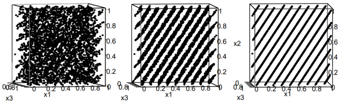
Algorithms and Data Structures

Random Numbers
Congruential Generators



Learning goals

- Linear congruential generator
- Multiplicative congruential generators

LINEAR CONGRUENTIAL GENERATOR

Let $a, c, m \in \mathbb{N}$, then a **linear congruential generator (LCG)** is defined by

$$x_{i+1} = (ax_i + c) \mod m.$$

Examples:

- Marsaglia II: $m = 2^{32}, a = 69069, c = 1$
  has maximum possible period of m.
- Longer I: $m = 2^{48}, a = 25214903917, c = 11$
  Longer II: $m = 2^{48}, a = 5^{17}, c = 1$
  Longer period, specifically designed for 48-bit fraction-arithmetic.

MULTIPLICATIVE CONGRUENTIAL GENERATORS

Special case for $c = 0$: **multiplicative congruential generator (MCG)**

Let $a, m \in \mathbb{N}$, we consider the sequence

$$x_{i+1} = ax_i \mod m.$$

For example, $x_1, \ldots, x_{m-1}$ is a permutation of the numbers $\{1, \ldots, m-1\}$ if

- m is a prime,
- $a^{(m-1)/q} \mod m \neq 1$ for all prime factors q from $m-1$.

MULTIPLICATIVE CONGRUENTIAL GENERATORS / 2

Example:

- $m = 17$ (prime number), $a = 27$, $x_1 = 5$

i	1	2	3	4	5	6	7	8	9	10
0	5	16	7	2	3	13	11	8	12	1
10	10	15	14	4	6	9	5	16	7	2
20	3	13	11	8	12	1	10	15	14	...

  At $i = 17$ the sequence starts from the beginning.

- $m = 17$, $a = 26$, $x_1 = 5$
  $26^{16/2} \mod 17 = 1$

i	1	2	3	4	5	6	7	8	9	10
0	5	11	14	7	12	6	3	10	5	11
10	14	7	12	6	3	10	5	11	14	7
20	12	6	3	10	5	11	14	7	12	...

  The sequence starts already at $i = 9$ from the beginning, period length $= 8$.

MULTIPLICATIVE CONGRUENTIAL GENERATORS / 3

Concrete implementations:

- Very popular for a long time: LEWIS, Goodman ▸ Lewis, Goodman, and J. M. Miller 1969 (e.g., IMSL, early Matlab versions, . . .):

$$m = 2^{31} - 1, \qquad a = 7^5$$

  Reason for choosing m: Largest prime number that can be represented as a normal integer on 32-bit machines (period $2^{31} - 2$).

- Infamous (very bad!!!): RANDU

$$m = 2^{31}, \qquad a = 65539 = 2^{16} + 3$$

  Period length of 2^{29} and quickly calculated, but major problems with distribution of consecutive triplets.

MULTIPLICATIVE CONGRUENTIAL GENERATORS / 4

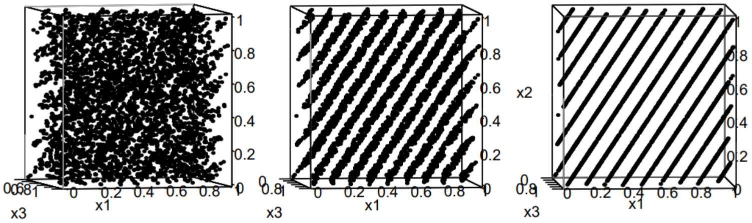
For RANDU, the relationship of three consecutive numbers is given by (the following lines are to be understood $\mod 2^{31}$):

$$
\begin{aligned}
x_{i+1} &= (2^{16}+3)x_i \\[1em]
x_{i+2} &= (2^{16}+3)^2 x_i \\
&= (2^{32}+6\cdot 2^{16}+9)x_i \text{ [1]} \\
&= (6\cdot(2^{16}+3)-9)x_i \\
&= 6\cdot(2^{16}+3)x_i - 9x_i \\
&= 6x_{i+1} - 9x_i
\end{aligned}
$$

[1] 2^{32} is a multiple of $m = 2^{31}$, thus canceled out considering $\mod m$.

MULTIPLICATIVE CONGRUENTIAL GENERATORS

To illustrate the problem, we use RANDU to generate 12000 random numbers and assign three consecutive numbers to each of the three columns of a matrix.
We are going to visualize the *points* in a 3D plot.



Note: It is the same plot from three different perspectives.

MULTIPLICATIVE CONGRUENTIAL GENERATORS / 2

Further examples for MCGs:

- Park, Miller ▸ Park, K. W. Miller, and Stockmeyer 1993: $m = 2^{31} - 1$, $a = 48271$.
- Marsaglia I: $m = 2^{32}$, $a = 69069$.
- SAS / IMSL: $m = 2^{31} - 1$, $a = 397204094$.
- Fishman-Moore I, II und III: $m = 2^{31} - 1$
  $a \in \{630360016, 742938285, 950706376\}$
  (Winner after extensive statistical investigations).