Problem Solutions

1. Find $a \text{ div } m$ and $a \text{ mod } m$ when

   (a) $a = 13$ and $m = 3$

   $\text{Solution.}$ $13 = 4 \cdot 3 + 1$, so $13 \text{ div } 3 = 1$ and $13 \text{ mod } 3 = 1$.

   (b) $a = -97$ and $m = 11$

   $\text{Solution.}$ $-97 = -9 \cdot 11 + 2$, so $-97 \text{ div } 11 = -9$ and $-97 \text{ mod } 11 = 2$.

   (c) $a = 155$ and $m = 19$

   $\text{Solution.}$ $155 = 8 \cdot 19 + 3$, so $155 \text{ div } 19 = 8$ and $155 \text{ mod } 19 = 3$.

   (d) $a = -221$ and $m = 23$.

   $\text{Solution.}$ $-221 = -10 \cdot 23 + 9$, so $-221 \text{ div } 23 = -10$ and $-221 \text{ mod } 23 = 9$.

2. Let $m \in \mathbb{Z}^+$. Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$. (Note: the second one is a little harder, try it for a challenge.)

   $\text{Solution.}$ Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ for $m \in \mathbb{Z}^+$ and $a, b, c, d \in \mathbb{Z}$.

   This means that $m$ divides $b - a$ and $d - c$. In other words, there exist $k, l \in \mathbb{Z}$ such that $b - a = mk$ and $d - c = ml$.

   Consider $(b + d) - (a + c) = (b - a) + (d - c) = mk + ml$ for the choice of $k, l$ above. $mk + ml = m(k + l)$, so we have shown that $m$ divides $(b + d) - (a + c)$. By the definition of congruence modulo $m$, this implies $a + c \equiv b + d \pmod{m}$.

   To show $ac \equiv bd \pmod{m}$, we first notice that $(b - a)(d - c) = bd - bc - ad + ac = bd - ac + (2ac - bc - ad)$. Rearranging terms, we have $bd - ac = (b - a)(d - c) - 2ac + bc + ad$. We would like to show that this is divisible by $m$. To see this, we rewrite the expression as follows:

   
   $$(b - a)(d - c) - 2ac + bc + ad = (b - a)(d - c) + (bc - ac) + (ad - ac)$$

   $$= (b - a)(d - c) + c(b - a) + a(d - c)$$

   $$= (mk)(ml) + c(ml) + a(ml)$$

   $$= m(ml + ck + al).$$

   Thus, $bd - ac$ is divisible by $m$, which completes the proof that $ac \equiv bd \pmod{m}$.

3. Compute the following.

   (a) $(12 \cdot 727) - 202 \pmod{8}$

   $\text{Solution.}$ By Problem 2, since $12 \equiv 4 \pmod{8}$ and $727 \equiv 7 \pmod{8}$, $12 \cdot 727 \equiv 4 \cdot 7 \pmod{8}$. $28 \equiv 4 \pmod{8}$ and $-202 \equiv 6 \pmod{8}$, so by Problem 2, $28 - 202 \equiv 4 + 6 \pmod{8}$. $10 \pmod{8} = 2$, so $(12 \cdot 727) - 202 \pmod{8} = 2$. 
(b) \((32 \mod 13)^2 \mod 11\)

Solution. Again, by applying Problem 2 multiple times, we get that \(32^2 \equiv 8^2 \pmod{13}\). \(8^2 \mod 13 = 12\), so now we are interested in \(12^2 \mod 11\). \(12 \equiv 1 \pmod{11}\), so this expression is equal to 1.

(c) \((7^3 \mod 23)^2 \mod 7\)

Solution. \(7^3 = 343\), which is congruent to 21 modulo 23. So the expression above is equal to \(21^2 \mod 7\). Since \(21 \equiv 0 \pmod{7}\), this is equal to 0.

4. Choose \(b \in \{3, \ldots, 9\}\). Find the base \(b\) expansion of 37, 241, and 106. Then, find the base \(b\) expansion of \(37 + 106\) and \(37 \cdot 106\) without finding the decimal expansions of these numbers.

Solution. Let \(b = 7\).

\[37 = 5 \cdot 7 + 2, \text{ so } 37 = (52)_7. \quad 241 = 4 \cdot 7^2 + 6 \cdot 7 + 3, \text{ so } 241 = (463)_7. \quad 106 = 2 \cdot 7^2 + 1 \cdot 7 + 1, \text{ so } 106 = (211)_7.\]

To find the base 7 expansion of \(37 + 106\) without finding the decimal expansion:

\[37 + 106 = (5 \cdot 7 + 2) + (2 \cdot 7^2 + 1 \cdot 7 + 1) = 2 \cdot 7^2 + (5 + 1) \cdot 7 + (2 + 1) = (263)_7.\]

To find the base 7 expansion of \(37 \cdot 106\) without finding the decimal expansion:

\[37 \cdot 106 = (5 \cdot 7 + 2) \cdot (2 \cdot 7^2 + 1 \cdot 7 + 1) = 5 \cdot 7(2 \cdot 7^2 + 1 \cdot 7 + 1) + 2(2 \cdot 7^2 + 1 \cdot 7 + 1) = 10 \cdot 7^3 + 5 \cdot 7^2 + 5 \cdot 7 + 2 \cdot 7^2 + 2 \cdot 7 + 2 = 10 \cdot 7^3 + 10 \cdot 7^2 + 2 = (7 + 3) \cdot 7^3 + 7 \cdot 7^2 + 7 \cdot 7 + 2 = 1 \cdot 7^4 + (3 + 1) \cdot 7^3 + 3 \cdot 7^2 + 2 = (14302)_7.\]

5. Let \(m \in \mathbb{Z}^+\). Show that if \(a \equiv b \pmod{m}\) and \(b \equiv c \pmod{m}\), then \(a \equiv c \pmod{m}\).

Solution. Let \(m \in \mathbb{Z}^+\) and \(a, b, c \in \mathbb{Z}\). Suppose \(a \equiv b \pmod{m}\) and \(b \equiv c \pmod{m}\), or, equivalently, \(m\) divides \(b - a\) and \(c - b\). Then there exist \(k, l \in \mathbb{Z}\) such that \(b - a = mk\) and \(c - b = ml\). Note that \(c - a = (c - b) + (b - a) = ml + mk = m(k + l)\). So \(c - a\) is divisible by \(m\), implying that \(a \equiv c \pmod{m}\).

6. Find a counterexample to the following false statement: Let \(a, b, c, m \in \mathbb{Z}\) with \(m \geq 2\). If \(ac \equiv bc \pmod{m}\), then \(a \equiv b \pmod{m}\).
Solution. One way for this to go wrong is if $c = m$. For example, let $c = m = 3$, and $a = 1$, $b = 2$. Then $ac = 3$ and $bc = 6$, which are congruent modulo 3, but $a$ and $b$ are not congruent modulo 3.

More generally, this can go wrong if $c$ and $m$ have any common divisors. For example, let $m = 12$, $a = 1$, $b = 5$, and $c = 3$. Then $ac = 3$ and $bc = 15$, which are congruent modulo 12, but 5 and 1 are not congruent modulo 12.