Midterm:

Elementary Number Theory

Math 414, Winter 2010, University of Washington

Due Wednesday, February 17, 2010

Rules: Do not communicate with other *people* about the contents of this exam. You may use your notes, computer, Sage, books, etc., though please cite sources you use to solve problems.

The first three problems are "theoretical" problems (they are all also exercises in the textbook). The other problems are computational problems.

1. Prove that no integer in the sequence $11, 111, 1111, 11111, \ldots$, is a perfect square.

2. Prove that $(\mathbb{Z}/2^n\mathbb{Z})^*$ is generated by -1 and 5.

3. Prove that for any $n \in \mathbb{Z}$, the integer $n^2 + n + 1$ does not have any divisors of the form $6k - 1$. [Hint: you can find an extensive hint in the course textbook since this is exercise 4.10.]

4. You and I wish to agree on a secret key using the Diffie-Hellman key exchange. I announce that $p = 2^{31} - 1$ and $g \equiv 7 \pmod{p}$. I choose a number n and state that $g^n \equiv 833287206$. You choose the random number $m = 9392$.

   (a) What is the secret key that we agree on?

   (b) What secret number n did I choose? (Hint: Sage has a command `discrete_log` which may be useful.)

5. What are the last 3 digits of $2011^{2008^{2010}}$?

6. Is $2^{997} - 1$ a perfect square modulo $p = 2^{1279} - 1$?