HW 8 CMSC 389. DUE Jan 20

(YES- this is due on THURSDAY)
NOTE- THIS HW IS TWO PAGES.

1. (0 points) READ my NOTES on line on POLLARD ALGORITHM ALSO READ my NOTES on line about FINDING INVERSES. ALSO STUDY FOR THE FINAL- Thursday will be REVIEW. What is your name? Write it clearly.

2. (25 points) (READ the entire question first.) Write a program that will simulate picking s numbers out of $\{1, \ldots, p\}$ and determine if two of them were the same.

   (a) Let $p = 1000$. For $s = 10, 20, 30, \ldots, 100$ simulate the program 10,000 times. In how many of those simulations did you get at least one number repeated? In how many did you not? what fraction of the time were two numbers the same? If for $s = 10x$ the fraction is LESS THAN 1/2 and for $s = 10(x+1)$ the fraction is MORE THAN 1/2 then do the experiment for $s+1, \ldots, s+9$. Our goal is to pin down when the percent goes over 1/2. (So hand in a CLEARLY READABLE table of data.)

   (b) For $p = 2000, 3000, \ldots, 10000$ do the same. Make a conjecture about exactly when the fraction goes over 1/2.

   (c) What data structure did you use to store the numbers?

3. (25 points) (READ my notes, or some other source, on finding the inverse of a number mod p.) Explain how to find the inverse of a number mod p. Use the method for the following problems.

   (a) Find the inverse of 36 mod 101.

   (b) Find the inverse of 36 mod 1001.

   (c) Find the inverse of 36 mod 10001. (10001 is not a prime but this is NOT a problem- 36 DOES have an inverse. Why is this?)

4. (25 points) In class we showed that if n is prime then $a^n \equiv a \pmod{n}$.

   (a) Find 3 numbers $a \in \{0, \ldots, 14\}$ such that $a^{15} \not\equiv a \pmod{15}$.

   (b) Find an x such that, for all $a \in \{0, \ldots, 14\}$, $a^x \equiv a \pmod{15}$. (TWO WAYS TO DO THIS: either try ALL possible x (use a program for that) OR look on the web for theorems about this. If you do that, state the theorem you use carefully and use it.)

   (c) Find an x such that, for all $a \in \{0, \ldots, 1926\}$, $a^x \equiv a \pmod{1926}$. Your answer should be a DESCRIPTION of the set- DO NOT list out all of the elements. (This one you HAVE to do using Math you find on the web.)

5. (25 points) Compute the following. Show all work (if you were in class then you know a short cut to use along with repeated squaring.)

   (a) $7^{1,000,000,000,000,000} \pmod{107}$

   (b) $7^{1,000,000,000,000,000} \pmod{10007}$