Linear Congruential Generator

June 14, 2022

Random number generator algorithm using LCG

$$x_{n+1} = ax_n + c \mod m$$

When $c \neq 0$

- m and c are relative prime
- a - 1 is divisible by all primve factor of m
- a - 1 is divisible by 4 if m is divisible by 4

The three requirements are referred to as Hull-Dobell Theorem The book Numerical Recipes choose the following $m = 2^{32} \quad a = 1664525 \quad c = 74$
Please validate m, a and c are satified above three requirements.

Proof. Proof: □

C implementation LCG

```
// Linear Congruential Generator
long LCG(long m, long a, long c, long seed){
    long x0 = seed;
    long x1 = (a * x0 + c) % m;
    return x1;
}

// KEY: random number
long randomNum(long seed){
    long m = (long)pow(2, 32);
    long a = 1664525;
    long c = 1013904223;
    long r = LCG(m, a, c, seed);
    return r;
}

// How to Use:
long seed = 104;
int num = 0;
while(num < 10){
    long r = randomNum(seed);
    printf("r=%lu\n", r);
    seed = r;
    num++;
}
```