Practice sheet for Math 3336 Fall 2016

October 24, **2016**

1. Define for integers a and b the relation $a|b$.
   Prove that $1|a$ and $a|0$. **Answer**: $a|b$ iff $\exists c\ a \cdot c = b$ We have $1|a$ because $1 \cdot a = a$ and $a|0$ because of $a \cdot 0 = 0$
2. 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? Prove that every integer a is congruent $\bmod m$ to a unique $0 \le r < m$. 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** $a = q_1m + r_1, 0 \le r_1 < m, b = q_2m + r_2, 0 \le r_2 < m$ **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
3. Evaluate these quantities.
   - **a.** $13 \bmod 3$ **Answer**: $13 = 4 \cdot 3 + 1$, **i.e.**, $13 \equiv 1 \bmod 3$
   - **b.** $-97 \bmod 11$ **Answer**: $-97 = (-9) \cdot 11 + 2$, **i.e.**, $-97 \equiv 2 \bmod 11$
   - **c.** $155 \bmod 19$ **Answer**: $155 = 8 \cdot 19 + 3$, **i.e.**, $155 \equiv 3 \bmod 19$
   - **d.** $-221 \bmod 23$ **Answer**: $-221 = (-10) \cdot 23 + 9$, **i.e.**, $-221 \equiv 9 \bmod 23$
4. Convert the decimal expansion of each of these integers to a binary expansion.
   - **a.** 22 **Answer**:
     $22 = 11 \cdot 2 + 0, 11 = 5 \cdot 2 + 1, 5 = 2 \cdot 2 + 1, 2 = 1 \cdot 2 + 0, 1 = 0 \cdot 2 + 1$, **i.e.**,
     $22 = (10110)_2$ **Check**:
     $0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 = 2 + 4 + 16 = 22$
   - **b.** 100 **Answer**:
     $100 = 50 \cdot 2 + 0, 50 = 25 \cdot 2 + 0, 25 = 6 \cdot 2 + 0, 6 = 3 \cdot 2 + 0, 3 = 1 \cdot 2 + 1, 1 = 0 \cdot 2$
   - **c.** 60 Answer:
     $60 = 30 \cdot 2 + 0, 30 = 15 \cdot 2 + 0, 15 = 7 \cdot 2 + 1, 7 = 3 \cdot 2 + 1, 3 = 1 \cdot 2 + 1, 1 = 0 \cdot 2 +$
     $60 = (111100)_2$
   - **d.** 9 **Answer**: $9 = 4 \cdot 2 + 1, 4 = 2 \cdot 2 + 0, 2 = 1 \cdot 2 + 0, 1 = 0 \cdot 2 + 1$, **i.e.**,
     $9 = 1001$
     Remember: **For expansion of** a **to base** b **you start with** $a = q \cdot b + a_0$ **and argue that you already know that** $q = a_1 + a_2b + \ldots + a_kb^{k-1}$, **therefore**, $a = a_1b + a_2b^2 + \ldots + a_kb^k + a_0$. **You successively divide the quotients by** b **to find the coefficients** $a_0, a_1, \ldots, a_k$.
5. Express the greatest common divisor of each of these pairs of integers as a combination of these integers.
   - **a.** $10, 11$ **Answer**: $11 = 1 \cdot 10 + 1, 10 = 10 \cdot 1 + 0$,
     $(11.10) = (10,1) = (1,0); 1 = 1 \cdot 11 - 1 \cdot 10$
   - **b.** $9, 16$ **Answer**:
     $16 = 1 \cdot 9 + 7, 9 = 1 \cdot 7 + 2, 7 = 3 \cdot 2 + 1, 2 = 2 \cdot 1 + 0, (16,9) = (9,7) = (7.2) = (2$
     $7 = 1 \cdot 16 - 1 \cdot 9, 2 = 1 \cdot 9 - 1 \cdot 7 = 1 \cdot 9 - 1 \cdot (1 \cdot 16 - 1 \cdot 9) = 2 \cdot 9 - 1 \cdot 16, 1 = 1$

$1 = 4 \cdot 16 - 7 \cdot 9$

c. $0, 20$ **Answer**: $20 = 1 \cdot 20 + 0$

d. $99, 101$ **Answer**:
$101 = 1 \cdot 99 + 2, 99 = 49 \cdot 2 + 1, 2 = 2 \cdot 1 + 0, (101, 99) = (99, 2) = (49, 1) = (1, 0)$

$2 = 1 \cdot 101 - 1 \cdot 99, 1 = 1 \cdot 99 - 49 \cdot 2 = 1 \cdot 99 - 49(1 \cdot 101 - 1 \cdot 49) = 50 \cdot 99 - 49$

6. Find all invertible elements and their inverses in

a. $(\mathbb{Z}_{10}, \cdot)$ **Answer**: **An element** $[a]$ **in** $\mathbb{Z}_{10}$ is invertible iff $(a, 10) = (1)$. The elements a that are relatively prime to 10 are $1, 3, 7, 9$ and we have $[1]^{-1} = [1], [3]^{-1} = [7], [7]^{-1} = [3], [9]^{-1} = [9]$

b. $(\mathbb{Z}_{11}, \cdot)$ **Answer**: Because 11 is prime, all numbers btween 1 and 10 are relativley prime to 11. We have $[1]^{-1} = [1], [2]^{-1} = [6], [3]^{-1} = [4], [4]^{-1} = [3], [5]^{-1} = [9], [6]^{-1} = [2], [7]^{-1} = [8], [8$

7. Solve $\bmod 5$ the linear equation $2x + 3 = 1$ **Answer**:
$2x = -2 = 3 \bmod 5, [2]^{-1} = [3]$. Thus $x = 9 = 4 \bmod 5$. Indeed, $2 \cdot 4 + 3 = 11 = 1 \bmod 5$

8. Which integers leave a remainder 1 when divided by 2 and also leave a remainder 1 when divided by 3. **Answer**: **Of course**, $x \equiv 1 \bmod 2, x \equiv 1 \bmod 3$ **has the solution** $x = 1$ **which**, **according to the Chinese Remainder Theorem is unique mod** $2 \cdot 3 = 6$.