

**A PALEY COLOURING SETTLES $D_{Q_p,1}$:
THE QUADRATIC-RESIDUE WEIGHTED DAVENPORT
CONSTANT IS 4 FOR EVERY PRIME $p \equiv 1 \pmod{4}$**

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. For an odd prime p let Q_p be the set of nonzero quadratic residues modulo p and let $\mathbf{1} = \{1\}$. A sequence $(x_1, \dots, x_k)$ in $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ is a $(Q_p, \mathbf{1})$ -weighted zero-sum sequence if there are $a_1, \dots, a_k \in Q_p$ with $a_1x_1 + \dots + a_kx_k = 0$ and $a_1 + \dots + a_k = 0$, and $D_{Q_p, \mathbf{1}}(p)$ is the least k such that every length- k sequence in $\mathbb{Z}_p$ has such a subsequence. Paul and Paul, who introduced this doubly-weighted constant, proved $D_{Q_p, \mathbf{1}} \in \{4, 5\}$ for every odd p and $D_{Q_p, \mathbf{1}} = 5$ for $p \equiv 3 \pmod{4}$, and wrote of the remaining case: “we believe that $D_{Q_p, \mathbf{1}} = 4$... However, despite our best efforts, we have been unable to show this”. We prove it. The mechanism is that for $p \equiv 1 \pmod{4}$ the element -1 is a square, so the quadratic character $\chi(x - y)$ is a well-defined 2-colouring of the edges of the complete graph on $\mathbb{Z}_p$ — the Paley colouring — and each of three configurations forces a weighted zero-sum subsequence: a repeated term, a monochromatic triangle, and a monochromatic perfect matching, the last through the weight vector $(1, -1, -u, u)$. Since every 2-colouring of the edges of K_4 contains a monochromatic triangle or a monochromatic perfect matching, four terms always suffice. With the authors’ own theorem for $p \equiv 3 \pmod{4}$ the value of $D_{Q_p, \mathbf{1}}(p)$ is now known at every odd prime, and their conditional consequence becomes unconditional: $D_{Q_p, B}(p) = 4$ for $p \equiv 1 \pmod{4}$ and every nonempty B with $0 \notin B$. Every theorem below is machine-checked in Lean 4; §10 says exactly what the machine checks. An independent exhaustive computation, outside the formal development, confirms the value at all 168 odd primes $p \leq 1009$.

1. INTRODUCTION

The objects. Throughout, p is a prime and $\mathbb{Z}_n$ denotes the ring $\mathbb{Z}/n\mathbb{Z}$ (not the p -adic integers). We follow the notation of Paul and Paul [8]: $U(n)$ is the group of units of $\mathbb{Z}_n$, and for an odd prime p ,

$$Q_p = \{x^2 : x \in U(p)\}, \quad N_p = U(p) \setminus Q_p,$$

so Q_p is the set of nonzero quadratic residues and N_p the set of nonzero non-residues. The subsets $\{0\}$ and $\{1\}$ of $\mathbb{Z}_n$ are written $\mathbf{0}$ and $\mathbf{1}$.

The Davenport constant of $\mathbb{Z}_n$ with a weight set A was defined by Adhikari and Rath [1]; their Theorem 3 determines it, and the weighted Erdős–Ginzburg–Ziv constant, when A is the set of quadratic residues modulo a prime. The *doubly-weighted* constants used here were introduced by Paul and Paul [7]. Their definition, quoted from [8], is:

We let A and B be non-empty subsets of $\mathbb{Z}_n \setminus \{0\}$. A sequence $(x_1, \dots, x_k)$ in $\mathbb{Z}_n$ is called an *A-weighted zero-sum sequence* if there exist $a_1, \dots, a_k \in A$ such that $a_1x_1 + \dots + a_kx_k = 0$. A sequence $(x_1, \dots, x_k)$ in $\mathbb{Z}_n$ is called an *(A, B)-weighted zero-sum sequence* if there exist $a_1, \dots, a_k \in A$ and $b_1, \dots, b_k \in B$ such that $a_1x_1 + \dots + a_kx_k = 0$ and $b_1a_1 + \dots + b_ka_k = 0$.

Their Definition 1.3 introduces $C_{A,B}(n)$, $D_{A,B}(n)$ and $E_{A,B}(n)$ in three clauses; the second reads: *the constant $D_{A,B}(n)$ is the least positive integer k such that any sequence in $\mathbb{Z}_n$ of length k has an (A, B) -weighted zero-sum subsequence*. Taking $B = \mathbf{1}$ makes the second condition $a_1 + \dots + a_k = 0$, and $D_{A, \mathbf{1}}$ is the constant this paper is about. Two remarks fix the reading. First, “subsequence” means a nonempty subfamily of the terms, indexed by a nonempty set of positions; the empty subsequence is excluded, or every constant would be 0. Second, $0 \notin A$ throughout, so a choice of weights $a_i \in A \cup \{0\}$, not all zero, is the same thing as a choice of subsequence together with its weights — the support of (a_i) is the subsequence. This is the encoding used in every computation reported below.

What the source proves, and what it leaves open. The paper [8] determines $E_{Q_p,1}$ and $C_{Q_p,1}$ (the length- p and consecutive-subsequence variants) and settles $D_{Q_p,1}$ except in one residue class. Its Theorem 4.2 is

$$D_{Q_p,1} = 4 \text{ or } 5,$$

proved by applying the Chevalley–Warning theorem [9] to the pair of quadrics $a_1 X_1^2 + \dots + a_5 X_5^2 = 0$, $X_1^2 + \dots + X_5^2 = 0$ of total degree $2 + 2 < 5$ for the upper bound, and by quoting $D_{Q_p} = 3$ for the lower bound. Its Theorem 4.3 is $D_{Q_p,1} = 5$ when $p \equiv 3 \pmod{4}$. The paper’s concluding section, §6, is three sentences long and we quote it in full:

When $p \equiv 1 \pmod{4}$, we believe that $D_{Q_p,1} = 4$. If this is true, it will follow that $D_{Q_p,B} = 4$ when $p \equiv 1 \pmod{4}$ and $0 \notin B$. However, despite our best efforts, we have been unable to show this.

No computation is reported in support of the belief: no prime is checked against it, and no verification range is attached to it.

Results. We prove the belief, for every prime in the class.

- (1) $D_{Q_p,1}(p) = 4$ for every prime $p \equiv 1 \pmod{4}$ (Theorem 6.2). Combined with Theorem 4.3 of [8], reproduced here as Theorem 7.3, the value of $D_{Q_p,1}(p)$ is now known at every odd prime: it is 4 when $p \equiv 1 \pmod{4}$ and 5 when $p \equiv 3 \pmod{4}$.
- (2) The upper half, which is the new content, is Theorem 5.2: every sequence of length four in $\mathbb{Z}_p$, $p \equiv 1 \pmod{4}$, has a $(Q_p, 1)$ -weighted zero-sum subsequence. Its core is Theorem 5.1, the case of four distinct terms.
- (3) The conditional consequence stated in §6 of [8] becomes unconditional: for every prime $p \equiv 1 \pmod{4}$ and every nonempty $B \subseteq \mathbb{Z}_p$ with $0 \notin B$ one has $D_{Q_p,B}(p) = 4$ (Theorem 6.3). This is exactly the hypothesis under which [8, Theorem 5.5] already gives $D_{Q_p,B} \in \{4, 5\}$ in this residue class; what is new is the value.

The proof is short and we can give it here in full outline. Let χ be the quadratic character of $\mathbb{Z}_p$. For $p \equiv 1 \pmod{4}$ the element -1 is a square, so $\chi(x - y) = \chi(y - x)$ and

$$\{x, y\} \mapsto \chi(x - y) \in \{+1, -1\} \quad (x \neq y)$$

is a well-defined 2-colouring of the edges of the complete graph on the vertex set $\mathbb{Z}_p$: the *Paley colouring*. Three configurations in a sequence force a $(Q_p, 1)$ -weighted zero-sum subsequence:

- a *repeated term* $x_i = x_j$, with weights $(1, -1)$ — admissible because $-1 \in Q_p$ (Lemma 3.1);
- a *monochromatic triangle*, three terms whose three cyclic differences all have the same character, with weights $((x_j - x_k)/(x_i - x_j), (x_k - x_i)/(x_i - x_j), 1)$ (Lemma 3.2);
- a *monochromatic perfect matching*, two disjoint pairs of positions whose differences have the same character, with weights $(1, -1, -u, u)$ where $u = (x_i - x_j)/(x_k - x_l)$ (Lemma 3.4).

The combinatorial fact that closes the argument is that *every 2-colouring of the edges of K_4 contains a monochromatic triangle or a monochromatic perfect matching* (Lemma 4.1). So four terms are always enough: if two of them coincide use the first construction, and otherwise the Paley colouring restricted to the four vertices offers one of the other two. The lower bound $D_{Q_p,1} \geq 4$ is the source’s, made explicit: $(1, n, 0)$ with n a non-residue has no $(Q_p, 1)$ -weighted zero-sum subsequence (Proposition 6.1).

What is old in this argument. This has to be said precisely, because two of the three constructions have a visible ancestor. The doubly-weighted constant $D_{A,B}$ was defined in [7], and that paper contains, for the trivial weight set $\mathbb{Z}'_n = \mathbb{Z}_n \setminus \{0\}$, both the repeated-term observation and the triple weight vector, and a four-term case split of the same shape as ours. Its Observation 3.1 is that a repeated term x makes (x, x) a $(\mathbb{Z}'_n, 1)$ -weighted zero-sum subsequence. Its Observation 3.2 is that for pairwise distinct x, y, z the weights $a = y - z$, $b = z - x$, $c = x - y$ satisfy $ax + by + cz = 0$ and $a + b + c = 0$, so (x, y, z) is a $(\mathbb{Z}'_n, 1)$ -weighted zero-sum sequence — this is exactly our triple weight vector, unnormalised. And the proof of its Theorem 3.4 ($C_{\mathbb{Z}'_n,1} = 4$) splits a four-term sequence into

“a distinct pair, hence Observation 3.2” and “two coincidences $x = z$, $y = w$, hence the identity $x + y - z - w = 0$ ”.

For $A = \mathbb{Z}'_n$ every nonzero element is an admissible weight, so no admissibility criterion and no colouring arises there. What is not in [7], not in [8], and not found in the literature, is: (i) that for three distinct terms the weight vector of Observation 3.2 is forced up to scale, so that for $A = Q_p$ admissibility becomes exactly the character condition $\chi(x - y) = \chi(y - z) = \chi(z - x)$, i.e. a monochromatic triangle of the Paley colouring; (ii) the matching construction $(1, -1, -u, u)$, which needs $-1 \in Q_p$ and has no $\mathbb{Z}'_n$ analogue, the four-term move of [7, Theorem 3.4] requiring the two equalities $x = z$, $y = w$ rather than a coincidence of characters; (iii) the K_4 dichotomy; and (iv) the resulting value. A reader who knows [7] will read the proof below as the case split of [7, Theorem 3.4] refined by a character condition, and that is a fair description.

Provenance of the quotations. The e-print [8] has exactly one version, v1 of 20 January 2026, and carries no journal reference; all quotations from it above and below are from that e-print, read directly. Numbered references to [7] are to its version v4 of 8 July 2026 (the source [8] cites v3). One reference of [8] could not be read: [2], from which [8] quotes $D_{Q_p}(p) = 3$ for its lower bound, is a paywalled volume; its bibliographic data below is verified, its text is not. Nothing here depends on it: the value $D_{Q_p}(p) = 3$ is also [1, Theorem 3], read directly, and in any case Proposition 6.1 proves the lower bound we use from scratch, with an explicit witness.

2. PRELIMINARIES

Fix a prime p . We write χ for the quadratic character of $\mathbb{Z}_p$, so $\chi(a) = 1$ if $a \in Q_p$, $\chi(a) = -1$ if $a \in N_p$, and $\chi(0) = 0$; for $a \neq 0$ we use “ a is a square” and “ $\chi(a) = 1$ ” interchangeably.

Definition 2.1. Let $A, B \subseteq \mathbb{Z}_p$ and let $x = (x_1, \dots, x_k)$ be a sequence in $\mathbb{Z}_p$. We say x has an (A, B) -weighted zero-sum subsequence if there are a nonempty set $J \subseteq \{1, \dots, k\}$ of positions and elements $a_i \in A$, $b_i \in B$ for $i \in J$ with

$$\sum_{i \in J} a_i x_i = 0 \quad \text{and} \quad \sum_{i \in J} b_i a_i = 0.$$

For $B = \mathbf{1}$ the second condition is $\sum_{i \in J} a_i = 0$, and we then say x has an $(A, \mathbf{1})$ -weighted zero-sum subsequence. Finally

$$D_{A,B}(p) = \min \left\{ k : \text{every } x \in \mathbb{Z}_p^k \text{ has an } (A, B)\text{-weighted zero-sum subsequence} \right\},$$

and $D_{A,1}(p)$ is the same with $B = \mathbf{1}$.

The two forms agree in the expected way: a sequence has an $(A, \mathbf{1})$ -weighted zero-sum subsequence if and only if it has one in the sense of Definition 2.1 with $B = \{1\}$, so $D_{A,1} = D_{A,\{1\}}$. We use both.

The elementary facts about Q_p that the constructions need are these. Since $\mathbb{Z}_p$ is a field, for $a, b \neq 0$ the quotient a/b is a square if and only if a and b have the same character, i.e.

$$(1) \quad a/b \in Q_p \iff (a \in Q_p \iff b \in Q_p).$$

And $-1 \in Q_p$ exactly when $p \not\equiv 3 \pmod{4}$; when that holds, $Q_p = -Q_p$ and $\chi(-a) = \chi(a)$ for all a . Both are standard, and both are used below only through (1) and the closure of Q_p under negation.

Definition 2.2 (the Paley colouring). Let $p \equiv 1 \pmod{4}$. Because $\chi(-a) = \chi(a)$, the assignment $\{x, y\} \mapsto \chi(x - y)$ is a well-defined 2-colouring of the edges of the complete graph on the vertex set $\mathbb{Z}_p$. A set of vertices is a *monochromatic triangle* if its three edges get the same colour; two disjoint edges of the same colour form a *monochromatic perfect matching* of their four endpoints.

3. THREE WEIGHT CONSTRUCTIONS

Each of the three lemmas below is proved for an arbitrary weight set A with the required memberships as hypotheses, and then specialised to $A = Q_p$; the general forms are what the control computations of §8 reuse. We state the Q_p forms.

Lemma 3.1 (repeated term). *Let p be a prime with -1 a square in $\mathbb{Z}_p$ (for odd p : $p \equiv 1 \pmod{4}$). If a sequence x in $\mathbb{Z}_p$ has two positions $i \neq j$ with $x_i = x_j$, then x has a $(Q_p, \mathbf{1})$ -weighted zero-sum subsequence.*

Proof. Take $J = \{i, j\}$ with weights $a_i = 1$ and $a_j = -1$. Both lie in Q_p , since $1 \in Q_p$ and $-1 \in Q_p$ by hypothesis; and $1 + (-1) = 0$, $1 \cdot x_i + (-1) \cdot x_j = x_i - x_j = 0$. $\square$

Lemma 3.2 (monochromatic triangle). *Let p be a prime, x a sequence in $\mathbb{Z}_p$ and i, j, k three distinct positions with x_i, x_j, x_k pairwise distinct. If the three cyclic differences have the same quadratic character,*

$$\chi(x_i - x_j) = \chi(x_j - x_k) = \chi(x_k - x_i),$$

then x has a $(Q_p, \mathbf{1})$ -weighted zero-sum subsequence.

Proof. Put $d = x_i - x_j \neq 0$ and take $J = \{i, j, k\}$ with

$$a_i = \frac{x_j - x_k}{d}, \quad a_j = \frac{x_k - x_i}{d}, \quad a_k = 1.$$

All three are nonzero, and $a_i, a_j \in Q_p$ by (1) together with the hypothesis that $x_j - x_k$ and $x_k - x_i$ have the same character as d ; $a_k = 1 \in Q_p$. Clearing the denominator, $a_i + a_j + a_k = ((x_j - x_k) + (x_k - x_i) + (x_i - x_j))/d = 0$ and $a_i x_i + a_j x_j + a_k x_k = ((x_j - x_k)x_i + (x_k - x_i)x_j + (x_i - x_j)x_k)/d = 0$, both identities in $\mathbb{Z}_p$. $\square$

Note that Lemma 3.2 needs no hypothesis on p : the character condition carries all the arithmetic. When -1 is a square, $\chi(x_i - x_j) = \chi(x_j - x_i)$ and the condition is exactly that $\{x_i, x_j, x_k\}$ is a monochromatic triangle of the Paley colouring.

Remark 3.3. The criterion of Lemma 3.2 is exact, though we use only the direction proved above. The following is an elementary observation and lies outside the formal development of §10. If x_i, x_j, x_k are pairwise distinct then the two linear conditions $\sum a = 0$, $\sum ax = 0$ have coefficient matrix of rank 2, so their solution space in $\mathbb{Z}_p^3$ is the line spanned by $(x_j - x_k, x_k - x_i, x_i - x_j)$; a nonzero multiple of that vector has all three coordinates in Q_p precisely when the three coordinates share a character. No proper subsequence can help: a singleton would need $a = 0$, and a pair of distinct terms would need $a(x_i - x_j) = 0$ with $a \neq 0$. So a triple of pairwise distinct terms is $(Q_p, \mathbf{1})$ -weighted zero-sum if and only if it is a monochromatic triangle. Theorem 9.2(c) verifies the “only if” direction in four instances at $p = 5$.

Lemma 3.4 (monochromatic perfect matching). *Let p be a prime with -1 a square in $\mathbb{Z}_p$, let x be a sequence in $\mathbb{Z}_p$ and let i, j, k, l be four distinct positions with $x_i \neq x_j$, $x_k \neq x_l$ and*

$$\chi(x_i - x_j) = \chi(x_k - x_l).$$

Then x has a $(Q_p, \mathbf{1})$ -weighted zero-sum subsequence.

Proof. Put $u = (x_i - x_j)/(x_k - x_l)$, which lies in Q_p by (1), and take $J = \{i, j, k, l\}$ with weights

$$a_i = 1, \quad a_j = -1, \quad a_k = -u, \quad a_l = u.$$

All four lie in Q_p : 1 and u do, and $-1, -u$ do because $Q_p = -Q_p$. Then $a_i + a_j + a_k + a_l = 1 - 1 - u + u = 0$, and

$$a_i x_i + a_j x_j + a_k x_k + a_l x_l = (x_i - x_j) - u(x_k - x_l) = (x_i - x_j) - (x_i - x_j) = 0. \quad \square$$

4. THE K_4 DICHOTOMY

Lemma 4.1. *Every 2-colouring of the edges of K_4 contains a monochromatic triangle or a monochromatic perfect matching.*

Proof. Suppose no perfect matching is monochromatic. The three perfect matchings of K_4 are the three pairs of opposite edges $\{01, 23\}$, $\{02, 13\}$, $\{03, 12\}$, and they partition the six edges; by hypothesis each pair is bichromatic, so each colour class contains exactly one edge from each pair and therefore has exactly three edges. A set of three edges of K_4 meeting every pair of opposite edges is either a triangle or a star at one vertex — there are eight such sets, four of each kind — and the complement of a star is a triangle. Either way one colour class contains a triangle. $\square$

Both clauses are needed on four vertices. The colouring with red class $\{01, 02, 12\}$ and blue class $\{03, 13, 23\}$ has no monochromatic perfect matching, and 18 of the 64 2-colourings of $E(K_4)$ have no monochromatic triangle. This is consistent with the Ramsey numbers: $R(K_3, K_3) = 6$, and the Ramsey number of two independent edges against itself is $R(2K_2, 2K_2) = 5$, a case of the Ramsey numbers for stripes of Cockayne and Lorimer [3]; so neither alternative alone holds on four vertices and only the disjunction does.

Remark 4.2. Lemma 4.1 is elementary and we have not found it stated anywhere under a name. In the formal development it appears in its propositional form: for any six propositions $P_{01}, P_{02}, P_{03}, P_{12}, P_{13}, P_{23}$, at least one of the four triangle conditions $(P_{01} \leftrightarrow P_{02}) \wedge (P_{02} \leftrightarrow P_{12})$, ..., $(P_{12} \leftrightarrow P_{13}) \wedge (P_{13} \leftrightarrow P_{23})$, or one of the three matching conditions $P_{01} \leftrightarrow P_{23}$, $P_{02} \leftrightarrow P_{13}$, $P_{03} \leftrightarrow P_{12}$, holds. That is a 64-case tautology.

5. THE UPPER BOUND

Theorem 5.1. *Let p be a prime with -1 a square in $\mathbb{Z}_p$ and let $x = (x_0, x_1, x_2, x_3)$ be a sequence of four distinct elements of $\mathbb{Z}_p$. Then x has a $(Q_p, 1)$ -weighted zero-sum subsequence.*

Proof. Colour the six pairs $\{x_a, x_b\}$ by $\chi(x_a - x_b)$; this is well defined because $\chi(-t) = \chi(t)$, and, the four terms being distinct, all six differences are nonzero. By Lemma 4.1 the colouring contains a monochromatic triangle or a monochromatic perfect matching. In the first case the three cyclic differences of the corresponding three terms share a character, and Lemma 3.2 applies. In the second case two disjoint pairs have differences of equal character, and Lemma 3.4 applies. $\square$

Theorem 5.2. *Let p be a prime with $p \equiv 1 \pmod{4}$. Then every sequence of length four in $\mathbb{Z}_p$ has a $(Q_p, 1)$ -weighted zero-sum subsequence; that is, $D_{Q_p,1}(p) \leq 4$.*

Proof. Since $p \equiv 1 \pmod{4}$, -1 is a square in $\mathbb{Z}_p$. If the four terms are not pairwise distinct, two of them coincide and Lemma 3.1 applies; otherwise Theorem 5.1 applies. $\square$

This is the whole of the new content; no case distinction beyond the two above is needed, and nothing in the proof is a computation.

6. THE VALUE

The lower bound is the source's, with an explicit witness in place of its appeal to $D_{Q_p} = 3$.

Proposition 6.1. *Let $p \equiv 1 \pmod{4}$ be a prime and let $n \in \mathbb{Z}_p$ be a non-residue. Then the length-three sequence $(1, n, 0)$ has no $(Q_p, 1)$ -weighted zero-sum subsequence. Hence $D_{Q_p,1}(p) \geq 4$.*

Proof. Write the three positions as 1, 2, 3, carrying the terms 1, n , 0, and suppose $J \neq \emptyset$ and $a_i \in Q_p$ ($i \in J$) satisfy $\sum_{i \in J} a_i = 0$ and $\sum_{i \in J} a_i x_i = 0$. The third term is 0, so the second condition involves only the positions 1, 2, and we distinguish four cases. If $1, 2 \in J$ it reads $a_1 + a_2 n = 0$, so $n = -a_1/a_2$; but $-a_1 \in Q_p$, since -1 is a square, and $a_2 \in Q_p$, so $-a_1/a_2 \in Q_p$ by (1), contradicting the choice of n . If $1 \in J$ and $2 \notin J$ it reads $a_1 = 0$, impossible; if $2 \in J$ and $1 \notin J$ it reads $a_2 n = 0$, impossible since $n \neq 0$. If neither lies in J then $J = \{3\}$, and the first condition reads $a_3 = 0$, impossible. Finally, a

sequence with no $(Q_p, \mathbf{1})$ -weighted zero-sum subsequence has prefixes with none either, so no length $k \leq 3$ can force one and $D_{Q_p, \mathbf{1}}(p) \geq 4$. $\square$

Theorem 6.2. *For every prime $p \equiv 1 \pmod{4}$,*

$$D_{Q_p, \mathbf{1}}(p) = 4.$$

Proof. Theorem 5.2 gives $D_{Q_p, \mathbf{1}}(p) \leq 4$. A non-residue n exists in every finite field of odd characteristic, so Proposition 6.1 applies and gives $D_{Q_p, \mathbf{1}}(p) \geq 4$. (Concretely, lengths 0, 1, 2 are also refuted by the empty sequence, by (0) and by (0, 1), in each case because $0 \notin Q_p$.) $\square$

This is the statement [8, §6] calls a belief. Its conditional consequence, with the hypothesis [8] states it under, now follows unconditionally.

Theorem 6.3. *Let $p \equiv 1 \pmod{4}$ be a prime and let $B \subseteq \mathbb{Z}_p$ be nonempty with $0 \notin B$. Then $D_{Q_p, B}(p) = 4$.*

Proof. Upper bound: fix any $c \in B$. Given a sequence of length four, Theorem 5.2 produces J and weights $a_i \in Q_p$ with $\sum_{i \in J} a_i = 0$ and $\sum_{i \in J} a_i x_i = 0$; taking $b_i = c$ for all $i \in J$ gives $\sum_{i \in J} b_i a_i = c \sum_{i \in J} a_i = 0$, so the same J works for (Q_p, B) . Lower bound: the witness $(1, n, 0)$ of Proposition 6.1 still has no (Q_p, B) -weighted zero-sum subsequence. Indeed three of the four cases of that proof use only the condition $\sum_{i \in J} a_i x_i = 0$ and are unchanged; the fourth, $J = \{3\}$, now requires $b_3 a_3 = 0$, which is impossible because $0 \notin B$ and $0 \notin Q_p$. Again a bad sequence has bad prefixes, so $D_{Q_p, B}(p) \geq 4$. $\square$

Remark 6.4. The source states the upper-bound step, in the proofs of its Theorems 5.1, 5.4 and 5.5, as “every $(Q_p, \mathbf{1})$ -weighted zero-sum sequence is a (Q_p, B) -weighted zero-sum sequence”, without an argument. The constant choice $b_i = c$ used above supplies one, for every nonempty B ; taking $b_i = 1$ instead would need $1 \in B$.

7. THE OTHER RESIDUE CLASS, AND THE CONSTANT AT EVERY ODD PRIME

For completeness we record the two theorems of [8] that settle the complementary class; both are reproduced here, not new. The first is the upper bound of its Theorem 4.2.

Theorem 7.1 ([8, Theorem 4.2, upper bound]). *For every odd prime p , every sequence of length five in $\mathbb{Z}_p$ has a $(Q_p, \mathbf{1})$ -weighted zero-sum subsequence; that is, $D_{Q_p, \mathbf{1}}(p) \leq 5$.*

Proof, following [8]. Given $x \in \mathbb{Z}_p^5$, consider the two forms $f_1 = \sum_i x_i X_i^2$ and $f_2 = \sum_i X_i^2$ in five variables over $\mathbb{Z}_p$. Their total degrees sum to $2 + 2 = 4 < 5$, so by Chevalley–Warning [9] the number of common zeros is divisible by p ; since the zero vector is one, there are at least $p > 1$ of them and hence a nonzero common zero u . Let $J = \{i : u_i \neq 0\}$, which is nonempty, and set $a_i = u_i^2$ for $i \in J$. Each a_i is a nonzero square, so $a_i \in Q_p$; $\sum_{i \in J} a_i = f_2(u) = 0$ and $\sum_{i \in J} a_i x_i = f_1(u) = 0$. $\square$

Proposition 7.2 ([8, Theorem 4.3, lower bound]). *Let $p \equiv 3 \pmod{4}$ be a prime. Then $(1, 1, 0, 0)$ has no $(Q_p, \mathbf{1})$ -weighted zero-sum subsequence, so $D_{Q_p, \mathbf{1}}(p) \geq 5$.*

Proof. For $p \equiv 3 \pmod{4}$ the element -1 is a non-residue, so no two elements of Q_p sum to 0: if $a + b = 0$ with $a, b \in Q_p$ then $a/b = -1$ would be a square by (1). Now let J and (a_i) witness a weighted zero-sum subsequence of $(1, 1, 0, 0)$, with the four positions numbered $1, \dots, 4$. Since the last two terms are 0, the condition $\sum_{i \in J} a_i x_i = 0$ says $a_1 + a_2 = 0$ if $1, 2 \in J$, and $a_1 = 0$ or $a_2 = 0$ if exactly one of them is in J ; all three are impossible. So $J \subseteq \{3, 4\}$, and then $\sum_{i \in J} a_i = 0$ says $a_3 + a_4 = 0$ or $a_3 = 0$ or $a_4 = 0$, impossible for the same two reasons. $\square$

Theorem 7.3 ([8, Theorem 4.3]). *For every prime $p \equiv 3 \pmod{4}$, $D_{Q_p, \mathbf{1}}(p) = 5$.*

Proof. Theorem 7.1 and Proposition 7.2, with lengths 0, 1, 2 excluded as in Theorem 6.2 and length three excluded by $(1, 1, 0)$, using again that no two elements of Q_p sum to 0. $\square$

Corollary 7.4. *For every odd prime p ,*

$$D_{Q_p,1}(p) = \begin{cases} 4, & p \equiv 1 \pmod{4}, \\ 5, & p \equiv 3 \pmod{4}. \end{cases}$$

Proof. Theorem 6.2 and Theorem 7.3. $\square$

8. CONTROLS AND VARIANTS

Two further values delimit the result. The first shows that 4 is not an artefact of the shape of Definition 2.1: enlarging the weight set to all of $U(p)$ lowers the constant. This value is known — it is [7, Theorem 3.3], stated there as $D_{\mathbb{Z}'_n,1} = 3$ for $\mathbb{Z}'_n = \mathbb{Z}_n \setminus \{0\}$, which for $n = p$ prime is $U(p)$.

Proposition 8.1 ([7, Theorem 3.3]). *For every prime p , $D_{U(p),1}(p) = 3$.*

Proof. For the upper bound, let x have length three. If two terms coincide, the weights $(1, -1)$ work, both being units. If the three terms are distinct, the weight vector of Lemma 3.2 works: for $A = U(p)$ its entries only have to be nonzero, which they are, and no character condition is needed. Lengths 0, 1, 2 are excluded as before, using $0 \notin U(p)$. $\square$

The second shows that Q_p is not distinguished between the two cosets of Q_p in $U(p)$.

Proposition 8.2. *For every prime $p \equiv 1 \pmod{4}$, $D_{N_p,1}(p) = 4$.*

Proof. Fix a non-residue n . Then $N_p = nQ_p$, and multiplying all weights by n (or by n^{-1}) turns a $(Q_p, \mathbf{1})$ -weighted zero-sum subsequence into an $(N_p, \mathbf{1})$ -weighted one and back, because both defining conditions are homogeneous of degree one in the weights. So the two constants agree and Theorem 6.2 applies; the lower bound transports likewise, the witness being the same $(1, n, 0)$. $\square$

9. INDEPENDENT EVALUATION AT SMALL PRIMES

The general argument was checked against direct evaluation. For the machine, the definition is rephrased with square roots of the weights: for $x \in \mathbb{Z}_p^k$ let $G_p(x)$ be the statement that there is a vector $u \in \mathbb{Z}_p^k$, not identically zero, with $\sum_i u_i^2 = 0$ and $\sum_i u_i^2 x_i = 0$.

Proposition 9.1. *For every prime p and every $x \in \mathbb{Z}_p^k$, $G_p(x)$ holds if and only if x has a $(Q_p, \mathbf{1})$ -weighted zero-sum subsequence.*

Proof. If u is as in $G_p(x)$, take $J = \{i : u_i \neq 0\}$ and $a_i = u_i^2 \in Q_p$; the terms with $u_i = 0$ contribute nothing to either sum. Conversely, given J and $(a_i)_{i \in J}$, choose for each $i \in J$ a square root u_i of a_i — nonzero because $a_i \neq 0$ — and set $u_i = 0$ off J . $\square$

Theorem 9.2. *The following hold, each by exhaustive evaluation of G_p .*

- (a) *Every $x \in \mathbb{Z}_5^4$ has a $(Q_5, \mathbf{1})$ -weighted zero-sum subsequence. (The instance $p = 5$ of Theorem 5.2, obtained without using it.)*
- (b) *The sequence $(1, 2, 0)$ in $\mathbb{Z}_5$, where 2 is a non-residue, has no $(Q_5, \mathbf{1})$ -weighted zero-sum subsequence. (The instance $p = 5$ of Proposition 6.1.)*
- (c) *At $p = 5$, none of the four triples $(0, 1, 2)$, $(0, 1, 3)$, $(0, 2, 3)$, $(1, 2, 3)$ has a $(Q_5, \mathbf{1})$ -weighted zero-sum subsequence, while the quadruple $(0, 1, 2, 3)$ does.*
- (d) *The sequence $(1, 1, 0, 0)$ has no $(Q_7, \mathbf{1})$ -weighted zero-sum subsequence, but does have a $(Q_5, \mathbf{1})$ -weighted one.*

Proof. Each item is decided by evaluating G_p over all vectors involved: for (a), over all 5^4 sequences and, for each, all 5^4 vectors u ; for (b)–(d), over the 5^3 , 5^4 or 7^4 vectors u attached to each of the sequences named. These are the only numbered statements in this paper that rest on exhaustive computation, and none of them is used in the proof of any other statement. (Remark 9.3 reports a further computation, outside the formal development, that nothing depends on.) $\square$

Item (c) is the non-vacuity control for the matching clause: at $p = 5$ the four-element set $\{0, 1, 2, 3\}$ carries no monochromatic triangle of the Paley colouring — by Remark 3.3 that is what the four negative statements say — yet the quadruple is good, necessarily through the monochromatic perfect matching $\{0, 1\} \mid \{2, 3\}$. So Lemma 3.4 is doing work that Lemma 3.2 cannot do. Item (d) shows that the hypothesis $p \equiv 1 \pmod{4}$ in Theorem 5.2 cannot be dropped, on one and the same sequence.

Remark 9.3 (a computation outside the formal development). Independently of everything above, three programs written directly from Definition 2.1 — a naive enumeration with no symmetry reduction, a dynamic program over the state $(\sum a, \sum ax) \in \mathbb{Z}_p^2$, and a meet-in-the-middle search over a $2 \mid 2$ split of the four positions — were used to evaluate $D_{Q_p,1}(p)$ directly. They agree wherever their ranges overlap, and the third confirms Corollary 7.4 at all 168 odd primes $p \leq 1009$: the value is 4 at all 81 primes $p \equiv 1 \pmod{4}$ in that range and 5 at all 87 primes $p \equiv 3 \pmod{4}$, in 453 seconds and 3.6 MB of memory. The same sweep counts, for $p \equiv 1 \pmod{4}$, the four-element subsets of $\mathbb{Z}_p$ that contain 0 and 1 — the normal form the sweep uses; the affine maps $x \mapsto cx + t$, $c \in U(p)$, carry every four-element subset to one of these and either preserve the colouring ($c \in Q_p$) or exchange the two colours ($c \in N_p$) — which carry no monochromatic triangle: 3, 21, 39, 111, 189, 228 at $p = 5, 13, 17, 29, 37, 41$ respectively, out of 3, 55, 105, 351, 595, 741 such subsets; every single one of them carries a monochromatic perfect matching. These figures are corroboration only; they are not part of the formal development and no theorem above depends on them.

10. VERIFICATION

Every numbered statement above except Remarks 3.3 and 9.3 has been machine-checked in Lean 4 [4] against Mathlib [5], in five files: the definitions and the arithmetic of Q_p ; the three weight constructions of §3, the K_4 dichotomy and the upper bound; the lower bounds, the value $D_{Q_p,1} = 4$, the (Q_p, B) theorem and the controls of §8; the Chevalley–Warning bound and the $p \equiv 3 \pmod{4}$ case, on Mathlib’s `char_dvd_card_solutions_of_add_1t`; and the decidable form G_p with the per-prime evaluations. Theorems 5.1, 5.2, 6.2, 6.3, 7.1 and 7.3, Lemmas 3.1, 3.2, 3.4 and 4.1, and Propositions 6.1, 7.2, 8.1, 8.2 and 9.1 are all kernel-checked with the standard axiom closure — propositional extensionality, quotient soundness and the axiom of choice — and no appeal to compiled evaluation. The four parts of Theorem 9.2 are the only statements that carry an additional axiom recording a compiled exhaustive evaluation, and, as noted there, nothing else depends on them: deleting them removes no statement that another file does not already prove. Corollary 7.4 is the conjunction of Theorems 6.2 and 7.3 and is checked through them. There is no `sorry` in the development. Repository reference to be added at submission.

11. WHAT REMAINS

- (1) *Other index- d weight sets.* Proposition 8.2 says the non-residues give the same constant, which is a rescaling. The genuine generalisation replaces Q_p by the d -th power residues, a subgroup of index d in $U(p)$. The mechanism above becomes a d -colouring of the complete graph on $\mathbb{Z}_p$ and asks for a monochromatic triangle or a monochromatic matching; Lemma 4.1 fails for $d \geq 3$, so the answer should grow with d , and we know no value.
- (2) *Composite modulus.* For n an odd prime power or a product of two primes the squares are no longer of index two in $U(n)$, and the criterion of Lemma 3.2 — which rests on (1) in a field — has to be replaced. We found no literature on $D_{Q_n,1}(n)$ for composite n .
- (3) *The other constants.* The source determines the consecutive-subsequence and length- p variants: $C_{Q_p,1} = 6$ for $p \equiv 1 \pmod{4}$ and 9 for $p \equiv 3 \pmod{4}$ (its Theorems 3.8–3.11), and $E_{Q_p,1} = p + 2$ for $p \neq 5$ with $E_{Q_5,1} = 9$ (its Theorem 2.14 and Corollary 2.4). We have reproduced neither, and neither is affected by the results here. The singly-weighted analogues $D_{Q_p}(p) = 3$ and $C_{Q_p}(p) = 3$ are [1, Theorem 3] and [6, Theorem 4].
- (4) *The $p \equiv 3 \pmod{4}$ half of the (Q_p, B) question.* Theorem 6.3 settles the class $p \equiv 1 \pmod{4}$ for every nonempty B avoiding 0, which is the half of [8, Theorem 5.5] that reads $D_{Q_p,B} \in \{4, 5\}$. Its other half, $D_{Q_p,B} = 5$ for $p \equiv 3 \pmod{4}$ under the stronger hypothesis $B \subseteq$

Q_p , is already a theorem there; we have not reproduced it. Its lower bound rests on [8, Observation 5.3], which is where $B \subseteq Q_p$ is used: it forces $-1 \in Q_p$, hence $p \equiv 1 \pmod{4}$, from a length-two (Q_p, B) -weighted zero-sum sequence, so for $p \equiv 3 \pmod{4}$ every such sequence has length at least three.

REFERENCES

- [1] S. D. Adhikari and P. Rath, *Davenport constant with weights and some related questions*, *Integers* **6** (2006), #A30. Its Theorem 3 gives, for A the set of quadratic residues mod p , the values $D_A(p) = 3$ and $E_A(p) = p + 2$.
- [2] S. D. Adhikari, Md. I. Molla and S. Paul, *Extremal sequences for some weighted zero-sum constants for cyclic groups*, in: M. B. Nathanson (ed.), *Combinatorial and Additive Number Theory IV*, Springer Proceedings in Mathematics & Statistics **347**, Springer, 2021, 1–10; DOI 10.1007/978-3-030-67996-5_1. Cited by [8] for $D_{Q_p}(p) = 3$. Not read; see §1.
- [3] E. J. Cockayne and P. J. Lorimer, *The Ramsey number for stripes*, *Journal of the Australian Mathematical Society, Series A* **19** (1975), 252–256. Used here only for $R(2K_2, 2K_2) = 5$, in the calibration remark after Lemma 4.1.
- [4] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: *Automated Deduction — CADE 28*, Lecture Notes in Computer Science 12699, Springer, 2021, 625–635; DOI 10.1007/978-3-030-79876-5_37.
- [5] The mathlib Community, *The Lean mathematical library*, in: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)*, ACM, 2020, 367–381; DOI 10.1145/3372885.3373824.
- [6] S. Mondal, K. Paul and S. Paul, *On a different weighted zero-sum constant*, *Discrete Mathematics* **346** (2023), no. 6, article 113350, 8 pp.; e-print arXiv:2110.02539. Its Theorem 4 gives $C_{Q_p}(p) = 3$ for every odd prime p (and $C_{Q_2}(2) = 2$); this is the numbering both of the e-print and of the citation “Theorem 4 of [6]” in [8].
- [7] K. Paul and S. Paul, *Doubly-weighted zero-sum constants*, arXiv:2311.00090 [math.NT]. The paper that introduces $D_{A,B}$; Observations 3.1 and 3.2, Theorems 3.3 and 3.4 are the items discussed in §1 and §8. Cited here in its latest e-print version (v4, 8 July 2026); no journal version is recorded.
- [8] K. Paul and S. Paul, *Q_p -weighted zero-sum constants*, arXiv:2601.14122 [math.NT] (20 January 2026), 14 pages. Its only version is v1; no journal reference is recorded, and every numbered reference to it above is to that version. Theorems 4.2 and 4.3 and the concluding §6 are quoted in §1.
- [9] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer, 1973. Chapter I contains the Chevalley–Warning theorem used in Theorem 7.1; it is the reference [8] gives for it.