Test 3, Math3336 **November 7, 2017**

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**) $n|0$ T

(**b**) $0|1$ F

(**c**) If $n|k$ and $m|l$ then $n \cdot m|k \cdot l$ T

(**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 *Divison Algorithm*, that is, the division of a by d with quotient q and remainder r.
Answer: $a = qd + r, 0 \leq r < d$

a. What is r if 256 is divided by 9? **Answer**: $256 = 28 \cdot 9 + 4, r = 4$

b. What is r if 100 is divided by 9? **Answer**: $100 = 11 \cdot 9 + 1, r = 1$

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

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 $0 \leq r < m$. **Answer**: $a \equiv b \bmod m$ iff $m|a - b$. If $a = q_1 m + r_1, b = q_2 m + r_2$ then $a - b = (q_1 - q_2)m + (r_1 - r_2)$. We may assume that $0 \leq r_1 \leq r_2 < m$. Then $m|a - b$ iff $m|\ r_1 - r_2$ which is possible only if $r_1 = r_2$. We have that $a = q \cdot m + r, a - r = q \cdot m$ and therefore $a \equiv r \bmod m$.

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

a. $[5]_8 + [7]_8$ **Answer**: $[5]_8 + [7]_8 = [12]_8 = [4]_8$

b. $[5]_8 \cdot [7]_8$ **Answer**: $[5]_8 \cdot [7]_8 = [35]_8 = [3]_8$

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

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

b. 85 **Answer**: $85 = (1010101)_2 = (10011)_3$

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

a. $2, 5$ **Answer**: $1 = (-2) \cdot 2 + 1 \cdot 5$

b. $16, 18$ **Answer**: $2 = (-1) \cdot 16 + 1 \cdot 18$

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

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

7.

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

$[14]_{15}^{-1} = [14]_{15}$; also $1 = (-1) \cdot (n-1) + 1 \cdot n, [1]_n = [-1]_n \cdot [n-1]_n$,thus $[n-1]_n^{-1} = [-1]_n = [-1+n]_n = [n-1]_n$

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

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**:
$n = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}, m = p_1^{m_1} \cdot \ldots \cdot p_{k.}^{m_k}, [n,m] = p_1^{\max(n_1,m_1)} \cdot \ldots \cdot p_k^{\max(n_k,m_k)},$
$(n,m) = p_1^{\min(n_1,m_1)} \cdot \ldots \cdot p_k^{\min(n_k,m_k)}, n \cdot m = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k} \cdot p_1^{m_1} \cdot \ldots \cdot p_{k.}^{m_k} = p_1^{n_1+m_1} \cdot \ldots \cdot p_k^{n_k+m_k},$
but note $n_1 + m_1 = \min(n_1,m_1) + \max(n_1,m_1)\ldots.$

9. Prove that 8 cannot have a multiplicative inverse $\mod 12.$ **Answer**:
$[8]_{12} \cdot [9]_{12} = [0]_{12}$ where $[9]_{12} \neq [0]_{12}$. If 8 had an inverse $\mod 12$ then we would get $[8]_{12}^{-1} \cdot ([8]_{12} \cdot [9]_{12}) = [9]_{12} = [8]_{12}^{-1} \cdot [0]_{12} = [0]_{12}$ a contradiction.

10. Let m_1 and m_2 be relatively prime integers and that $b_1m_1 + b_2m_2 = 1.$

a. Prove that $b_1m_1 \equiv 1 \mod m_2$ and $b_2m_2 \equiv 1 \mod m_1$. **Answer**: We have that $b_2m_2 = 0 \mod m_2,$ and $b_1m_1 = 0 \mod m_1$

b. $x \equiv a_1 \mod m_1$ and $x \equiv a_2 \mod m_2$ has $x = a_1b_2m_2 + a_2b_1m_1$ as a solution. **Answer**: If $x = a_1b_2m_2 + a_2b_1m_1$ then $\mod m_1$ we get $x \equiv a_1b_2m_2 \equiv a_1$ because $b_2m_2 \equiv 1 \mod m_1$ and $a_2b_1m_1 \equiv 0 \mod m_1$ etc

c. Find some x such that $x \equiv 2 \mod 4$ and $x \equiv 3 \mod 5$. **Answer**:
$1 = (-1) \cdot 4 + 1 \cdot 5,$ so
$b_1 = -1, b_2 = 1, x = 2 \cdot 1 \cdot 5 + 3 \cdot (-1) \cdot 4 = 10 - 12 = -2.$ Check:
$-2 \equiv 2 \mod 4\surd, -2 \equiv 3 \mod 5\surd.$ we also have that
$x = (-2) \equiv (-2) + 4 \cdot 5 \equiv 18 \mod 4$ as well as $x = -2 \equiv 18 \mod 5$