- Integers, arithmetic, and induction
  - Suggested review: HW #1 problems 5 and 7(a), HW #2 problems 7(b)-(c).
  - Suggested reading: lecture notes 1.1.
- Divisibility, GCDs and LCMs, and the Euclidean algorithm
  - Suggested review: HW #1 problems 1 and 7(b), HW #2 problems 1(a)-(e) and 7(a).
  - Suggested reading: lecture notes 1.2.
- Primes and prime factorization
  - Suggested review: HW #1 problems 2/3/6/7(c), HW #2 problem 4.
  - Suggested reading: lecture notes 1.3.
- Rings, units, and basic ring operations
  - Suggested review: HW #2 problems 1(f)/2/5, HW #3 problem 7.
  - Suggested reading: lecture notes 1.4.
- Modular congruences, residue classes, units and zero divisors mod m.
  - Suggested review: HW #2 problems 1(g)-(h)/3/6, HW #3 problems 1/4/5/6, HW #4 problem 4
  - Suggested reading: lecture notes 2.1.
- Solving linear congruences, the Chinese remainder theorem
  - Suggested review: HW #3 problems 2-3
  - Suggested reading: lecture notes 2.2.
- Powers mod m, orders of elements, properties of orders
  - Suggested review: HW #4 problems 1(a)-(f) and 2.
  - Suggested reading: lecture notes 2.3.1.
- Theorems of Fermat/Wilson/Euler, the Euler φ-function, computing orders
  - Suggested review: HW #4 problems 1(g)-(l)/3/5/6/7/8, HW #5 problem 1.
  - Suggested reading: lecture notes 2.3.2-2.3.3.
- Primitive roots and discrete logarithms
  - Suggested review: HW #5 problem 3.
  - Suggested reading: lecture notes 2.3.4.
- Repeating decimals
  - Suggested review: HW #5 problems 2 and 6.
  - Suggested reading: lecture notes 2.4.
- Cryptography, Rabin and RSA encryption, zero-knowledge proofs
  - Suggested review: HW #5 problems 4/5/7, HW #6 problems 1-4 and 6-8.
  - Suggested reading: lecture notes 3.2-3.4.
- Primality testing and factorization algorithms
  - Suggested review: HW #6 problem 5.
  - Suggested reading: lecture notes 3.5-3.6.