Generatori di numeri pseudocasuali

Algoritmi che hanno come input una breve sequenza (*seme*) e in output un flusso di n bit, che contiene una sottosequenza (*periodo*) che si ripete. Il seme deve essere segreto.

Dato un seme da s bit, il generatore produce al più 2^s sequenze diverse. Questo è assai inferiore alle 2^n sequenze possibili, visto che tipicamente $s \ll n$.

Un generatore pseudocasuale è un *amplificatore di casualità* del seme.

Generatore lineare

$$x_i = (ax_{i-1} + b) \bmod m$$

dove $a, b, m \in \mathbb{N}^+$ sono parametri del generatore, insieme al seme x_0. Il periodo è $\leq m$, e se i parametri sono scelti correttamente il generatore produce una permutazione degli interi da 0 a $m-1$.

Criteri (non importa che ve li ricordiate):

- $(b, m) = 1$;
- $a - 1$ deve essere divisibile per ogni fattore primo di m.

Per esempio $a = 3141592653$, $b = 2718281829$, $m = 2^{32}$.

Se si vogliono sequenze binarie, si calcola:

$$b_i = \frac{x_i}{m} \bmod 2.$$

Supera i test per i generatori non crittograficamente sicuri, ma ci sono algoritmi polinomiali che trovano i parametri a partire dagli elementi generati.

Generatore polinomiale

$$x_i = (a_t x_{i-1}^t + \cdots + a_1 x_{i-1} + a_{t-1}) \bmod m$$