Random number generation

Although somewhat less glamorous than gambling devices (dice, roulette, cards, etc.) random number generators on the computer are more efficient (>10^9 random numbers / s)

A simple (psudo) random number generator

Linear congruential generator

$$r_{n+1} = ar_n + c \bmod 2^m$$

For suitably chosen multiplier a, all numbers in the set $\{0,\ldots,2^m-1\}$ are generated in random-like order

The increment c should be odd (value not critical)

Let's try some cases, using c=1 and starting with $r_0=0$

```
m=2  a    sequence:
     1    0 1 2 3 0
     2    0 1 3 3 3
     3    0 1 0 1 0
     4    0 1 1 1 1
```

```
m=3  a     sequence:
     1     0 1 2 3 4 5 6 7 0
     2     0 1 3 7 7 7 7 7 7
     3     0 1 4 5 0 1 4 5 0
     4     0 1 5 5 5 5 5 5 5
     5     0 1 6 7 4 5 2 3 0
     6     0 1 7 3 3 3 3 3 3
     7     0 1 0 1 0 1 0 1 0
     8     0 1 1 1 1 1 1 1 1
```

```
m=4   a      sequence:
       3      0 1 4 13 8 9 12 5 0 1 4 13 8 9 12 5 0
       5      0 1 6 15 12 13 2 11 8 9 14 7 4 5 10 3 0
      11      0 1 12 5 8 9 4 13 0 1 12 5 8 9 4 13 0
      13      0 1 14 7 12 13 10 3 8 9 6 15 4 5 2 11 0
```

seems more random-like as m increases

Integer operations on the computer have wrap-around behavior
- exactly like taking the mod

For 64-bit integers this generator is quite OK

```
r=2862933555777941757*r+1013904243
```

- with some caveats
- you will investigate in homework (posted, we discuss it next)

The multiplier is considered one of the best
- many investigations using various statistical criteria