Math 437/537 Homework #1

due Friday, September 12, 2008 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.

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.

III. Niven, Zuckerman, and Montgomery, Section 1.3, p. 29, #13

IV. Niven, Zuckerman, and Montgomery, Section 1.3, p. 31, #26

V. Define $K(i, j)$ to be the $(i + j)$-digit number with decimal expansion

$$K(i, j) = \underbrace{11\dots11}_{i}\underbrace{00\dots00}_{j}.$$

Given a nonzero integer m, find positive integers $i(m)$ and $j(m)$ such that $m \mid K(i, j)$. Your recipe for finding $i(m)$ and $j(m)$ from m doesn't have to be simple, but it should be explicit, rather than a "there exist $i(m)$ and $j(m)$" argument.

VI. (a) Let p be an odd prime and r a positive integer. Let $\{a_1, \dots, a_{\phi(p^r)}\}$ 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, and set $s = (p^r - 1)/(p - 1)$. Prove that $(p^r)!$ is divisible by p^s and that $(p^r)!/p^s \equiv (-1)^r \pmod{p}$.

VII. Find the last four digits of the integer $1254^{(4003^{1601})}$. (Hint: How can you get around the fact that Euler's Theorem can't be immediately applied? Believe it or not, this problem can be done by hand!)

VIII. Niven, Zuckerman, and Montgomery, Section 2.1, p. 57, #14; do not use induction.

IX. Niven, Zuckerman, and Montgomery, Section 2.1, p. 57, #20; do not use induction.

X. Niven, Zuckerman, and Montgomery, Section 2.1, p. 57, #27; do not use induction.

XI. Niven, Zuckerman, and Montgomery, Section 2.1, p. 59, #54(b) (you should work through part (a), but you don't have to write it up)

(continued on next page)

XII. (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.