Test 3, **Math3336** **November** , **2016**

You have the full class period to complete the test. **Every problem is worth 20 points**.

1. Define for integers a and b the relation $a|b$. Then prove

(**a**) *if* $a|b$ *and* $a|c$ *then* $a|b+c$; **Answer**: $a|b$ iff $\exists u a \cdot u = b$. Assume $a|b$ and $a|c$. Then $a \cdot u = b, a \cdot v = c$ and $b + c = a \cdot (u+v)$. Thus $a|b+c$.

(**b**) *if* $a|b$ *and* $b|c$ *then* $a|c$. **Answer**: $a \cdot u = b, b \cdot v = c$. Thus $c = a \cdot (u \cdot v)$, i.e., $a|c$.

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**: $a = q \cdot d + r, 0 \leq r < d$.

a. What is q and what is r if 0 is divided by 1?
Answer: $\mathbf{0 = 0 \cdot 1 + 0; q = 0, r = 0}$.

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

c. Let $0 < a < d$. What is q and what is r if a is divided by d. **Answer**:
$a = 0 \cdot d + a; q = 0, r = a$

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

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 $0 \leq r < m$. A**nswer**: $a \equiv b \bmod m$ **iff** $m|a-b$ **iff** $a - b \in m\mathbb{Z} = \{mk | k \in \mathbb{Z}\}$ **iff in** $a = q_1 m + r_1, 0 \leq r_1 < m, b = q_2 m + r_2, 0 \leq r_2 < m$ **one has that** $r_1 = r_2$. **The elements of** $m\mathbb{Z}$ **are congruent to** $0 \bmod m$. **And** $a = qm + r$, **i.e.**, $a - r = qm \in m\mathbb{Z}$ **shows that** $a \equiv r$ **where** r **is the unique remainder for** a **if divided by** m

4. Evaluate these quantities.

a. $[12]_8 + [20]_8$ **Answer**: $[12]_8 + [20]_8 = [32]_8 = [0]_8$

b. $[12]_8 \cdot [20]_8$ **Answer**: $[12]_8 \cdot [20]_8 = [240]_8 = [0]_8$

5. Convert the decimal expansion of each of these integers to a binary and ternary expansion. You need to show your calculations.

a. 5 **Answer**: $5 = 2 \cdot 2 + 1, 2 = 1 \cdot 2 + 0, 1 = 0 \cdot 1 + 1; \mathbf{5 = (101)_2}$;
$5 = 1 \cdot 3 + 2, 1 = 0 \cdot 3 + 1; \mathbf{5 = (12)_3}$

b. 25 **Answer**:
$25 = 12 \cdot 2 + 1, 12 = 6 \cdot 2 + 0, 6 = 3 \cdot 2 + 0, 3 = 1 \cdot 2 + 1, 1 = 0 \cdot 2 + 1; \mathbf{25 = (11001}$
$25 = 8 \cdot 3 + 1, 8 = 2 \cdot 3 + 2, 2 = 0 \cdot 3 + 2; \mathbf{25 = (221)_3}$

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

a. $1, 6$ **Answer**: $\mathbf{1 = 1 \cdot 1 + 0 \cdot 6}$

b. $5, 7$ **Answer**: $\mathbf{1 = 3 \cdot 5 - 2 \cdot 7}$

c. $10, 12$ **Answer**: $\mathbf{2} = (\mathbf{-1}) \cdot \mathbf{10} + \mathbf{1} \cdot \mathbf{12}$

d. $12, 21$ **Answer**:
$21 = 1 \cdot 12 + 9, 12 = 1 \cdot 9 + 3, 9 = 3 \cdot 3 + 0, (12, 21) = (3);$
$9 = 1 \cdot 21 - 1 \cdot 12, 3 = 1 \cdot 12 - 1 \cdot 9 = 1 \cdot 12 - 1 \cdot (1 \cdot 21 - 1 \cdot 12) = 2 \cdot 12 - 1 \cdot 21$
$\mathbf{3} = \mathbf{2} \cdot \mathbf{12} - \mathbf{1} \cdot \mathbf{21}$

7. Find all invertible elements and their inverses in

a. $(\mathbb{Z}_{12}, \cdot)$. **Answer**: $[\mathbf{1}]^{-1} = [\mathbf{1}], [\mathbf{5}]^{-1} = [\mathbf{5}], [\mathbf{7}]^{-1} = [\mathbf{7}], [\mathbf{11}]^{-1} = [\mathbf{11}]$

b. $(\mathbb{Z}_{13}, \cdot)$. **Answer**: $[\mathbf{1}]^{-1} = [\mathbf{1}], [\mathbf{2}]^{-1} = [\mathbf{7}], [\mathbf{3}]^{-1} = [\mathbf{9}], [\mathbf{4}]^{-1} = [\mathbf{10}],$
$[\mathbf{5}]^{-1} = [\mathbf{8}], [\mathbf{6}]^{-1} = [\mathbf{11}], [\mathbf{7}]^{-1} = [\mathbf{2}], [\mathbf{8}]^{-1} = [\mathbf{5}], [\mathbf{9}]^{-1} = [\mathbf{3}], [\mathbf{10}]^{-1} = [\mathbf{4}], [\mathbf{11}]^{-1} = [\mathbf{6}]$

8. Solve $\bmod 13$ the linear equation $4x + 3 = 1$ **Answer**: $\mathbf{x} = [\mathbf{6}]_{13}$
$[\mathbf{4}]\mathbf{x} = [\mathbf{-2}] = [\mathbf{11}]. [\mathbf{4}]^{-1}[\mathbf{4}]\mathbf{x} = \mathbf{x} = [\mathbf{4}]^{-1} \cdot [\mathbf{11}] = [\mathbf{10}] \cdot [\mathbf{11}] = [\mathbf{110}] = [\mathbf{6}]$

9. Prove that 9 cannot have a multiplicative inverse $\bmod 12$. **Answer**:
$[9] \cdot [4] = [0],$ if we had a $[9]^{-1}$ then $[4] = [0]$ a contradiction.

10. Which integers are divisible by 5 but leave a remainder of 1 when dividedby 4? **Answer**: **We need to solve** $x \equiv 0 \bmod 5, x \equiv 1 \bmod 4;$ **simple inspection gives** $x = 5$ **as a solution** x **is unique up to** $\bmod 20$