RANDOM NUMBER GENERATOR

PSEUDO-RANDOM NUMBER (PRNG)

$X \sim U(0,1)$ UNIFORM R.V.

PRNG genera numeri in $\left\{0, \frac{1}{m}, \frac{2}{m}, \dots \frac{m-1}{m}\right\}$, per $m >> 0$

PRNG are mostly based on arithmetic / number theory.

FIRST ARITHMETIC METHOD (METROPOLIS / VON NEUMANN, 1940s)

1) Parti da z_0 intero positivo di 4 cifre
2) calcola z_0^2
3) keep 4 inner digits
4) Divide by 10^4

Iterate!

Can have low period

Can reach zero and get stuck there

7182		51 581 124
5811	0,5811	33 767 721
7677	0,7677	

Good PRGN

1) uniform in (0,1), uncorrelated
2) fast, use little memory
3) reproducibility (for debugging, or coupling)
4) large period
5) Portability (not depending on a given machine)

LINEAR CONGRUENTIAL GENERATORS

$z_0 \leftarrow$ SEED, $z_i \in \mathbb{N}$

$$z_i = (a \cdot z_{i-1} + c) \bmod m$$

a: multiplier, c: increment, m: modulus

$$0 \le z_i \le m-1 \Rightarrow u_i := \frac{z_i}{m} \in [0,1)$$

$$z_i = \left[a^i z_0 + \frac{c(a^i - 1)}{a-1}\right] \bmod m$$

z_i è determinato da input z_0, a, c, m

If chosen well, u_i look random. $m = 2^{31}$ o $m = 2^{63}$ (long)

Condizioni per un full period

- c and m are relatively prime (no prime factors in common)
- If $q \mid m$, q prime, then $q \mid a-1$
- If 4 divides m, then 4 divides $a-1$

Example: $a=5$, $c=3$, $m=16$

A full period is not enough: need good statistical properties.

m

If $z_{i_1}, z_{i_2}, \ldots, z_{i_J}$ LCG with different moduli

$$z_i = \left(\delta_1 z_{i_1} + \ldots + \delta_J z_{i_J} \right) \bmod m \quad , m_i = \frac{z_1}{m}$$

period 2^{191} (m rand. c)

TESTING PRNG.

χ^2-TEST

$X_1, \dots, X_n$ generated by PRNG

H_0: " $X_1, \dots, X_n \sim U(0,1)$ and iid "

1) Divide $[0,1]$ in K subintervals, $I_1, \dots, I_K$, of same length

2) $N_j = \sum_{i=1}^{n} \mathbb{I}\{X_i \in I_j\}$

$$\chi^2 = \sum_{j=1}^{K} \frac{\left(N_j - \frac{n}{K}\right)^2}{n/K}$$

χ^2 is $\approx$ distributed according to a χ^2-distribution with $K-1$ degrees of freedom ($Z = Y_1^2 + \dots + Y_{K-1}^2$, $Y_i \sim N(0,1)$)

ACCEPT H_0 if $\chi^2 \le y$, where y is such that $P(Z \le y) = 0.95$ otherwise reject.

Can be used to test also block-behaviour on $(X_1, \dots, X_d), \dots$

$X_1, X_2, \ldots, X_d, X_{d+1}, \ldots, X_n$

$\underbrace{(X_1, X_2, \ldots X_d)}, \underbrace{(X_{d+1}, X_{d+2}, \ldots X_{2d})}, \ldots \underbrace{(X_{n-d+1}, \ldots, X_n)}$

do χ^2 on these blocks, that have to be unif. distr in $[0,1]^d$

($d=2$)