Staff Solutions to In-Class Problems Week 7, Wed.

**STAFF NOTE**: Chapter 9.5. *Turing* through 9.9. Cancelli ng \( (\mod n) \)

**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*: \( 10 \equiv 1 \) (mod 9).

**Solution.** Since \( 10 \equiv 1 \) (mod 9), so is
\[
10^k \equiv 1^k \equiv 1 \quad (\mod 9). \tag{1}
\]

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
\[
d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0 \equiv d_k + d_{k-1} + \ldots + d_1 + d_0 \quad (\mod 9)
\]

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.

**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 \( 10 \equiv -1 \) (mod 11), we know:
\[
d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0
\]
\[
\equiv d_k \cdot (-1)^k + d_{k-1} \cdot (-1)^{k-1} + \ldots + d_1 \cdot (-1)^1 + d_0 \cdot (-1)^0 \quad (\mod 11)
\]
\[
\equiv d_k - d_{k-1} + \ldots - d_1 + d_0 \quad (\mod 11)
\]

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 \( (\equiv 0 \mod 11) \) iff the original number was divisible by 11.

© 2015, Albert R Meyer. This work is available under the terms of the Creative Commons Attribution-ShareAlike 3.0 license.
Problem 2.
Find the inverse of 17 modulo 29 in the interval \([1, 28]\).

Solution. We first use the Pulverizer to find \(s, t\) such that \(\gcd(17, 29) = s \cdot 17 + t \cdot 29\), namely,

\[
1 = 12 \cdot 17 - 7 \cdot 29.
\]

This implies that \(s = 12\) is an inverse of 17 modulo 29.

Let \(a = 29, b = 17\). Here is the Pulverizer calculation:

\[
\begin{array}{ccc}
29 & 17 & \text{rem}(x, y) = x - q \cdot y \\
17 & 12 & 12 = a - b \\
17 & 12 & 5 = b - 12 \\
5 & 2 & 2 = 12 - 2 \cdot 5 \\
5 & 2 & 1 = 5 - 2 \cdot 2 \\
2 & 1 & 0 \\
\end{array}
\]

So the inverse is 12. 

Problem 3.
Find

\[
\text{remainder} \left( 9876^{3456789} (99)^{5555} - 6789^{3414259}, 14 \right). \tag{2}
\]

Solution. Its remainder is 7.

Following the General Principle of Remainder Arithmetic from Section 9.7, replace the numbers being raised to powers by their remainders. Since \(\text{rem}(9876, 14) = 6\) and \(\text{rem}(6789, 14) = 13\), we find that (2) equals the remainder on division by 14 of

\[
6^{3456789} (99)^{5555} - 13^{3414259}. \tag{3}
\]

But let’s look at the remainders of powers of 6:

\[
\begin{align*}
\text{rem}(6^1, 14) &= 6 \\
\text{rem}(6^2, 14) &= 8 \\
\text{rem}(6^3, 14) &= 6 \\
\text{rem}(6^4, 14) &= 8 \\
\vdots
\end{align*}
\]

That is, the remainder on division by 14 of 6 raised to any odd power is 6. In particular

\[
\text{rem}(6^{3456789}, 14) = 6
\]

Similarly,

\[
\begin{align*}
\text{rem}(9^1, 14) &= 9 \\
\text{rem}(9^2, 14) &= 11 \\
\text{rem}(9^3, 14) &= 1.
\end{align*}
\]
so
\[ \text{rem}(9^{99}, 14) = \text{rem}(9^{33}, 14) = \text{rem}(13^{33}, 14) = 1, \]
and therefore
\[ \text{rem}(9^{99})^{5555}, 14) = \text{rem}(13^{5555}, 14) = 1. \]
Finally,
\[ \text{rem}(13^1, 14) = 13 \]
\[ \text{rem}(13^2, 14) = 1. \]
so
\[ \text{rem}(13^{3456789}, 14) = \text{rem}(13 \cdot (13^2)^{34567878/2}, 14) = \text{rem}(13 \cdot 13^{34567878/2}, 14) = 13. \]
Therefore, the number (3) has the same remainder on division by 14 as
\[ 6 \cdot 1 - 13 = -7, \]
which has the same remainder on division by 14 as -7, namely 7.

Notice that it would be a disastrous blunder to replace an exponent by its remainder. The General Principle applies to numbers that are operands of plus and times, whereas the exponent is a number that controls how many multiplications to perform. Watch out for this blunder.

### Problem 4.
Prove that if \( a \equiv b \pmod{14} \) and \( a \equiv b \pmod{5} \), then \( a \equiv b \pmod{70} \).

**Solution.** We know \( a \equiv b \pmod{14} \) means 14 | \( a - b \). Likewise, \( a \equiv b \pmod{5} \) means 5 | \( a - b \). Also, 14 and 5 are relatively prime.

But if \( m, n \), are relatively prime and \( m \) and \( n \) both divide \( x \), then \( mn | x \). So, applying that reasoning with \( x = a - b, m = 14 \) and \( n = 5 \) yields 70 | \( a - b \), proving \( a \equiv b \pmod{70} \) as required.

This also follows straightforwardly from the Chinese Remainder Theorem, described in Problem 9.58.

### Problem 5.
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
\[ x \equiv m \pmod{a}, \tag{4} \]
\[ x \equiv n \pmod{b}. \tag{5} \]
Moreover, \( x \) is unique up to congruence modulo \( ab \), namely, if \( x' \) also satisfies (4) and (5), then
\[ x' \equiv x \pmod{ab}. \]

(a) Prove that for any \( m, n \), there is some \( x \) satisfying (4) and (5).

**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
\[ e_a := b^{-1} b = \begin{cases} 1 \mod{a}, \\ 0 \mod{b}, \end{cases} \]
and likewise for $e_b$. Therefore
\[ me_a + ne_b \equiv \begin{cases} 
  m \cdot 1 + n \cdot 0 = m \mod a \\
  m \cdot 0 + n \cdot 1 = n \mod b.
\end{cases} \]

(b) Prove that
\[ [x \equiv 0 \mod a \ \text{AND} \ x \equiv 0 \mod b] \ \text{implies} \ x \equiv 0 \mod ab. \]

**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 9.4.1, $ab \mid x$, that is, $x \equiv 0 \mod ab$. 

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

**STAFF NOTE:** If needed suggest “Look at $x' - x$.”

**Solution.** $(x' - x)$ is $\equiv 0 \mod a$ by (4) and $\equiv 0 \mod b$ by (5), 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 left is to prove $x$ is unique up to congruence modulo $ab$. But if $x$ and $x'$ both satisfy (4) and (5), then $x' \equiv x \mod a$ and $x' \equiv x \mod b$, so $x' \equiv x \mod ab$ by part (c).

The Chinese Remainder Theorem underlies a way of reducing arithmetic calculations with “large” numbers into parallel calculations with “small” numbers at a significant gain in speed and effort. Refer to Problem 9.63 for a discussion.

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

**Solution.** The converse is true too: if $cd$ divides $(x' - x)$, then $c$ itself must also be a divisor of $(x' - x)$. This means that
\[ x' \equiv x \mod cd \ \text{implies} \ x' \equiv x \mod c. \]

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