UWO CS2214

Tutorial #6

Problem 1
1. Find all integers x such that $0 \leq x < 15$ and $4x + 9 \equiv 13 \mod 15$. Justify your answer.
2. Find all integers x and y such that $0 \leq x < 15$, $0 \leq y < 15$, $x + 2y \equiv 4 \mod 15$ and $3x - y \equiv 10 \mod 15$. Justify your answer.

Solution 1
1. We have $4 \times 4 \equiv 1 \mod 15$. That is, 4 is the inverse of 4 modulo 15. We multiply by 4 each side of:
$$4x + 9 \equiv 13 \mod 15,$$
leading to:
$$x + 4 \times 9 \equiv 4 \times 13 \mod 15,$$
that is:
$$x \equiv 4(13 - 9) \mod 15,$$
which finally yields: $x \equiv 1 \mod 15$.
2. We eliminate y in order to solve for x first. Multiplying
$$3x - y \equiv 10 \mod 15$$
by 2 yields
$$6x - 2y \equiv 5 \mod 15.$$
Adding this equation side-by-side with
$$x + 2y \equiv 4 \mod 15$$
yields
$$7x \equiv 9 \mod 15.$$
Since
$$7 \times 13 \equiv 1 \mod 15,$$
we have

$$x \equiv 9 \times 13 \mod 15,$$

that is,

$$x \equiv 12 \mod 15.$$

Substituting x with 12 into

$$3x - y \equiv 10 \mod 15$$

yields

$$y \equiv 11 \mod 15.$$

Problem 2 Let a, b, q, r be non-negative integer numbers such that $b > 0$ and we have

$$\begin{array}{c|c} a & b \\ \cline{2-2} r & q \end{array} \tag{1}$$

That is:

$$a = bq + r \text{ and } 0 \leq r < b.$$

Prove that we have:

$$q \;=\; \lfloor \frac{a}{b} \rfloor. \tag{2}$$

Solution 2 From $a = bq + r$ and $0 \leq r < b$ we derive

$$bq \leq bq + r < b(q + 1), \tag{3}$$

thus

$$bq \leq a < b(q + 1), \tag{4}$$

that is

$$q \leq a/b < q + 1, \tag{5}$$

which means:

$$q \;=\; \lfloor \frac{a}{b} \rfloor. \tag{6}$$

Problem 3 Let a, b, q_1, r_1, q_2, r_2 be non-negative integer numbers such that $b \neq 0$ and we have

$$\begin{array}{c|c} a & b \\ \cline{2-2} r_1 & q_1 \end{array} \quad \text{and} \quad \begin{array}{c|c} a & b \\ \cline{2-2} r_2 & q_2 \end{array}. \tag{7}$$

Thus we have: $a = bq_1 + r_1 = bq_2 + r_2$ as well as $0 \leq r_1 < b$ and $0 \leq r_2 < b$. Prove that $q_1 = q_2$ and $r_1 = r_2$ necessarily both hold

Solution 3 Let $a = bq_1 + r_1 = bq_2 + r_2$, with $0 \leq r_1 < b$ and $0 \leq r_2 < b$, where a, b, q_1, r_1, q_2, r_2 are non-negative integers. We wish to show that $q_1 = q_2$ and $r_1 = r_2$.

Assume that $r_1 \neq r_2$ holds. Then, without loss of generality, assume that $r_2 > r_1$ holds. We then have:

$$b(q_1 - q_2) = r_2 - r_1. \tag{8}$$

Since $0 \leq r_1 < b$ and $0 \leq r_2 < b$, and $r_2 > r_1$, it must be that

$$0 < (r_2 - r_1) < b, \tag{9}$$

since the largest difference has $r_2 = b-1$ and $r_1 = 0$, and $r_1 \neq r_2$ by assumption (so $r_2 - r_1 \neq 0$). But Equation (8) implies that b divides $r_2 - r_1$, which cannot be given Equation (9), because the multiples of b are $0, \pm b, \pm 2b, \ldots$. This is a contradiction, and we conclude that $r_1 = r_2$.

Since we have shown that $r = r_1 = r_2$ holds, it follows that

$$\Rightarrow b(q_1 - q_2) = 0. \tag{10}$$

Equation (10) implies that either $b = 0$ or $q_1 - q_2 = 0$ holds. Since we have $b \neq 0$ by assumption, we conclude that it must be that $q_1 - q_2 = 0$ holds, meaning that $q_1 = q_2$, which is what we set out to prove. QED

Problem 4 In the previous exercise, if a, b, q_1, q_2, are non-negative integer numbers satisfying $a = bq_1 + r_1 = bq_2 + r_2$ while r_1, r_2 are integers satisfying $-b < r_1 < b$ and $-b < r_2 < b$. Do we still reach the same conclusion? Justify your answer.

Solution 4 No, we do not. Indeed, with $a = 7$ and $b = 3$, we then have two possible divisions:

$$\begin{array}{r|l} 7 & 3 \\ \cline{2-2} 1 & 2 \end{array} \quad \text{and} \quad \begin{array}{r|l} 7 & 3 \\ \cline{2-2} -2 & 3 \end{array}.$$

Problem 5 Let a and b be integers, and let m be a positive integer. Then, the following properties are equivalent.

1. $a \equiv b \mod m$,
2. $a \ \mathbf{mod}\ m = b \ \mathbf{mod}\ m$.

Solution 5 Let q_a, r_a be the quotient and the remainder in the division of a by m. Similarly, let q_b, r_b be the quotient and the remainder in the division of b by m. Thus, we have:

$$\begin{array}{r|l} a & m \\ \cline{2-2} r_a & q_a \end{array} \quad \text{and} \quad \begin{array}{r|l} b & m \\ \cline{2-2} r_b & q_b \end{array}.$$

That is:

$$a = q_a m + r_a \quad \text{and} \quad 0 \leq r_a < m,$$

and

$$b = q_b m + r_b \quad \text{and} \quad 0 \leq r_b < m.$$

We now prove the desired equivalence.

1. We first assume that $a \equiv b \mod m$ holds and prove that $a \ \mathbf{mod}\ m = b \ \mathbf{mod}\ m$ holds as well. The assumption means that there exists an integer k such that we have $a - b = km$. It follows that

   $$a - b = km = (q_a - q_b)m + r_a - r_b.$$

   Thus:

   $$r_a - r_b = m(k - q_a + q_b).$$

   That is, m divides $r_a - r_b$. Meanwhile, $0 \leq r_a < m$ and $0 \leq r_b < m$ imply:

   $$-m < r_a - r_b < m.$$

   The only way $r_a - r_b$ could be a multiple of m while satisfying the above constraint is with $r_a - r_b = 0$. Therefore, we have proved $a \ \mathbf{mod}\ m = b \ \mathbf{mod}\ m$.

2. Conversely, assume that $a \ \mathbf{mod}\ m = b \ \mathbf{mod}\ m$ and let us $a \equiv b \mod m$ holds as well. This follows immediately from the equalities:

   $$a = q_a m + r_a \quad \text{and} \quad b = q_b m + r_b.$$

   Indeed, $r_a = r_b$ then implies $a - b = (q_a - q_b)m$.

Problem 6 Let a and b be integers, and let m be a positive integer. Prove the following properties

1. $a + b \ \mathbf{mod}\ m \ = \ (\ a \ \mathbf{mod}\ m\ ) + (\ b \ \mathbf{mod}\ m\ ) \ \mathbf{mod}\ m$,
2. $ab \ \mathbf{mod}\ m \ = \ (\ a \ \mathbf{mod}\ m\ ) \times (\ b \ \mathbf{mod}\ m\ ) \ \mathbf{mod}\ m$.

Solution 6

1. Let $q_a, r_a, q_b, r_b, q_{a+b}, r_{a+b}, q, r$ be integers such that

$$\begin{array}{r|l} a & m \\ \cline{2-2} r_a & q_a \end{array}, \quad \begin{array}{r|l} b & m \\ \cline{2-2} r_b & q_b \end{array}, \quad \begin{array}{r|c} a+b & m \\ \cline{2-2} r_{a+b} & q_{a+b} \end{array}, \quad \text{and} \quad \begin{array}{c|c} r_a + r_b & m \\ \cline{2-2} r & q \end{array}. \tag{11}$$

   We are asked to prove:

$$r_{a+b} \ = \ r \tag{12}$$

   From the hypotheses, we have:

$$\begin{array}{rcl} r_{a+b} & = & a + b - mq_{a+b} \\ & = & q_a m + r_a + q_b m + r_b - mq_{a+b} \\ & = & r_a + r_b + m(q_a + q_b - q_{a+b}) \\ & = & r + qm + m(q_a + q_b - q_{a+b}) \\ & = & r + m(q + q_a + q_b - q_{a+b}) \end{array} \tag{13}$$

   It follows that $r_{a+b} \equiv r \mod m$ holds, that is, m divides $r_{a+b} - r$. From the hypotheses, we also have:

$$0 \leq r_{a+b} < m \ \text{ and } \ 0 \leq r < m, \tag{14}$$

   from which we derive:

$$-m < r_{a+b} - r < m \tag{15}$$

   Since $r_{a+b} - r$ is a multiple of m, satisfying the above double inequality, we must have $r_{a+b} - r = 0$. Q.E.D.

2. The proof is similar to the one of the previous property.