Test 3, Math3336 October 29, 2019

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**) $n|0$ T

(**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: $a = qd + r, 0 \leq r < d$

a. What is r if 100 is divided by 9? $100 = 11 \cdot 9 + 1, r = 1$

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

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

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

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 $1 \bmod m$? **Answer**: $a \equiv b \bmod (m)$ iff $m|a-b$;$1 \equiv a \bmod m$ iff $a \in m\mathbb{Z} + 1$

4. Evaluate these quantities. Your answer should be a congruence class $[x]_9$ where $0 \leq x < 9$.

a. $[7]_9 + [7]_9 \quad [7]_9 + [7]_9 = [14]_9 = [5]_9$

b. $[7]_9 \cdot [7]_9 \quad [7]_9 \cdot [7]_9 = [49]_9 = [4]_9$

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

a. $66 = (0100001)_2, \quad 66 = (0112)_3$

b. $86 = (0110101)_2 \quad 86 = (21001)_3$

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

a. $2, 9 \quad (2,9) = 1 = (-1) \cdot 4 + 1 \cdot 9$

b. $15, 35 \quad (15, 35) = 5 = (-2) \cdot 15 + 1 \cdot 35$

c. $62, 63 \quad (62, 63) = 1 = (-1) \cdot 62 + 1 \cdot 63$

d. $6, 10 \quad (6, 10) = 2 = 2 \cdot 6 - 1 \cdot 10$

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 $4x + 3 = 1 \bmod 5$ Answer: $[4]_5^{-1} = [4], 4x = -2 = 3 \bmod 5, x = 12 = 2 \bmod 5$

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 8 cannot have a multiplicative inverse $\bmod 12$. **Answer**: $[6]_{12} \cdot [8]_{12} = [48]_{12} = [0]_{12}$ If $[8]_{12}$ had an inverse, then $[6]_{12} = [0]_{12}$

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 $b_2 m_2 \equiv 1 \bmod m_1$.
- **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.
- **c**. Find some x such that $x \equiv 2 \bmod 3$ and $x \equiv 3 \bmod 7$. **Answer**: $(3,7) = (1), 1 = (-2) \cdot 3 + 1 \cdot 7, x = 3 \cdot (-2) \cdot 3 + 2 \cdot 7 = -18 + 14 = -4$ check: $-4 \equiv 2 \bmod 3, -4 \equiv 3 \bmod 7$