Math 437/537 Homework #2

due Friday, September 26, 2008 at the beginning of class

For all of these problems, show all of your calculations; do not use brute-force or exhaustive approaches, and do not use a computer (although using a calculator for arithmetic is fine). Note: the symbol (H) next to a problem in Niven, Zuckerman, and Montgomery means that there is a hint in the back of the book.

I. A *squarefree number* is an integer that is not divisible by any nontrivial square; that is, $n \in \mathbb{Z}$ is squarefree if and only if $d^2 \mid n$ implies $d = \pm 1$. Prove that there are arbitrarily large gaps between consecutive squarefree numbers. (Hint: Chinese Remainder Theorem.)

II. (a) Find all solutions to each of the following congruences (individually):

$$76x \equiv 90 \pmod{105}; \quad 77x \equiv 91 \pmod{105}; \quad 78x \equiv 92 \pmod{105}.$$

(b) Find all lattice points on the line $77x - 105y = 91$. Which of these lattice points have the property that the line segment connecting them to the origin contains other lattice points?

III. For any positive integer k, define

$$f_k(x) = k! \sum_{j=0}^{k} \frac{x^j}{j!} = x^k + kx^{k-1} + k(k-1)x^{k-2} + \cdots + k!x + k!.$$

Prove that f_k has a singular root (mod p) if $p \le k$ but no singular roots (mod p) if $p > k$.

IV. Using Hensel's Lemma, find all solutions to the congruence $x^4+x^3+2x^2+x \equiv 13 \pmod{7^3}$; show your work. (You may use trial and error to find all solutions to the congruence (mod 7).)

V. (a) 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 $x^{10} - 1$.)

(b) How many solutions are there to the congruence

$$x^4 - x^3 + x^2 - x + 1 \equiv 0 \text{ (mod 2,269,355)?}$$

VI. Prove that every integer of the form $x^{18} + y^{18}$ lies in one of 15 residue classes modulo 703.

VII. Let a, b, and m be integers with $m \ne 0$ and $(a, m) = (b, m) = 1$. Let r denote the order of a (mod m), let s denote the order of b (mod m), and let t denote the order of ab (mod m). Prove that

$$\frac{rs}{(r,s)^2} \mid t \quad \text{and} \quad t \mid \frac{rs}{(r,s)}.$$

VIII. Suppose that for some integer a, we have $a^{n-1} \equiv 1 \pmod{n}$ while $a^{(n-1)/p} \not\equiv 1 \pmod{n}$ for every prime p dividing $n-1$. Show that n is prime.

(continued on next page)

IX. (a) Niven, Zuckerman, and Montgomery, Section 2.8, p. 107, #18
(b) Niven, Zuckerman, and Montgomery, Section 2.8, p. 109, #37

X. Niven, Zuckerman, and Montgomery, Section 2.8, p. 107, #26

XI. Find all Carmichael numbers of the form $3pq$ where p and q are prime.

XII. Niven, Zuckerman, and Montgomery, Section 2.8, p. 108, #32