Math 210 Homework Assignment 2

DUE DATE: JAN. 24, 2008

1. For each of the following a's and b's, use the Euclidean algorithm to compute $d = \gcd(a, b)$, and use the extended algorithm to find numbers u and v such that $d = au+bv$.

(a) $a = 1001$, $b = 9471$.

(b) $a = 99958$, $b = 315905$.

(c) $a = 117$, $b = 325$.

2. Recall from class that $\gcd(a, b) = 1$ if and only if there are integers u, and v such that $au + bv = 1$.

(a) Find such a u and v for $a = 79$, $b = 323$.

(b) Suppose that $\gcd(a, b) = d$, and set $a_1 = \frac{a}{d}$ and $b_1 = \frac{b}{d}$. Since $d|a$ and $d|b$, the numbers a_1 and b_1 are both integers. Show that $\gcd(a_1, b_1) = 1$. (Try and find a solution that does not involve prime factorization).

(c) If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, prove or find a counterexample to the statement that $\gcd(ab, n) = 1$. (Again, you should be able to find an argument that does not involve prime factorization).

3. Suppose that a, b, and r are integers and that we have a relation $b = a \cdot q + r$. Suppose that we also have an equation of the form $e = ru_1 + av_1$ for some integers u_1 and v_1 (here e could be any number, not necessarily the gcd).

(a) Substitute the relation $b = a \cdot q + r$ into $e = ru_1 + av_1$ to find u_2 and v_2 so that $e = au_2 + bv_2$. What are the formulas for u_2 and v_2 in terms of u_1 and v_1?

(b) Find a 2×2 matrix M so that your formulas from (a) can be written in the form

$$\begin{bmatrix} u_2 \\ v_2 \end{bmatrix} = M \begin{bmatrix} u_1 \\ v_1 \end{bmatrix}.$$

(c) In question 1(c), the Euclidean algorithm should have taken four steps. Let q_1 be the number you used in the first step to compute division with remainder, and similarly q_2, q_3, and q_4 the numbers in the second, third, and fourth steps.

Multiply the matrices

$$\begin{bmatrix} -q_1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -q_2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -q_3 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -q_4 & 1 \\ 1 & 0 \end{bmatrix}.$$

(d) Compare the last column of your answer from (c) above with your answer from 1(c). Compare the first column of your answer from (c) with the numbers $\frac{a}{d}$ and $\frac{b}{d}$, where $a = 117$, $b = 325$, and $d = \gcd(a, b)$.

(e) Use your answers from (a) and (b) to explain what happened in (d).

NOTE: The practical importance of the computations in this question are: (1) the u and v in the relation $au+bv = \gcd(a, b)$ only depend on the sequence of numbers $q_1, \ldots, q_n$ in the Euclidean algorithm, and (2) since matrix multiplication can be done starting from either end, we can actually compute the u and v as we go forward through the algorithm, and not have to go back again. This is especially useful for very large numbers: once we're finished with each step, we can throw away the results of the previous step and just keep going.

4. Prove that for every positive integer n, $\gcd(n + 2, n^2 + 5n + 7) = 1$.

(NOTE: despite the phrase "for all positive integers n", you should *not* try and prove this by induction.)