Math F490: Final Exam **Due: 4:00pm May 11, 2006**

Rules and format:

1. You are welcome to discuss this exam with me (David Maxwell) to ask for hints and so forth.
2. You my not discuss the exam with anyone else until after the due date/time.
3. You are permitted to use Burns and any other texts you like. If you use another text, you must cite it when you use it.
4. Each problem is weighted equally.
5. The due date/time is absolutely firm.
6. There will be a hints session held during finals week at a time to be arranged later.

1. Suppose $\gcd(a, n) = 1$. Without resorting to an argument using prime factorization, prove that if $n \mid ab$, then $n \mid b$.

2. Find the remainder of 5^{3476} when divided by 19.

3. Let a and b be integers with $\gcd(a, b) = 1$. Suppose x_0 and y_0 are a solution of

$$ax_0 + by_0 = 1.$$

Prove that the complete set of solutions of the equation

$$ax + by = 1$$

are given by

$$\begin{aligned} x &= x_0 + kb \\ y &= y_0 - ka \end{aligned}$$

where k is an arbitrary integer.

4. For each of the following equations, determine if an (integer) solution exists. If a solution exists, make a complete list of all such solutions.

a. $39x + 12y = 7$.

b. $343x + 259y = 658$.

5. Let n be a positive integer with $n > 1$. Prove that M_n is a group under multiplication.

6. Compute $\phi(22568)$.

7. Determine the remainder of $1234^{5678} + 5678^{1234}$ upon division by 12. (Careful: 12 is not prime).

8. An RSA message has been sent with encryption key $e = 197$ and $n = 6887$. The encrypted message was 5647. Determine the original message.

9. Determine if there exists a solution of $4x^2 + 28x + 9 = 0$ modulo 131. You do not need to find a solution (if one exists). *Hint:* Complete the square, and use your knowledge of quadratic residues.

10. Use the law of quadratic reciprocity to determine if 219 a quadratic residue modulo 383.

11.

a Exhibit that 13 and 17 can be written as a sum of squares.

b Determine which of the following integers can be written as a sum of squares. For those that can, use your answer from part a, and problem 6.15, to write the integer as a sum of squares.

- 221
- 663
- 1989

12. Show that there is no Pythagorean triple (a, b, c) with $c = 2b$. Conclude that $\sqrt{3}$ is irrational. *Hint:* If $4 \mid a^2 + b^2$, what can be said about the parity of a and b?

13. Complete the proof by induction from problem 7.28.