









Slide 5

A Little About Random Numbers

- (Canonical reference discussion in volume 2 of Knuth's *The Art of Computer Programming*. Very mathematical. Other references may be easier.)
- Many application areas that depend on "random" numbers (whatever we mean by that) — simulation (of physical phenomena), sampling, numerical analysis (Monte Carlo methods, e.g.), etc.
- Early on, people used physical methods (currently still in use in lotteries), and thought about building hardware to generate "random" results. No good large-scale solution, though, and besides it seemed useful to be able to repeat a calculation.
- Hence need for "random number generator" (RNG) way to generate "random" sequences of elements from a given set (e.g., integers or doubles). Tricky topic. Many early researchers got it wrong. Many application writers

Slide 6



Slide 7

Desirable Properties of RNG -- "Randomness"

• Obviously a key goal, if tricky to define. A thought-experiment definition: Suppose we're generating integers in the range from 1 through d, and we let an observer examine as much of the sequence as desired, and ask for a guess for any other element in the sequence. If the probability of the guess being right is more than 1/d, the sequence isn't random.

Slide 8

- Also want uniformity for each element, equal probability of getting any of the possible values.
- For some applications, also need to consider "uniformity in higher dimensions": Consider treating sequence as sequence of points in 2D, 3D, etc., space. Are the points spread out evenly?

