Math 437/537 Homework #2

due Friday, October 3, 2003 at the beginning of class

This homework is typical for this course, in that it is not short and the problems are (for the most part) not trivial. Start thinking about them early on, and if you've thought about a problem for a while but are still stuck, ask me for a hint. Several hints are pretty ubiquitous, so consider first whether any of the following will help with your problem-stuck-on *du jour*:

> Chinese Remainder Theorem; clever factorizations of polynomials; Euler's Theorem; Hensel's Lemma; induction.

I. Let a and k be integers greater than 1.
   (a) Suppose that $a^k - 1$ is prime. Prove that $a = 2$ and that k is prime.
   (b) Suppose that $a^k + 1$ is prime. Prove that a is even and that k is a power of 2.

II. Niven, Zuckerman, and Montgomery, Section 2.5, p. 86, #5

III. Niven, Zuckerman, and Montgomery, Section 2.8, p. 108, #30

IV. Let a, b, and m be integers with $m \neq 0$ and $(a,m) = (b,m) = 1$. Then the orders of a, b, and ab modulo m are all well-defined; let them be denoted by h, k, and ℓ, respectively. Prove that

$$\frac{hk}{(h,k)^2} \mid \ell \quad \text{and} \quad \ell \mid \frac{hk}{(h,k)}.$$

V. (a) Let $k \geq 0$ be a fixed integer and p a fixed prime. Find, with proof, a formula for the number of solutions of the congruence $x^k \equiv 1 \pmod{p}$ in terms of k and p. Do not use any results from Niven, Zuckerman, and Montgomery past page 99. [Note: the restriction $k \geq 0$ is not really necessary, as long as we interpret x^{-k} as $\bar{x}^k$.]
   (b) Let a be an integer and p a prime. Let $f(x)$ and $g(x)$ be polynomials with integer coefficients, and set $h(x) = f(x)g(x)$. Suppose that a is a root of f modulo p but not a root of h' modulo p. Prove that a is not a root of f' modulo p.
   (c) Let p be a prime and k a positive integer. How many solutions are there to the congruence

$$x^4 - x^3 + x^2 - x + 1 \equiv 0 \pmod{p^k}?$$

   [Remark: the polynomials $x^n - 1$ for $n \mid 10$ seem relevant.]
   (d) How many solutions are there to the congruence

$$x^4 - x^3 + x^2 - x + 1 \equiv 0 \pmod{2{,}269{,}355}?$$

(continued on back of page)

VI. Consider the sequence 2, 2^2, 2^{2^2}, $2^{2^{2^2}}$, ... (In other words, this is the sequence $\{x_k\}$ defined recursively by $x_1 = 2$ and $x_{k+1} = 2^{x_k}$ for $k \geq 1$.) Prove that for any positive integer m, this sequence is eventually constant modulo m.

VII. Prove the formula

$$\sum_{d|n} \phi(d) = n$$

by writing n in terms of its prime-power factorization, using the known formula for the Euler phi-function on a factored argument, and manipulating the resulting sums and products (i.e., "Proof 1" from class). At some point you will switch the order of sums and products; justify the correctness of this step explicitly.

VIII. Define $g(x) = (x^2 - 2)(x^2 - 17)(x^2 - 34)$. Prove that for every integer m, the congruence $g(x) \equiv 0 \pmod{m}$ has a solution. [Remark: it is obvious that $g(x) = 0$ has a solution in the reals but no solution in the rational numbers. Therefore $g(x)$ is an example of a polynomial that has "local" solutions everywhere, in the sense alluded to in the lecture on p-adic numbers, but no "global" solutions.]

IX. Do *one* of the following two problems, one of which involves some knowledge from abstract algebra, the other of which involves a technique from real analysis. (You may do both for extra credit if you wish.)

- Prove that every finite abelian group can be found inside some multiplicative group $\mathbb{Z}_m^\times$. In other words, for every finite abelian group G, prove that there exists a positive integer m such that there is an injective group homomorphism from G into $\mathbb{Z}_m^\times$. [Hint: structure theorem.]
- Fix a prime p and a polynomial $f(x)$ with integer coefficients. Suppose that the congruence $f(x) \equiv 0 \pmod{p^k}$ has a solution for every $k \geq 1$. Prove that $f(x)$ has a root in the p-adic integers. [Recall that every p-adic integer can be represented uniquely in the form

  $$y = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \dots,$$

  where $0 \leq a_j < p$ for each $j \geq 0$. Any such p-adic integer can be considered modulo p^k by truncation: $y \equiv a_0 + a_1 p + \dots + a_{k-1} p^{k-1} \pmod{p^k}$. Two quantities in the p-adic integers are equal if and only if they are congruent modulo p^k for every $k \geq 1$.]