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)
   Use the table of indices modulo 37 to find all solutions to the following congruences.

   a) $12x \equiv 23 (\mathrm{mod} 37)$
   b) $5x^{23} \equiv 18 (\mathrm{mod} 37)$
   c) $x^{12} \equiv 11 (\mathrm{mod} 37)$
   d) $7x^{20} \equiv 34 (\mathrm{mod} 37)$

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

   (a) Create a table of indices modulo 17 using the primitive root 3.
   (b) Use your table to solve the congruence $4x \equiv 11 \bmod 17$.
   (c) Use your table to find all solutions to the congruence $5x^6 \equiv 7 \bmod 17$.

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

   (a) If k divides $p-1$, show that the congruence $x^k \equiv 1 \bmod p$ has exactly k distinct solutions modulo p.
   (b) More generally, consider the congruence $x^k \equiv a \bmod p$. Find a simple way to use the values of k, p, and the index $I(a)$ to determine how many solutions this congruence has.
   (c) The number 3 is a primitive root modulo the prime 1987. How many solutions are there to the congruence $x^{111} \equiv 729 \bmod 1987$?
   Hint: $729 = 3^6$.

4. (Textbook 29.6, on the Elgamal encryption scheme)
   In this exercise we describe a public key cryptosystem called the ElGamal Cryptosystem that is based on the difficulty of solving the discrete logarithm problem. Let p be a large prime number and let g be a primitive root modulo p. Here's how Alice creates a key and Bob sends Alice a message.

   The first step is for Alice to choose a number k to be her secret key. She computes the number $a \equiv g^k \bmod p$. She publishes this number a, which is the public key that Bob (or anyone else) will use to send her messages.

   Now suppose that Bob wants to send Alice the message m, where m is a number between 2 and $p-1$. He randomly chooses a number r and computes the two numbers

   $$e_1 \equiv g^r (\mathrm{mod} p) \quad \text{and} \quad e_2 \equiv m a^r (\mathrm{mod} p)$$

   Bob sends Alice the pair of numbers (e_1, e_2). Finally, Alice needs to decrypt the message. She first uses her secret key k to compute $c \equiv e_1^k (\mathrm{mod} p)$. Next she computes $u \equiv c^{-1} (\mathrm{mod} p)$. Finally, she computes $v \equiv u\, e_2 \bmod p$. We can summarize Alice's computation by the formula

$$v \equiv e_2 \cdot \left(e_1^k\right)^{-1} (\mathrm{mod} p)$$

(a) Show that when Alice finishes her computation the number v that she computes equals Bob's message m.

(b) Show that if someone knows how to solve the discrete logarithm problem for the prime p and base g then he or she can read Bob's message.

5. (Textbook 20.1)
Make a list of all the quadratic residues and all the nonresidues modulo 19.

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)
Here is a list of the first few primes for which 3 is a quadratic residue and a nonresidue.

$$\text{Quadratic Residue: } p = 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107, 109$$
$$\text{Nonresidue: } p = 5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89, 101, 103, 113, 127$$

Try reducing this list modulo m for various m's until you find a pattern, and make a conjecture explaining which primes have 3 as a quadratic residue.