MATH 242 — 20 April 2026

How do computers generate ~~random~~ pseudorandom numbers?

MIDDLE-SQUARE METHOD

example: seed 5146 → square → 26 4813 16 (4 digits)

4813 → square → 23 1649 69

1649 → ⟶

sequence: 5146, 4813, 1649, ...

individual digits: 5, 1, 4, 6, 4, 8, 1, 3, 1, 6, 4, 9, ...

↑ Is this sequence sufficiently random? How would you tell?

LINEAR CONGRUENTIAL METHOD

parameters:

seed	S_0
multiplier	α
increment	β
modulus	N

Compute:

$$S_n = \alpha \cdot S_{n-1} + \beta \pmod{N}$$

for $n > 0$

Example: $S_0 = 17, \quad \alpha = 37, \quad \beta = 1, \quad N = 100$

$S_0 = 17$

$S_1 = 37 \cdot 17 + 1 = 630 \equiv 30 \pmod{100}$

$S_2 = 37 \cdot 30 + 1 = 511 \equiv 11 \pmod{100}$

$S_3 = 37 \cdot 11 + 1 = 408 \equiv 08 \pmod{100}$

sequence: 17, 30, 11, 08, ...

digits: 1, 7, 3, 0, 1, 1, 0, 8, ...