Oscar
Cortez

HOW COMPUTERS FAKE RANDOMNESS

Pseudo-Random Numbers

Oscar
Cortez

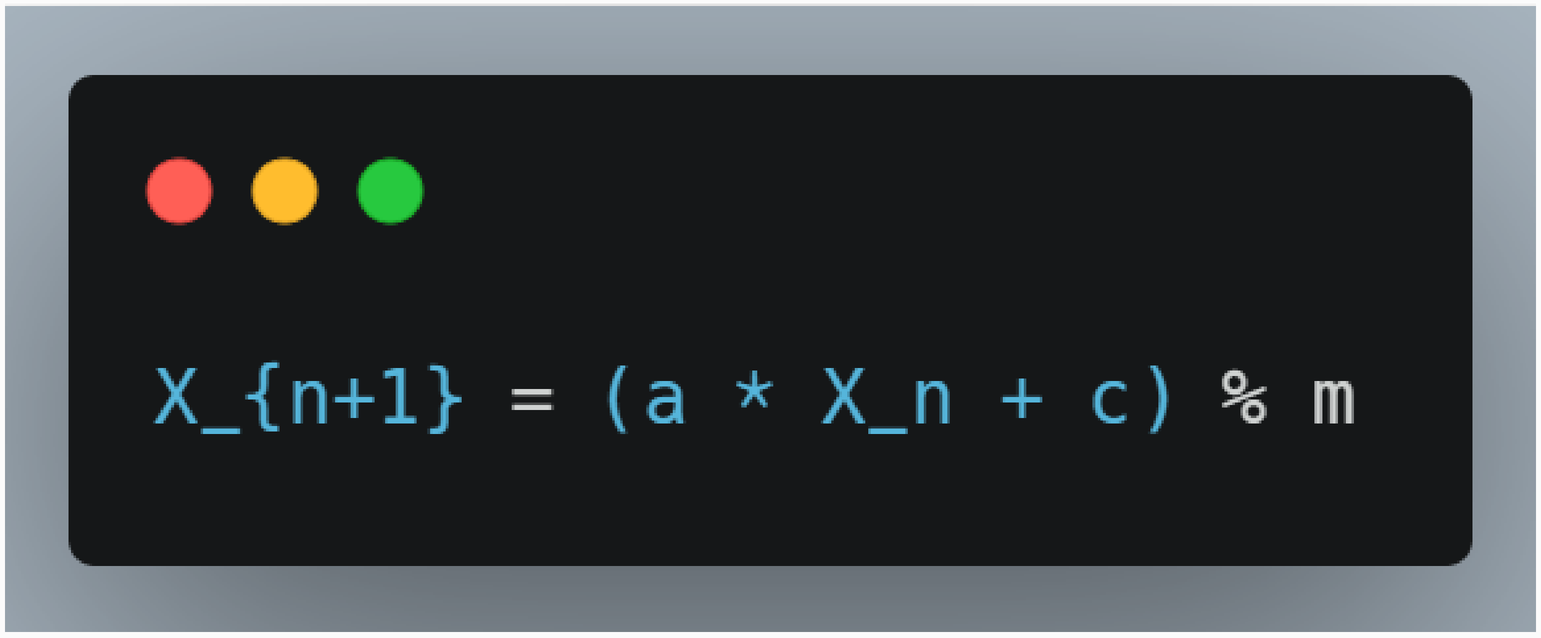
Computers are deterministic machines. So how do they generate random numbers?

They don’t.
They generate pseudo-random numbers (PRNs) using formulas that look random.

Oscar
Cortez

A Simple PRN Generator

The Linear Congruential Generator (LCG) is one of the simplest PRN methods:



```
X_{n+1} = (a * X_n + c) % m
```

You pick a starting number (seed) and repeat the formula.
It looks random... but it’s not

Short Cycle: 37184 37184 37184 37184
Long Cycle:1492838502029341 1492838502029341

Cycles and Periods

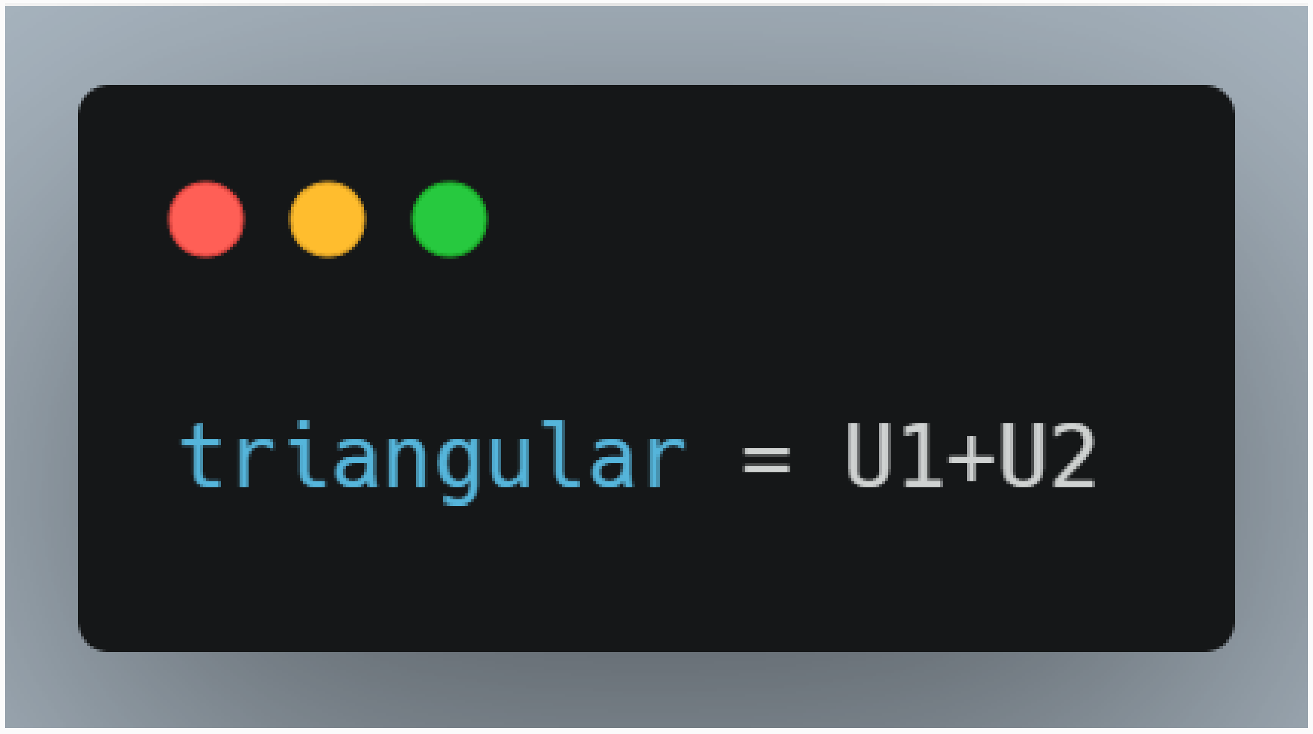
Because it’s algorithmic, a PRN will eventually repeat itself.
That’s called its cycle.

The period = how many values it generates before looping.

Poor parameters → short cycles → bad randomness.

Oscar
Cortez

Uniform at Heart



```
triangular = U1+U2
```

Most PRNs generate numbers that follow a Uniform(0, 1) distribution.
From there, you can create other distributions via transformation:

✅ Normal
✅ Triangular
✅ Exponential
... and more.

Key Takeaways

✅ PRNs are deterministic, but look random
✅ LCG is a good teaching example (but not great in practice)
✅ Most PRNs give you Uniform(0,1), which you can transform
✅ Better PRNGs = better simulations = better results