Midterm 2 practice problems

As you study for the second midterm, you might find it helpful to make sure you know how to do the following problems. There is no guarantee that all midterm problems will look like problems from this list.

(1) Compute $(\frac{23}{51})$. Show your work. What does your answer tell you about $23 \pmod{51}$?
(2) Alice and Bob use an RSA cryptosystem. Alice's public key is (n_A, e_A), and Bob's public key is (n_B, e_B). Alice's private key is d_A, and Bob's private key is d_B. Describe how Alice can send a message m to Bob in such a way that Bob can be sure that only Alice could have sent the message, and Alice cannot deny sending the message once Bob has received it. Additionally, should Eve intercept the message, she should not be able to read it. What numbers does Alice compute and send to Bob? How does Bob decrypt the message? How does Bob know that Alice sent the message?
(3) Use the Baby Step, Giant Step method to calculate $L_2(3)$ for the prime $p = 53$. Show your work.
(4) The Prime Supply Company produces RSA keys. It has a database of 10^8 primes with 200 decimal digits and a database of 10^{10} primes with 250 decimal digits. Whenever it is asked for an RSA modulus, it randomly chooses a 200-digit prime p and a 250-digit prime q from its databases, and then computes $n = pq$. It advertises that it has 10^{18} possible moduli to distribute and brags about its great level of security. After the Prime Supply Company has used this method to supply RSA moduli to 20000 customers, Eve tries computing the gcd of pairs of moduli of these clients (that is, for each pair of clients, with RSA moduli n_1 and n_2, she computes $gcd(n_1, n_2)$). What is the likely outcome of Eve's computations? What will this allow Eve to do? Explain.
(5) Find all four square roots of $23 \pmod{143}$. (Recall that $143 = 11 \cdot 13$.) Explain how knowing these square roots would allow you to factor 143 if you somehow forgot that $143 = 11 \cdot 13$.
(6) Suppose that n is a large odd number. You calculate that $3^{(n-1)/2} \equiv k \pmod{n}$, where k is some integer with $k \not\equiv \pm 1 \pmod{n}$.
   (a) Suppose that $k^2 \not\equiv 1 \pmod{n}$. Explain why n is not prime.
   (b) Suppose that $k^2 \equiv 1 \pmod{n}$. Explain how you can use this information to factor n.
   (c) If $(n-1)/2 = 2^{45} + 2^{11}$, explain how you can calculate $3^{(n-1)/2} \pmod{n}$ in fewer than 500 steps. (Note that you cannot simply multiply 3 by itself $(n-1)/2$ times, because $2^{45} + 2^{11} = 35184372088832$, which is larger than 500.)
(7) If Bob has ElGamal public key $(p, \alpha, \beta) = (67, 2, 7)$ and Alice encodes the message $m = 20$ with secret exponent $k = 5$, what is the ciphertext she sends to Bob?
(8) (a) Compute $35^{630} \pmod{1261}$. Show your work. If you want, you can use the fact that 630 is 1001110110.
   (b) Compute $(\frac{35}{1261})$. Show your work. What does this tell you about $35 \pmod{1261}$?
   (c) What does the Solovay-Strassen primality test tell you about 1261?
(9) Let $p \equiv 3 \pmod{4}$ be a prime. Show that $x^2 \equiv -1 \pmod{p}$ has no solutions.
(10) Briefly describe the following attacks on RSA and the circumstances in which they are likely to be useful: brute force factorization, Pollard $p-1$ algorithm, Wiener's low exponent attack, Fermat factorization, quadratic sieve factorization.