22 April 2024

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

MIDDLE-SQUARE METHOD

example: seed: 5146 → square → 26481316

divide by $10^{k/2}$ / 100, forget remainder

remainder mod $10{,}000 = 10^k$

4-digit numbers ($k=4$)

4813 → square → 23164969

1649 → 02719201

sequence: 5146, 4813, 1649, 7192, ...

individual digits: 5, 1, 4, 6, 4, 8, 1, 3, 1, 6, 4, 9, 7, 1, 9, 2, ...

LINEAR CONGRUENTIAL METHOD

PARAMETERS:

- multiplier: α
- increment: β
- modulus: N
- seed: S_0

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

($\alpha \cdot S_{n-1} + \beta$: linear eq.; $\pmod N$: congruence)

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

$S_0 = 17$

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

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

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

sequence: 17, 30, 11, 08

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