Math 480 (Spring 2007): Homework 4

Due: Monday, April 23

There are 5 problems. Each problem is worth 6 points and parts of multipart problems are worth equal amounts. You may work with other people and use a computer, unless otherwise stated. Acknowledge those who help you.

1. (Work by hand alone on this.) Find all *four* solutions x with $0 \leq x < 55$ to the equation
$$x^2 - 1 \equiv 0 \pmod{55}.$$

2. (Work by hand alone on this.) How many solutions (with $0 \leq x < 15015$) are there to the equation
$$x^2 - 1 \equiv \pmod{15015}.$$
You may use that $15105 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$.

3. Find the first prime $p > 19$ such that the smallest primitive root modulo p is 19. (This requires a computer.)

4. You and Nikita wish to agree on a secret key using the Diffie-Hellman key exchange. Nikita announces that $p = 3793$ and $g = 7$. Nikita secretly 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?

5. In this problem you will digitally sign the number 2007. The grader will verify your digital signature.
   (a) Choose primes p and q with 5 digits each, but do not write them down on your homework assignment. Instead, write down $n = pq$. (Your answer to this problem is n. The grader will factor n using a computer and verify that indeed $n = pq$ with p,q both prime.)
   (b) Let $e = 3$. Compute the decryption key d such that $ed \equiv 1 \pmod{\varphi(n)}$. Do not write down d. Instead encrypt the number 2007 using (d, n), i.e., digitally sign 2007. Your answer is the number m modulo n. (The grader will encrypt m using your public key $(3, n)$; if the grader gets 2007 as the encryption, you get full credit; otherwise no credit.)