Math 437/537 Homework #1

due Friday, September 19, 2003 at the beginning of class

Homework policies: You are permitted to consult one another concerning the homework assignments, but your submitted solutions must be written by you in your own words. I will consider not only correctness but also clarity when evaluating your work. You should attempt all of the problems, but if you consistently solve 75% of the homework problems correctly or with only minor errors, you will earn at least an A– for your homework mark. Endeavor to understand later how to solve any problems you omit.

I. Calculate $(3724, 817)$ and the least common multiple $[3724, 817]$. Find integers x and y such that $3724x + 817y = (3724, 817)$. (Do this problem by hand, showing your work.)

II. For this problem, use only the material up to Section 1.2 in your proof. (In particular, don't use the notion of a prime!)

(a) Suppose that a, b, and d are integers with $d \mid ab$. Prove that there are integers e and f with $e \mid a$ and $f \mid b$ such that $d = ef$.

(b) If we add the assumption in part (a) that $(a, b) = 1$, prove that the integers e and f are unique up to sign. Show by example that without the added assumption, this uniqueness can fail.

(c) Prove that $(ab, m) \mid (a, m)(b, m)$ for any integers a, b, and m (for which all three greatest common divisors are defined).

(d) If we add the assumption in part (c) that $(a, b) = 1$, prove that $(ab, m) = (a, m)(b, m)$. Show by example that without the added assumption, this equality can fail.

III. Niven, Zuckerman, and Montgomery, Section 1.3, p. 30–31, #19 and #26

IV. For any prime p and any nonzero integer m, let $v_p(m)$ be the power of p that appears in the prime power factorization of m (possibly 0), so that $m = \prod_{\text{primes } p} p^{v_p(m)}$.

Prove that

$$(m, n) = \prod_{\text{primes } p} p^{\min\{v_p(m), v_p(n)\}}.$$

V. Define $K(i, j)$ to be the $i + j$-digit number $K(i, j) = \underbrace{11\ldots11}_{i}\underbrace{00\ldots00}_{j}$. Prove that any nonzero integer m divides some integer of the form $K(i, j)$.

(continued on back of page)

VI. (a) Let p be an odd prime and r a positive integer. Let $\{a_1, \ldots, a_{\phi(p^r)}\}$ be a reduced residue system modulo p^r. Prove that $a_1 \times \cdots \times a_{\phi(p^r)} \equiv -1 \pmod{p^r}$.

(b) Let p be any prime and r a positive integer. Write $(p^r)! = kp^s$, where k and s are integers and $p \nmid k$. Determine (as functions of p and r) both s and the least nonnegative residue of $k \pmod{p}$. (The *least nonnegative residue* of $n \pmod{m}$ is the unique integer ℓ with $0 \leq \ell < m$ and $n \equiv \ell \pmod{m}$.)

VII. 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!)

VIII. Niven, Zuckerman, and Montgomery, Section 2.1, p. 57–59, #20, #27, and #48

IX. (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.