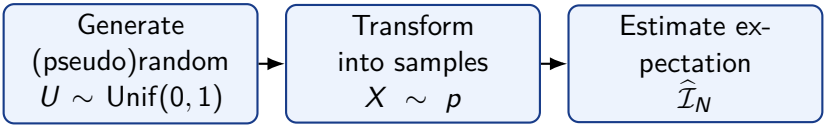
Why do Monte Carlo methods need random numbers?

Suppose our quantity of interest is

$$\mathcal{I} = \mathbb{E}_p[f(X)] = \int f(x)p(x)\,dx.$$

If $X_1, \ldots, X_N$ are sampled from p, basic Monte Carlo uses

$$\widehat{\mathcal{I}}_N = \frac{1}{N}\sum_{i=1}^{N} f(X_i).$$



The starting point for most sampling methods is a stream of uniform random numbers.

True randomness

- Comes from a genuinely unpredictable physical process.
- Can be relatively difficult or costly to obtain at scale.

Pseudorandomness

- Produced by a deterministic algorithm.
- Designed to *behave statistically* like random draws.
- Fast and reproducible.

Key distinction

Unpredictable-looking is not the same as *fundamentally random*. The same PRNG and seed reproduce the same sequence.

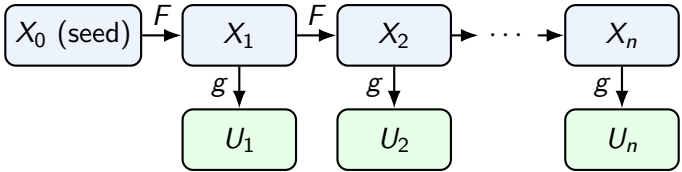
Anatomy of a pseudorandom number generator

A general PRNG has a finite set of states S and two deterministic functions:

$$F : S \to S, \qquad g : S \to [0, 1].$$

Starting from an initial **seed** $X_0 \in S$:

$$\boxed{X_n = F(X_{n-1}), \qquad U_n = g(X_n), \quad n \geq 1.}$$



Determinism

If the seed X_0, the functions F, g, and their implementation are identical, the entire output sequence is identical.

- Same seed $\Rightarrow$ same sequence.
- A new seed usually changes the sequence.
- Reproducibility makes simulation experiments easier to verify and debug.

Example

Seed 123 $\rightarrow$ 0.682, 0.054, ...

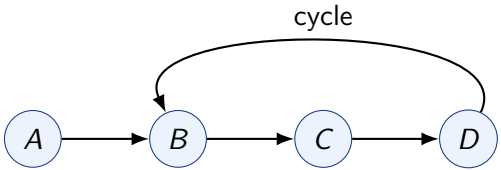
Seed 123 $\rightarrow$ 0.682, 0.054, ...

The displayed values are illustrative only; the actual sequence depends on the chosen PRNG.

Why finite-state generators eventually repeat

Suppose S contains M possible states.

- The deterministic map F generates $X_0, X_1, X_2, \ldots$.
- Among $M + 1$ successive states, at least two must coincide.
- Once a state repeats, the future evolution repeats as well.



Period

The *period* is the number of states in the eventual repeating cycle. A longer period is desirable, but does not guarantee good statistical quality.

Linear congruential generator (LCG)

An LCG uses the integer recurrence

$$X_{n+1} = (aX_n + c) \bmod m, \qquad U_n = \frac{X_n}{m}.$$

- $m \geq 2$: **modulus**
- a: **multiplier**
- c: **increment**
- $X_0 \in \{0, \ldots, m-1\}$: **seed**

Hence $U_n \in \{0, 1/m, \ldots, (m-1)/m\} \subset [0, 1)$.

Meaning of "mod"

$19 \bmod 16 = 3$

$37 \bmod 16 = 5$

The state is always in $\{0, \ldots, m-1\}$.

Worked example: calculate an LCG by hand

Choose $m = 16$, $a = 5$, $c = 1$ and $X_0 = 0$:

$$X_{n+1} = (5X_n + 1) \bmod 16.$$

n	0	1	2	3	4	5	6	7	8
X_n	0	1	6	15	12	13	2	11	8
$U_n = X_n/16$	0	1/16	6/16	15/16	12/16	13/16	2/16	11/16	8/16

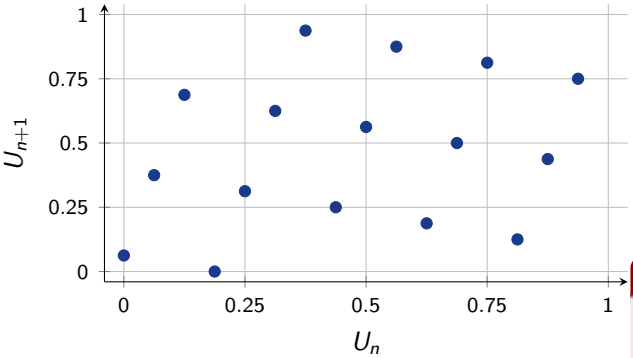
For instance,

$$X_2 = (5 \cdot 1 + 1) \bmod 16 = 6, \qquad X_3 = (5 \cdot 6 + 1) \bmod 16 = 15.$$

What happens later?

$X_{15} = 3$ and $X_{16} = 0 = X_0$. All 16 states appear once before repeating: **period** $= 16$.

Visualising an LCG sequence



- Each point is a consecutive pair (U_n, U_{n+1}).
- Outputs are discrete and related by the same deterministic rule.
- Small LCGs expose visible patterns.

Important

A long period alone does not imply independent uniform samples.

Choosing PRNG parameters matters

A useful generator should aim for:

1. **Long period:** avoid repeating within a typical simulation.
2. **Good distributional properties:** approximate uniformity and weak unwanted dependence.
3. **Efficient implementation:** fast, reproducible, and reliable.

For an LCG

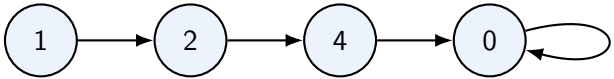
Its performance depends strongly on a, c, and m; arbitrary values may give short cycles or structured output.

Modern numerical libraries usually provide better-tested PRNGs than small hand-built LCGs. LCGs remain useful for understanding the mechanism.

A poor LCG: how quickly can it get stuck?

Consider $m = 8$, $a = 2$, $c = 0$, $X_0 = 1$:

$$X_{n+1} = 2X_n \bmod 8.$$



$$U_n : \quad \frac{1}{8}, \quad \frac{2}{8}, \quad \frac{4}{8}, \quad 0, \quad 0, \quad 0, \ldots$$

Lesson

The sequence enters a fixed point: its eventual cycle has period 1.

Quick exercise 1: find the period

Try it (2 minutes)

For the LCG

$$X_{n+1} = (3X_n + 1) \bmod 8, \qquad X_0 = 0,$$

calculate X_1, X_2, X_3, X_4.

1. What is the first repeated state?
2. What is the period for this seed?
3. Is this a full-period generator modulo 8?

Work out the sequence before moving to the solution.

Quick exercise 1: solution

$$
\begin{aligned}
X_0 &= 0, \\
X_1 &= (3 \cdot 0 + 1) \bmod 8 = 1, \\
X_2 &= (3 \cdot 1 + 1) \bmod 8 = 4, \\
X_3 &= (3 \cdot 4 + 1) \bmod 8 = 5, \\
X_4 &= (3 \cdot 5 + 1) \bmod 8 = 0.
\end{aligned}
$$

Answer

$0 \to 1 \to 4 \to 5 \to 0 \to \cdots$: the period is **4**, not 8.

The example illustrates why the choice of LCG parameters is important.

Section 6.2

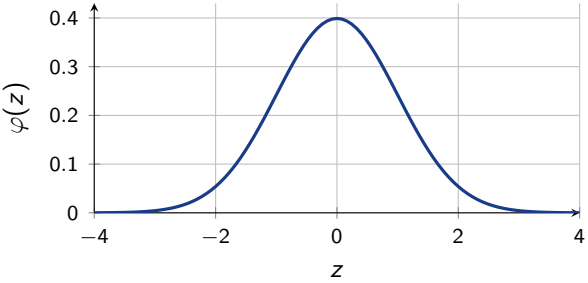
The Box–Muller method

Transforming uniform random numbers into Gaussian samples



The standard Gaussian distribution has density

$$\varphi(z) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{z^2}{2}\right), \qquad z \in \mathbb{R}.$$



- Symmetric about 0.
- $\mathbb{E}[Z] = 0$.
- $\mathrm{Var}(Z) = 1$.
- The distribution has support over the entire real line.

Let U_1, U_2 be **independent** Unif$(0,1)$ random variables. Define

$$R = \sqrt{-2\log U_1}, \qquad \Theta = 2\pi U_2.$$

Then set

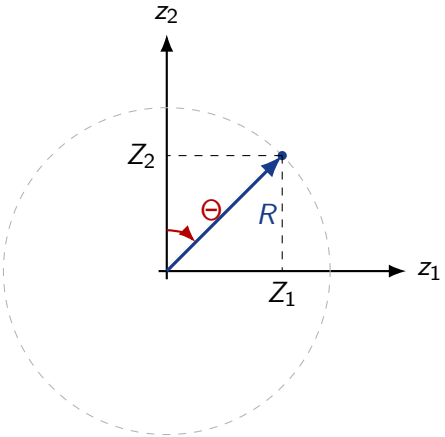
Box–Muller transformation (lecture-note convention)

$$\boxed{Z_1 = R\sin\Theta, \qquad Z_2 = R\cos\Theta.}$$

$$\boxed{Z_1, Z_2 \text{ are independent } \mathcal{N}(0,1) \text{ random variables.}}$$

The method produces *two* Gaussian samples from *two* independent uniforms.

Geometric intuition: radius and angle



- U_2 determines a **uniform angle** $\Theta \in [0, 2\pi)$.
- U_1 determines a nonnegative **radius** R.
- Convert polar coordinates to Cartesian coordinates using sine and cosine.

Why the particular choice $R = \sqrt{-2 \log U_1}$? It creates the correct radial distribution for a 2D Gaussian.

Where does the radius formula come from?

Let $U_1 \sim \text{Unif}(0,1)$ and $R = \sqrt{-2\log U_1}$. For $r \geq 0$,

$$\begin{aligned} F_R(r) &= \Pr(R \leq r) \\ &= \Pr\left(\sqrt{-2\log U_1} \leq r\right) \\ &= \Pr\left(U_1 \geq e^{-r^2/2}\right) \\ &= 1 - e^{-r^2/2}. \end{aligned}$$

Resulting radial distribution

$$\boxed{F_R(r) = 1 - e^{-r^2/2}}, \quad r \geq 0.$$

Radius and angle have simple densities

Differentiate the CDF of R to obtain

$$p_R(r) = F_R'(r) = re^{-r^2/2}, \qquad r > 0.$$

Since $U_2 \sim \text{Unif}(0,1)$,

$$\Theta = 2\pi U_2 \sim \text{Unif}(0, 2\pi), \qquad p_\Theta(\theta) = \frac{1}{2\pi}.$$

Because U_1 and U_2 are independent, **R and Θ are independent**:

$$\boxed{p_{R,\Theta}(r,\theta) = \frac{r}{2\pi} e^{-r^2/2}, \quad r > 0,\ 0 \le \theta < 2\pi.}$$

This is the polar-coordinate density associated with two independent standard Gaussians.

Proof strategy: a change of variables

We know the joint density of the input uniforms:

$$p_{U_1,U_2}(u_1, u_2) = 1, \qquad (u_1, u_2) \in (0,1)^2.$$

For an invertible smooth transformation (away from measure-zero boundaries),

$$\boxed{p_{Z_1,Z_2}(z_1, z_2) = p_{U_1,U_2}(u_1, u_2) \left| \det \frac{\partial(u_1, u_2)}{\partial(z_1, z_2)} \right|.}$$

1. Express u_1, u_2 in terms of z_1, z_2.
2. Calculate the absolute Jacobian determinant.
3. Factorise the resulting joint density.