Linear congruential method

- $x_{i+1} = (ax_i + c) \pmod{M}, i \geq 0$

(x_0 = initial value = seed, a = multiplier, c = increment, M = modulus, are all positive integers)

- $x_i \in \{0, 1, \ldots, M-1\}$, $U_i = \frac{x_i}{M} \in [0, 1), i \geq 0$ are approximations to uniform random numbers.

Drawbacks

(a) The sequence of numbers will repeat itself after atmost M steps and hence is periodic.

(b) eg: i) $a = 5, c = 1, M = 7, x_0 = 2$

ii) $a = 5, c = 0, M = 16, x_0 = 1$.

Choice of parameters

- Seed is generally fixed by using the date and time functions.
- If M is prime, we can take $c = 0$.

Theorem: $M = 2^m, c > 0$

(a) The full period is obtained iff $a = 1 \pmod 4$ and c is odd. For a full period, $a = 4N + 1$, $N \in \mathbb{Z}$.

- $M = 2^m, c = 0$

Max. period $= 2^{m-2}$, $a = 3 \pmod 8$ or $a = 5 \pmod 8$