Test 3, Math3336 **November 8, 2018**

You have the full class period to complete the test. You cannot use any books or notes. Every problem is worth 20 points.

1. Mark as true or false. $n,m,k,l \in \mathbb{Z}$

(**a**) $1|n$ T

(**b**) $0|n$ F

(**c**) If $n|k \cdot l$ then $n|k$ or $n|l$ F

(**d**) If $n|k$ and $n|l$ then $n|k+l$ T

2. Let a be an integer and d be a positive integer. Define the *Division Algorithm*, that is, the division of a by d with quotient q and remainder r. **Answer**: $a = qd + r, 0 \le r < d$

a. What is r if 200 is divided by 9? **Answer**: $200 -= 22 \cdot 9 + 2, r = 2$

b. What is r if 1000 is divided by 9? **Answer**: $1000 = 111 \cdot 9 + 1, r = 1$

c. What is q and what is r if 1 is divided by 2? **Answer**: $1 = 0 \cdot 2 + 1, q = 0, q = 0, r = 1$

d. What is q and what is r if n is divided by $n-1$? Answer: $n = 1 \cdot (n-1) + 1, q = 1, r = 1$

3. Let a and b be integers and let m be a positive integer. Define that a is congruent to b modulo m. What are the elements congruent to $0 \bmod m$? Prove that every integer a is congruent $\bmod m$ to a unique $0 \le r < m$. **Answer**: $a \equiv b \bmod (m)$ iff $m|a-b$ iff In $a = q_1 m + r_1 b = q_2 m + r_2$ one has that $r_1 = r_2$. we have that $a = qm + r$ where $a - r = qm$, thus $a - r$ is divisible by m Hence $a \equiv r \bmod (m)$ where $0 \le r < m$. If we had $a \equiv r$ and $a \equiv s$ where say $r > s$ and both $< m$ then $r - s < m$ and $0 \equiv r - s$ and therefore divisible by m. This is absurd. A number less that m cannot be divisible by m.

4. Evaluate these quantities. Your answer should be a congruence class $[x]_8$ where $0 \le x < 8$.

a. $[7]_8 + [7]_8$ **Answer**: $[7]_8 + [7]_8 = [14]_8 = [6]_{14}$

b. $[7]_8 \cdot [7]_8$ **Answer**: $[7]_8 \cdot [7]_8 = [49]_8 = [1]_8$

5. Convert the decimal expansion of each of these integers to a binary and ternary expansion.

a. 67 **Answer**: $67 = (1000011)_2, 67 = (2111)_3$

b. 85 **Answer**: $85 = (1010101)_{2,}, 85 = (100011)_3$

6. Express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

a. $2,7$ **Answer**: $(2,7) = (1), 1 = (-3) \cdot 2 + 1 \cdot 7$

b. $15,20$ **Answer**: $(15,20) = (5), 5 = 1 \cdot 20 - 1 \cdot 15$

c. $82,83$ **Answer**: $(82,83) = (1), 1 = 1 \cdot 83 - 1 \cdot 82$

d. $6,8$ **Answer**: $(6,8 = (2), 2 = 1 \cdot 8 - 1 \cdot 6$

7.

a. Prove that $\bmod n$ the class of $n-1$ has an inverse.
Find$[14]_{15}^{-1}$. **Answer**: $(n-1)(n-1) = n^2 - 2n + 1 = 1 \bmod n$, Thus $[n-1]_n^{-1} = [n-1]_n$. Thus $[14]_{15}^{-1} = [14]_{15}$

b. Solve $14x + 3 = 1 \bmod 15$ Answer:
$14x = -2, x = 14 \cdot (-2) = -28 = 2 \bmod 15$, check:
$14 \cdot 2 + 3 = 31 = 1 \bmod 15$

8. Let $[n,m]$ denote the least common multiple of n and m, and (n,m) denote the greatest common divisor. Prove that $[n,m] \cdot (n,m) = n \cdot m$ **Answer**:
$n = p_1^{n_1} \cdot p_2^{n_2} \cdot\cdot\cdot p_k^{n_k}, m = p_1^{m_1} \cdot p_2^{m_2} \cdot\cdot\cdot p_k^{m_k}, s_i = \min(n_i, m_i), t_i = \max(n_i, m_i)$ then $(n,m) = p_1^{s_1} \cdot p_2^{s_2} \cdot\cdot\cdot p_k^{s_k}, [n,m] = p_1^{t_1} \cdot p_2^{t_2} \cdot\cdot\cdot p_k^{t_k}$ and obviously
$[n,m] \cdot (n,m) = n \cdot m$.

9. Prove that 6 cannot have a multiplicative inverse $\bmod 12$. **Answer**:
$[6] \cdot [2] = [12] = [0]$, if $[6]$ had an inverse we could conclude that
$[2] = [0] \bmod 12$

10. Let m_1 and m_2 be relatively prime integers and that $b_1 m_1 + b_2 m_2 = 1$.

a. Prove that $b_1 m_1 \equiv 1 \bmod m_2$ and $b_2 m_2 \equiv 1 \bmod m_1$. **Answer**: $\bmod m_1$ we have that $b_2 m_2 = 0$, thus $b_2 m_2 \equiv 1 \bmod m_1$, similarly $\bmod m_2$ we have that $b_1 m_1 = 0$, thus $b_1 m_1 \equiv 1 \bmod m_2$,

b. $x \equiv a_1 \bmod m_1$ and $x \equiv a_2 \bmod m_2$ has $x = a_1 b_2 m_2 + a_2 b_1 m_1$ as a solution.
Answer:
$[x]_{m_1} = [a_1 b_2 m_2]_{m_1} = [a_1]_{m_1}[b_2 m_2]_{m_1} = [a_1], [x]_{m_2} = [a_2 b_1 m_1]_2 = [a_2]_2$

c. Find some x such that $x \equiv 2 \bmod 3$ and
$x \equiv 3 \bmod 7$. **Answer**:$1 = (-2) \cdot 3 + (1) \cdot 7, x = 2 \cdot 7 + 3 \cdot (-6) = -4$,

check: $-4 \equiv 2 \bmod 3, -6 \equiv 0 \bmod 3$, OK; $-4 \equiv 3 \bmod 7, -7 \equiv 0 \bmod 7$, OK