \in \{1, \ldots, k+1\}$ and (4) holds.

Let A and B satisfy one of the conditions (1)-(4). It is obvious that the pair (A, B) satisfies (i) and (iii). We have also $|AB| = |B|$ since, for the four possible cases, the set AB is

(1): aB, where $\{a\} = A^*$;
(2): $d^2\{0, 1, 2, \ldots, p-1\} = dB$;
(3): $d^2\{1, 2, \ldots, p-1\} = dB$;
(4): $dc_j B$. ■

Proposition 6. *Suppose p is finite and let A and B be two finite subsets of $\mathbb{F}$ such that $|B| \geq |A| \geq 2$. Then, the pair (A, B) satisfies*

(i): $|A| + |B| = p$*;*
(ii): $|AB| = |B|$*;*
(iii): *There exists $d \in \mathbb{F}^*$ such that, for all $a \in A$, $b \in B$, $A \subsetneq a + d\{0, 1, \ldots, p-1\}$, $B \subsetneq b + d\{0, 1, \ldots, p-1\}$ and $(b + d\{0, 1, \ldots, p-1\}) \setminus B = a + b + nd - A$, for some $n \in \{1, 2, \ldots, p-1\}$, depending on a and b;*

if and only if one of the following cases holds:

(1): *$A = d\{0, \ell\}$ and $B = d\{0, 1, \ldots, p-1\} \setminus d\{n, n-\ell\}$, for some $d \in \mathbb{F}^*$, $\ell, n \in \{1, 2, \ldots, p-1\}$, with $n \neq \ell$;*
(2): *There exist $\{1\} \neq H \subsetneq \{1, 2, \ldots, p-1\}$ subgroup of $(\mathbb{F}^*, \cdot)$, $d \in \mathbb{F}^*$, $c_1, c_2, \ldots, c_{k+1} \in \{1, 2, \ldots, p-1\}$, where $k = \frac{p-1}{|H|} - 1$, such that*

$$\{1, 2, \ldots, p-1\} = \dot{\bigcup_{i=1}^{k+1}} c_i H\,, \quad B = \{0\} \dot{\cup} \dot{\bigcup_{i=1}^{k}} dc_i H$$

and $A = -dc_{k+1}H$.

Proof: Let A and B be subsets of $\mathbb{F}$ such that (i)-(iii) hold. Let A^*, B^*, H and t be as in the proofs of the previous propositions. Then $0 \in AB \Leftrightarrow 0 \in B$, $|A^*B^*| = |B^*|$ and $|B^*| \geq |A^*|$.

If $|A^*| = 1$ then (1) holds.

Suppose $|A^*| \geq 2$. As in the proof of Proposition 5, $t \geq 2$, $H \subseteq \{1, \dots, p-1\}$, $p \equiv 1 (\mathrm{mod}\ t)$, $A^* \subseteq aH$, for all $a \in A^*$ and $B^* \subseteq d\{1, \dots, p-1\}$ is the union of H-cosets. We denote by k be the number of such H-cosets, that is, $k = \frac{|B^*|}{t}$.

We consider three cases:

(a): $0 \notin B$

Then $kt = |B| < p = |A| + |B| \leq (k+1)t$. From $p \equiv 1(\mathrm{mod}\ t)$ it follows that $p = kt + 1$. Then $|A| + |B| = kt + 1$ and $|A| = 1$, which is absurd.

(b): $0 \in B$ and $0 \notin A$

In this case we have $kt+1 = |B| < p = |A|+|B| \leq (k+1)t+1$. Then $p = (k+1)t + 1$ and $|A| = t$. Hence $A = aH$, for all $a \in A$.

Let $c_1, c_2, \dots, c_{k+1} \in \{1, 2, \dots, p-1\}$ be such that $\{1, 2, \dots, p-1\} = \dot{\bigcup}_{i=1}^{k+1} c_iH$. Since $B^* \subseteq d\{1, 2, \dots, p-1\} = \dot{\bigcup}_{i=1}^{k+1} dc_iH$ and B^* is an union of k H-cosets we may assume that $B = \{0\} \dot{\cup} \dot{\bigcup}_{i=1}^{k} dc_iH$.

Let $a \in A$. Since $0 \in B$, from (iii) it follows that, for some $n \in \{1, 2, \dots, p-1\}$,

$$\begin{aligned} a + nd - A &= d\{0, 1, \dots, p-1\} \setminus B = d\{1, \dots, p-1\} \setminus B^* \\ &= dc_{k+1}H \, . \end{aligned} \tag{4}$$

Since $nd \in a + nd - A$, and $a + nd - A$ is an H-coset, we have $ndH = a + nd - A$.

Suppose $H = < h > = \{1, h, \dots, h^{t-1}\}$. From $a + nd - aH = a + nd - A = ndH$ we have

$$\sum_{j=1}^{t-1} (a + nd - ah^j) = \sum_{j=1}^{t-1} ndh^j \Leftrightarrow a + nd = 0 \, .$$

Then, from (4), if follows that $A = -dc_{k+1}H$ and (2) holds.

(c): $0 \in B$ and $0 \in A$

Then $kt+1 = |B| < p = |A|+|B| \leq (k+1)t+2$. Then $p = (k+1)t+1$ and $|A| = t$. Hence $A = \{0\}\dot{\cup}a_1H \setminus \{a_1\}$, for some $a_1 \in \mathbb{F}^*$. Since $0 \in A \cap B$, from (iii) it follows that, for some $n \in \{1, 2, \dots, p-1\}$,

$$nd - A = d\{0, 1, \dots, p-1\} \setminus B = d\{1, \dots, p-1\} \setminus B^* .$$

Then $nd-A$ is an H-coset. Since $nd \in nd-A$, we have $nd-A = ndH$.

Suppose $H =< h >= \{1, h, \dots, h^{t-1}\}$. From $ndH = nd - A = nd - \{0\}\dot{\cup}(a_1H \setminus \{a_1\})$ it follows that

$$\sum_{j=1}^{t-1}(nd - a_1h^j) = \sum_{j=1}^{t-1} ndh^j \Leftrightarrow a_1 = -tnd .$$

But, from $nd - A = ndH = \{x \in \mathbb{F}^* : x^t = (nd)^t\}$, we also have that, for $j = 1, \dots, t-1$,

$$(nd - a_1h^j)^t = (nd)^t \Leftrightarrow (1 + th^j)^t = 1 .$$

Then, $H = \{1 + th^j : j = 1, \dots, t-1\}\dot{\cup}\{1\}$ and, from Corollary 1, $H = \{1, p-1\}$ or $H = \{1, \dots, p-1\}$. None of these two cases is possible since $|A| = |H|$, $|A| + |B| = p$ and $p > |B| \geq |A| \geq 3$.

Let A and B satisfy condition (1). Then $|A| + |B| = p$ and $|AB| = |B|$ since $AB = \{0\}\dot{\cup}\ell\, d(B \setminus \{0\})$.

Let $a = rd$ and $b = sd$ be any two elements of A and B, respectively, where $r \in \{0, \ell\}$, $s \in \{0, 1, \dots, p-1\} \setminus \{\ell, n-\ell\}$. It is obvious that $A \subsetneq a + d\{0, 1, \dots, p-1\}$ and $B \subsetneq b + d\{0, 1, \dots, p-1\}$. Let $n' \in \{0, 1, \dots, p-1\}$ be such that $r + s + n' \equiv n (\text{mod } p)$. From $nd \notin A + B$ it follows that $n' \neq 0$. Also,

$$\begin{aligned} a + b + n'd - A &= (r + s + n')d - A = nd - A = d\{0, 1, \dots, p-1\} \setminus B \\ &= (b + d\{0, 1, \dots, p-1\}) \setminus B . \end{aligned}$$

Now suppose the pair (A, B) satisfies condition (2). Then $|A| + |B| = p$ and $|AB| = |B|$, since $AB = \{0\}\dot{\cup}\dot{\bigcup}_{i=1}^{k} -d^2c_ic_{k+1}H$.

Since $H \subsetneq \{1, 2, \dots, p-1\}$ and $c_1, c_2, \dots, c_{k+1} \in \{1, 2, \dots, p-1\}$, then $B \subsetneq d\{0, 1, \dots, p-1\}$ and $A \subsetneq d\{1, \dots, p-1\}$. Then, trivially, $B \subsetneq b + d\{0, 1, \dots, p-1\}$ and $A \subsetneq a + d\{1, \dots, p-1\}$, for all $b \in B$, $a \in A$.

Let $a = rd$ and $b = sd$ be any two elements of A and B, respectively, where $r \in \{1, \dots, p-1\}$, $s \in \{0, 1, \dots, p-1\}$. Let $n' \in \{0, 1, \dots, p-1\}$ be such that $r + s + n' \equiv 0(\text{mod } p)$. From $B \cap -A = \emptyset$ it follows that $n' \neq 0$. Also,

$$a+b+n'd-A = -A = d\{0,1,\dots,p-1\} \setminus B = (b+d\{0,1,\dots,p-1\}) \setminus B\,.$$

■

Remarks - Let A and B be two finite subsets of $\mathbb{F}$ such that $|B| \geq |A| \geq 2$.

(1) If (A, B) satisfies condition (1) of Proposition 5 then (A, B) satisfies condition (1) of Proposition 4;
(2) If (A, B) satisfies condition (5) of Proposition 4 then (A, B) satisfies condition (3) of Proposition 5;
(3) If (A, B) satisfies condition (6) of Proposition 4 then (A, B) satisfies condition (2) of Proposition 5.

From Propositions 3, 4, 5 and 6 we obtain next result.

Theorem 2. *Let A and B be two finite subsets of $\mathbb{F}$ such that $|B| \geq |A| \geq 1$. Then $|AB| = |B|$ and $|A+B| = \min\{p, |A|+|B|-1\}$ if and only if one of the following alternatives holds:*

- $1 = |A| \leq |B| \leq p$;
- $A = d\{0, 1\}$ *and B is an arithmetic progression with difference d that contains 0, for some $d \in \mathbb{F}^*$;*
- $A = \{-d, 0, d\}$ *and* $B = d\{-k, \dots, -1, 0, 1, \dots, k\}$, *for some $d \in \mathbb{F}^*$ and $k \in \mathbb{N}$ such that $p > 2k+1$;*
- $A = \{-\frac{d}{2}, \frac{d}{2}\}$ *and* $B = d\{-k, \dots, -1, 0, 1, \dots, k\}$, *for some $d \in \mathbb{F}^*$ and $k \in \mathbb{N}$ such that $p > 2k+1$;*
- $A = \{-\frac{d}{2}, \frac{d}{2}\}$ *and* $B = d\{-k + 2^{-1} + i : i = 0, 1, \dots, 2k-1\}$, *for some $d \in \mathbb{F}^*$ and $k \in \mathbb{N}$ such that $p > 2k+1$;*
- *p is finite,* $A = d\{0, \ell\}$ *and* $B = d\{0, 1, \dots, p-1\} \setminus d\{n, n-\ell\}$, *for some $d \in \mathbb{F}^*$ and $\ell, n \in \{1, 2, \dots, p-1\}$, with $n \neq \ell$;*
- *p is finite and* $A \subseteq B = d\{0, 1, 2, \dots, p-1\}$, *for some $d \in \mathbb{F}^*$;*
- *p is finite and* $A \subseteq B = d\{1, 2, \dots, p-1\}$, *for some $d \in \mathbb{F}^*$;*
- *p is finite and there exist $\{1\} \neq H \subsetneq \{1, 2, \dots, p-1\}$ subgroup of $(\mathbb{F}^*, \cdot)$, $d \in \mathbb{F}^*$, $c_1, c_2, \dots, c_{k+1} \in \{1, 2, \dots, p-1\}$, where $k = \frac{p-1}{|H|} - 1$, and $j \in \{1, 2, \dots, k+1\}$ such that*

$$\{1, 2, \dots, p-1\} = \dot{\bigcup_{i=1}^{k+1}} c_i H\,, \quad B = \{0\} \dot{\cup} \dot{\bigcup_{i=1}^{k}} dc_i H$$

and $A=\{0\}\dot{\cup}dc_jH$*;*

- p *is finite and there exist* $\{1\}\neq H\subsetneq\{1,2,\dots,p-1\}$ *subgroup of* $(\mathbb{F}^*,\cdot)$, $d\in\mathbb{F}^*$, $c_1,c_2,\dots,c_{k+1}\in\{1,2,\dots,p-1\}$, *where* $k=\frac{p-1}{|H|}-1$, *such that*

$$\{1,2,\dots,p-1\}=\dot{\bigcup_{i=1}^{k+1}}c_iH\,,\quad B=\{0\}\dot{\cup}\dot{\bigcup_{i=1}^{k}}dc_iH$$

and $A=-dc_{k+1}H$*.*

References

[1] C. Caldeira, Critical pairs of matrices for the degree of the minimal polynomial of the Kronecker sum, *Linear and Multilinear Algebra* 42(1997), 73-88.

[2] A. Cauchy, Recherches sur les nombres, *J. École Polytech.* 9(1813),99-116.

[3] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* 10(1935), 30-32.

[4] H. Davenport, A historical note, *J. London Math. Soc.* 22(1947), 100-101.

[5] J. A. Dias da Silva and Y. O. Hamidoune, A note on the minimal polynomial of the Kronecker sum of two linear operators, *Linear Algebra and its Applications* 141(1990), 283-287.

[6] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* 58(1953), 459-484.

[7] M. Kneser, Ein Satz über abelschen Gruppen mit Anwendungen auf die Geometrie der Zahlen *Math. Z.* 61(1955), 429-434.

[8] S. Lang, *Algebra*, Addison-Wesley Publishing Company, Inc., 1993.

[9] M. B. Nathanson, *Additive Number Theory-Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics 165, Springer-Verlag, New York, 1996.

[10] A. G. Vosper, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.* 31(1956), 200-205.

[11] A. G. Vosper, Addendum to "The critical pairs of subsets of a group of prime order", *J. London Math. Soc.* 31(1956), 280-282.

Cristina Caldeira
CMUC, Department of Mathematics, University of Coimbra, 3001-454 Coimbra, Portugal
E-mail address: caldeira@mat.uc.pt