Staff Solutions to In-Class Problems Week 5, Fri.

Problem 1. (a) Why is a number written in decimal evenly divisible by 9 if and only if the sum of its digits is a multiple of 9? Hint: \(10 \equiv 1 \pmod{9}\).

Solution. Since \(10 \equiv 1 \pmod{9}\), so is \(10^k \equiv 1^k \equiv 1 \pmod{9}\). (1)

Now a number in decimal has the form:

\[ d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0. \]

From (1), we have

\[ d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0 \equiv d_k + d_{k-1} + \ldots + d_1 + d_0 \pmod{9} \]

This shows something stronger than what we were asked to show, namely, it shows that the remainder when the original number is divided by 9 is equal to the remainder when the sum of the digits is divided by 9. In particular, if one is zero, then so is the other.

(b) Take a big number, such as 37273761261. Sum the digits, where every other one is negated:

\[ 3 + (-7) + 2 + (-7) + 3 + (-7) + 6 + (-1) + 2 + (-6) + 1 \equiv -11 \]

Explain why the original number is a multiple of 11 if and only if this sum is a multiple of 11.

Solution. A number in decimal has the form:

\[ d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0 \]

Observing that \(10 \equiv -1 \pmod{11}\), we know:

\[ d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0 \]

\[ \equiv d_k \cdot (-1)^k + d_{k-1} \cdot (-1)^{k-1} + \ldots + d_1 \cdot (-1)^1 + d_0 \cdot (-1)^0 \pmod{11} \]

\[ \equiv d_k - d_{k-1} + \ldots - d_1 + d_0 \pmod{11} \]

assuming \(k\) is even. The case where \(k\) is odd is the same with signs reversed.

The procedure given in the problem computes \(\pm\) this alternating sum of digits, and hence yields a number divisible by 11 (\(\equiv 0 \pmod{11}\)) iff the original number was divisible by 11.

Problem 2. (a) Use the Pulverizer to find integers \(s, t\) such that

\[ 40s + 7t = \gcd(40, 7). \]
Solution. \( s = 3 \) and \( t = -17 \)

Here is the table produced by the Pulverizer:

<table>
<thead>
<tr>
<th>( x )</th>
<th>( y )</th>
<th>( \text{rem}(x, y) )</th>
<th>( x - q \cdot y )</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>7</td>
<td>5</td>
<td>( 40 - 5 \cdot 7 )</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>2</td>
<td>( 7 - 5 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>( = 7 - (40 - 5 \cdot 7) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>( = -1 \cdot 40 + 6 \cdot 7 )</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>1</td>
<td>( 5 - 2 \cdot 2 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>( = (40 - 5 \cdot 7) - 2 \cdot (1 \cdot 40 + 6 \cdot 7) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>( = 3 \cdot 40 - 17 \cdot 7 )</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

(b) Adjust your answer to part (a) to find an inverse modulo 40 of 7 in \([1, 40]\).

Solution.

\[
1 = 3 \cdot 40 - 17 \cdot 7 \\
= 3 \cdot 40 - 7 \cdot 40 + 40 \cdot 7 - 17 \cdot 7 \\
= (3 - 7) \cdot 40 + (40 - 17) \cdot 7 \\
= -4 \cdot 40 + 23 \cdot 7 
\]

Therefore, \( 23 \cdot 7 \equiv 1 \pmod{40} \) and 23 is the inverse of 7 modulo 40.

Alternatively, since \(-17\) is an inverse, so is \( \text{rem}(-17, 40) = 23 \).

Problem 3.

Suppose \( a, b \) are relatively prime and greater than 1. In this problem you will prove the **Chinese Remainder Theorem**, which says that for all \( m, n \), there is an \( x \) such that

\[
x \equiv m \pmod{a}, \quad (2) \\
x \equiv n \pmod{b}. \quad (3)
\]

Moreover, \( x \) is unique up to congruence modulo \( ab \), namely, if \( x' \) also satisfies (2) and (3), then

\[
x' \equiv x \pmod{ab}.
\]

(a) Prove that for any \( m, n \), there is some \( x \) satisfying (2) and (3).

Hint: Let \( b^{-1} \) be an inverse of \( b \) modulo \( a \) and define \( e_a := b^{-1} b \). Define \( e_b \) similarly. Let \( x = me_a + ne_b \).

Solution. We have by definition

\[
e_a := b^{-1} b \equiv \begin{cases} 1 \pmod{a}, \\ 0 \pmod{b}, \end{cases}
\]

and likewise for \( e_b \). Therefore

\[
me_a + ne_b \equiv \begin{cases} m \cdot 1 + n \cdot 0 = m \pmod{a}, \\ m \cdot 0 + n \cdot 1 = n \pmod{b}. \end{cases}
\]
(b) Prove that
\[ x \equiv 0 \mod a \text{ AND } x \equiv 0 \mod b \] implies \( x \equiv 0 \mod ab \).

**Solution.** If \( x \equiv 0 \mod a \), then by definition, \( a \mid x \). Likewise, \( b \mid x \). But \( a \) and \( b \) are relatively prime, so by Unique Factorization 8.3.1, \( ab \mid x \), that is, \( x \equiv 0 \mod ab \).

(c) Conclude that
\[ [x \equiv x' \mod a \text{ AND } x \equiv x' \mod b] \] implies \( x \equiv x' \mod ab \).

**STAFF NOTE:** If needed suggest “Look at \( x' - x \).”

**Solution.** \((x'-x)\) is \( \equiv 0 \mod a \) by (2) and \( \equiv 0 \mod b \) by (3), so by part (b), \((x'-x)\) \( \equiv 0 \mod ab \). Adding \( x \) to both sides of this \( \equiv \) gives
\[ x' \equiv x \mod ab. \]

(d) Conclude that the Chinese Remainder Theorem is true.

**Solution.** The existence of an \( x \) is given in part (a), so all that’s let is to prove \( x \) is unique up to congruence modulo \( ab \). But if \( x \) and \( x' \) both satisfy (2) and (3), then \( x' \equiv x \mod a \) and \( x' \equiv x \mod a \), so \( x' \equiv x \mod ab \) by part (c).

(e) What about the converse of the implication in part (c)?

**Solution.** The converse is true too: if \( cd \mid (x' - x) \), then obviously \( c \mid (x' - x) \). This means that
\[ x' \equiv x \mod cd \] implies \( x' \equiv x \mod c. \)

So in particular,
\[ x \equiv x' \mod ab \] implies \( [x \equiv x' \mod a \text{ AND } x \equiv x' \mod b] \).

So this together with part (c) gives a basic fact worth calling a

**Lemma.** For \( a, b \) are relatively prime and greater than 1,
\[ [x' \equiv x \mod a \text{ AND } x' \equiv x \mod b] \] iff \( x' \equiv x \mod ab \).