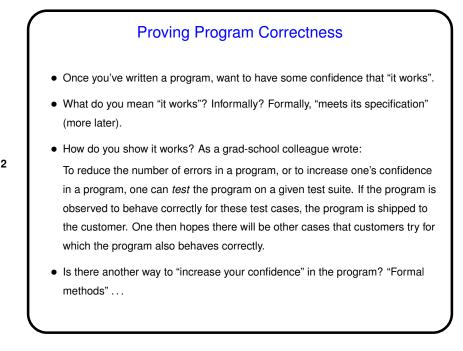
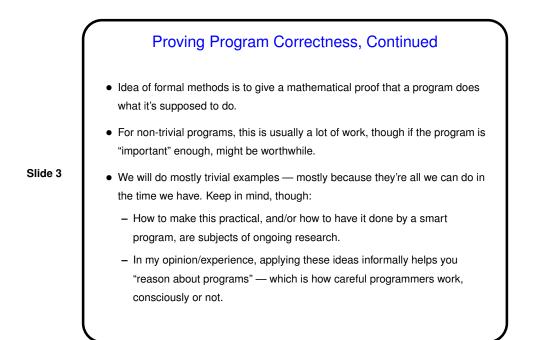


• Reminder: Homework 3 due today (but accepted through Friday without penalty).

Slide 1





	Program Specifications
	<ul> <li>Before we can prove that a program "works", we have to define what that means — "specification".</li> </ul>
ł	• For many programs (the ones we'll talk about here), we care that the program produces the right output for all allowed inputs. So we can write a specification in terms of "precondition" and "postcondition". E.g., for a function sqrt that takes a double <i>x</i> as input and returns a double, we could have:
	Precondition: $x \ge 0$ .
	Postcondition: For return value $y, y \ge 0$ and $y^2 = x$ .
	• This is trivial? Consider the following proposed specification for a sorting function with two inputs <i>A</i> (array of integers) and <i>n</i> (size of <i>A</i> ). Okay?
	Precondition: A is of size $n, n \ge 0$ .
	Postcondition: $(\forall i)(((0 < i < n) \rightarrow A[i-1] \leq A[i])$

