Simulation & Sampling

Q: How can we generate random numbers?

Psuedo-Random Number Genation

Goal: Generate a sequence that "seem" random.

Idea: "Multiplicative Congruence Generator"

$$R_n = (a R_{n-1}) \bmod m$$

$R_0 \neq 0$ the "seed"

$a = a \bmod m \neq 0$ "multiplier"

m usually a large prime

Ex: $m = 7$ $\quad a = 3$ $\quad R_0 = 5$

R	aR	3r mod 7
5	15	1
1	3	

1	3	3
3	9	2
2	6	6
6	18	4
4	12	5
5	...	...

"Full period"

Ex: $m = 7 \quad a = 2 \quad R_0 = 5$

R	$2R$	$2R \bmod 7$
5	10	3
3	6	6
6	12	5
5	...	...

Not full period

So the trick is to choose a, m s.t. the sequence looks random.

Also want full period & comp efficient.

Note that we can produce "random samples" deviates from $U(0,1)$ by taking R_n/m

How do we get full period?

Assume that m is prime then

$$R_{n+2} = (a R_{n+1}) \bmod m$$
$$= [a(R_n \bmod m)] \bmod m$$
$$= [a^2 R_n \bmod m] \bmod m$$
$$= a^2 R_n \bmod m$$

So since we seek full period we can assume WLOG $R_0 = 1$

$$R_n = (a^n R_0) \bmod m$$
$$= a^n \bmod m$$

Since m is prime $a^{m-1} \bmod m = 1$

So to have full period we need

a s.t. $a^n \bmod m \neq 1$ for

$n = 1, 2, \ldots, m-2$ thus a needs

to be a primative root modulo m.

Ex: $a = 3$ is a primative root

root mod 7.

Ex: (Park-Miller Minimal Standard)

$m = 2^{31} - 1$ $\quad$ $a = 7^5 = 16807$

primative root mod 7

Ex: (Bad geneator) Randu

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

$$R_{n+2} = (a^2 R_n) \bmod m$$

$$= \left[\left(2^{32} + 6 \cdot 2^{16} + 9\right) R_n \right] \bmod 2^{31}$$

$$= \left[\left(6 \cdot 2^{16} + 18 - 9\right) R_n \right] \bmod 2^{31}$$

$$= \left[6 (\underbrace{2^{16} + 3}_{a}) R_n \right] \bmod 2^{31}$$

$$= \left[(6a - 9) R_n \right] \bmod 2^{31}$$

$$= \left[6 (a R_n \bmod m) - 9 R_n \right] \bmod 2^{31}$$

$$= \left[6 R_{n+1} - 9 R_n \right] \bmod m$$

$$\Rightarrow \left[R_{n+2} - 6 R_{n+1} + 9 R_n \right] \bmod m = 0$$

<u>Rmk:</u> Randomness only extends two terms

Rmk: $R_n = (aR_{n-1} + c) \bmod m$

↳ incriment

"Linear Congruence Generator"

Rmk: Popular RNG: "Measure Twister"

Generalized Feedback Shift Twister

period: $2^{19937} - 1$

Ex: $m = 7 \quad a = 3 \quad R_0 = 1$

i	R	$3R$	$3R \bmod 7$	3^i	$3^i \bmod 7$
1	1	3	3	3	3
2	3	9	2	$3^2 = 3 \times 3$	2
3	2	6	6	$3^3 \equiv 2 \times 3$	6
4	6	18	4	$3^4 \equiv 6 \times 3$	4
5	4	12	5	$3^5 \equiv 4 \times 3$	5
6	5	15	1	$3^6 \equiv 5 \times 3$	1