Math 432/537 Homework #2

due Friday, October 4, 2002 at the beginning of class

For the computational problems (I–V(a) and VI#7), you don't have to show every step of your calculations, but I do want to see enough details to tell that you are finding the answer in an "intelligent" way (that is, a way that would work even if the numbers were larger) rather than brute force or guessing.

I. For each of the numbers 1816, 1817, and 1818, find a representation as the sum of two squares or explain why no such representation exists.

II. Find the last three digits of the integer $987^{(1203^{321})}$. (Hint: Euler's Theorem. Believe it or not, this one can be done by hand!)

III. (a) Which integers x satisfy all of the congruences $x \equiv 3 \pmod{14}$, $x \equiv 5 \pmod{15}$, and $x \equiv 7 \pmod{17}$ simultaneously?

(b) Find the smallest positive integer n such that $2n \equiv 3 \pmod{5}$, $3n \equiv 4 \pmod{7}$, $4n \equiv 5 \pmod{9}$, and $5n \equiv 6 \pmod{11}$. Hint: there's a painless way.

IV. Prove that there are 15 residue classes modulo 703 that contain every integer of the form $x^{18} + y^{18}$. (Hint: $703 = 37 \times 19$.) State a generalization of this assertion and sketch a proof.

V. (a) Find all solutions to each of the congruences $76x \equiv 90 \pmod{105}$, $77x \equiv 91 \pmod{105}$, $78x \equiv 92 \pmod{105}$. Find all lattice points on the line $77x - 105y = 91$.

(b) Let S be a set consisting of 13 consecutive lattice points on the line from part (a). Show that 12 of the points in S have the property that the line segments joining them to the origin contain no lattice points other than their endpoints. Show that the line segment joining the (lucky) 13th lattice point in S to the origin contains 14 lattice points including its endpoints. (Hint: what does the greatest common divisor of x and y have to do with the line segments joining the lattice point (x, y) to the origin?)

VI. Niven, Zuckerman, and Montgomery, Section 2.6, p. 91, #7 and #10

VII. Niven, Zuckerman, and Montgomery, Section 2.8, pp. 107–108, #26 and #30

VIII. Recall that we gave an argument in class that every prime divides some number of the form $n! + 1$. Prove that every prime number greater than 3 also divides some number of the form $n! - 1$ with $n \geq 2$.

IX. If p is a prime, how many solutions are there to the congruence $x^4 - x^3 + x^2 - x + 1 \equiv 0 \pmod{p}$? The answer should only depend on the last digit of p. (Hint: factor the polynomial $x^{10} - 1$.)

X. Let $\{a_1, \ldots, a_{\phi(m)}\}$ be a reduced residue system modulo m, and set $A = a_1 \times \cdots \times a_{\phi(m)}$.

(a) Suppose that m is a power of an odd prime. Prove that $A \equiv -1 \pmod{m}$. (Hint: Wilson wouldn't have been able to solve this one.)

(b) What is A congruent to modulo m, if m is a power of 2? (Hint: Corollary 2.44.)

(c) Determine what A is congruent to modulo m, with no restriction on m. (You will still receive almost full credit if you solve this part assuming that m is odd, and/or that m is square-free, for instance.)