Test 3, **Math3336** **March 29**, **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. Define for integers the relation $a|b$. **Answer**: $a \cdot c = b$ for some c

a. is there an integer a such that $a|n$ for every integer n?**Answer**: Yes, $a = 1$

b. Is there an integer b such that $n|b$ for every integer n?**Answer**: Yes, $b = 0$

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**: $256 = 28 \cdot 9 + 4$

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

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

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

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 $m|a - b$. $a \equiv 0 \bmod m$ iff $a \in m\mathbb{Z}$. We have $a = qm + r, 0 \leq r < m$ shows that $a \equiv r \bmod m$ for a unique r.

4. Evaluate these quantities. Your answer should be a congruence class $[x]_3$ where $0 \leq x < 3$.

a. $[1]_3 + [4]_3$ **Answer**: $[1]_3 + [4]_3 = [5]_3 = [2]_3$

b. $[5]_3 \cdot [7]_3$ **Answer**: $[5]_3 \cdot [7]_3 = [35]_3 = [2]_3$

c. $[2]_3^{-1}$ **Answer**: $[2]_3^{-1} = [2]_3$

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

a. 23 **Answer**: $23 = (10111)_2$
$23 = 11 \cdot 2 + 1, 11 = 5 \cdot 2 + 1, 5 = 2 \cdot 2 + 1, 2 = 1 \cdot 2 + 0, 1 = 0 \cdot 2 + 0 : 23 = (10111$

b. $23 = (212)_3$
$23 = 7 \cdot 3 + 2, 7 = 2 \cdot 3 + 1, 2 = 0 \cdot 3 + 2, 23 = (212)_3$

c. $59 = (111011)_2$
$59 = (2012)_3$
$29 \cdot 2 + 1, 29 = 14 \cdot 2 + 1, 7 = 3 \cdot 2 + 1, 3 = 1 \cdot 2 + 1, 1 = 0 \cdot 2 + 1, 59 = (111011)_2$;
$59 = 19 \cdot 3 + 2, 19 = 6 \cdot 3 + 1, 6 = 2 \cdot 3 + 0, 2 = 0 \cdot 3 + 2,$

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

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

b. $12, 18$ **Answer**: $(12, 18) = 6 = (-1) \cdot 12 + 1 \cdot 18$

c. $20, 32$ **Answer**: $(20, 32) = 4 = 2 \cdot 32 - 3 \cdot 20$:
$32 = 1 \cdot 20 + 12, 20 = 1 \cdot 12 + 8, 12 = 1 \cdot 8 + 4, 8 = 2 \cdot 4 + 0, (32, 12) = 4, 12 = 1 \cdot 32$
$1 \cdot 32, 4 = 12 - 8 = (1 \cdot 32 - 1 \cdot 20) - (2 \cdot 20 - 1 \cdot 32) = 2 \cdot 32 - 3 \cdot 20$

7.

a. What is $(n-1)(n-1) \bmod n$? **Answer**:
$(n-1)(n-1) = n^2 - 2n + 1 = 1 \bmod n$

b. Solve $3x + 3 = 1 \bmod 4$ **Answer**: $x = 2 \bmod 4$
$[3]_4^{-1} = [3]_4, x + [3][3] = [3], x + [9] = [3], x = [-6] = [2]_4$

8. Let p be a prime. Prove that every $1 \leq a < p$ has a multiplicative inverse $\bmod p$. **Answer**: Each such a is relatively prime to p. Therefore
$1 = c \cdot a + d \cdot p, [1]_p = [c]_p \cdot [a]_p, [a]_p^{-1} = [c]_p$

9. Prove that 10 cannot have a multiplicative inverse $\bmod 12$. **Answer**: 10 and 12 are not relatively prime. Also $[6]_{12} \cdot [10]_{12} = [60]_{12} = [0]_{12}$. If $[10]_{12}$ had a multiplicative inverse then $[6]_{12} = [0]_{12}$ which is not true.

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**:
$[b_1 m_1 + b_2 m_2]_{m_1} = [b_2 m_2]_{m_1} = [1]_{m_1}, [b_1 m_1 + b_2 m_2]_{m_2} = [b_1 m_1]_2 = [1]_{m_1}$. Which is the assertion.

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**: $[a_1 b_2 m_2 + a_2 b_1 m_1]_{m_1} = [a_1]_{m_1} [b_2 m_2]_{m_1} = [a_1]_{m_1}$ which is $x \equiv a_1 \bmod m_1$. Same argument for $x \equiv a_2 \bmod m_2$

c. Find some x such that $x \equiv 2 \bmod 8$ and $x \equiv 3 \bmod 9$. **Answer**: $x = -6$
$1 = (-1) \cdot 8 + 1 \cdot 9, x = 2 \cdot 1 \cdot 9 + 3 \cdot (-1) \cdot 8 = -6$