Math 4450/6450 Cryptography Homework #4 -- Diffie-Hellman and Arithmetic in Z/pZ

1) Please find a primitive root in Z/409Z, being sure to carefully describe your algorithm. How many multiplications did you use? How few multiplications could you have used (if you were luckier)?

2) a) How many primitive roots are there in Z/409Z?

   b) How many units are there of order 11? of order 17?

   c) Please find all elements of order 3 in Z/409Z.

3) Please compute the GCD of 12345 and 67890 by Euclid's Algorithm.

4) a) What is the shared secret if p=8191, g=3, your secret number is 1029, and your partner calls out 1702?

   b) Is it easy or hard to determine your partner's secret number? Why?

5) Describe a system for using the Diffie-Hellman Secret Sharing algorithm to generate a key for a Classical cipher (Cryptogram, Hill Cipher, Permutation Cipher, etc.). How large of a prime do you need to use to do this with a reasonable level of security? (Here you should define what you mean by "reasonable" as part of your answer.)

6) a) Please determine the shared secret Alice and Bob know when p=8191, g=2, Alice announces the number 2048 and Bob announces the number 4096.

   b) What can we say about Bob's secret number? Can we determine it?

   c) What could be done to improve the security of this system?

7) For x a unit in Z/NZ, we define Order(x) to be the smallest positive integer so that x^Order(x) = 1 (mod N). Please prove the following assertions:

   a) If Order(x) = a and d>0 divides a, then Order(x^d) = a/d.

   b) If Order(x) = a and b>0 with GCD(a,b) = 1, then Order(x^b) = a.

   c) If Order(x) = a and Order(y) = b with GCD(a,b) = 1, then Order(xy) = ab.

8) ***Challenge:*** State and prove the Division Algorithm for the natural numbers.

9) ***Challenge:*** Show that the following definitions of GCD(a,b) are equivalent when a and b are positive integers:
   a) The largest common divisor of a and b
   b) The most divisible positive common divisor of a and b
   c) The smallest positive integer linear combination of a and b

10) ***Challenge:*** Please describe the pairs of numbers which (for their size) take the longest amount of time for Euclid's algorithm to find their GCD.