HOMEWORK

For this week, please answer the following questions from the text. I've copied the problem itself below and the question numbers for your convenience.

(1) (3.36) This exercise asks you to use the index calculus to solve a discrete logarithm problem. Let $p = 19079$ and $g = 17$.
   (a) Verify that $g^i \mod p$ is 5-smooth for each of the values $i = 3030, i = 6892$, and $i = 18312$.
   (b) Use your computations in part (a) and linear algebra to compute the discrete logarithms $\log_g(2), \log_g(3)$, and $\log_g(5)$. (Note that $19078 = 2 \cdot 9539$ and that 9539 is prime.)
   (c) Verify that $19 \cdot 17^{-12400} \mod p$ is 5-smooth.
   (d) Use the values from (b) and the computation in (c) to solve the discrete logarithm problem
$$17^x = 19 \mod 19079$$

(2) (3.37) Let p be an odd prime and let a be an integer with $p \nmid a$.
   (a) Prove that $a^{(p-1)/2}$ is congruent to either 1 or -1 modulo p.
   (b) Prove that $a^{(p-1)/2}$ is congruent to 1 modulo p if and only if a is a quadratic residue modulo p. (Hint: Let g be a primitive root for p and use the fact, proven during the course of proving Proposition 3.61, that g^m is a quadratic residue if and only if m is even.)
   (c) Prove that $a^{(p-1)/2} = \left(\frac{a}{p}\right) \mod p$.
   (d) Use (c) to prove Theorem 3.62(a), that is prove that
$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p = 1 \mod 4 \\ -1 & \text{if } p = 3 \mod 4 \end{cases}$$

(3) (3.39) Let p be a prime satisfying $p = 3 \mod 4$.
   (a) Let a be a quadratic residue modulo p. Prove that the number
$$b = a^{(p+1)/4} \mod p$$
   has the property that $b^2 = a \mod p$. (Hint: Write $(p+1)/2$ as $1 + (p-1)/2$ and use Exercise 3.37.) This gives an easy way to take square roots modulo p for primes that are congruent to 3 modulo 4.
   (b) Use (a) to compute the following square roots modulo p. Be sure to check your answers.
      (i) Solve $b^2 = 116 \mod 587$
      (ii) Solve $b^2 = 3217 \mod 8627$
      (iii) Solve $b^2 = 9109 \mod 10663$

(4) (3.40) Let p be an odd prime, let $g \in \mathbb{F}_p^\times$ be a primitive root, and let $h \in \mathbb{F}_p^\times$. Write $p - 1 = 2^s m$ with m odd and $s \geq 1$, and write the binary expansion of $\log_g(h)$ as
$$\log_g(h) = \epsilon_0 + 2\epsilon_1 + 4\epsilon_2 + 8\epsilon_3 + \cdots \text{ with } \epsilon_i \in \{0, 1\}.$$

Give an algorithm that generalizes Example 3.69 and allows you to rapidly compute $\epsilon_1, \epsilon_2, \ldots, \epsilon_{s-1}$, thereby proving that the first s bits of the discrete logarithm are insecure. You may assume you have a fast algorithm to compute square roots in $\mathbb{F}_p^\times$, as provided by for example by Exercise 3.39(a). (Hint: Use Example 3.69 to compute the 0th bit, take the square root of either h or $g^{-1}h$ and repeat.) $p = 3 \mod 4$