FINAL EXAM – 12/19/06

Math 406

Instructor: T. Haines

Name:

Answer all problems in the exam books provided. Clearly label your work on each problem with the corresponding number (and letter). If solving problems out of numerical order, indicate this prominently. Give clear and complete explanations (proofs should contain words explaining what you are doing, not just an assortment of numbers or symbols!). Calculators are permitted.

Good luck!

1. (a) [6 points] Write $\gcd(93, 39)$ as a linear combination of 93 and 39.

   (b) [4 points] Find all solutions to the congruence equation $39x \equiv 6 \pmod{93}$.

2. (a) [6 points] Find the least positive residue of $3^{114} \pmod{40}$.

   (b) [4 points] Use the answer to (a) to find the last two digits of $3^{(3^{114})}$.

3. [13 points] Find the smallest positive number which is a multiple of 11 and leaves a remainder of 1 when divided by 5 and a remainder of 1 when divided by 7.

4. (a) [5 points] Find $\mathrm{ord}_{19}\, 2$. Explain your reasoning.

   (b) [5 points] How many primitive roots modulo 19 are there?

   (c) [5 points] List all the primitive roots modulo 19 (express each as a least positive residue modulo 19).

   (d) [5 points] Find all solutions (if any) to the equation $x^9 \equiv 8 \pmod{19}$. Explain your reasoning.

5. [7 points] Can 2006 be expressed as the sum of the squares of two integers? Explain your answer.

6. [15 points] Is there a solution to the congruence equation $x^2 \equiv -222 \pmod{991}$? Note: 991 is prime.

7. [15 points] Consider the RSA encryption scheme using the key $(e, n) = (27, 187)$. Find the decryption transformation.

8. [10 points] *This problem is an application of quadratic reciprocity which proves that there are infinitely many primes of the form* $8k - 1$. Prove that for any integer $n > 1$, there is a prime of the form $8k-1$ which is bigger than n. HINT: Consider the number $8(n!)^2-1 = Q$. Show first that for any prime divisor p of Q, we have $\left(\frac{2}{p}\right) = 1$. Think about what forms such p can have.

9. [HOLIDAY BONUS PROBLEM –DO AT HOME OVER EGGNOG, or turn in now for 10 EXTRA CREDIT POINTS] Let p, q be odd primes such that $q = 4p + 1$. Show that 2 is a primitive root modulo q.