Mathematical proof note

The Euclidean-Weight GCD of Self-Dual Codes over Odd Residue Rings

Yang Shifu
National Mobile Communications Research Laboratory and the Frontiers Science Center for Mobile Information Communication and Security, Southeast University, Nanjing 211189, China
Version 1.0 — October 8, 2026

Result overview

For a self-dual code over an integer residue ring, self-orthogonality makes the modulus a common divisor of the Euclidean weights. We prove that, for every odd modulus $m \geq 3$, the greatest common divisor of all nonzero Euclidean weights is exactly m. The proof applies to nonfree codes as well as free codes. A finite-field character coefficient isolates coordinate lines and excludes every prime different from the characteristic. Residue–top-torsion duality transfers this exclusion to prime-power rings. A saturation argument and scalar-orbit sum rule out one additional factor of the characteristic. Exact scaling of balanced representatives then assembles the result over composite odd moduli.

1 Context and Main Theorem

Euclidean-weight divisibility connects self-dual ring codes to Construction A and unimodular lattices. It concerns the entire integer weight spectrum together with its minimum. The corresponding divisibility questions are discussed in [1]; the published even-modulus alternative is recorded in [2]. The odd case must accommodate nonfree modules and exact integer representatives, which require the full residue-ring module structure and the Chinese remainder theorem (CRT).

Let $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. For odd m, write $\mathrm{bal}_m(a)$ for the unique integer congruent to a in $[-(m-1)/2, (m-1)/2]$, and define

$$\mathrm{ew}_m(a) = \mathrm{bal}_m(a)^2, \qquad w_m(c) = \sum_{j=1}^{n} \mathrm{ew}_m(c_j). \tag{1}$$

For a nonzero code $C \leq \mathbb{Z}_m^n$, let

$$D_m(C) = \gcd\{w_m(c) : c \in C \setminus \{0\}\}. \tag{2}$$

Duality uses the standard dot product modulo m. The pairing is nondegenerate and $|C||C^\perp| = m^n$ [3]. A positive-length self-dual code is therefore nonzero. Self-orthogonality gives

$$w_m(c) \equiv c \cdot c \equiv 0 \pmod{m}, \qquad m \mid D_m(C). \tag{3}$$

Theorem 1.1. *For every odd $m \geq 3$, every $n \geq 1$, and every self-dual code $C \leq \mathbb{Z}_m^n$,*

$$D_m(C) = m. \tag{4}$$

No freeness assumption is needed.

The proof separates prime support from prime-adic valuation. Section 2 establishes a field obstruction for dual-containing codes. Section 3 transfers it through the top-torsion layer and excludes an extra characteristic factor. Section 4 uses an exact CRT weight identity.

2 A Foreign-Prime Obstruction over the Field

Let p be an odd prime and $\ell \neq p$ another prime. In an algebraic closure K of $\mathbb{F}_\ell$, choose a primitive pth root ζ and put $\chi(t) = \zeta^t$ for $t \in \mathbb{F}_p$. For $f : \mathbb{F}_p \to K$ with $f(0) = 0$, define

$$\widehat{f}(\lambda) = \sum_{t \in \mathbb{F}_p} f(t)\chi(-\lambda t). \tag{5}$$

The character transform is invertible because p is nonzero in K. If f is nonconstant, some $s \neq 0$ has $\widehat{f}(s) \neq 0$.

Lemma 2.1. *Let G have nonzero columns $\gamma_r \in \mathbb{F}_p^k$, with zero columns omitted. For $F(x) = \sum_r f(x \cdot \gamma_r)$ and $y \in \mathbb{F}_p^k$,*

$$\sum_x F(x)\chi(-x \cdot y) = p^{k-1} \sum_r \sum_{y = \lambda\gamma_r} \widehat{f}(\lambda). \tag{6}$$

Each coordinate contributes only on its coefficient line.

Proof. For a nonzero γ_r, the map $x \mapsto x \cdot \gamma_r$ is onto, with fibres of size p^{k-1}. On a fibre with value t, the character sum is zero unless $y \in \mathbb{F}_p\gamma_r$. If $y = \lambda\gamma_r$, the sum equals $p^{k-1}\chi(-\lambda t)$. Summing over t and then over the coordinates proves (6). A zero column contributes $f(0) = 0$. □

This line-support calculation is the coordinate-retaining coefficient form underlying the complete weight enumerator MacWilliams transform [4]. Here it is proved directly, so the needed rigidity follows from the coordinate-retaining coefficient identity.

Proposition 2.2. *If $U \leq \mathbb{F}_p^n$ has positive length and $U^\perp \leq U$, no prime $\ell \neq p$ divides every Euclidean weight $w_p(u)$.*

Proof. Suppose such an ℓ exists. Put $k = \dim U \geq n/2$ and, after a coordinate permutation, choose $G = [I_k \mid A]$. Denote the columns of A by a_j. Reduce $f(t) = \mathrm{ew}_p(t)$ modulo ℓ, viewing the result in K. Since $f(0) = 0$ and $f(1) = 1$, choose $s \neq 0$ with $\widehat{f}(s) \neq 0$. The assumed divisibility says

$$F(x) = \sum_{i=1}^{k} f(x_i) + \sum_{j=1}^{n-k} f(x \cdot a_j) = 0.$$

The coefficient at $y = se_i$ in (6) contains the nonzero systematic contribution $p^{k-1}\widehat{f}(s)$. Hence some parity column lies on $\mathbb{F}_p^* e_i$. Distinct systematic lines require distinct parity columns, giving $n - k \geq k$. Therefore $n = 2k$ and A is monomial. Dual containment becomes self-duality, so

$$AA^{\mathsf{T}} = -I_k. \tag{7}$$

Each nonzero entry α satisfies $\alpha^2 = -1$. This is impossible for $p \equiv 3 \pmod 4$.

For $p \equiv 1 \pmod 4$, fix such an entry and put $r = \lfloor \sqrt{p} \rfloor$. Among the $(r+1)^2 > p$ residues $a + \alpha b$ with $0 \leq a, b \leq r$, two coincide. Their difference gives integers u, v, not both zero, with $|u|, |v| \leq r$ and $u + \alpha v \equiv 0 \pmod p$. Thus $v \equiv \alpha u$ and $p \mid u^2 + v^2$. Since

$$0 < u^2 + v^2 \leq 2r^2 < 2p,$$

we have $u^2 + v^2 = p$. Moreover $r < p/2$ for $p \geq 5$, so u, v are balanced representatives. The information vector ue_i gives a codeword whose two nonzero coordinates are u and αu, with weight exactly p. This contradicts divisibility by ℓ. □

3 Prime-Power Rings without Freeness

Fix $R_e = \mathbb{Z}/p^e\mathbb{Z}$, and let $C \leq R_e^n$ be self-dual. Define its residue and top-torsion codes by

$$B = C \bmod p, \qquad T = \{x \in \mathbb{F}_p^n : p^{e-1}x \in C\}. \tag{8}$$

The condition defining T is independent of the lift of x.

Lemma 3.1. *$T = B^\perp$, and $B = T^\perp \leq T$. Every prime divisor of $D_{p^e}(C)$ is p.*

Proof. The condition $x \in B^\perp$ is equivalent to $p^{e-1}x$ being orthogonal over R_e to every word of C, and hence, by self-duality, to $p^{e-1}x \in C$. Reduction of self-orthogonality gives $B \leq B^\perp = T$, so T is dual-containing. Exact balanced-representative scaling gives

$$w_{p^e}(p^{e-1}x) = p^{2e-2}w_p(x). \tag{9}$$

If $\ell \neq p$ divided every weight of C, (9) would make it divide every weight of T, contrary to Proposition 2.2. □

Lemma 3.2. *If $e \geq 2$ and every weight of C is divisible by p^{e+1}, then B is self-dual over $\mathbb{F}_p$.*

Proof. Let $K_1 = \{x \in R_{e-1}^n : px \in C\}$. The integer identity $w_{p^e}(px) = p^2 w_{p^{e-1}}(x)$ implies $x \cdot x = 0$ in R_{e-1} for every $x \in K_1$. Since p is odd, polarization gives $K_1 \leq K_1^\perp$, so $|K_1| \leq p^{(e-1)n/2}$. Reduction gives an exact sequence

$$0 \longrightarrow K_1 \xrightarrow{x \mapsto px} C \longrightarrow B \longrightarrow 0.$$

Since $|C| = p^{en/2}$, we get $|B| \geq p^{n/2}$. But B is self-orthogonal, whence $|B| \leq p^{n/2}$. Equality forces $B = B^\perp$; in particular, its dimension is $n/2$. □

Lemma 3.3. *For odd M, let $S_M = \sum_{a\in\mathbb{Z}_M} \mathrm{ew}_M(a)$. Then*

$$S_M = \frac{M(M^2-1)}{12}, \qquad \sum_{t\in R_e} \mathrm{ew}_{p^e}(ta) = p^{3v} S_{p^{e-v}} \tag{10}$$

for nonzero $a \in R_e$ of valuation $v < e$.

Proof. The first identity is $2\sum_{j=1}^{(M-1)/2} j^2$. Multiplication by $a = p^v u$ maps R_e onto $p^v R_e$ with each image occurring p^v times. Balanced representatives in the image scale by p^v, which proves the second identity. □

Proposition 3.4. *For every positive-length self-dual $C \le R_e^n$, $D_{p^e}(C) = p^e$.*

Proof. By (3) and Lemma 3.1, the gcd is a power of p divisible by p^e. Suppose every weight were divisible by p^{e+1}. The residue code B is self-dual, directly if $e = 1$ and by Lemma 3.2 otherwise.

For $c \in C$, put $N_v(c) = \#\{j : \nu_p(c_j) = v\}$, omitting zero coordinates. Sum the assumed divisibility over all scalar multiples of c. Lemma 3.3 yields

$$\sum_{v=0}^{e-1} N_v(c) p^{3v} S_{p^{e-v}} \equiv 0 \pmod{p^{e+1}}. \tag{11}$$

For $p \ge 5$, division by p^e and reduction modulo p leave $-N_0(c)/12 = 0$. Thus every Hamming weight of B is divisible by p. For $p = 3$, division by 3^{e-1} gives

$$\sum_{v=0}^{e-1} N_v(c) 3^{2v} \frac{3^{2(e-v)} - 1}{4} \equiv 0 \pmod 9.$$

All terms with $v \ge 1$ vanish modulo 9, and the $v = 0$ factor is a unit modulo 9. Hence every Hamming weight of B is divisible by 9.

Both conclusions contradict the Gleason–Pierce Hamming-divisor classification for positive-length self-dual field codes [5, 6]: for odd prime $p \ge 5$, a Hamming divisor p is impossible; the ternary case permits divisor 3 and excludes 9. This rules out p^{e+1} and proves the proposition. □

4 Exact Chinese Remainder Assembly

Proof of Theorem 1.1. Write $m = \prod_{i=1}^s q_i$ as a product of coprime odd prime powers, and let $M_i = m/q_i$. Under CRT, C decomposes into self-dual component codes $C_i \le \mathbb{Z}_{q_i}^n$ [3]. Choose u_i with $M_i u_i \equiv 1 \pmod{q_i}$. The idempotent $\varepsilon_i = M_i u_i \pmod m$ embeds C_i into C with every other component zero.

For $y \in \mathbb{Z}_{q_i}$, the integer $M_i \,\mathrm{bal}_{q_i}(y)$ has absolute value strictly below $m/2$. Therefore

$$\mathrm{bal}_m(M_i y) = M_i \,\mathrm{bal}_{q_i}(y), \qquad \mathrm{ew}_m(M_i y) = M_i^2 \,\mathrm{ew}_{q_i}(y). \tag{12}$$

Applying this to $\varepsilon_i x = M_i(u_i x)$ gives $w_m(\varepsilon_i x) = M_i^2 w_{q_i}(u_i x)$. Since multiplication by the unit u_i permutes C_i, Proposition 3.4 implies

$$D_m(C) \mid M_i^2 D_{q_i}(C_i) = M_i^2 q_i = m M_i \tag{13}$$

for every i. Write $D_m(C) = md$ using (3). Then $d \mid M_i$ for all i. No prime divides all the complementary factors M_i, so $d = 1$. □

5 A Nonfree Example and the Result

The length-one code $C = 3\mathbb{Z}_9 \leq \mathbb{Z}_9$ is self-dual: orthogonality to 3 requires a residue to be divisible by 3. Its two nonzero words have balanced representatives $3, -3$ and Euclidean weight 9, so $D_9(C) = 9$. This example lies outside the free-code setting.

The general theorem follows by excluding foreign primes through coordinate-line rigidity, excluding excess characteristic valuation through saturation and scalar orbits, and assembling exact integer weights under CRT. These three steps establish the Euclidean-weight gcd for every self-dual module type over every odd modulus.

Sources

[1] D. Joyner and J.-L. Kim, *Selected Unsolved Problems in Coding Theory*, ser. Applied and Numerical Harmonic Analysis. Boston: Birkhäuser Boston, 2011, doi: 10.1007/978-0-8176-8256-9.

[2] E. Bannai, S. T. Dougherty, M. Harada, and M. Oura, "Type II codes, even unimodular lattices, and invariant rings," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1194–1205, May 1999, doi: 10.1109/18.761269.

[3] S. T. Dougherty, M. Harada, and P. Solé, "Self-dual codes over rings and the Chinese Remainder Theorem," *Hokkaido Mathematical Journal*, vol. 28, no. 2, pp. 253–283, 1999, doi: 10.14492/hokmj/1351001213.

[4] J. A. Wood, "Foundations of linear codes defined over finite modules: The extension theorem and the MacWilliams identities," in *Codes over Rings*. Singapore: World Scientific, 2009, pp. 124–190, doi: 10.1142/9789812837691_0004.

[5] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, ser. Algorithms and Computation in Mathematics. Berlin: Springer, 2006, vol. 17, doi: 10.1007/3-540-30731-1.

[6] H. N. Ward, "An introduction to divisible codes," *Designs, Codes and Cryptography*, vol. 17, no. 1–3, pp. 73–79, Sep. 1999, doi: 10.1023/A:1008302520762.