Study guide

- (§29) Understand the "rules for indices" in Theorem 29.1.
- (§20) Know the definition of *quadratic residue* modulo p.
- How can you tell from the index $I(a)$ whether or not a is a quadratic residue?
- (§20) Prove: there are exactly $\frac{1}{2}(p-1)$ quadratic residues modulo p.

1. (Textbook 29.1, solving congruences using indices, four parts)

2. (Textbook 29.2, making and using an index table mod17)

3. (Textbook 29.4, counting solutions to kth root congruences, in general)

4. (Textbook 29.6, on the Elgamal encryption scheme)

5. (Textbook 20.1, listing quadratic residues mod19)

6. One of the laws of ordinary logarithms is that logarithms of different bases are related by the formula $\log_b(x) = \log_c(x)/\log_c(b)$. Formulate and prove a similar law for indices (i.e. discrete logarithms).

7. (Textbook 21.3, on primes for which 3 is a quadratic residue)