Randomness

→ unpredictability?

Applications?

- Video games
  Spawning, random drops
  Procedural generation. — predictability!
- LLMs (generation, temp)
- Games (dice, gambling)
- Cryptography

predictability bad!

- Simulations
- Random testing.

predictability! reproducibility good!

2 main types of computer-generated randomness:

1. using physical source of randomness
   radio waves, thermal noise, quantum effects, dice, coin flips, lava lamps.

   pros: very unpredictable
   cons: slow
2. Pseudo random number generator (PRNG) — deterministic function whose output looks unpredictable

   pros: fast
   predictable.

PRNGs?

Linear Congruential Generator (LCG)

$$\underline{X_{n+1} = (\underline{\underline{a x_n}} + c}\,) \text{ mod } m$$

↳ typically power of 2.

Choose a, c carefully

Java uses $m = 2^{48}$, $c = 11$, $a = 5DEECE66D_{16}$.

Python uses a Mersenne Twister.

Xorshift: eg. for 64-bit

```
x = x ^ (x << 13)
x = x ^ (x >> 7)
x = x ^ (x << 17)
```