Homework Assignment 2
Due Wednesday October 9

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2002**

Instructions: *Please work with others,* and acknowledge who you work with in your write up. Some of these problems will require a computer; others look like a computer might be helpful, but in fact it isn't. If you use a computer, please describe how you use the computer (you are *not* required to use MAGMA).

1. (3 points) What is the largest order of an element of $(\mathbb{Z}/(2^{13466917}-1))^{\times}$? You may assume that the Mersenne number $2^{13466917}-1$ is prime.

2. (4 points) You and Nikita wish to agree on a secret key using the Diffie-Hellman protocol. Nikita announces that $p = 3793$ and $g = 7$. Nikita secretely chooses a number $n < p$ and tells you that $g^n \equiv 454 \pmod{p}$. You choose the random number $m = 1208$. What is the secret key?

3. (5 point) You see Michael and Nikita agree on a secret key using the Diffie-Hellman key exchange protocol. Michael and Nikita choose $p = 5003$ and $g = 2$. Nikita chooses a random number n and tells Michael that $g^n \equiv 3003 \pmod{p}$, and Michael chooses a random number m and tells Nikita that $g^m \equiv 2683 \pmod{p}$. Crack their code by brute force: What is the secret key that Nikita and Michael agree upon? What is n? What is m?

4. (9 points) Let p be any prime.

   (a) Prove that there is a primitive root modulo p^2. [Hint: Write down an element of $(\mathbb{Z}/p^2)^{\times}$ that looks like it might have order p, and prove that it does. Recall that if a, b have orders n, m, with $\gcd(n,m) = 1$, then ab has order nm.]

   (b) Suppose now that p is odd. Prove that for any n, there is a primitive root modulo p^n.

   (c) Why did your proof in part (b) not work when $p = 2$?

5. (8 points) Prove that there are infinitely many primes of the form $4x + 1$ as follows. Suppose $p_1, \ldots, p_n$ are all primes of the form $4x + 1$. Let

   $$a = 4(p_1p_2\cdots p_n)^2 + 1.$$

   Suppose p is a prime divisor of a.

   (a) Show that $p \neq p_i$ for any i and that p is odd.

   (b) Prove that the equation $x^2 + 1 = 0$ has a solution in $\mathbb{Z}/p$.

   (c) Deduce that $p \equiv 1 \pmod{4}$.

   (d) Conclude that there are infinitely many primes of the form $4x + 1$.

6. (6 points) In class I asserted that the Riemann Hypothesis is equivalent to the assertion that for all $x \geq 2.01$,

   $$|\pi(x) - \mathrm{Li}(x)| \leq \sqrt{x}\mathrm{Log}(x).$$

   (a) Give numerical evidence for (or against?) this assertion. (I mean the asserted inequality, not the assertion that the inequality is equivalent to the Riemann Hypothesis.)

   (b) What goes wrong for $0 < x < 2.01$?