

Multiplicative subgroups of $\mathbb{Z}_p^*$ that are generalized arithmetic progressions

by

ALBERT COCHRANE

Abstract. We prove that a multiplicative subgroup A_k of $\mathbb{Z}_p^*$ is a generalized arithmetic progression if and only if $|A_k| = 2, 4$, or $p - 1$. Much of the argument builds upon recent work studying additive decompositions of subgroups, and we generalize a result of Hanson and Petridis to show that any additive n -decomposition of a subgroup must be a direct sum. We also show how this classification quickly follows from Kalmynin's recent work resolving Sárközy's conjecture for quadratic residues.

1. Introduction. Our primary goal in this paper is to completely answer the question of when multiplicative subgroups can have the additive structure of a generalized arithmetic progression (GAP) in the finite field of p elements. Let p be a prime number, $\mathbb{Z}_p$ be the finite field of integers modulo p , and $\mathbb{Z}_p^*$ denote its multiplicative group of units. For a divisor k of $p - 1$ and $t = \frac{p-1}{k}$, we denote the multiplicative subgroup of $\mathbb{Z}_p^*$ with order t as $A_k = \{x^k : x \in \mathbb{Z}_p^*\}$. A GAP of dimension n in $\mathbb{Z}_p$ is a set of the form

$$S = \{a + x_1 d_1 + \cdots + x_n d_n : x_i \in [0, L_i - 1], 1 \leq i \leq n\},$$

where $d_i \in \mathbb{Z}_p^*$ and $L_i \geq 2$ for all $1 \leq i \leq n$. We say that S is a *proper* generalized arithmetic progression if $|S| = \prod_{i=1}^n L_i$.

For $n = 1$, Chowla, Mann, and Straus [2] proved that a subgroup A_k is an arithmetic progression if and only if $t = 1, 2$ or $p - 1$. Moving on to the case of $n = 2$, it is easy to see that any subgroup of order 4 is a proper two-dimensional GAP. Let p be a prime congruent to 1 (mod 4) and set $k = \frac{p-1}{4}$. Then for a generator ω , the subgroup A_k equals $\{\pm 1, \pm \omega\}$, which can be written as

$$A_k = \{-1 + x_1(1 - \omega) + x_2(1 + \omega) : x_1, x_2 \in [0, 1]\}.$$

2020 *Mathematics Subject Classification*: Primary 11B30; Secondary 11B13, 11B25.

Key words and phrases: sumset, progression, additive decomposition, finite field.

Received 24 February 2026; revised 25 February 2026.

Published online 18 October 2026.

We claim that over all prime numbers p , there are no other cases where a subgroup of $\mathbb{Z}_p^*$ can be a GAP.

THEOREM 1.1. *Let A_k be a multiplicative subgroup of $\mathbb{Z}_p^*$ with $|A_k| = t$. Then A_k is a generalized arithmetic progression if and only if $t = 2, 4$, or $p - 1$.*

2. Definitions and notation. We use several standard definitions from additive combinatorics. Letting $A, B \subseteq \mathbb{Z}_p$, we define the sumset $A + B = \{a + b : a \in A, b \in B\}$. For a positive integer $l \geq 2$, we denote the l -fold sumset as $lA = A + \cdots + A = \{a_1 + \cdots + a_l : a_i \in A\}$. We note here that GAPs of dimension 1 will simply be referred to as arithmetic progressions, with an occasional reminder that we are speaking of the $n = 1$ case depending on context. The definition of GAP in the introduction follows [15] and other papers on the topic, for example [4]. We equivalently use the shorthand notation found in [18], presenting the GAP structure as a sumset of arithmetic progressions:

$$S = a + d_1[0, L_1 - 1] + \cdots + d_n[0, L_n - 1].$$

This notation is particularly useful when considering GAPs as a special type of additive decomposition, and we may informally refer to L_i as being the size of the i th component of the progression.

A subset B of $\mathbb{Z}_p$ admits a non-trivial *additive decomposition* if $B = S_1 + S_2$ for some $S_1, S_2 \subseteq \mathbb{Z}_p$ with $|S_1|, |S_2| \geq 2$. More generally, we say B admits an n -*decomposition* if there exist $S_i \subseteq \mathbb{Z}_p$ with $|S_i| \geq 2$ such that

$$B = S_1 + \cdots + S_n.$$

Any n -decomposition with $n > 2$ can also be expressed as a 2-decomposition, $B = S_1 + (S_2 + \cdots + S_n)$. Following Shkredov [13], we say that a decomposition $B = S_1 + \cdots + S_n$ is a *direct sum* if $|B| = \prod_{i=1}^n |S_i|$. Notice that for both GAPs and n -decompositions, we include the standard conditions for non-triviality in the definition statement. That is, in this paper we are only interested in the cases where for each i , $L_i \geq 2$ for GAPs and $|S_i| \geq 2$ for decompositions.

3. Background. The question of whether a multiplicative subgroup can be a generalized arithmetic progression directly points at the sum-product phenomenon in $\mathbb{Z}_p$. Indeed, the results in this paper illustrate that in nearly all cases the additive structure of progressions is incompatible with the multiplicative structure found in subgroups of k th powers.

A closely related question which has received much attention in recent years is whether a subgroup can be expressed as a sumset, that is, admit an additive decomposition. Sárközy [11] conjectured that for p sufficiently large, the subgroup of quadratic residues R cannot be expressed as a non-trivial

2-decomposition. Many investigations into the additive irreducibility of multiplicative subgroups have followed; see for example, [5, 12, 14, 16, 17]. A recent preprint of Kalmynin [9] resolves this conjecture for quadratic residues, and provides new insights on decompositions of arbitrary subgroups of k th powers which we consider in Section 6.

Specifically relevant to our main argument, Chen and Yan [1] refined bounds on decompositions of R , proving that any additive decomposition of the form $R = U + V$ must satisfy $|V| \geq |U| \geq 5$, a result we use in Section 5. Hanson and Petridis [8] showed that any 2-decomposition of a multiplicative subgroup must be a direct sum. This result in particular proved instrumental in allowing us to consider generalized progressions of arbitrarily large dimension. In the next section we extend this result to cover n -decompositions with $n > 2$, and ultimately are able to restrict our attention to proper GAPs such that $L_i = 2$ uniformly.

4. GAPs and additive decompositions. By definition, any GAP admits an additive decomposition where each component is a (1-dimensional) arithmetic progression of size at least 2. A nice feature of arithmetic progressions is that they can always be written as a decomposition of sets with size exactly 2. Suppose S is an arithmetic progression with L terms. Then for some $a \in \mathbb{Z}_p$ and $d \in \mathbb{Z}_p^*$, we can express S as the sum of $\{a, a + d\}$ and $\{0, d\}$ added to itself $L - 2$ times:

$$S = \{a, a + d, \dots, a + (L - 1)d\} = \{a, a + d\} + (L - 2)\{0, d\}.$$

Plainly, any sumset of additive decompositions will itself be a decomposition, so this proves the following lemma. For now we use m instead of n to avoid conflating dimension with the number of components in the decomposition.

LEMMA 4.1. *Suppose $S \subseteq \mathbb{Z}_p$ is a generalized arithmetic progression. Then, for some positive integer m , there exist subsets $S_i \subseteq \mathbb{Z}_p$ with $|S_i| = 2$ for $1 \leq i \leq m$ such that $S_1 + \dots + S_m = S$.*

That is, any GAP admits an additive decomposition where each component is of size exactly 2.

We now shift our attention to the condition of a decomposition being a direct sum. Hanson and Petridis [8] proved the following for 2-decompositions.

LEMMA 4.2 ([8, Corollary 1.3]). *Let p be a prime and A_k be the multiplicative subgroup of k th powers for some $k \mid (p - 1)$ with $k \neq 1$. Suppose $S, T \subseteq \mathbb{Z}_p$ satisfy $S + T = A_k$. Then $|S| |T| = |A_k|$.*

We also need the following theorem of Gyarmati, Matolcsi, and Ruzsa [7].

THEOREM 4.3 ([7, Theorem 1.2]). *Let $n \geq 3$ be an integer and $S_1, \dots, S_n$ be non-empty subsets of $\mathbb{Z}_p$. Let $S = S_1 + \dots + S_n$, and for $1 \leq i \leq n$, set*

$$\hat{S}_i = S_1 + \dots + S_{i-1} + S_{i+1} + \dots + S_n.$$

Then

$$|S| \leq \left(\prod_{i=1}^n |\hat{S}_i| \right)^{\frac{1}{n-1}}.$$

Applying this to Lemma 4.2, we obtain the following generalization.

COROLLARY 4.4. *Let $k \neq 1$ be a divisor of $p-1$, and A_k be the group of k th powers in $\mathbb{Z}_p^*$. If $A_k = S_1 + \dots + S_n$ for some non-empty subsets S_i of $\mathbb{Z}_p$, then $|A_k| = \prod_{i=1}^n |S_i|$.*

Proof. Lemma 4.2 proves this for $n = 2$. Suppose now that $n \geq 3$ and that $A_k = S_1 + \dots + S_n = S_i + \hat{S}_i$. Applying Lemma 4.2 to the decomposition $A_k = S_i + \hat{S}_i$, we obtain $|A_k| = |S_i| |\hat{S}_i|$ for $1 \leq i \leq n$. Then by Theorem 4.3 we have

$$|A_k|^{n-1} \leq \prod_{i=1}^n |\hat{S}_i| = \prod_{i=1}^n \frac{|A_k|}{|S_i|} = \frac{|A_k|^n}{\prod_{i=1}^n |S_i|}.$$

This yields $\prod_{i=1}^n |S_i| \leq |A_k|$, and it is trivial that $|A_k| \leq \prod_{i=1}^n |S_i|$. ■

Combining this with Lemma 4.1, we arrive at the following corollary, which sets up the proof of Theorem 1.1.

COROLLARY 4.5. *Let p be a prime and A_k be the subgroup of k th powers in $\mathbb{Z}_p^*$ for some $k \mid (p-1)$. Suppose A_k is a generalized arithmetic progression and $k > 1$. Then, $|A_k| = 2^n$ for some positive integer n , and A_k is a proper generalized arithmetic progression of dimension n with $L_i = 2$ uniformly.*

Proof. Suppose A_k is a GAP. Lemma 4.1 tells us that for some positive integer n , $A_k = S_1 + \dots + S_n$ for subsets $S_i \subseteq \mathbb{Z}_p$ with $|S_i| = 2$. It follows from Corollary 4.4 that such a decomposition must be a direct sum; that is, $|A_k| = \prod_{i=1}^n |S_i| = 2^n$. By definition, this means A_k is a proper GAP of dimension n . ■

Note that this recovers the result of Chowla, Mann, and Straus [2] on arithmetic progressions stated in the introduction. For $k = 1$, $A_k = \mathbb{Z}_p^*$ is trivially an arithmetic progression. For $k > 1$, it follows from Corollary 4.5 that only subgroups of order 2 can form a GAP of dimension 1.

5. Proof of Theorem 1.1. We begin by considering $k = 2$, where A_k is the group of quadratic residues.

LEMMA 5.1 ([1, Lemma 2.6]). *If $k = 2$ and $A_k = U + V$ with $|V| \geq |U| \geq 2$, then $|U| \geq 5$.*

Then by Corollary 4.5 it follows that for $t > 2$, no subgroup of quadratic residues can be expressed as a generalized arithmetic progression.

For $k > 2$, we consider subgroups in two primary cases, $t < 64$ and $t \geq 64$, or equivalently, $n < 6$ and $n \geq 6$. For the first case, we look at the doubling properties of subgroups. For the second, we employ classical estimates on the number of solutions to the equation $x^k + y^k = cz^k$. Lemma 5.2 below is used in both cases.

For any $c \in \mathbb{Z}_p$, let $r(c)$ denote the representation function which counts the number of ways c can be written as a sum of two elements of A_k :

$$r(c) := \#\{(x, y) \in A_k \times A_k : x + y = c\}.$$

LEMMA 5.2. *Suppose that $A_k = S_1 + \cdots + S_n$ for subsets S_i each of cardinality 2. Then, $r(c) \geq t/2$ for some $c \neq 0$.*

Proof. Suppose that $A_k = S_1 + \cdots + S_n$ for subsets S_i , each of cardinality 2. By translation we can assume $0 \in S_i$ for the first $n-1$ sets, say $S_i = \{0, d_i\}$ and $S_n = \{a, a + d_n\}$ for some $d_i \in \mathbb{Z}_p^*$, $1 \leq i \leq n$, and $a \in \mathbb{Z}_p$. Let $c = 2a + \sum_{i=1}^{n-1} d_i$. We claim $c = -d_n \neq 0$. Indeed, the sum of the elements in A_k is zero, so

$$\begin{aligned} 0 &= \sum_{x_1=0}^1 \cdots \sum_{x_n=0}^1 (d_1 x_1 + \cdots + d_n x_n + a) \\ &= 2^{n-1}(2a + d_1 + \cdots + d_n) = 2^{n-1}(c + d_n). \end{aligned}$$

For $x = a + \sum_{i=1}^{n-1} x_i d_i$ with $x_i \in \{0, 1\}$, $1 \leq i \leq n-1$, and $y = a + \sum_{i=1}^{n-1} (1 - x_i) d_i$, we have $x + y = c$. Moreover, the pairs x, y are uniquely determined by the choice of the x_i , because by Corollary 4.4, the decomposition of A_k must be a direct sum. Thus $r(c) \geq 2^{n-1} = t/2$. ■

Now we examine subgroups with $k > 2$ and $t < 64$. In the introduction, we showed that subgroups of order 2 and 4 will always be GAPs, and by Corollary 4.5 we know that no subgroup with $k > 1$ and $t \notin \{2, 4, 8, 16, 32\}$ can be a GAP. We restrict our attention here to $t \in \{8, 16, 32\}$, and use $\phi(t)$ to denote the Euler totient function. For $p < \frac{1}{2}3^{\phi(t)+1}$, a direct computation confirms that $r(c) < t/2$ holds for all such subgroups and $c \in \mathbb{Z}_p^*$. For $p > \frac{1}{2}3^{\phi(t)+1}$ we have the following lemma.

LEMMA 5.3 ([3, Lemma 4]). *For a prime number p and $k \mid (p-1)$, let A_k denote the multiplicative subgroup of k th powers in $\mathbb{Z}_p^*$ with order t . If t is even and $p > \frac{1}{2}3^{\phi(t)+1}$, then*

$$\frac{|A_k + A_k|}{|A_k|} = \frac{t}{2} + \frac{1}{t}.$$

It follows that for $t = 2^n$ and $p > \frac{1}{2}3^{\phi(t)+1}$,

$$\frac{|A_k + A_k|}{|A_k|} > 2^{n-1}.$$

Now suppose that S is a GAP of dimension n with $|S| = 2^n$, that is,

$$S = a + d_1[0, 1] + \cdots + d_n[0, 1].$$

The sumset $S + S$ is of the form

$$S + S = 2a + d_1[0, 2] + \cdots + d_n[0, 2],$$

so plainly $|S + S| \leq 3^n$. Then for $n \in \{3, 4, 5\}$ we have

$$\frac{|S + S|}{|S|} \leq \left(\frac{3}{2}\right)^n < 2^{n-1}.$$

Thus, if $k > 2$ and $t < 64$, A_k cannot be a GAP unless $t = 2$ or 4 .

Finally, we examine the case with $k > 2$ and $t \geq 64$. Consider the projective Fermat curve defined by $x^k + y^k = cz^k$ with $c \neq 0$, which has genus $g = \frac{1}{2}(k-1)(k-2)$. The Hasse–Weil estimate [6] for the number $N(c)$ of projective points over $\mathbb{Z}_p$ on such a curve is $|N(c) - (p+1)| \leq 2g\sqrt{p}$, which gives $N(c) \leq (k-1)(k-2)\sqrt{p} + p + 1$. Then, because the map $(x, y, 1) \mapsto (x^k, y^k)$ from points on the curve with $xyz \neq 0$ to solutions of $u + v = c$ with $(u, v) \in A_k \times A_k$ is k^2 -to-1, we find that for all non-zero c ,

$$(5.1) \quad r(c) \leq \frac{N(c)}{k^2} \leq \frac{p+1}{k^2} + \frac{(k-1)(k-2)}{k^2} \sqrt{p}.$$

For small subgroups, we use the following refinement obtained by Mattarei [10].

LEMMA 5.4 ([10, Corollary]). *If $k \geq 4$ and $t \leq \frac{1}{4}k^3$, then for any non-zero c we have*

$$r(c) \leq 3 \cdot 2^{-2/3} t^{2/3}.$$

LEMMA 5.5. *If $k > 2$ and $t = 2^n$ with $n \geq 6$, then A_k cannot be expressed as a sum of sets each of cardinality 2. That is, if $A_k = S_1 + \cdots + S_n$ for some subsets S_i of $\mathbb{Z}_p$, then $|S_i| \geq 3$ for some i .*

Proof. Suppose that $A_k = S_1 + \cdots + S_n$ for subsets S_i with $|S_i| = 2$. If $t > \frac{1}{4}k^3$ we deduce from Lemma 5.2 and (5.1) that for some $c \in \mathbb{Z}_p^*$,

$$(5.2) \quad \frac{t}{2} \leq r(c) \leq \frac{t}{k} + \frac{2}{k^2} + \left(1 - \frac{1}{k}\right) \left(1 - \frac{2}{k}\right) \sqrt{kt+1},$$

from which we get

$$t \left(\frac{1}{2} - \frac{1}{k} \right) \leq \frac{2}{k^2} + \left(1 - \frac{1}{k}\right) \left(1 - \frac{2}{k}\right) \sqrt{kt+1},$$

that is,

$$t \leq \frac{4}{k(k-2)} + 2 \left(1 - \frac{1}{k}\right) \sqrt{kt+1}.$$

For $k \geq 3$ and $t \geq 2^6$, the last quantity is less than $2\sqrt{kt}$. Thus $t < 2\sqrt{kt}$, and so $t < 4k$. Combining this with the assumption $t > \frac{1}{4}k^3$, we get $\frac{1}{4}k^3 < 4k$, implying that $k < 4$. For $k = 3$, (5.2) implies $t \leq 8$, contrary to assumption.

Suppose now that $t \leq \frac{1}{4}k^3$. In particular, $k \geq 4^{1/3}t^{1/3} \geq 4^{1/3}64^{1/3} > 4$. It follows from Lemmas 5.2 and 5.4 that for some $c \neq 0$, we have $\frac{1}{2}t \leq r(c) \leq 3 \cdot 2^{-2/3}t^{2/3}$ and so $t \leq 54$, contrary to assumption. ■

Thus, no subgroup with $k > 2$ and $t \geq 64$ can be a GAP, completing the proof of Theorem 1.1.

6. Another proof of Theorem 1.1. Upon completion of this manuscript, it was brought to our attention that a recent preprint of Kalmynin [9] provides an alternative direct path to proving Theorem 1.1. Of particular relevance is the following result.

LEMMA 6.1 ([9, Corollary 1]). *For all primes p , no proper subgroup A_k of $\mathbb{Z}_p^*$ can satisfy $A_k = S_1 + S_2 + S_3$ with $|S_1|, |S_2|, |S_3| > 1$.*

For a prime p , suppose that a proper subgroup A_k of $\mathbb{Z}_p^*$ is a generalized arithmetic progression. Then by Lemma 4.1, this means that for some positive integer m and subsets $S_i \subseteq \mathbb{Z}_p$ with $|S_i| = 2$,

$$A_k = S_1 + \cdots + S_m = S_1 + S_2 + (S_3 + \cdots + S_m).$$

From Lemma 6.1, we immediately deduce that such a decomposition is possible only if $m \leq 2$. Together with Lemma 4.2, it follows that if a proper subgroup A_k of $\mathbb{Z}_p^*$ forms a GAP, then $|A_k| = 2$ or 4.

Acknowledgements. We thank anonymous referees for their valuable suggestions, and for bringing Kalmynin's work to our attention. We also thank Craig Spencer for many helpful conversations.

References

- [1] Y.-G. Chen and X.-H. Yan, *A conjecture of Sárközy on quadratic residues*, J. Number Theory 229 (2021), 100–124.
- [2] S. Chowla, H. B. Mann, and E. G. Straus, *Some applications of the Cauchy–Davenport theorem*, Norske Vid. Selsk. Forh. Trondheim 32 (1959), 74–80.
- [3] A. Cochrane, T. Cochrane, and C. Spencer, *Doubling constant for subgroups of $\mathbb{Z}_p^*$* , Integers 23 (2023), art. A35, 30 pp.
- [4] E. Croot, N. Lyall, and A. Rice, *Polynomials and primes in generalized arithmetic progressions*, Int. Math. Res. Notices 2015, 6021–6043.
- [5] C. Dartyge and A. Sárközy, *On additive decompositions of the set of primitive roots modulo p* , Monatsh. Math. 169 (2013), 317–328.
- [6] H. Davenport und H. Hasse, *Die Nullstellen der Kongruenzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. 172 (1935), 151–182.

- [7] K. Gyarmati, M. Matolcsi, and I. Z. Ruzsa, *A superadditivity and submultiplicativity property for cardinalities of sumsets*, *Combinatorica* 30 (2010), 163–174.
- [8] B. Hanson and G. Petridis, *Refined estimates concerning sumsets contained in the roots of unity*, *Proc. London Math. Soc.* (3) 122 (2021), 353–358.
- [9] A. Kalmynin, *On additive irreducibility of multiplicative subgroups*, arXiv:2504.10202v2 (2025).
- [10] S. Mattarei, *On a bound of Garcia and Voloch for the number of points of a Fermat curve over a prime field*, *Finite Fields Appl.* 13 (2007), 773–777.
- [11] A. Sárközy, *On additive decompositions of the set of quadratic residues modulo p* , *Acta Arith.* 155 (2012), 41–51.
- [12] I. D. Shkredov, *Sumsets in quadratic residues*, *Acta Arith.* 164 (2014), 221–243.
- [13] I. D. Shkredov, *On common energies and sumsets*, *J. Combin. Theory Ser. A* 213 (2025), art. 106026, 11 pp.
- [14] I. E. Shparlinski, *Additive decompositions of subgroups of finite fields*, *SIAM J. Discrete Math.* 27 (2013), 1870–1879.
- [15] T. Tao and V. H. Vu, *Additive Combinatorics*, *Cambridge Stud. Adv. Math.* 105, Cambridge Univ. Press, 2006.
- [16] H.-L. Wu, N.-L. Wei, and Y.-B. Li, *On sumsets involving k th powers of finite fields*, *Discrete Math.* 347 (2024), art. 113870, 10 pp.
- [17] C. H. Yip, *Additive decompositions of large multiplicative subgroups in finite fields*, *Acta Arith.* 213 (2024), 97–116.
- [18] Y. Zhao, *Graph Theory and Additive Combinatorics: Exploring Structure and Randomness*, Cambridge Univ. Press, 2023.

Albert Cochrane
Department of Mathematics
Kansas State University
Manhattan, KS 66506, USA
E-mail: albertc@ksu.edu