AN ARITHMETIC CRITERION FOR ORTHOGONAL BASES OF CYCLIC RATIONAL LATTICES

Abstract. For $a \in \mathbb{Q}^n$, we give a finite arithmetic criterion for $\mathbb{Z}^n + \mathbb{Z}a$ to have an orthogonal integral basis. The test examines primitive integer directions of squared length at most the least common denominator of a, using two divisibility conditions and a count. Its proof computes the exact lattice spacing on each rational line and identifies the rank-one orthogonal factors. This addresses the literal criterion requested in Kourovka Problem 9.45; no efficiency or priority claim is made.

1. The criterion

Problem 9.45 of the *Kourovka Notebook* [2] reads:

> Let a be a vector in $\mathbb{R}^n$ with rational coordinates and set
> $$S(a) = \{ka + b \mid k \in \mathbb{Z},\ b \in \mathbb{Z}^n\}.$$
> It is obvious that $S(a)$ is a discrete subgroup in $\mathbb{R}^n$ of rank n. Find necessary and sufficient conditions in terms of the coordinates of a for $S(a)$ to have an orthogonal basis with respect to the standard scalar product in $\mathbb{R}^n$.
>
> Yu. D. Popov, I. V. Protasov

Assume $n \geq 1$ and write $L = \mathbb{Z}^n + \mathbb{Z}a$. Write each coordinate $a_j = p_j/r_j$ in lowest terms, with $r_j > 0$ and $r_j = 1$ if $a_j = 0$. Set

$$q = \operatorname{lcm}(r_1, \ldots, r_n), \qquad c = qa \in \mathbb{Z}^n.$$

For a primitive integer vector $u = (u_1, \ldots, u_n)$, meaning $\gcd(u_1, \ldots, u_n) = 1$, put

$$D(u) = \sum_{j=1}^{n} u_j^2, \qquad t(u) = \gcd\bigl(q, \{c_i u_j - c_j u_i : 1 \leq i < j \leq n\}\bigr).$$

Gcds are positive; the gcd of q and an empty list is q. Define the finite set

$$U(a) = \{u \in \mathbb{Z}^n : \gcd(u_1, \ldots, u_n) = 1, \quad 1 \leq D(u) \leq q, \quad D(u) \mid t(u), \quad qD(u) \mid t(u)\langle c, u\rangle\}. \tag{1}$$

Theorem 1. *The lattice L has an orthogonal $\mathbb{Z}$-basis if and only if $|U(a)| = 2n$. Always $|U(a)| \leq 2n$. When equality holds, choose one representative $u^{(i)}$ from each pair $\{u, -u\}$ in $U(a)$. Then*

$$b_i = \frac{u^{(i)}}{t(u^{(i)})} \qquad (1 \leq i \leq n)$$

is an orthogonal $\mathbb{Z}$-basis of L.

This is a condition solely in the coordinates of a: it requires gcds, divisibility and a count in the fixed box $|u_j| \leq \lfloor\sqrt{q}\rfloor$. It makes no claim of polynomial complexity. For $n = 1$, it gives $U(a) = \{-1, 1\}$, $t = q$ and the basis $1/q$. For integral a, it gives $q = 1$ and $U(a) = \{\pm e_j : 1 \leq j \leq n\}$, where e_j are the standard coordinate vectors. In dimension zero the empty basis settles the question separately.

Bardakov's known sufficient condition is that the reduced coordinate denominators be pairwise coprime [1, §4, Proposition 1]. The criterion here imposes no such hypothesis and allows all

Date: Draft, September 15, 2026.

rational directions. Its proof uses elementary integer arithmetic and orthogonal projection, with every required implication proved below. The contribution under review is the explicit gcd-of-minors formula and direction count. The earlier paper *Cyclic lattices* by Popov and Protasov [3] has been identified bibliographically, but its original text was unavailable for comparison. Accordingly, originality remains provisional; no first-algorithm claim is made.

2. Exact spacing on a rational line

By the choice of reduced denominators, q is the least positive integer with $qa \in \mathbb{Z}^n$. Thus $L/\mathbb{Z}^n$ is cyclic of order q, the residue of c modulo q has order q, and $\gcd(q, c_1, \dots, c_n) = 1$. Indeed, a common divisor greater than one would produce a smaller common denominator. Membership is given by

$$z/q \in L \quad \Longleftrightarrow \quad z \equiv kc \pmod{q} \text{ for some } k \in \mathbb{Z} \qquad (z \in \mathbb{Z}^n). \tag{2}$$

Lemma 2. *For each primitive $u \in \mathbb{Z}^n$,*

$$L \cap \mathbb{R}u = \mathbb{Z}\frac{u}{t(u)}.$$

Proof. Choose integers v_j with $\sum_j v_j u_j = 1$. If $\lambda u \in L$, then $q\lambda u$ is integral, so $q\lambda = \sum_j v_j(q\lambda u_j) \in \mathbb{Z}$. The allowed scalars therefore form a subgroup between $\mathbb{Z}$ and $(1/q)\mathbb{Z}$. Such a subgroup is $(1/s)\mathbb{Z}$ for some divisor s of q. Put $t = t(u)$.

Since $u/s \in L$, there is $k \in \mathbb{Z}$ with $(q/s)u \equiv kc \pmod{q}$. Primitivity makes the order of the residue on the left exactly s, whereas that of kc is $q/\gcd(q,k)$. Hence $k = (q/s)k'$ with $\gcd(k', s) = 1$. Dividing the congruence gives $u \equiv k'c \pmod{s}$. Thus s divides every minor $c_i u_j - c_j u_i$, and $s \mid t$.

Conversely, put $\rho = \sum_j v_j c_j$. For each i, the defining congruences for t give

$$c_i - \rho u_i = \sum_j v_j(c_i u_j - c_j u_i) \equiv 0 \pmod{t}.$$

A prime dividing both ρ and t would divide q and every c_i, which is impossible. Thus choose $h \in \mathbb{Z}$ with $h\rho \equiv 1 \pmod{t}$. Then $hc \equiv u \pmod{t}$, so $h(q/t)c \equiv (q/t)u \pmod{q}$. By (2), $u/t \in L$. Since the scalar subgroup is $(1/s)\mathbb{Z}$, this says $t \mid s$. Consequently $s = t$, including when $t = 1$. □

3. Orthogonal factors and proof of the criterion

For a full lattice $M \subset \mathbb{R}^n$, define

$$M^* = \{y \in \mathbb{R}^n : \langle y, x\rangle \in \mathbb{Z} \text{ for all } x \in M\}.$$

A nonzero $b \in M$ generates a rank-one orthogonal direct factor exactly when $b^* = b/\langle b, b\rangle$ lies in M^*. In fact, for $x \in M$ the coefficient $\langle b^*, x\rangle$ is then integral, and subtracting $\langle b^*, x\rangle b$ gives

$$M = \mathbb{Z}b \perp (M \cap b^\perp).$$

Conversely, this decomposition forces every such coefficient to be an integer. For our particular lattice, its generators give directly

$$L^* = \{y \in \mathbb{Z}^n : \langle c, y\rangle \equiv 0 \pmod{q}\}. \tag{3}$$

Lemma 3. *If $b, d \in M \setminus \{0\}$ and both $b/\langle b, b\rangle$ and $d/\langle d, d\rangle$ belong to M^*, then either $b \perp d$ or $d = \pm b$.*

Proof. The numbers $\alpha = \langle b, d\rangle/\langle b, b\rangle$ and $\beta = \langle b, d\rangle/\langle d, d\rangle$ are integers. If $\langle b, d\rangle \neq 0$, then Cauchy–Schwarz gives

$$0 < \alpha\beta = \frac{\langle b, d\rangle^2}{\langle b, b\rangle\langle d, d\rangle} \leq 1.$$

Thus $\alpha\beta = 1$, so both integers are 1 or both are -1. Equality in Cauchy–Schwarz makes b, d proportional, giving $d = \pm b$. $\square$

Proof of Theorem 1. Fix a primitive u and abbreviate $D = D(u)$, $t = t(u)$. Lemma 2 gives $b = u/t \in L$, and

$$b^* = \frac{tu}{D}.$$

Primitivity implies $b^* \in \mathbb{Z}^n$ exactly when $D \mid t$: necessity follows by applying a Bézout combination of the coordinates of u to the integers tu_j/D. Subject to this, (3) gives

$$b^* \in L^* \iff q \mid (t/D)\langle c, u\rangle \iff qD \mid t\langle c, u\rangle.$$

These are precisely the divisibility conditions in (1). They imply $D \le t \le q$, so the norm bound discards no such factor.

Conversely, any generator b of a rank-one orthogonal direct factor of L is rational, hence parallel to a primitive integer u. Its integral projection coefficients imply $L \cap \mathbb{R}b = \mathbb{Z}b$. Lemma 2 therefore forces $b = \pm u/t(u)$. Thus the pairs $\{u, -u\}$ in $U(a)$ parametrize exactly these factors. Lemma 3 makes distinct directions perpendicular, so there are at most n pairs and $|U(a)| \le 2n$.

If equality holds, the n resulting vectors b_i are nonzero and pairwise perpendicular, hence a real basis. For $x \in L$, its real basis coefficients are $\langle x, b_i\rangle/\langle b_i, b_i\rangle$, all integers since $b_i^* \in L^*$. Consequently the b_i form a $\mathbb{Z}$-basis of L. Conversely, in an orthogonal $\mathbb{Z}$-basis each of these coefficients is integral for every $x \in L$. Each basis vector therefore generates a rank-one orthogonal direct factor and contributes one pair to $U(a)$. The bound already proved gives $|U(a)| = 2n$. $\square$

Open questions

The criterion answers the question for every dimension and denominator. It leaves algorithmic efficiency and a classification without bounded integer quantifiers open. A primary-text comparison with the identified 1985 Popov–Protasov paper is still needed to settle the priority question.

Methods and AI disclosure

This draft was assembled with `gpt-6-astra` in Codex from an internal proof candidate. The original argument passed two independent adversarial reviews and a separate citation audit. Independent Python and GAP calculations corroborated exact finite cases; no computation is a premise of the proof. Source notes, reviews and transcripts are preserved in the accompanying repository under `problems/9.45/`. The primary text of Popov–Protasov (1985) was not obtained, so originality remains provisional. This is an internal candidate awaiting human assessment, without a claim of publication or editor acceptance.

References

1. V. G. Bardakov, *On orthogonal bases of rational lattices*, Sibirsk. Mat. Zh. **39** (1998), no. 6, 1236–1250, Russian.
2. E. I. Khukhro and V. D. Mazurov (eds.), *Unsolved problems in group theory: The Kourovka notebook*, 21 ed., Sobolev Institute of Mathematics, Novosibirsk, 2026, Version arXiv:1401.0300v45, 3 July 2026, Problem 9.45.
3. Yu. D. Popov and I. V. Protasov, *Cyclic lattices*, Dokl. Akad. Nauk Ukr. SSR, Ser. A (1985), no. 8, 67–69, Russian; Zbl 0577.10030. Bibliographic record checked; original text unavailable.