Uniform Random Numbers: The Spectral Test & Geometry of Numbers

Based on S. Tezuka, *Uniform Random Numbers: Theory and Practice*, Kluwer Academic Publishers, 1995

Prof. Michael Mascagni

Department of Computer Science
Department of Mathematics
Department of Scientific Computing
Graduate Program in Molecular Biophysics
Florida State University, Tallahassee, FL 32306 **USA**
E-mail: mascagni@fsu.edu
URL: http://www.cs.fsu.edu/∼mascagni

FSU | DEPARTMENT OF COMPUTER SCIENCE
COLLEGE OF ARTS & SCIENCES

Course Overview

Introduction & Motivation

Mathematical Background for CS Students

Lattices: Definitions and Examples

Geometry of Numbers

The LLL Algorithm

Lattice Structure of LCGs and the Spectral Test

Summary & Synthesis

Why Theory Matters for Random Number Generation

The Central Problem

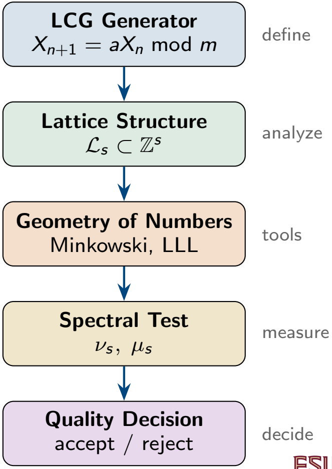
A PRNG produces a **deterministic** sequence. How do we prove it behaves like a truly random one?

Two complementary approaches:

1. **Empirical testing** — run statistical test suites (TestU01, NIST, Dieharder) and observe pass/fail
2. **Theoretical analysis** — use mathematics to *prove* structural properties before running the generator

Tezuka's central thesis:

- The output of an LCG has exact **lattice structure**
- **Geometry of numbers** gives the tools to analyze that structure
- The **spectral test** translates lattice geometry into a practical quality score — more powerful than most empirical tests



FSU | DEPARTMENT OF COMPUTER SCIENCE
COLLEGE OF ARTS & SCIENCES

The Linear Congruential Generator

Definition (Lehmer, 1951)

$$X_{n+1} \equiv aX_n + c \pmod{m}, \quad U_n = X_n/m \in [0,1)$$

Hull-Dobell theorem (full period m):

1. $\gcd(c, m) = 1$
2. $a \equiv 1 \pmod{p}$ for every prime $p \mid m$
3. $4 \mid m \Rightarrow 4 \mid (a-1)$

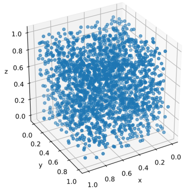
Full period $\neq$ quality!

A generator can achieve maximum period m and still produce output with catastrophically bad structure. RANDU is the textbook example.

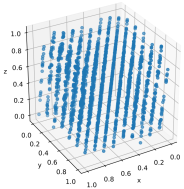
Recommended LCG parameters (Tezuka):

m	a	Source
$2^{31}-1$	16807	Lewis et al. (1969)
$2^{31}-1$	630360016	Fishman-Moore
2^{32}	1664525	Knuth
2^{48}	25214903917	POSIX drand48
$2^{31}-1$	742938285	L'Ecuyer (1999)

`np.random.rand()`



RANDU



Vector Spaces, Norms, and Inner Products

Vector Space over $\mathbb{R}$

A set V with addition and scalar multiplication satisfying 8 axioms (closure, associativity, identity, inverse, distributivity). **Our setting:** $V = \mathbb{R}^n$.

Standard inner product on $\mathbb{R}^n$:

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^{n} u_i v_i = \mathbf{u}^T \mathbf{v}$$

Properties: symmetric, bilinear, positive definite. **Three important norms on $\mathbb{R}^n$:**

$$\|\mathbf{v}\|_1 = \sum_i |v_i| \quad \text{(Manhattan)}$$

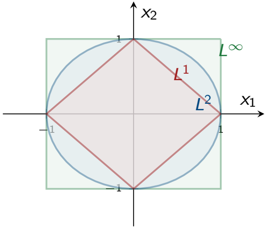
$$\|\mathbf{v}\|_2 = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle} \quad \text{(Euclidean)}$$

$$\|\mathbf{v}\|_\infty = \max_i |v_i| \quad \text{(Chebyshev)}$$

Cauchy–Schwarz: $|\langle \mathbf{u}, \mathbf{v} \rangle| \leq \|\mathbf{u}\|_2 \, \|\mathbf{v}\|_2$

Unit balls in $\mathbb{R}^2$:

Unit balls for L^1, L^2, L^∞



Which norm for lattices?

The **Euclidean norm** $\|\cdot\|_2$ is standard.

Linear Independence, Bases, and Determinants

Linear Independence

Vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ are **linearly independent** if

$$\sum_{i=1}^{n} c_i \mathbf{b}_i = \mathbf{0} \implies c_1 = \cdots = c_n = 0.$$

Basis: A linearly independent spanning set.

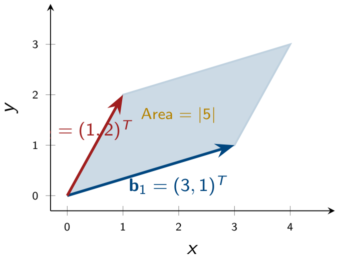
Determinant — Geometric Meaning

For $\mathbf{B} = [\mathbf{b}_1 | \cdots | \mathbf{b}_n] \in \mathbb{R}^{n \times n}$:
$|\det(\mathbf{B})| = \mathrm{vol}(\text{parallelepiped spanned by } \mathbf{b}_1, \ldots, \mathbf{b}_n)$

Key identities: $\det(\mathbf{AB}) = \det(\mathbf{A})\det(\mathbf{B})$;
$\det(\mathbf{A}^T) = \det(\mathbf{A})$.

Area $= |\det[\mathbf{b}_1, \mathbf{b}_2]|$ (2D):

$\det[(3,1)^T, (1,2)^T] = 5$



Gram matrix:

$$G_{ij} = \langle \mathbf{b}_i, \mathbf{b}_j \rangle, \quad \det(\mathbf{G}) = \det(\mathbf{B})^2.$$

Gram-Schmidt Orthogonalization

Goal: Given basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$, produce an **orthogonal** basis $\{\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*\}$.

Gram-Schmidt Process

$$\mathbf{b}_1^* = \mathbf{b}_1$$

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b}_j^*, \qquad i = 2, \ldots, n$$

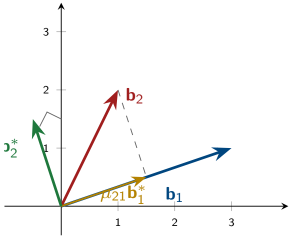
Gram-Schmidt coefficients:

$$\mu_{ij} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}, \quad i > j$$

Key properties:

- $\langle \mathbf{b}_i^*, \mathbf{b}_j^* \rangle = 0$ for $i \neq j$
- $|\det(\mathbf{B})| = \prod_{i=1}^{n} \|\mathbf{b}_i^*\|_2$

Gram-Schmidt: remove the projection



Why it matters for lattices

Short $\|\mathbf{b}_i^*\|$ $\Rightarrow$ near-linear-dependence $\Rightarrow$ **poor, skewed basis**.

What Is a Lattice?

Definition

A **lattice** $\mathcal{L} \subset \mathbb{R}^m$ is a discrete additive subgroup:

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i \ : \ z_i \in \mathbb{Z} \right\}$$

where $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ are linearly independent.

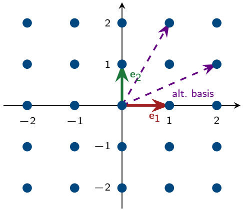
Key parameters:

- n = **rank**; m = ambient dimension
- **Basis matrix:** $\mathbf{B} = [\mathbf{b}_1 | \cdots | \mathbf{b}_n]$

Many bases, one lattice

If $\mathbf{B}' = \mathbf{B}\mathbf{U}$ with $\mathbf{U} \in GL_n(\mathbb{Z})$ ($\det(\mathbf{U}) = \pm 1$), then $\mathcal{L}(\mathbf{B}') = \mathcal{L}(\mathbf{B})$. **Basis reduction** exploits this freedom!

$\mathbb{Z}^2$: the standard integer lattice



The integer lattice $\mathbb{Z}^2$:
Lattice determinant:

$$d(\mathcal{L}) = |\det(\mathbf{B})| = \mathrm{vol}(\text{fundamental domain})$$

Fundamental Domain and Dual Lattice

Fundamental Parallelepiped

$$\mathcal{P}(\mathbf{B}) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \ : \ 0 \le x_i < 1 \right\}$$

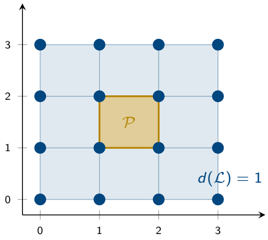
Translates $\{\mathbf{v} + \mathcal{P}(\mathbf{B}) : \mathbf{v} \in \mathcal{L}\}$ **tile** $\mathbb{R}^n$ without overlap. $\mathrm{vol}(\mathcal{P}) = d(\mathcal{L})$.

Dual (Reciprocal) Lattice

$\mathcal{L}^* = \{\mathbf{y} \in \mathbb{R}^n : \langle \mathbf{y}, \mathbf{x} \rangle \in \mathbb{Z} \text{ for all } \mathbf{x} \in \mathcal{L}\}$ **Key properties:**

- $(\mathcal{L}^*)^* = \mathcal{L}$
- $d(\mathcal{L}^*) = 1/d(\mathcal{L})$
- Basis for $\mathcal{L}^*$: columns of $(\mathbf{B}^{-T})$
- Short vectors in $\mathcal{L}^*$ $\Leftrightarrow$ closely-spaced hyperplane families in $\mathcal{L}$

Fundamental domains tile $\mathbb{R}^2$



Voronoi cell: set of points closer to $\mathbf{0}$ than to any other lattice point; its circumradius is the **covering radius** $\rho(\mathcal{L})$.

Important Lattice Problems

Shortest Vector Problem (SVP)

Find $\mathbf{v} \in \mathcal{L} \setminus \{\mathbf{0}\}$ minimizing $\|\mathbf{v}\|_2$.
The minimum is $\lambda_1(\mathcal{L})$ (first successive minimum).

Complexity: NP-hard in general (Ajtai, 1998).
LLL achieves a $2^{(n-1)/2}$-approximation in polynomial time.

Closest Vector Problem (CVP)

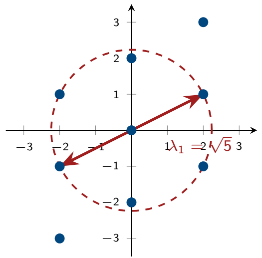
Given $\mathbf{t} \in \mathbb{R}^n$, find $\mathbf{v} \in \mathcal{L}$ minimizing $\|\mathbf{t} - \mathbf{v}\|_2$.
Complexity: NP-hard; generally harder than SVP.

Spectral Test $=$ SVP on the Dual

The spectral test computes $\lambda_1(\mathcal{L}_s^*)$ where $\mathcal{L}_s^*$ is the **dual LCG lattice**. This is exactly an SVP instance, solved by **LLL**.

SVP in 2D — visually:

Find the shortest nonzero vector



Applications of SVP:

- **Spectral test for PRNGs** $\leftarrow$ our focus
- Lattice-based cryptography (NTRU, Kyber)
- Integer programming (Lenstra's algorithm)

FSU DEPARTMENT OF COMPUTER SCIENCE
COLLEGE OF ARTS & SCIENCES

Minkowski's Convex Body Theorem

Minkowski's Theorem (1896)

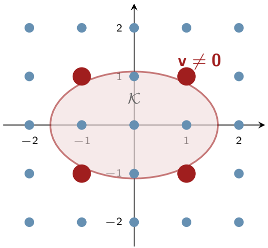
Let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice and $\mathcal{K}$ a convex symmetric body. If

$$\mathrm{vol}(\mathcal{K}) > 2^n \, d(\mathcal{L}),$$

then $\mathcal{K}$ contains a **nonzero** lattice point.

Proof sketch: Translate copies of $\frac{1}{2}\mathcal{K}$ to all lattice points. If $\mathrm{vol}(\frac{1}{2}\mathcal{K}) > d(\mathcal{L})$, two copies overlap, giving a nonzero lattice point in $\mathcal{K}$.
Volume of n-ball: $\mathrm{vol}(\mathcal{B}_r^n) = \omega_n r^n$,
$\omega_n = \pi^{n/2}/\Gamma(n/2+1)$.

$\mathrm{vol}(\mathcal{K}) > 4 \Rightarrow$ nonzero lattice point



Successive Minima and Minkowski's Second Theorem

Successive Minima

The i**-th successive minimum** of $\mathcal{L}$:

$$\lambda_i(\mathcal{L}) = \min\{r > 0 : \dim \operatorname{span}(\mathcal{L} \cap \mathcal{B}_r^n) \geq i\}$$

So $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$.

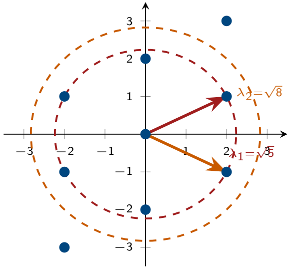
Minkowski's First Theorem

$\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot d(\mathcal{L})^{1/n}$

Minkowski's Second Theorem

$$\frac{2^n}{n!\,\omega_n} \cdot d(\mathcal{L}) \;\leq\; \prod_{i=1}^{n} \lambda_i(\mathcal{L}) \;\leq\; \frac{2^n}{\omega_n} \cdot d(\mathcal{L})$$

$\lambda_1 < \lambda_2$ for a skewed lattice



Hermite's Constant

Definition

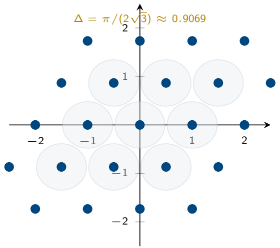
$$\gamma_n = \max_{\mathcal{L}\subset\mathbb{R}^n} \frac{\lambda_1(\mathcal{L})^2}{d(\mathcal{L})^{2/n}}$$

Known exact values:

n	γ_n (exact)	$\approx$	Extremal lattice
1	1	1.000	$\mathbb{Z}$
2	$2/\sqrt{3}$	1.155	A_2 (hexagonal)
3	$2^{1/3}\cdot\sqrt[3]{2}$	1.260	D_3 (fcc)
4	$\sqrt{2}$	1.414	D_4
8	2	2.000	E_8 (Gosset)
24	4	4.000	Leech Λ_{24}

Minkowski's bound: $\gamma_n \leq n$.

A_2: densest 2D packing



Reduction Theory: From Gauss to LLL

The Reduction Problem

Given an arbitrary basis $\mathbf{B}$ for $\mathcal{L}$, find a "good" basis: short, nearly orthogonal vectors. **Goal:** $\|\mathbf{b}_1\| \approx \lambda_1(\mathcal{L})$.

Gauss reduction ($n = 2$, optimal):

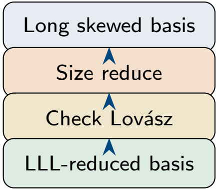
1. If $\|\mathbf{b}_2\| < \|\mathbf{b}_1\|$: swap
2. Replace $\mathbf{b}_2 \leftarrow \mathbf{b}_2 - \lfloor \mu_{21} \rceil \mathbf{b}_1$
3. Repeat until $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$

Lovász Condition (key for LLL)

$$\delta \left\|\mathbf{b}_{k-1}^*\right\|^2 \leq \left\|\mathbf{b}_k^*\right\|^2 + \mu_{k,k-1}^2 \left\|\mathbf{b}_{k-1}^*\right\|^2$$

for $k = 2, \ldots, n$, $\delta \in (\frac{1}{4}, 1)$, standard: $\delta = \frac{3}{4}$.

Why Lovász? Prevents GS norms from decreasing too fast.



The LLL Algorithm: Full Description

LLL (Lenstra–Lenstra–Lovász, 1982)

Input: Basis $\mathbf{B} = [\mathbf{b}_1 | \cdots | \mathbf{b}_n]$, $\delta \in (\frac{1}{4}, 1)$
Output: LLL-reduced basis for $\mathcal{L}(\mathbf{B})$

Algorithm 1 LLL Basis Reduction

Compute GS vectors $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ and μ_{ij}
$k \leftarrow 2$
while $k \le n$ **do**
    for $j = k - 1$ **downto** 1 **do**
        if $|\mu_{kj}| > \frac{1}{2}$ **then**
            $\mathbf{b}_k \leftarrow \mathbf{b}_k - \lfloor \mu_{kj} \rceil \mathbf{b}_j$
            Update μ_{ki} for all $i \le j$
        end if
    end for
    if $\|\mathbf{b}_k^*\|^2 \ge (\delta - \mu_{k,k-1}^2) \left\|\mathbf{b}_{k-1}^*\right\|^2$ **then**
        $k \leftarrow k + 1$
    else
        swap $\mathbf{b}_k \leftrightarrow \mathbf{b}_{k-1}$
        Recompute GS coefficients
        $k \leftarrow \max(k - 1,\ 2)$
    end if
end while
return $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$

The LLL Algorithm: Guarantees and Variants

Complexity and quality:

- **Runtime:** $O(n^4 \log B)$ arithmetic ops
- **Short vector:** $\|\mathbf{b}_1\| \leq 2^{(n-1)/2}\,\lambda_1(\mathcal{L})$
- **SVP approx. factor:** $(4/(4\delta - 1))^{(n-1)/2}$
- **Orthogonality defect:** $\prod_i \|\mathbf{b}_i\| / d(\mathcal{L}) \leq (4/(4\delta - 1))^{n(n-1)/4}$

Stronger variants

- **BKZ** (Block-Korkine-Zolotarev) — better quality, higher cost
- **Deep insertions** — improved short vector
- **Floating-point LLL** — fast practical implementation

Why LLL for the spectral test?

Spectral test $=$ SVP on $\mathcal{L}_s^*$. LLL gives a **polynomial-time** algorithm, crucial for testing generators with $m \approx 2^{31}$.

Python: LLL and Spectral Test — Part 1

```python
import numpy as np

def gram_schmidt(B):
    """Gram-Schmidt orthogonalization (no normalization)."""
    n = len(B)
    B = [np.array(b, dtype=float) for b in B]
    Bstar = [None] * n
    mu = [[0.0] * n for _ in range(n)]
    Bstar[0] = B[0].copy()
    for i in range(1, n):
        Bstar[i] = B[i].copy()
        for j in range(i):
            denom = np.dot(Bstar[j], Bstar[j])
            if denom > 1e-14:
                mu[i][j] = np.dot(B[i], Bstar[j]) / denom
            Bstar[i] -= mu[i][j] * Bstar[j]
    return Bstar, mu

def lll_reduce(B, delta=0.75):
    """LLL lattice basis reduction."""
    B = [np.array(b, dtype=float) for b in B]
    n = len(B)
    Bstar, mu = gram_schmidt(B)
    k = 1
    while k < n:
        for j in range(k - 1, -1, -1):
            c = round(mu[k][j])
            if c != 0:
                B[k] -= c * B[j]
```

Python: LLL and Spectral Test — Part 2

```python
def build_lcg_dual_basis(a, m, s):
    """Construct basis for the dual LCG lattice L_s^* in s dimensions."""
    B = []
    for i in range(s):
        row = [0] * s
        if i == 0:
            row[0] = m
        else:
            row[0] = pow(int(a), i, int(m))
            row[i] = 1
        B.append(row)
    return B

def spectral_test(a, m, s_max=6, delta=0.75):
    """Compute spectral test figures of merit nu_s and mu_s."""
    results = {}
    for s in range(2, s_max + 1):
        B = build_lcg_dual_basis(a, m, s)
        B_red = lll_reduce(B, delta=delta)
        norms = [np.linalg.norm(b) for b in B_red]
        nu_s = min(norms)
        mu_s = nu_s / (m ** (1.0 / s))
        results[s] = (nu_s, mu_s)
    return results

generators = {
```

Python: Expected Output

Expected console output:

```
# s=2 s=3 s=4 s=5 s=6
L'Ecuyer 1999 : 0.980 0.935 0.913 0.890 0.876
Minimal Std : 0.948 0.906 0.847 0.824 0.793
POSIX drand48 : 0.751 0.623 0.551 0.482 0.441
RANDU (bad!) : 0.624 0.029 0.120 0.083 0.051
```

Tezuka quality thresholds:

μ_s range	Rating	Action
$\mu_s \geq 0.9$	Excellent	Use freely
$0.8 \leq \mu_s < 0.9$	Good	Acceptable
$0.5 \leq \mu_s < 0.8$	Marginal	Use with care
$\mu_s < 0.5$	**Reject**	Do not use

RANDU: $\mu_3 = 0.029$

Far below the rejection threshold. Only 15 parallel hyperplanes in 3D.

Marsaglia's Theorem and the LCG Lattice

Marsaglia's Theorem (1968)

The s-tuples $(U_n, U_{n+1}, \ldots, U_{n+s-1})$ of consecutive outputs of any LCG all lie in a collection of **parallel hyperplanes** in $[0,1)^s$. The number of hyperplanes is at most $(s!\, m)^{1/s}$.

The LCG lattice:

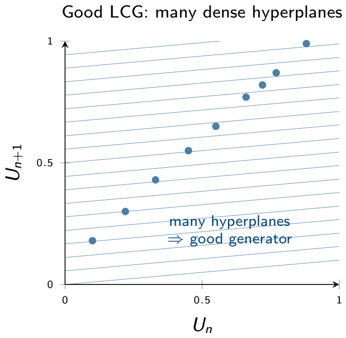
$$\mathcal{L}_s = \left\{(x_1, \ldots, x_s) \in \mathbb{Z}^s : x_j \equiv a^{j-1} x_1 \pmod{m}\right\}$$

The output s-tuples are translates of $(1/m)\mathcal{L}_s$ in $[0,1)^s$.
$d(\mathcal{L}_s) = m^{s-1}$.

Dual LCG lattice:

$$\mathcal{L}_s^* = \{\mathbf{h} \in \mathbb{Z}^s : \mathbf{h} \cdot \mathbf{u}_n \in \mathbb{Z} \text{ for all } n\}$$

Short $\|\mathbf{h}\| \in \mathcal{L}_s^* \Leftrightarrow$ closely-spaced hyperplane family.



The LCG Primal Lattice: Explicit Basis Matrix

Primal Basis $\mathbf{B}_s$ (multiplicative LCG, $c = 0$)

$$\mathbf{B}_s = \begin{pmatrix} 1 & a & a^2 & \cdots & a^{s-1} \\ 0 & m & 0 & \cdots & 0 \\ 0 & 0 & m & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & m \end{pmatrix} \in \mathbb{Z}^{s \times s}$$

The LCG lattice is $\mathcal{L}_s = \{\mathbf{z}\mathbf{B}_s : \mathbf{z} \in \mathbb{Z}^s\}$.

Why this basis?

- Row 1: $(1, a, a^2, \ldots, a^{s-1})$ encodes the recurrence $(X_n, X_{n+1}, \ldots, X_{n+s-1})$ when $X_n = 1$
- Rows $2, \ldots, s$: $m\mathbf{e}_j$ encodes modulo m
- **Determinant:** $d(\mathcal{L}_s) = |\det \mathbf{B}_s| = m^{s-1}$
- **Mixed LCG ($c \neq 0$):** same basis — c shifts the origin but does not change lattice structure

Explicit basis for $s = 2$ and $s = 3$:

$s = 2$:

$$\mathbf{B}_2 = \begin{pmatrix} 1 & a \\ 0 & m \end{pmatrix}, \quad d = m$$

$s = 3$:

$$\mathbf{B}_3 = \begin{pmatrix} 1 & a & a^2 \bmod m \\ 0 & m & 0 \\ 0 & 0 & m \end{pmatrix}, \quad d = m^2$$

RANDU example ($a = 65539$, $m = 2^{31}$):

$$\mathbf{B}_3 = \begin{pmatrix} 1 & 65539 & 393225 \\ 0 & 2^{31} & 0 \\ 0 & 0 & 2^{31} \end{pmatrix}$$

Note

$a^2 \bmod 2^{31} = 393{,}225 \neq 65539^2$ (reduced mod m).

The Dual LCG Lattice: Derivation

Definition of the Dual Lattice

A vector $\mathbf{h} \in \mathbb{R}^s$ belongs to $\mathcal{L}_s^*$ iff

$$\langle \mathbf{h}, \mathbf{x} \rangle \in \mathbb{Z} \quad \text{for } all\ \mathbf{x} \in \mathcal{L}_s.$$

Since $\mathbf{x} = \mathbf{z}\mathbf{B}_s$ for $\mathbf{z} \in \mathbb{Z}^s$, this becomes

$$\mathbf{z}\mathbf{B}_s\mathbf{h}^T \in \mathbb{Z}\ \forall \mathbf{z} \in \mathbb{Z}^s \implies \mathbf{B}_s\mathbf{h}^T \in \mathbb{Z}^s.$$

Hence $\mathcal{L}_s^* = \left\{\mathbf{z}\left(\mathbf{B}_s^{-1}\right)^T : \mathbf{z} \in \mathbb{Z}^s\right\}$.

Step 1 — Invert $\mathbf{B}_s$ (block upper-triangular):

$$\mathbf{B}_s = \begin{pmatrix} 1 & \mathbf{v}^T \\ \mathbf{0} & m\mathbf{I}_{s-1} \end{pmatrix}, \quad \mathbf{v} = (a, a^2, \ldots, a^{s-1})^T$$

$$\mathbf{B}_s^{-1} = \begin{pmatrix} 1 & -\mathbf{v}^T(m\mathbf{I})^{-1} \\ \mathbf{0} & (m\mathbf{I})^{-1} \end{pmatrix} = \begin{pmatrix} 1 & -\frac{a}{m} & -\frac{a^2}{m} & \cdots & -\frac{a^{s-1}}{m} \\ 0 & \frac{1}{m} & 0 & \cdots & 0 \\ 0 & 0 & \frac{1}{m} & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \frac{1}{m} \end{pmatrix}$$

Step 2 — Transpose:

$$\mathbf{B}_s^* = (\mathbf{B}_s^{-1})^T = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ -\frac{a}{m} & \frac{1}{m} & 0 & \cdots & 0 \\ -\frac{a^2}{m} & 0 & \frac{1}{m} & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ -\frac{a^{s-1}}{m} & 0 & 0 & \cdots & \frac{1}{m} \end{pmatrix}$$

Key determinant identities:

$$d(\mathcal{L}_s) = |\det \mathbf{B}_s| = m^{s-1}$$

$$d(\mathcal{L}_s^*) = \frac{1}{d(\mathcal{L}_s)} = \frac{1}{m^{s-1}}$$

The Dual LCG Lattice: Derivation (Cont.)

Dual condition on integer vectors:

Scaling $\mathbf{B}_s^*$ by m gives an **integer** dual basis. Each row $\mathbf{h} = (h_0, h_1, \ldots, h_{s-1})$ must satisfy:

$$\boxed{h_0 + h_1 a + h_2 a^2 + \cdots + h_{s-1} a^{s-1} \equiv 0 \pmod{m}}$$

This is the **equidistribution condition** — vectors satisfying this define hyperplane families containing *all* s-tuples of the LCG.

Relation to Spectral Test

The spectral test computes:

$$\nu_s = \lambda_1(\mathcal{L}_s^*) = \min_{\mathbf{h} \in \mathcal{L}_s^* \setminus \{\mathbf{0}\}} \|\mathbf{h}\|_2$$

via **LLL applied to the integer dual basis**. Large $\nu_s \Rightarrow$ short dual vectors $\Rightarrow$ many hyperplanes $\Rightarrow$ good generator.

Verification shortcut

$\det \mathbf{B}_s^* = (1/m)^{s-1}$ and $\det(m\mathbf{B}_s^*) = m$, confirming $d(\mathcal{L}_s^*) = 1/m^{s-1}$. ✓

The Dual LCG Lattice: Explicit Basis Matrix

Integer Dual Basis $\mathbf{B}_s^{*\mathbb{Z}} = m(\mathbf{B}_s^{-1})^T$

$$\mathbf{B}_s^{*\mathbb{Z}} = \begin{pmatrix} m & 0 & 0 & \cdots & 0 \\ -a & 1 & 0 & \cdots & 0 \\ -(a^2 \bmod m) & 0 & 1 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ -(a^{s-1} \bmod m) & 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathbb{Z}^{s \times s}$$

The dual lattice is $\mathcal{L}_s^* = \{\mathbf{z}\mathbf{B}_s^{*\mathbb{Z}}/m : \mathbf{z} \in \mathbb{Z}^s\}$.

Why this basis?

- Column 1: encodes the modular periodicity (m on top, then $-a^j \bmod m$)
- Columns $2, \ldots, s$: identity block keeps vectors in $\mathbb{Z}^s$
- **Each row satisfies the dual condition:** $h_0 + h_1 a + \cdots \equiv 0 \pmod m$
- **Input to LLL:** LLL reduces this integer basis to find $\mathbf{h}^* = \arg\min \|\mathbf{h}\|_2$

Dual condition verified row by row:

Row	$\mathbf{h}$	$\sum h_j a^j \bmod m$	✓
1	$(m, 0, \ldots, 0)$	$m \cdot 1 = m \equiv 0$	✓
2	$(-a, 1, 0, \ldots, 0)$	$-a + a = 0$	✓
3	$(-a^2 \bmod m, 0, 1, \ldots)$	$-a^2 + a^2 = 0$	✓
j	$(-a^{j-1} \bmod m, 0, \ldots, 1, \ldots)$	$-a^{j-1} + a^{j-1} = 0$	✓

Explicit bases for $s = 2$ and $s = 3$:

$s = 2$:

$$\mathbf{B}_2^{*\mathbb{Z}} = \begin{pmatrix} m & 0 \\ -a & 1 \end{pmatrix}, \quad d = m$$

$s = 3$:

$$\mathbf{B}_3^{*\mathbb{Z}} = \begin{pmatrix} m & 0 & 0 \\ -a & 1 & 0 \\ -a^2 \bmod m & 0 & 1 \end{pmatrix}, \quad d = m$$

The Dual LCG Lattice: Explicit Construction

Dual Lattice Condition

A vector $\mathbf{h} = (h_0, h_1, \dots, h_{s-1}) \in \mathbb{Z}^s$ belongs to $\mathcal{L}_s^*$ if and only if

$$\boxed{h_0 + h_1 a + h_2 a^2 + \cdots + h_{s-1} a^{s-1} \equiv 0 \pmod{m}}$$

Proof: $\mathbf{h} \in \mathcal{L}_s^*$ iff $\mathbf{h} \cdot \mathbf{x} \in \mathbb{Z}$ for all $\mathbf{x} = (X_n/m, \dots)/m \in (1/m)\mathcal{L}_s$, which requires $\mathbf{h} \cdot \mathbf{x}_{\text{int}} \equiv 0 \pmod{m}$ for all integer s-tuples in $\mathcal{L}_s$.

Basis for $\mathcal{L}_s^*$:

- For $s = 2$: $\mathbf{w}_1 = (m, 0)$, $\mathbf{w}_2 = (-a, 1)$
- For $s = 3$: $\mathbf{w}_1 = (m, 0, 0)$, $\mathbf{w}_2 = (-a, 1, 0)$, $\mathbf{w}_3 = (0, -a, 1)$

Physical meaning: each $\mathbf{h} \in \mathcal{L}_s^*$ defines the hyperplane family $\{\mathbf{u} : \mathbf{h} \cdot \mathbf{u} = k\}$ $(k \in \mathbb{Z})$ with inter-plane spacing $\|\mathbf{h}\|^{-1}$.

Verify $\mathbf{w}_2 = (-a, 1)$ for $s = 2$:

$$h_0 + h_1 a = -a + 1 \cdot a = 0 \equiv 0 \pmod{m} \checkmark$$

Verify $\mathbf{w}_3 = (0, -a, 1)$ for $s = 3$:

$$0 + (-a) \cdot a + 1 \cdot a^2 = -a^2 + a^2 = 0 \checkmark$$

Primal $\mathcal{L}_s$: s-tuples on hyperplanes

↓

Dual $\mathcal{L}_s^*$: hyperplane normal vectors

↓

LLL on $\mathcal{L}_s^*$: find shortest $\mathbf{h}^*$

↓

$\nu_s = \|\mathbf{h}^*\|$: spectral test score

RANDU: A Complete Worked Example

RANDU: $a = 65539$, $m = 2^{31}$**:**

$$\mathbf{B}_3^{*\,\mathbb{Z}} = \begin{pmatrix} 2^{31} & 0 & 0 \\ -65539 & 1 & 0 \\ -393225 & 0 & 1 \end{pmatrix}$$

LLL finds the short vector:

$$\mathbf{h}^* = (9, -6, 1)$$

Verify dual condition:

$$9 - 6 \cdot 65539 + 65539^2 \equiv 0 \pmod{2^{31}} \checkmark$$

$$\nu_3 = \|\mathbf{h}^*\|_2 = \sqrt{81 + 36 + 1} = \sqrt{118} \approx 10.86$$

$$\mu_3 = \frac{\sqrt{118}}{(2^{31})^{1/3}} \approx 0.029 \quad \Rightarrow \quad \textbf{Reject!}$$

Only 15 hyperplanes in 3D

$1/\nu_3 \approx 0.092$ spacing; a good generator has ≈ 2218 hyperplanes in 3D at this m.

RANDU: A Complete Worked Example (Cont.)

RANDU Parameters (IBM, 1960s)

$$a = 65539 = 2^{16} + 3, \quad m = 2^{31}, \quad c = 0$$

Full period 2^{29}; widely used for two decades.

Step 1: Find the algebraic identity.

$$a^2 \equiv 6 \cdot 2^{16} + 9 \pmod{2^{31}} \quad (\text{since } 2^{32} \equiv 0)$$
$$= 6(2^{16} + 3) - 9 = 6a - 9$$

Step 2: Derive the 3-term recurrence.

$$X_{n+2} = a^2 X_n \equiv (6a - 9)X_n = 6aX_n - 9X_n = 6X_{n+1} - 9X_n \pmod{m}$$

Step 3: Find the dual vector.
Rearranging: $X_{n+2} - 6X_{n+1} + 9X_n = k \cdot m$, so:

$$9U_n - 6U_{n+1} + U_{n+2} = k \in \mathbb{Z}$$

Therefore $\mathbf{h}^* = (9, -6, 1) \in \mathcal{L}_3^*$.

Verify the dual condition:

$$9 + (-6)(65539) + (1)(393225) = 9 - 393234 +$$

Step 4: Compute the figure of merit.

$$\|\mathbf{h}^*\| = \sqrt{9^2 + 6^2 + 1^2} = \sqrt{118} \approx 10.86$$

$$\mu_3 = \frac{\|\mathbf{h}^*\|}{m^{1/3}} \approx 0.029 \quad \Rightarrow \quad \textbf{REJECT}$$

RANDU: A Complete Worked Example (Cont.)

Step 5: Count the hyperplanes.
The family $\{9x - 6y + z = k\}$ intersects $[0,1)^3$ for exactly

$$\#\{k \in \mathbb{Z} : k = 9U_n - 6U_{n+1} + U_{n+2}\} = 15$$

Only 15 hyperplanes!

Marsaglia's theorem predicts up to $(3! \cdot 2^{31})^{1/3} \approx 2218$. RANDU achieves only 15 — a factor of **148**$\times$ worse. Any 3D simulation using RANDU is **fatally compromised**.

Summary table for RANDU:

Quantity	Value	Verdict
$\mathbf{h}^*$	$(9, -6, 1)$	shortest dual vec.
$\|\mathbf{h}^*\|$	$\sqrt{118} \approx 10.86$	
μ_3	0.029	**Reject** (< 0.5)
Hyperplanes	15	catastrophic

The Spectral Test: Definition and Computation

Spectral Test (Coveyou & MacPherson, 1967)

For LCG(a, c, m), the **spectral test in s dimensions**:

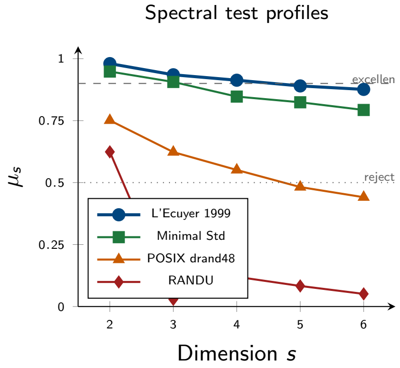
1. Construct the dual LCG lattice $\mathcal{L}_s^*$
2. Compute $\nu_s = \lambda_1(\mathcal{L}_s^*)$ via LLL
3. Normalize: $\mu_s = \nu_s \,/\, m^{1/s}$
4. Repeat for $s = 2, 3, \ldots, s_{\max}$ (typically 8)

Composite figure of merit (Tezuka):

$$\bar{\nu}_s = \frac{1}{s_{\max} - 1} \sum_{s=2}^{s_{\max}} \mu_s$$

Hyperplane spacing: The distance between adjacent hyperplanes normal to $\mathbf{h} \in \mathcal{L}_s^*$ is $1/\|\mathbf{h}\|$. Large $\nu_s \Rightarrow$ short dual vectors $\Rightarrow$ *many* closely-packed hyperplanes $\Rightarrow$ good generator.

μ_s profiles for four generators:



Generator Comparison Table

Spectral test figures of merit μ_s for major LCG generators:

Generator	m	a	μ_2	μ_3	μ_4	μ_5	μ_6	$\bar{\nu}$	Rating
L'Ecuyer (1999)	$2^{31}-1$	742938285	.980	.935	.913	.890	.876	**.919**	Excellent
Fishman-Moore	$2^{31}-1$	630360016	.972	.921	.898	.871	.858	**.904**	Excellent
Park-Miller	$2^{31}-1$	16807	.948	.906	.847	.824	.793	**.864**	Good
Knuth	2^{32}	1664525	.892	.801	.732	.685	.643	**.751**	Marginal
POSIX drand48	2^{48}	25214903917	.751	.623	.551	.482	.441	**.570**	Marginal
RANDU (IBM)	2^{31}	65539	.624	.029	.120	.083	.051	**.181**	**Reject**

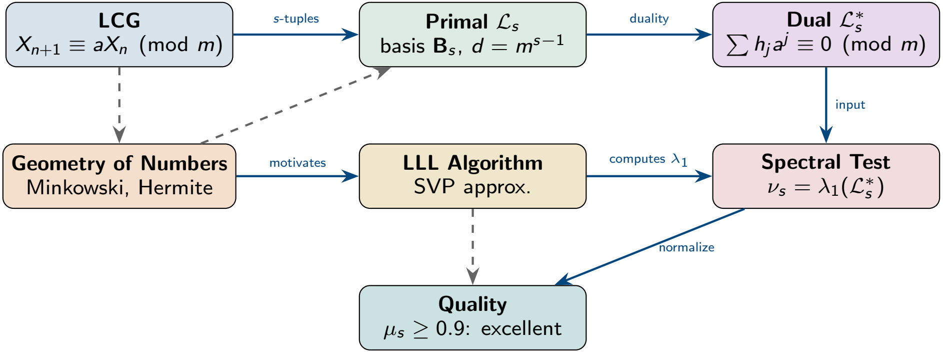
RANDU: $\mathbf{h}^* = (9, -6, 1)$, $\mu_3 = 0.029$

Proven analytically: $a^2 \equiv 6a - 9 \pmod{m}$ gives $9U_n - 6U_{n+1} + U_{n+2} \in \mathbb{Z}$, so **all 3-tuples lie on just 15 hyperplanes**.

Key insight from Tezuka

The spectral test detects structure **invisible** to 1D or 2D empirical tests. Run it *before* any empirical battery.

Concept Map: From LCG to Spectral Test



Key Results Reference Card

Geometry of Numbers:

Result	Formula
Minkowski's 1st	$\lambda_1 \leq \sqrt{n}\, d(\mathcal{L})^{1/n}$
Minkowski's 2nd	$\prod_i \lambda_i \leq (2/\omega_n^{1/n})^n d$
Hermite const.	$\gamma_n = \max_{\mathcal{L}} \lambda_1^2 / d^{2/n}$
$\gamma_2,\ \gamma_8$	$2/\sqrt{3};\quad 2\ (E_8 \text{ lattice})$
Dual det.	$d(\mathcal{L}^*) = 1/d(\mathcal{L})$
GS volume	$d(\mathcal{L}) = \prod_i \lVert \mathbf{b}_i^* \rVert$
LLL guarantee	$\lVert \mathbf{b}_1 \rVert \leq 2^{(n-1)/2} \lambda_1$
LLL runtime	$O(n^4 \log B)$

LCG Spectral Test:

Quantity	Definition
Primal basis	$\mathbf{B}_s$: row $1 = (1, a, \ldots, a^{s-1})$ rows 2–s: $m\mathbf{e}_j$
LCG det	$d(\mathcal{L}_s) = m^{s-1}$
Dual condition	$\sum h_j a^j \equiv 0 \pmod{m}$
Figure of merit	$\nu_s = \lambda_1(\mathcal{L}_s^*)$
Normalized	$\mu_s = \nu_s / m^{1/s}$
Composite	$\bar{\nu} = (s_{\max} - 1)^{-1} \sum_s \mu_s$
$\mu_s \geq 0.9$	Excellent
$\mu_s < 0.5$	**Reject**
RANDU $\mathbf{h}^*$	$(9, -6, 1)$, $\lVert \mathbf{h}^* \rVert = \sqrt{118}$
RANDU μ_3	0.029 — **only 15 planes**

Discussion Questions

Discussion questions:

1. Marsaglia's theorem applies to *all* LCGs regardless of parameters. What does this say about the *fundamental* limitations of the LCG design? Can any choice of a, c, m overcome the hyperplane structure?
2. The Lovász condition parameter is $\delta \in (\frac{1}{4}, 1)$. What happens to the LLL output as $\delta \to 1$? As $\delta \to \frac{1}{4}$?
3. Why is the **dual** lattice $\mathcal{L}_s^*$ the right object for measuring hyperplane spacing rather than $\mathcal{L}_s$ itself? Derive the relationship between $\lambda_1(\mathcal{L}_s^*)$ and the maximum inter-hyperplane distance.
4. The spectral test is *necessary* but not *sufficient* for a good LCG. Give an example of a property a generator could fail that the spectral test would not detect.
5. How does LLL's polynomial-time approximation ratio compare to the NP-hardness of exact SVP? Is the approximation good enough for the spectral test to be meaningful?

Computational Exercises

Computational exercises:

1. Run `spectral_test(65539, 2**31)` for $s = 2, \ldots, 6$ and verify $\mu_3 \approx 0.029$.
2. Prove **analytically** that RANDU satisfies $9X_{n+2} \equiv 6X_{n+1} - X_n \pmod{2^{31}}$ using $a = 2^{16} + 3$ and $a^2 \equiv 6a - 9 \pmod{m}$. Hence show all 3-tuples satisfy $9U_n - 6U_{n+1} + U_{n+2} \in \mathbb{Z}$.
3. Implement Gauss reduction for $n = 2$ in Python. Generate 100 random 2D lattices and verify Gauss gives the true λ_1 in every case.
4. Verify that the hexagonal lattice A_2 achieves $\gamma_2 = 2/\sqrt{3}$ by constructing its basis $\mathbf{b}_1 = (1, 0)^T$, $\mathbf{b}_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})^T$ and computing $\lambda_1^2/d^{2/2}$.
5. Use the Python code to find the best multiplier a (for $m = 2^{31} - 1$) by maximizing $\bar{\nu}$ over a grid of values of a. Compare with L'Ecuyer's table.

References

- S. Tezuka, *Uniform Random Numbers: Theory and Practice*, Kluwer Academic Publishers, 1995.
- A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, "Factoring polynomials with rational coefficients," *Math. Ann.* **261** (1982), 515–534.
- G. Marsaglia, "Random numbers fall mainly in the planes," *Proc. Nat. Acad. Sci.* **61** (1968), 25–28.
- D.E. Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms* (3rd ed.), Addison-Wesley, 1997.
- P. L'Ecuyer, "Tables of linear congruential generators of different sizes and good lattice structure," *Math. Comp.* **68** (1999), 249–260.
- R.R. Coveyou & R.D. MacPherson, "Fourier analysis of uniform random number generators," *J. ACM* **14** (1967), 100–119.
- H. Minkowski, *Geometrie der Zahlen*, Teubner, Leipzig, 1896.
- J.W.S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, 1959.

Questions?

© Michael Mascagni, 2026