

# Using formal methods to verify a program

**Static analysis** - analyzing the code to detect security flaws

- Control flow - analyzing the sequence of instructions
  - Data flow - analyzing how the data are accessed
  - Data structure - analyzing how data are organized
- ➔ Abstract interpretation [Cousot]
- ✓ Verification of critical embedded software in Airbus aircrafts

# Using formal methods to generate a program

Mathematical description of the problem

*Refinement  
steps*



Proof of correctness



Executable code  
or hardware design