Math 173A - Midterm Practice

1. (a) What is the order of 2 in $\mathbb{F}_{31}$?

   (b) Is 3 a primitive root in $\mathbb{F}_{31}$?

2. Let g be a primitive root of $\mathbb{F}_p$, where p is a prime. Show that g^k is a primitive root of $\mathbb{F}_p$ if and only if $\gcd(k, p-1) = 1$.

3. Alice and Bob agree to use the prime $p = 71$ and the base $g = 7$ for a Diffie-Hellman key exchange.

   (a) Alice chooses $a = 12$ as her secret and Bob chooses $b = 31$ as his secret. What are the values A and B that they should send to each other?

   (b) What is their shared secret?

4. Use the baby step giant step algorithm to find $\log_2(15)$ in $\mathbb{F}_{29}$.

5. (a) Describe each step in the ElGamal cipher.

   (b) If Eve has an oracle that solves the discrete logarithm problem, can she decrypt Elgamal ciphertexts? How?

6. (a) Define what $f(x) = O(g(x))$ means.

   (b) Is $e^{x^2} = O(e^x)$?

   (c) Is $e^x = O(e^{x^2})$?

   (d) Is $\ln(x) = O(\log x)$?

7. Let p and q be primes and suppose that $p = 2q + 1$. Let $h \in \mathbb{F}_p^\times$ and assume that $h \neq 1$. Prove that $x^2 \equiv h \pmod{p}$ has a solution if and only if the order of h is q.