COLS — Coupled Order Lattice System: A Geometric–Spectral Theory of Modular Systems

Committee-Ready FINAL (October 11, 2025)

Éric Pouhier
Independent Mathematician (France)
EricPOUHIER.COLSproject@gmail.com

Abstract

Units. *All angles are in radians*; we write $A_{\mathrm{b}}(n) = A(n)/(\pi/2) \in [0,1]$ for the triangular carrier.

We present a geometric–spectral diagnostic for semiprimes $M = pq$ based on coupling a triangular-wave geometry with multiplicative dynamics. For even n, the GOLS triangle on the unit circle yields an asymmetry $A(n)$; modular proximities $h_r(n)$ (nearness of $a^{n/2}$ to $\pm 1 \bmod r$) produce energies $E_{\mathrm{uni}} = A_{\mathrm{b}}(1 - h_{\min})$ and $E_{\mathrm{bi}} = A_{\mathrm{b}}(1 - h_{\max})$ whose peaks align with successful $\gcd(a^{n/2} \pm 1, M)$. We formalise the *mixed-torus equidistribution* and prove a density law: the prevalence of peaks factorises as *area* $\times$ *arithmetical mass*, with a precise correction when $\gcd(M, 2\lambda) > 1$. For the blind regime (unknown p, q), we introduce the fully observable energy $\widetilde{E}_{\mathrm{uni}} = A_{\mathrm{b}} \cdot X$ based only on trial gcd hits X, and specify a robust spectral module (Hann apodisation, real DFT, harmonic-aware integer micro-grid, and autocorrelation-based fundamental promotion). We give a practitioner recipe and an experimental blueprint (ROC/AUC, recall of fundamentals vs. window length, cost, ablations).

1 Orientation

Goal. Prioritise even exponents n at which $a^{n/2} \pm 1$ reveals a nontrivial factor of $M = pq$.
Idea. Large geometry $A_{\mathrm{b}}(n)$ times small modular distance (via h_r) produces high energy; peaks align with nontrivial gcd outcomes.
New here. (i) Radians throughout and a formal mixed-torus theorem; (ii) blind observable $\widetilde{E}_{\mathrm{uni}}$; (iii) Hann+ACF in the spectral module; (iv) clear blind vs. supervised recipe; (v) expanded metrics.

2 Definitions and basic properties

Let $M = pq$ be an odd semiprime with distinct primes p, q and fix $a \in (\mathbb{Z}/M\mathbb{Z})^{\times}$. All angles are in radians.

GOLS triangle and triangular carrier. For $n \in \mathbb{Z}$, set $\theta = 2\pi n/M$ and $S_0 = (1,0)$, $S_N = (-1,0)$, $S_n = (\cos\theta, \sin\theta)$. Thales gives a right angle at S_n when $S_n \neq S_0, S_N$. Define

$$A(n) = \arcsin\big(\,|\sin(\pi n/M)|\,\big) \in [0, \pi/2], \qquad A_{\mathrm{b}}(n) = \frac{A(n)}{\pi/2} \in [0,1]. \tag{1}$$

Local linearisation. If $n = M/2 + \delta$, then $A(n) = \frac{\pi}{2} - \frac{\pi}{M}\,|\delta| + O(\delta^3/M^3)$, so $A_{\mathrm{b}}(n) = 1 - \frac{2}{M}\,|\delta| + O(\delta^3/M^3)$.

Proximities and energies. For even n let $t = n/2$ and for $r \in \{p, q\}$ define

$$|x|_r = \min(x \bmod r,\ r - (x \bmod r)), \qquad h_r(n) = \frac{1}{r} \min\left(\left|a^t - 1\right|_r,\ \left|a^t + 1\right|_r \right) \in [0, \tfrac{1}{2}]. \quad (2)$$

Set $h_{\min} = \min(h_p, h_q)$ and $h_{\max} = \max(h_p, h_q)$, and define

$$E_{\text{uni}}(n) = A_{\text{b}}(n)(1 - h_{\min}(n)), \qquad E_{\text{bi}}(n) = A_{\text{b}}(n)(1 - h_{\max}(n)). \quad (3)$$

Periods. Let $\lambda_r = \operatorname{ord}_r(a)$ and $\lambda = \operatorname{lcm}(\lambda_p, \lambda_q) = \operatorname{ord}_M(a)$. Then $(a^t \bmod p,\ a^t \bmod q)$ repeats with period λ in t and 2λ in n, while A_{b} has period M. Hence $E_{\text{uni}}, E_{\text{bi}}$ repeat with period $\operatorname{lcm}(M, 2\lambda)$.

3 Mixed torus and density of peaks

We formalise the equidistribution underlying the *area* $\times$ *mass* law.

Definition 3.1 (Mixed torus and alignment classes)**.** Let $\lambda = \operatorname{lcm}(\lambda_p, \lambda_q)$, $L = \operatorname{lcm}(M, 2\lambda)$ and $d = \gcd(M, 2\lambda)$. Index even exponents by $n = 2s$ and define

$$\Phi:\ \mathbb{Z}/L\mathbb{Z} \to (\mathbb{Z}/M\mathbb{Z}) \times (\mathbb{Z}/2\lambda\mathbb{Z}), \qquad s \mapsto (s \bmod M,\ s \bmod 2\lambda).$$

Its image is

$$\Sigma = \{(x, y) \in (\mathbb{Z}/M\mathbb{Z}) \times (\mathbb{Z}/2\lambda\mathbb{Z}) :\ x \equiv y \pmod d\},$$

and Φ is bijective; transport the uniform measure on $\mathbb{Z}/L\mathbb{Z}$ to Σ.

Lemma 3.2 (Conditional equidistribution)**.** *Within each congruence class modulo d, the pairs $(n \bmod M,\ t \bmod \lambda)$ with $t = n/2$ are uniformly distributed over the corresponding fibre of Σ.*

Theorem 3.3 (Density of energy peaks: area $\times$ mass)**.** *Fix $\tau \in (0, 1)$. Over one full cycle of length L,*

$$\frac{1}{L} \#\{n :\ A_{\text{b}}(n) \geq \tau \text{ and } [h_p(n) = 0 \text{ or } h_q(n) = 0]\} = (1 - \tau) \cdot \mu_{\text{arith}} + \varepsilon(M, a), \quad (4)$$

where μ_{arith} is the average (on $\mathbb{Z}/2\lambda\mathbb{Z}$) of the indicator that $a^t \equiv \pm 1 \bmod p$ or $\bmod q$, lifted to $t \bmod 2\lambda$; and $\varepsilon(M, a) = 0$ if $d = 1$, while for $d > 1$ it is the average of class-wise deviations on the alignment classes of Σ.

Remark 3.4. The geometric factor $(1 - \tau)$ is exact (triangular wave). The arithmetical mass depends only on $t \bmod \lambda$ and on the lifted ± 1 windows. Independence holds when $d = 1$.

4 Blind observability (unknown factors)

When p, q are unknown, the proximities h_r are not directly accessible. We therefore base the observable on *trial gcd hits.* For even n with $t = n/2$ define

$$X(n) = \mathbf{1}\{\gcd(a^t - 1, M) > 1 \text{ or } \gcd(a^t + 1, M) > 1\}, \quad (5)$$

and the blind energy

$$\widetilde{E}_{\text{uni}}(n) = A_{\text{b}}(n) \cdot X(n). \quad (6)$$

An optional graded version weights $X(n)$ by $\log \gcd(\cdot, M)$. The support of $\widetilde{E}_{\text{uni}}$ coincides with $h_{\min} = 0$ events, so short windows already reveal divisors or subharmonics of $(2\lambda_p, 2\lambda_q)$.

5 Spectral module (Hann + DFT + harmonic-aware grid + ACF)

We estimate two periods (T_1, T_2) from a short window of either E_{uni} (supervised) or $\widetilde{E}_{\text{uni}}$ (blind).

5.1 Preprocessing and apodisation

Choose an analysis window $\mathcal{W} = \{n_0, \ldots, n_0 + N - 1\}$ and form

$$Y(n) = \begin{cases} E_{\text{uni}}(n)/A_{\text{b}}(n), & \text{if supervised and } A_{\text{b}}(n) > 0, \\ \widetilde{E}_{\text{uni}}(n)/\max(A_{\text{b}}(n), \eta), & \text{if blind } (\eta = 10^{-6}). \end{cases} \tag{7}$$

Centre Y by subtracting its mean on $\mathcal{W}$, apply a *Hann window* $w(n) = \frac{1}{2}(1 - \cos(2\pi(n - n_0)/(N-1)))$, and set $Y_w = w \cdot Y$. Compute the real DFT of Y_w and discard very low frequencies ($f \le 10^{-3}$). Keep the top-K peaks $\{f_k\}$, convert to candidate periods $P_k = 1/f_k$, and prune near-duplicates within ε to obtain a small set P.

5.2 Integer micro-grid and two-sinusoid fit

Build an integer grid G around P:

$$G_{\text{plain}} = \bigcup_{P \in P} \{\lfloor P \rceil - \Delta, \ldots, \lfloor P \rceil + \Delta\},$$
$$G_{\text{harm}} = G_{\text{plain}} \cup \bigcup_{P \in P} \bigcup_{m \in \{2,3,4\}} \{\lfloor mP \rceil - \Delta, \ldots, \lfloor mP \rceil + \Delta\}.$$

Fit

$$Y_e(n; T_1, T_2) = c_0 + \sum_{j=1}^{2} \left(a_j \cos(2\pi n/T_j) + b_j \sin(2\pi n/T_j)\right) \tag{8}$$

by least squares over $(T_1, T_2) \in G^2$ with $T_1 < T_2$ (ridge regularisation on (a_j, b_j) if N is very small). Define the reconstructed energy $\widehat{E_{\text{uni}}}(n) = A_{\text{b}}(n)\, Y_e(n; T_1, T_2)$ and select (T_1, T_2) by RMSE/MAE on $\mathcal{W}$.

5.3 ACF-based fundamental promotion

Compute the (biased) autocorrelation of Y_w. If a strong ACF peak occurs at a multiple of the DFT maximiser, promote the harmonic to its fundamental (e.g. $T \leftarrow T/m$ for $m \in \{2, 3, 4\}$).

Practical settings. $W \in \{2M, 3M, 4M\}$; $K \in [6, 12]$; $\varepsilon \in [10^{-3}, 10^{-2}]$; $\Delta \in [3, 8]$; mask $A_{\text{b}} > 0.15$ to avoid geometric zeros.

6 Practitioner recipe: blind vs. supervised

1. **Pick a base** a (e.g. 2 or a small prime coprime to M).
2. **Choose regime.** If p, q unknown $\Rightarrow$ *blind*: compute $\widetilde{E}_{\text{uni}}$ on a short window and run Section 5. If p, q known $\Rightarrow$ *supervised*: compute $E_{\text{uni}}, E_{\text{bi}}$ via (h_p, h_q).
3. **Prioritise tests.** Use (T_1, T_2) (or subharmonics) to score even n and test $\gcd(a^{n/2} \pm 1, M)$ near predicted peaks; threshold $\tau \approx 0.30$–0.35 works well.
4. **Dyadic descent.** If needed, descend dyadically in n; in practice the 2-adic depth v_2 is small (≤ 4).

7 Experimental blueprint

Datasets. Seeded draws of (p, q) up to 8192 bits; bases $a \in \{2, 3, 5, 7\}$; include Blum/non-Blum, safe primes, and pathological cases (very small λ_r).
Metrics. (i) ROC/AUC for predicting hits by sorting E_{uni} (and $\widetilde{E}_{\text{uni}}$) vs. baselines $1 - h_{\min}$, $1 - h_{\max}$; (ii) recall of the *fundamentals* $(2\lambda_p, 2\lambda_q)$ vs. window length; (iii) cost: #powmod, #gcd per window and time per suggested n.
Ablations. Remove A_{b}, remove the mask $A_{\text{b}} > 0.15$, disable harmonic-aware grid and ACF-promotion.

8 Scope, limitations, and outlook

COLS is a geometric–spectral *diagnostic/prior*; it does not replace asymptotically best factorisation algorithms. When $\lambda_p \approx \lambda_q$ and windows are short, subharmonics may dominate; enlarging the window or enabling G_{harm} mitigates.

9 Appendix: basic lemmas and proofs

Lemma 9.1 (Odd order implies no -1)**.** *If* $\mathrm{ord}_r(a)$ *is odd for a prime* r*, then* $a^t \equiv -1 \pmod r$ *has no solution.*

Proof. If $a^t \equiv -1$ then $a^{2t} \equiv 1$; thus $\mathrm{ord}_r(a) \mid 2t$ but $\mathrm{ord}_r(a) \nmid t$, giving an element of order 2 in $\langle a \rangle$, contradiction. □

Remark 9.2 (Prime powers)**.** Most definitions extend verbatim to prime powers $r = p^e \mid M$ by using $\lambda_r = \mathrm{ord}_{p^e}(a)$ and replacing $\{p, q\}$ with $\{p^e\}$ in (2)–(3).

Acknowledgements. Thanks to early readers for helpful discussions leading to corrected geometry, the unilateral/bilateral split, a formal mixed-torus law, and the blind listening module. The author also wishes to thank Sam Altman for having made possible a true dialogue with artificial intelligence not as a substitute for thought, but as an accelerator of a vision long in gestation.

References (select). K. Ireland, M. Rosen (1990); H. Iwaniec, E. Kowalski (2004); H. Weyl (1952).