HW 9 CMSC 389. DUE Jan 22- YES THURSDAY. THIS HW IS TWO PAGES

1. (0 points) Staple HW, put name, Read all notes—Thu is rev for final

2. (0 points but you need to do this for the next two problems) (READ the entire question first and the next one also.) In this problem you will be guided to how to write a program for Pollard's algorithm (the version which stores all of the triples).

   Throughout this there are two parameters p a prime and g a generator of $\{1, \ldots, p-1\}$.

   (a) Write code that will, given numbers a, b computer $a^b \pmod{p}$ using repeated squaring.

   (b) Write code that will, given a number $a \in \{1, \ldots, p-1\}$, determine if it is relatively prime to $p-1$, and if it is then find its inverse mod $p-1$.

   (c) Write code for a data structure D that will store triples (c, d, z) (all numbers between 1 and $p-1$) and support the following two functions.

   - FIND: Given (c, d, z) determine if there is already a triple $(c', d'z)$ in D such that $c - c' \neq 0$ and $c - c'$ is relatively prime to $p-1$.
   - INSERT: Given (c, d, z) insert it into D.

   (Advice: You can use a hash package from the language you use.)

   (d) Write code that will, given y, generate triples $(c, d, y^c g^d)$ randomly, (NOTE- use repeated squaring algorithm to compute y^c and g^d) insert them into the Data Structure until triples (c, d, z) and (c', d', z) are found so that $c - c'$ is rel prime to $p-1$. Have the program keep track of many triples it had to generate before it found what it wanted.

   (e) Write code that will, given (c, d) and (c', d') such that $y^c g^d = y^{c'} g^{d'}$ and $c - c'$ is rel prime to $p-1$, output $(c-c')^{-1}(d'-d)$ (all operations, including the inverse, are mod $p-1$).

   (f) Use all of the code you've written above to write a program that will, given y, find the discrete log of y (mod p with generator g).

3. (30 points) For this problem $p = 1009$ and $g = 17$. Use your program to determine the the discrete log of the following numbers: $10, 20, \ldots, 1000$. ALSO output how many random triples had to be generated before the program found what it wanted. Find e_1 and e_2 such that the number of iterations was always between $e_1\sqrt{1009}$ and $c_2\sqrt{1009}$.

4. (30 points) For this problem $p = 10007$ and $g = 63$. $100, 200, \ldots, 10000$. Use your program to determine the the discrete log of the following numbers: ALSO output how many random triples had to be generated before the program found what it wanted. Find e_1 and e_2 such that the number of iterations was always between $e_1\sqrt{10007}$ and $c_2\sqrt{10007}$.

5. (30 points) Try your program on primes that are around 20000, around 30000, etc until its slows down. (If it takes more than 5 minutes shut it off). Around what prime does it take 1 minute? 2 minutes? 3 minutes? 4 minutes? 5 minutes?