

One-Point Extensions of Multiplicative Subgroups as Self-Sumsets

Alper Ferudun*

October 7, 2026

Abstract

Let p be an odd prime, let G be a proper multiplicative subgroup of $\mathbb{F}_p^*$, and let $e \notin G$. We classify all subsets $A \subseteq \mathbb{F}_p$ satisfying $A + A = G \cup \{e\}$, where diagonal sums are included. Necessarily $p \geq 5$, $G = \{-1, 1\}$, and

$$(e, A) = (0, \{-1/2, 1/2\}), \quad (3, \{-1/2, 3/2\}), \quad (-3, \{-3/2, 1/2\}).$$

For a nonzero exceptional value, a differential polynomial built from the Hanson–Petridis auxiliary polynomial forces a subset of A of size $|A| - 1$ to be invariant under reflection about $e/2$. A shifted-subgroup intersection bound then reduces the proof to $|A| \leq 5$, and moments exclude the remaining cases. The zero-exception case is a known consequence of Hanson–Petridis. The theorem settles the one-point enlargement regime, not the general near-equality or small-exponent containment questions in the AIM additive-combinatorics problem list.

1 The classification and its scope

Throughout, sumsets are unrestricted: $A + A = \{a + b : a, b \in A\}$ includes every diagonal $2a$. Problem 4.7 of the AIM additive-combinatorics list [1], attributed to Granville and Tao, asks whether a self-sumset can equal a proper multiplicative subgroup of a prime field or be slightly larger, and what structure this imposes. The following theorem gives a complete classification when the enlargement consists of exactly one element.

Theorem 1.1. *Let p be an odd prime, $G < \mathbb{F}_p^*$ a proper multiplicative subgroup, and $e \in \mathbb{F}_p \setminus G$. Then $A + A = G \cup \{e\}$ if and only if $p \geq 5$, $G = \{-1, 1\}$, and (e, A) is one of the three pairs listed in the abstract.*

The prime-field hypothesis and the inclusion of diagonal sums are essential to the formulation here. No classification with two or more exceptional values is asserted. In particular, this theorem does not answer whether $A + A \subseteq G$ can occur with $|A| > p^\varepsilon$ for small fixed $\varepsilon > 0$, the other formulation in [1].

Hanson and Petridis [2, Theorem 1.2] proved

$$|B||C| \leq |G| + |B \cap (-C)| \quad \text{when } B + C \subseteq G \cup \{0\}. \quad (1)$$

Thus exact equality $A + A = G$ is already impossible for a nontrivial proper subgroup: if $n = |A|$ and $m = |G|$, then $n^2 \leq m \leq n(n + 1)/2$. The zero-exception part of Theorem 1.1 is also a short

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: <https://github.com/AlperTheKing>. Unrefereed preprint. CC BY 4.0.

consequence of this prior work. The additional argument below concerns a single arbitrary nonzero exception.

Shkredov's near-equality estimate for quadratic residues [3, Theorem 3.2] involves the number of *ordered representations* outside the residues. One exceptional value can carry many such representations, so that estimate is not a bound on the number of exceptional values used here. We make no absolute priority claim.

2 An auxiliary polynomial with exceptional values

Assume $A + A = G \cup \{e\}$, and put $n = |A|$, $m = |G|$. A singleton has only one self-sum, whereas two distinct elements in odd characteristic have three distinct self-sums. Hence $n, m \geq 2$. Properness and the inclusion of a translate of A in its sumset give

$$m \leq \frac{p-1}{2}, \quad n \leq m+1, \quad D := m+n-1 \leq 2m < p. \quad (2)$$

All following polynomial identities are over $\mathbb{F}_p$.

For $a \in A$, define

$$c_a = \prod_{a' \in A \setminus \{a\}} (a - a')^{-1}, \quad F(x) = -1 + \sum_{a \in A} c_a (x + a)^D.$$

This is the auxiliary polynomial of Hanson and Petridis [2]. Lagrange interpolation gives

$$\sum_{a \in A} c_a a^j = 0 \quad (0 \leq j < n-1), \quad \sum_{a \in A} c_a a^{n-1} = 1, \quad \sum_{a \in A} c_a (x + a)^{n-1} = 1.$$

In particular, F has degree exactly m with leading coefficient $L = \binom{D}{n-1} \neq 0$. Writing $s_1 = \sum_{a \in A} a$, its coefficient B of x^{m-1} satisfies

$$B = \binom{D}{n} s_1, \quad \frac{B}{L} = \frac{m}{n} s_1. \quad (3)$$

Indeed $\sum c_a a^n = s_1$, by reducing x^n modulo $\prod_{a \in A} (x - a)$ and comparing its degree- $(n-1)$ coefficient.

For the next three sections assume $e \neq 0$. Set

$$C = A \cap (e - A), \quad r = |C|.$$

For $b \in A \setminus C$, every $b + a$ lies in G , so F has a zero of order at least n at b . To see this, differentiate the last interpolation identity and use $(b + a)^m = 1$. For $b \in C$, only the partner $a = e - b$ is exceptional. If $(D)_j$ denotes the falling factorial, then for $0 \leq j < n$,

$$F^{(j)}(b) = (D)_j c_{e-b} (e^m - 1) e^{n-1-j}. \quad (4)$$

All factorials involved are invertible by (2). Equivalently, in the local variable h ,

$$F(b + h) = c_{e-b} (1 - e^{-m}) (e + h)^D \pmod{h^n}. \quad (5)$$

The scalar is nonzero because $e \notin G$ and G is exactly the set of roots of $x^m - 1$ in $\mathbb{F}_p$.

Lemma 2.1. *The polynomial*

$$K = DFF'' - (D - 1)(F')^2$$

has degree $2m - 2$, leading coefficient $-L^2m(n - 1)$, and zeros of orders at least $2n - 2$ on $A \setminus C$ and $n - 2$ on C . Consequently,

$$(2n - 2)n - nr \leq 2m - 2. \quad (6)$$

The sum of all roots of K , counted with multiplicity in an algebraic closure, is

$$-\frac{2(m - 1)}{n}s_1. \quad (7)$$

Proof. The leading coefficient is $L^2m(m - D) = -L^2m(n - 1) \neq 0$. A zero of order n in F gives order at least $2n - 2$ in both terms of K . At an exceptional point use (5): the differential expression vanishes on every scalar multiple of $(e + h)^D$, and two differentiations of the error lose at most two powers of h . This proves the multiplicities and (6). The coefficient of x^{2m-3} in K is $2LB(m - 1)(m - D)$; Vieta's formula and (3) give (7). $\square$

3 Reflection rigidity

The involution $a \mapsto e - a$ on C has at most one fixed point. Thus e has exactly $\lceil r/2 \rceil$ unordered representations in $A + A$, including diagonals. Coverage of G gives

$$m \leq \frac{n(n + 1)}{2} - \left\lceil \frac{r}{2} \right\rceil. \quad (8)$$

Combining (6) and (8) yields

$$(n - 1)(n - 2 - r) + (r \bmod 2) \leq 0,$$

so $r \geq n - 2$.

Lemma 3.1. *Exactly one element of A is outside C ; that is, $r = n - 1$.*

Proof. If $r = n$, then $A = e - A$ and its sumset is invariant under $s \mapsto 2e - s$. This reflection fixes e , so it also preserves G . Since $m \geq 2$, $\sum_{g \in G} g = 0$, and reflection would imply $2me = 0$, a contradiction.

Suppose instead that $r = n - 2$. The preceding inequality forces n even and equality in both (6) and (8), with $m = n^2/2 + 1$. The case $n = 2$ would give $r = 0$, impossible because $e \in A + A$, so $n \geq 4$. Put $U = \sum_{a \in A \setminus C} a$. All roots of K have now been accounted for by the multiplicities in Lemma 2.1. Equating their sum with (7) gives

$$(n - 2)s_1 + nU = -ns_1, \quad (2n - 2)s_1 + nU = 0.$$

Furthermore, $U = s_1 - (n - 2)e/2$. Equality in (8) means that each sum other than e has exactly one unordered representation. Summing all unordered sums therefore gives

$$(n + 1)s_1 = \frac{n - 2}{2}e.$$

Eliminating s_1 and U gives

$$(n - 2)(n^2 - 2n + 2)e = 0.$$

But $p \geq 2m + 1 = n^2 + 3$, so neither positive integer factor vanishes modulo p . This contradiction leaves $r = n - 1$. $\square$

Lemma 3.2. *For every $c \in \mathbb{F}_p^*$,*

$$|G \cap (c - G)| \leq \left\lfloor \frac{m+1}{2} \right\rfloor.$$

Proof. Set $\epsilon = (-1)^m$ and $Q(x) = x^{m+1} - \epsilon(x - c)^{m+1} - c$. For $x \in G \cap (c - G)$, one has $x^m = 1$ and $(x - c)^m = \epsilon$, so both $Q(x)$ and $Q'(x)$ vanish. If m is odd, Q has degree $m + 1$ and leading coefficient 2. If m is even, it has degree m and leading coefficient $(m + 1)c \neq 0$. Counting double roots proves the bound. $\square$

Write $A = C \cup \{u\}$, where $C = e - C$. Then $(C + C) \setminus \{e\} \subseteq G \cap (2e - G)$, and

$$A + A = (C + C) \cup (u + C) \cup \{2u\}.$$

The latter two sets add at most n sums. Lemma 3.2 and $e \neq 0$ give

$$m - n \leq |C + C| - 1 \leq \left\lfloor \frac{m+1}{2} \right\rfloor, \quad m \leq 2n + 1.$$

On the other hand, (6) gives $m \geq n(n - 1)/2 + 1$. It follows that $n \leq 5$. Together with (8), the only possibilities are

$$(n, m) \in \{(2, 2), (3, 4), (3, 5), (4, 7), (4, 8), (5, 11)\}. \quad (9)$$

4 The remaining cases

For a multiplicative subgroup of order m , $\sum_{g \in G} g^j = 0$ for $1 \leq j < m$. Write $s_j = \sum_{a \in A} a^j$, and let U_j sum the j th powers of $a + b$ over all unordered pairs from A , including diagonals. Taking half the ordered sum and half the diagonal sum gives

$$U_1 = (n + 1)s_1, \quad U_2 = (n + 2)s_2 + s_1^2, \quad U_3 = (n + 4)s_3 + 3s_1s_2. \quad (10)$$

4.1 Three elements

For $n = 3$, write $A = e/2 + \{-v, v, w\}$. Here $v \neq 0$ and $w/v \notin \{0, 1, -1\}$: the last exclusions express distinctness and the fact that w is outside the reflection core. Both possible subgroup orders require $p \geq 11$.

If $m = 4$, the six formal offsets of the sums from e are

$$-2v, 0, 2v, w - v, w + v, 2w.$$

Exactly one collision is required. Comparing pairs shows $w/v \in \{3, -3\}$; every other possible collision requires an excluded ratio 0, 1, -1. Replacing v by $-v$ if necessary, we obtain $G = e + vR$, where $R = \{-2, 2, 4, 6\}$. The first two vanishing moments of G imply

$$4 \sum_{x \in R} x^2 - \left(\sum_{x \in R} x \right)^2 = 4 \cdot 60 - 10^2 = 140 = 0 \quad \text{in } \mathbb{F}_p.$$

No prime $p \geq 11$ divides 140, so this is impossible.

If $m = 5$, all six unordered sums are distinct, and $U_j = e^j$ for $j = 1, 2, 3$. Put $u = e/2 + w$. The first two equations in (10) give $u = -3e/4$ and $v^2 = -7e^2/16$. Consequently,

$$s_1 = e/4, \quad s_2 = 3e^2/16, \quad s_3 = -95e^3/64, \quad U_3 = -41e^3/4.$$

The equation $U_3 = e^3$ forces $45e^3 = 0$, again impossible.

4.2 Four elements

Now $C = e/2 + \{-v, 0, v\}$, with $v \neq 0$, and $A = C \cup \{u\}$. Both orders in (9) have $p \geq 17$.

For $m = 8$, there are ten unordered sums but nine distinct values; the two representations of e account for the only repetition. Thus $U_j = 2e^j$ for $j = 1, 2, 3$. From (10),

$$u = -\frac{11e}{10}, \quad v^2 = -\frac{62e^2}{75}, \quad s_1 = \frac{2e}{5}, \quad s_2 = \frac{23e^2}{75}, \quad s_3 = -\frac{859e^3}{250}.$$

It follows that $U_3 = -678e^3/25$, so $728e^3 = 0$. Since $728 = 2^3 \cdot 7 \cdot 13$, this is impossible for $p \geq 17$.

For $m = 7$, write $u = e/2 + w$ and $t = w/v \notin \{0, 1, -1\}$. The nine formal offsets, in units of v , are

$$-2, -1, 0, 1, 2, t-1, t, t+1, 2t.$$

To give eight distinct values there must be exactly one collision. Pairwise comparison leaves $t \in \{\pm 2, \pm 3, \pm 1/2\}$. The choices ± 2 cause two collisions and are excluded. For $t = 3$ and $t = 1/2$, respectively, the nonzero offsets form, after rescaling,

$$R_1 = \{-2, -1, 1, 2, 3, 4, 6\}, \quad R_2 = \{-4, -2, 2, 4, -1, 1, 3\}.$$

Negative t gives their negatives. If $G = e + vR$ and $S_j = \sum_{x \in R} x^j$, the first three moments require

$$7S_2 - S_1^2 = 0, \quad 49S_3 - 21S_1S_2 + 2S_1^3 = 0.$$

For R_1 the two integers are 328 and 54, whose gcd is 2; for R_2 they are 348 and -1836 , whose gcd is 12. No prime $p \geq 17$ can divide either pair.

4.3 Five elements

Here $m = 11$, $p \geq 23$, and $s_1 = 2e + u$. Equality holds in (6). Comparing the prescribed root sum with (7) gives

$$3s_1 + 5u = -4s_1, \quad 14e + 12u = 0. \tag{11}$$

Lemma 3.2 gives $|C+C| \leq 7$. Since $|A+A| = 12$ and the outlier adds at most five sums, $|C+C| = 7$, and $C+C$, $u+C$, $\{2u\}$ are pairwise disjoint. The first set is symmetric about e , so its sum is $7e$; the sum of the second is $4u + 2e$. Removing e from the sumset therefore gives

$$0 = \sum_{g \in G} g = 8e + 6u.$$

Twice this identity minus (11) yields $2e = 0$, a contradiction.

4.4 Two elements and the zero exception

Only $n = m = 2$ remains when $e \neq 0$. Then $G = \{-1, 1\}$, and the three sums of a two-element set form an arithmetic progression. An arithmetic progression containing -1 and 1 has third element 0 , 3 or -3 . Solving for the two elements of A gives exactly the pairs in Theorem 1.1.

Finally, suppose $e = 0$. Inequality (1) gives $n^2 \leq m + z$, where $z = |A \cap (-A)| \leq n$, while coverage gives $m + 1 \leq n(n + 1)/2$. Therefore $(n - 1)(n - 2) \leq 0$, and $n = 2$. Its self-sumset has three elements, so $m = 2$ and $p \geq 5$. If $0 \in A$, write $A = \{0, b\}$. Then $\{b, 2b\} = \{-1, 1\}$, which would force $p = 3$. Hence zero is not in A , and its representation as a sum forces $A = \{a, -a\}$. The other two sums give $a = \pm 1/2$. Conversely, direct addition checks all three displayed examples for every $p \geq 5$. This completes the proof of Theorem 1.1.

5 Reproducibility

The source package includes the research proof, its detailed self-audit, and an exact-arithmetic Python checker. The checker tests polynomial coefficients, exceptional derivatives, multiplicities, subgroup moments and the small-case identities. It also exhausts all one-point-enlargement systems for odd primes through 101, using a clique enumeration cross-checked by powerset enumeration on small graphs. It finds precisely the 72 stated examples over the 24 primes from 5 to 101. The ordinary and optimized runs agree on 749,359 checks. These finite tests supplement, and do not replace, the all-primes proof above.

This preprint is unrefereed; no independent review, formal verification or absolute priority is claimed. AI assistance was used for mathematical exploration, drafting and reproducibility checks. The author is responsible for the manuscript and its claims.

References

- [1] American Institute of Mathematics, *Recent trends in additive combinatorics: Palo Alto problems*, Problem 4.7, p. 11. <https://aimath.org/WWN/additivecomb/additivecomb.pdf>.
- [2] B. Hanson and G. Petridis, Refined estimates concerning sumsets contained in the roots of unity, *Proc. Lond. Math. Soc.* (3) **121** (2020), no. 2, 287–292. doi:10.1112/plms.12322. arXiv:1905.09134.
- [3] I. D. Shkredov, Sumsets in quadratic residues, *Acta Arith.* **164** (2014), no. 3, 221–244. doi:10.4064/aa164-3-2.