CS70 Recap: What you should've learned thus far

As with any discrete math course, the topics we've been covering in CS70 thus far have probably looked a bit like a collection of somewhat-unrelated bits and pieces without a clear "grand picture". Here's the "big picture" as we, the instructors, see it:

Our *primary* objective is to present a collection of basic mathematical tools that are useful throughout computer science, to give you a thorough understanding of how they work, and to get you comfortable enough with them to apply them to new problems. The tools you've seen thus far are:

- Rigid mathematical proofs in general
  - logic, including implications and deMorgan's Law (both for propositional logic — ANDs and ORs — and for quantifiers)
  - inductive proofs, including strong induction
- GCD and Euclid's algorithm
- Modular arithmetic
  - modular inverses
  - solving modular systems of equations
- Polynomials
  - basic properties of polynomials
  - polynomial interpolation
- Graphs

In the context of learning these tools, we've presented several applications of these tools. We also want you to understand how these tools are applied to:

- reasoning about algorithms in general, and the stable marriage algorithm in particular, using inductive proofs
- secret sharing using polynomial interpolation
- error correction codes using polynomial interpolation
- Eulerian cycles in graphs using basic graph concepts