SOLUTIONS TO MIDTERM I; MAT 312 (SPRING, 08)

Instructions: Complete 4 of the following 6 problems; at least one of the four problems you do should be a "proof" problem (i.e. #5,6). Be sure to show your work and give reasons for your answers.

(1)

(a) Compute (168,54,28).
(b) Compute lcm(168,54,28).

Solution: $168 = 2^3 \times 3 \times 7$, $54 = 2 \times 3^3$ and $28 = 2^2 \times 7$. Thus $(168, 54, 28) = 2$ and $lcm(168, 54, 28) = 2^3 \times 3^3 \times 7$.

(2)

(a) Compute $([3]_{88})^{-1}$.
Solution: The matrix

$$\begin{matrix} 1 & 0 & 3 \\ 0 & 1 & 88 \end{matrix}$$

is row equivalent to the matrix

$$\begin{matrix} 1 & 0 & 3 \\ -29 & 0 & 1, \end{matrix}$$

from which it follows that

$$3(-29) + 88(1) = 1.$$

Thus $[3]_{88}[-29]_{88} = [1]_{88}$, or $[3]_{88}^{-1} = [-29]_{88} = [59]_{88}$.

(b) Compute $([3]_{88})^{123}$.
Solution: $\phi(88) = \phi(2^3)\phi(11) = (8-4)(11-1) = 40$. So by by Euler's theorem $([3]_{88})^{40} = [1]_{88}$. Thus $([3]_{88})^{123} = (([3]_{88})^{40})^3([3]_{88})^3 = [27]_{88}$.

(3) Find one solution to the following simultaneous congruence equations:

$$x \equiv 4 \quad mod \quad 110$$
$$x \equiv 3 \quad mod \quad 63$$

.

Solution: Note that $110 = 2 \times 5 \times 11$ and $63 = 3^2 \times 7$ have no primes in common, so $110 \times \alpha + 63 \times \beta = 1$ for some integers α, β. So one solution to the congruence equations is $x = (3)(110)(\alpha) + (4)(63)(\beta)$.

Note that the matrix

$$\begin{matrix} 1 & 0 & 110 \\ 0 & 1 & 63 \end{matrix}$$

is row equivalent to the matrix

$$\begin{matrix} 3 & -5 & 15 \\ -4 & 7 & 1, \end{matrix}$$

from which we conclude that $\alpha = -4$ and $\beta = 7$. Thus $(3)(110)(-4) + (4)(63)(7)$ is one solution to the given simultaneous equivalence equations.

(4) Find all solutions to the following congruence equation:

$$35x \equiv 20 \quad mod \quad 130.$$

Solution: Divide this congruence by 5 to get

$$7x \equiv 4 \quad mod \quad 26.$$

$(7, 26) = 1$ so 7 is invertible mod 26. The matrix

$$\begin{matrix} 1 & 0 & 7 \\ 0 & 1 & 26 \end{matrix}$$

is row equivalent to the matrix

$$\begin{matrix} 4 & -1 & 2 \\ -11 & 3 & 1, \end{matrix}$$

from which it follows that

$$(7)(-11) + (26)(3) = 1.$$

Thus $([7]_{26})^{-1} = [-11]_{26} = [15]_{26}$, and the solution to $7x \equiv 4 \quad mod \quad 26$ is $[15]_{26}[4]_{26} = [8]_{26}$. It follows that $x = 8 + 26y, y = 0, 1, 2, 3, 4$ are the solutions to the original congruence equation (mod 130).

(5) Suppose that $b = aq+r$, where a, b, q, r are positive integers. Prove that $(a, b, r) = (a, b)$.

Solution: If a positive integer divides each of a, b, r then it divides each of a, b; thus (a, b, r) divides (a, b).

If a positive integer c divides each of a, b then $a = a'c$ and $b = b'c$, from which it follows that $r = b - aq = b'c - a'cq = c(b' - a'q)$. Thus if c divides a, b it also divides r; hence (a, b) divides (a, b, r).

(6) Prove that $[a]_n$ is a zero divisor (in $\mathbb{Z}_n$) iff every prime divisor of n is also a prime divisor of a.

Remark: This problem was incorrectly stated. Here is a counter example. Set $n = 6$, $a = 2$. Then 3 is a prime factor of 6 but is not a prime factor of 2. On the other hand $[2]_6[3]_6 = [0]_6$ and $[2]_6 \neq [0]_6 \neq [3]_6$, showing that $[2]_6$ is a divisor of zero.

What I meant to write down for problem (6) is the statement (i) below. Compare this with statements (ii) and (iii) below which we have proven in class.

(i) Suppose $[a]_n \neq [0]_n$. Then $([a]_n)^k = [0]_n$ holds for some positive integer k iff every prime divisor of n is also a divisor of a.

(ii) Suppose that $[a]_n \neq [0]_n$. Then $[a]_n$ is a zero divisor iff a,n have a prime factor in common.

(iii) Suppose that $[a]_n \neq [0]_n$. Then $[a]_n$ is invertible iff a,n have no prime factors in common.