Morena De Poli

GENERATORI DI NUMERI PSEUDO-CASUALI

I generatori di numeri casuali sono impiegati in moltissimi campi, in particolare nella simulazione e, di conseguenza, nella programmazione dei giochi.

Prima dell'avvento dei computer (cioè fino a pochi decenni fa!!!!), venivano anche utilizzate delle tavole contenenti milioni di numeri casuali, ma come può essere facile immaginare, la loro gestione era certamente onerosa in termini di tempo e di spazio. Molti studiosi si sono impegnati nella generazione di sequenze di numeri casuali, ideando macchine a volte anche molto ingegnose. Quella più conosciuta è certamente la roulette del casinò di Montecarlo (dal quale deriva il nome di una intera classe di metodi di simulazione). Le macchine di tipo meccanico si basavano infatti sul principio di un disco, diviso in settori numerati di uguale ampiezza, che veniva fatto ruotare da un motore e arrestato dopo un tempo arbitrario: il numero casuale generato era quello visibile dopo lo stop.

E' possibile anche costruire un generatore domestico col metodo classico dell'urna contenente palline numerate da 0 a 9, dove ogni pallina estratta viene reinserita nell'urna per l'estrazione successiva; ad ogni estrazione, la pallina rappresenta la cifra di un numero casuale che va via via componendosi e che avrà lunghezza arbitraria in base al numero di estrazioni effettuate.

Ma l'avvento dei computer, con le loro elevate capacità di calcolo, ha cambiato completamente l'approccio.
E' stato grazie agli studi di Donald Knuth negli anni '60 del secolo scorso che sono stati sviluppati dei metodi detti deterministici poiché si basano sull'applicazione di formule matematiche: a partire da un numero iniziale detto "seme", e fissato un valore detto "modulo", esse consentono di ottenere sequenze casuali, o meglio pseudo-casuali; infatti, la lunghezza massima della sequenza sarà pari al "modulo" e, a parità degli altri parametri, semi uguali produrranno sequenze uguali. Devono essere quindi individuati dei modi per scegliere semi sempre diversi e per allungare le sequenze scegliendo moduli più grandi, cosa sempre più facile grazie alle caratteristiche fisiche dei computer in continua evoluzione ed espansione.

Donald Knuth è il padre del metodo della *Congruenza Lineare modulo m* con il quale, scelto un valore iniziale x_0 detto seme, si ottiene una sequenza di numeri pseudo-casuali mediante l'applicazione ripetuta della seguente formula:

$$x_{i+1} = (a * x_i + c) \quad (MOD\ m)$$

dove:

- ***a*** è un coefficiente intero strettamente positivo detto moltiplicatore
- ***c*** è un coefficiente intero non negativo detto incremento
- ***m*** è un coefficiente intero strettamente positivo detto modulo
- x_i è il generico numero della sequenza

Si ricorda che MOD è l'operazione "modulo" e la scrittura *a (MOD b)* rappresenta il resto della divisione intera tra i numeri *a* e *b*; pertanto, la lunghezza massima delle sequenze ottenute sarà pari cioè al modulo *m* dato che i possibili resti della divisione intera per *m* sono tutti compresi tra *0* ed *m-1.*

Facciamo un esempio scegliendo il seme $x_0 = 3$ e

- $a = 3$
- $c = 5$
- $m = 11$

La sequenza che si ottiene applicando la formula della congruenza modulo *m* è la seguente: 3, 3, 3, 3, …, cioè una sequenza assolutamente **non casuale**.

Mumble, mumble …. sembra che il metodo non funzioni!!!!

Ma se scegliamo $x_0 = 1$ le cose cambiano e otteniamo 1, 8, 7, 4, 6, 1, 8, 7, 4, 6, 1, … dove notiamo che i primi 5 numeri vengono riprodotti continuamente!

Con $x_0 = 2$ si ottiene 2, 0, 5, 9, 10, 2, 0, 5, 9, 10, 2, … ancora una sequenza di 5 numeri ripetuta.

Non va ancora bene!!! Vediamo cosa accede se modifichiamo il moltiplicatore *a* oppure l'incremento *c.*

Scegliamo *a* = 12 anziché 3: col seme $x_0 = 1$ si ottiene 1, 6, 0, 5, 10, 4, 9, 3, 8, 2, 7, 1, 6, 0, 5, 10, … cioè una sequenza di lunghezza 11, la massima lunghezza possibile.

E se con questi nuovi valori cambiassimo anche *c*? Con *c* = 6 si ottiene 1, 7, 2, 8, 3, 9, 4, 10, 5, 0, 6, 1, 7, 2, 8, 3, 9 … ancora una sequenza di lunghezza massima ma con i numeri mescolati rispetto alla precedente!!!

Da tutto ciò possiamo ricavare che:
- Il valore di x_0 può essere determinante nella lunghezza della sequenza
- Particolari scelte di *a,* ma anche di *c,* possono ridurre notevolmente la lunghezza della sequenza o renderla massima

Donald Knuth, ma insieme a lui anche altri matematici/informatici, ha approfondito questi aspetti e ha individuato i seguenti criteri necessari e sufficienti che garantiscono l'ottimalità del metodo:

1. I parametri *c* e *m* devono essere coprimi cioè *MCD(c,m) = 1*
2. ogni divisore primo di *m* deve dividere anche *a - 1*
3. se *m* è multiplo di 4, anche *a-1* lo deve essere.

Ecco quindi alcuni valori dei coefficienti suggeriti nel rispetto dei suddetti criteri di ottimalità:

KNUTH $m = 2^{31}$; $a = int(\pi * 10^{8})$; $c = 453806245$

GOODMAN e MILLER $m = 2^{31}-1$; $a = 7^{5}$; $c = 0$

GORDON $m = 2^{31}$; $a = 5^{13}$; $c = 0$

LEORMONT e LEWIS $m = 2^{31}$; $a = 2^{16} + 3$; $c = 0$

In ogni caso, per rendere più aleatorio il processo, il seme viene fissato in modo hardware, prelevandone il valore da un contatore interno al computer usato normalmente per altri scopi, oppure ne viene richiesto il valore all'inizio del processo di generazione.
Mediante l'uso di un foglio di calcolo sarà molto semplice applicare la formula della congruenza lineare modulo *m* e realizzare quindi un generatore per verificare che le scelte dei parametri possono essere determinanti.

	A	B	C
1			
2	a	12	
3	c	6	
4	m	11	
5			
6	x0	1	
7	x1	=RESTO(B2*B6+B3;B4)	
8	x2	2	
9	x3	8	
10	x4	3	
11	x5	9	
12	x6	4	
13	x7	10	
14	x8	5	
15	x9	0	
16	x10	6	
17	x11	1	
18	x12	7	
19	x13	2	
20	x14	8	
21	x15	3	

Come si può notare il valore 1 si ripete in corrispondenza dell'elemento x_{11}, cioè proprio dopo 11 elementi della sequenza.

Applicazione nel gioco della tombola

Il metodo ci deve consentire di generare i 90 numeri della tombola, quindi la scelta del modulo deve ricadere su $m = 90$.
Poiché è necessario generare esattamente tutti i 90 numeri, applichiamo i criteri di ottimalità per individuare i valori corretti per il moltiplicatore *a* e per l'incremento *c* e per questo scomponiamo il modulo $m = 90$ in fattori primi: $m = 2 \cdot 3^2 \cdot 5$.
Il primo criterio impone di scegliere *c* in modo tale da non avere fattori comuni con *m,* quindi il valore 7 potrebbe andar bene.
Il secondo criterio impone che ogni divisore primo di *m* debba dividere anche $a - 1$; quindi, ponendo $a = 91$ accade che $a - 1 = 90$ e che anche il secondo criterio sia verificato.
Fortunatamente, il numero 4 non è un divisore di 90, quindi non è necessario procedere oltre, ma la modalità di scelta di *a* lo avrebbe comunque garantito.

Riassumendo: $a = 91$; $c = 7$; $m = 90$.

Ora sarà sufficiente scegliere il seme per dare il via all'estrazione dei numeri per il nostro gioco.

Ecco la realizzazione del gioco con snap!: