Slide 1

Administrivia

- Reminder: Homework 5 due Friday.
- Review sheet for midterm on the Web. Mostly about exam format but also has list of topics.

  Aside: In general my idea is that students who have kept up reasonably well with reading and homeworks won't have to spend a lot of time preparing for exams. The goal is to test whether you understand the material rather than whether you can memorize!

Slide 2

Minute Essay From Last Lecture

- Many interesting replies; discussion next time maybe.

Slide 3

Numerical-Integration Example — Recap

- Programs written in class do two things: `for` loop to iterate over fixed range, `do while` loop to loop until convergence.
- We might usefully have them do one more thing — compare result with the best-available library value for π. (Surprisingly, there's a library constant `M_PI`, but it isn't standard, so use `acos()` to compute?)

Slide 4

A Little About "Random" Numbers

- Among the C library functions discussed briefly in the textbook chapter on functions are `srand()` and `rand()`. A few words about what they do ...
- First, what we mean by "random" is (I think!) an interesting question with no obvious answer. What's often wanted is something that can't be predicted, and it's not clear we can get that with a system that's deterministic. Further, even if we could, we might not want that, since we often want to be able to repeat a test.
- So, often what we really want is a "pseudo-random number generator" — something that generates a sequence of numbers that looks random but is repeatable given some reproducible starting point.

Slide 5

Pseudo-Random Number Generators

- Mathematically interesting topic; classic reference is in one of the volumes of Donald Knuth's *The Art of Computer Programming*.

  (Aside: Some of you may know Knuth as the inventor of the typesetting system TEX. It's an extreme example of a "side project" that turned into something much more?)

- Early researchers apparently thought more-complex algorithms would give better results, but — not necessarily. Very simple algorithms can give quite good results. For example, one reasonable one (not the best, but good) computes each element of the sequence in terms of the previous one:

  $x_{n+1} = (ax_n + b) \bmod M$

  for carefully selected values of a, b, and M.

- Uses in programming include simulating various things in the physical world. Textbook examples often involve simulating rolling dice, shuffling cards, etc.

Slide 6

Pseudo-Random Number Generators in C

- C library includes functions `srand()`, `rand`. `srand()` uses a "seed" to initialize some behind-the-scenes variables, after which you call `rand()` repeatedly to generate a sequence of "random" numbers. If you do this more than once with the same seed you get the same sequence; using different values of the seed gives different sequences.

- "Monte Carlo" algorithms are based on "random" numbers. An example is a program to estimate π by simulating throwing darts into a board containing a quarter circle. (Example program.)

Slide 7

Minute Essay

- None — quiz.