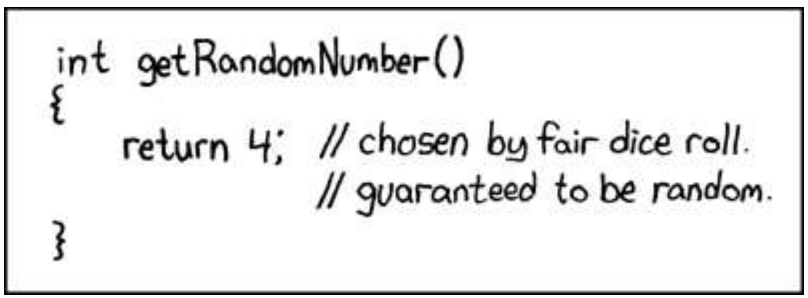
RANDOM NUMBER GENERATORS

MATH CLUB 12/06/2010

WHAT ARE RANDOM NUMBERS?

- 1, 3, 5, 7, 9, 11, …?
- 3, 7, 0, 7, 7, 4, 1, 5, 6, 1, 7, 8, 5 …?
- 44, 22, 16, 33, 67, 29, 68, 38, 49, 89, …?
- 4, 4, 4, 4, 4, 4, 4, 4, …?



HOW DO WE GENERATE RANDOM NUMBERS?

Simple. Hook up a computer to a radio that detects atmospheric noise and converts them into numbers.

WELL WITHOUT A RADIO…

- You can’t.
- But on the other hand, there’s pseudorandom number generators…

JASON GIN'S FAULTY DICEROLL RNG

```
x = rand()
y = rand()
r = x * y * 100
return round(r)
```

rand() gives a random real from 0 to 1, and round() rounds a real to the nearest integer.

- Jason is getting the number 100 less frequently than he should. What is wrong with his code?

MATHEMATICAL ANALYSIS OF JASON'S RNG

- **What is the chance of Jason's function returning 100?**
- $\boldsymbol{xy \geq 0.995}$
- $\boldsymbol{y \geq \frac{0.995}{x}}$
- **If $x < 0.995$ then it is impossible for any y.**
- **If $x \geq 0.995$ then y has a $1 - \frac{0.995}{x}$ chance.**
- $\boldsymbol{\int_{0.995}^{1} 1 - \frac{0.995}{x}\,dx}$
- **Integral is $x - 0.995\ln(x) + C$**
- $\boldsymbol{= 1 - 0.995\ln(1) - 0.995 + 0.995\ln(0.995) \approx 0.00001252}$
- **About once every 79867 trials.**

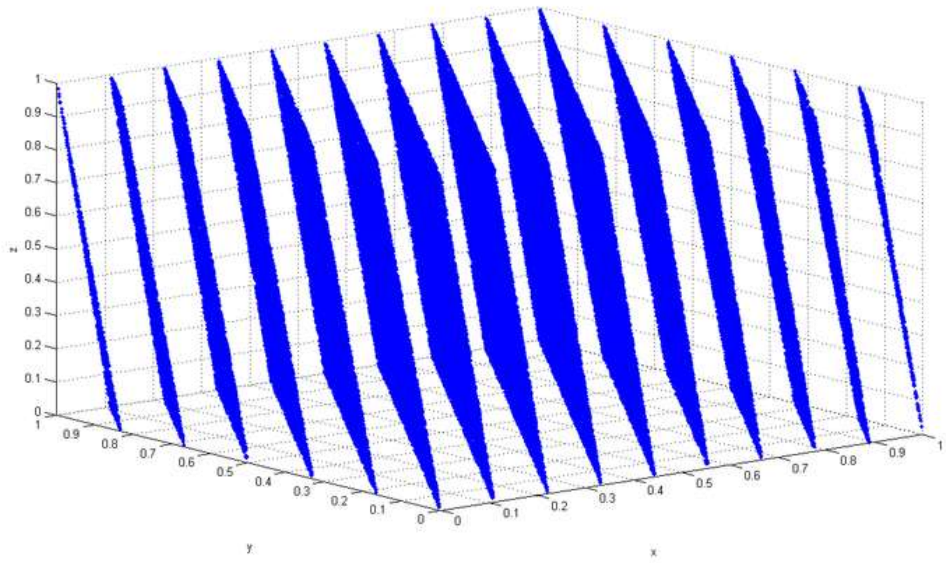
PARK-MILLER RNG

$$x_{k+1} = g \cdot x_k \bmod n$$

- Very simple.
- Let's say $x_0 = 2$, $g = 7$, and $n = 15$.
- $x_1 = 14$
- $x_2 = 8$
- $x_3 = 11$
- 2, 14, 8, 11, …

RANDU

$$x_{k+1} = 65539x_k \bmod 2^{31}$$



- **Above: 100,000 supposedly ‘random’ points**
- **What went wrong?**

MATHEMATICAL ANALYSIS OF RANDU

- $x_{k+1} = 65539 x_k \bmod 2^{31}$
- **Notice that $65539 = 2^{16} + 3$.**
- $x_{k+2} = \left(2^{16} + 3\right) \cdot x_{k+1} = \left(2^{16} + 3\right)^2 \cdot x_k$
- $= \left(2^{32} + 6 \cdot 2^{16} + 9\right) \cdot x_k$
- $\equiv \left(6 \cdot 2^{16} + 9\right) \cdot x_k$
- $= \left[6\left(2^{16} + 3\right) - 9\right] \cdot x_k$
- $= 6\left(2^{16} + 3\right) \cdot x_k - 9 x_k$
- **Very, very bad:** $x_{k+2} = 6 x_{k+1} - 9 x_k$

LINEAR CONGRUENTIAL RNG

$$x_{k+1} = (g \cdot x_k + c) \bmod n$$

- **Standard random number generator in many programming languages**
- **Java –** $(g, c) = (25214903917, 11)$
- **Glibc –** $(g, c) = (1103515245, 12345)$
- **Microsoft Visual C++ –** $(g, c) = (214013, 2531011)$

WHAT ABOUT X_0?

$$x_{k+1} = (g \cdot x_k + c) \bmod n$$

- What is x_0?
- Also known as the seed.

- Current system time, or sometimes hardware.

FOR THE MASTER NUMBER-THEORIST

$$x_{k+1} = (g \cdot x_k + c) \bmod n$$

A good random number generator has a long *period* (number of terms before it starts repeating).

1. **Explain why it is best if $c \perp n$**
2. **Explain why it is best if $g - 1$ is divisible by all prime factors of n.**
3. **Suppose $4|n$. Explain why it is best if $g \equiv 1 \bmod 4$.**