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

STAFF NOTE: Chapter 9.5. Turing through 9.9. Cancelling \((\mod n)\)

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: \(10 \equiv 1 \pmod{9}\).

COMMENTS:
- CP_multiples_of_9_and_11
- from: S09.cp8t, S06.cp7m, S04.ps7

keywords = [ series number_theory divides remainders ]

Solution. Since \(10 \equiv 1 \pmod{9}\), so is 
\[
10^k \equiv 1^k \equiv 1 \pmod{9}. 
\]
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:
\[
3 + (-7) + 2 + (-7) + 3 + (-7) + 6 + (-1) + 2 + (-6) + 1 = -11 
\]
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:
\[
d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0 
\equiv d_k \cdot (-1)^k + d_{k-1} \cdot (-1)^{k-1} + \ldots + d_1 \cdot (-1) + d_0 \cdot (-1)^0 \pmod{11} 
\equiv d_k - d_{k-1} + \ldots - d_1 + d_0 \pmod{11} 
\]
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.
Find the inverse of 17 modulo 29 in the interval \([1, 28]\).

**COMMENTS:**
- FP\_inverse17mod29
- variant of S11.ps4.prob2
- by Tigran Sloyan 5/12/11

**keywords** = [ number\_theory Pulverizer modular\_arithmetic inverses Fermat\_theorem remainder ]

**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:

\[
\begin{array}{ccc}
\hline
x & y & \text{rem}(x, y) = x - q \cdot y \\
\hline
29 & 17 & 12 = a - b \\
17 & 12 & 5 = b - 12 \\
& & = b - (a - b) \\
& & = (-1) \cdot a + 2 \cdot b \\
12 & 5 & 2 = 12 - 2 \cdot 5 \\
& & = (a - b) - 2 \cdot ((-1) \cdot a + 2 \cdot b)) \\
5 & 2 & 1 = 5 - 2 \cdot 2 \\
& & = (-1) \cdot a + 2 \cdot b - 2 \cdot (3 \cdot a - 5 \cdot b) \\
2 & 1 & 0 \\
\hline
\end{array}
\]

So the inverse is \(12\).

Problem 3.
Find

\[
\text{remainder } \left( 9876^{3456789} \left( 9^{99} \right)^{5555} - 6789^{3414259} \cdot 14 \right).)
\]

**COMMENTS:**
- CP\_remainder\_computation\_practice
- by ARM 3/6/12
- similar to equation “labelex44427 in number\_theory chapter

**keywords** = [ number\_theory modular\_arithmetic exponent remainder ]

**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

\[
6^{3456789} \left( 9^{99} \right)^{5555} - 13^{3414259}. \tag{3}
\]
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

\[
\text{rem}(9^{99}, 14) = \text{rem}((9^3)^{33}, 14) = \text{rem}(1^{33}, 14) = 1,
\]

and therefore

\[
\text{rem}((9^{99})^{5555}, 14) = \text{rem}(1^{5555}, 14) = 1.
\]

Finally,

\[
\begin{align*}
\text{rem}(13^1, 14) &= 13 \\
\text{rem}(13^2, 14) &= 1,
\end{align*}
\]

so

\[
\text{rem}(13^{3456789}, 14) = \text{rem}(13 \cdot (13^2)^{34567878/2}, 14) = \text{rem}(13 \cdot 1^{34567878/2}, 14) = 13.
\]

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.

\[\blacksquare\]

**Problem 4.**

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

**COMMENTS:**

- MQ_congruent_mod_product
- Chinmay, ARM edit 3/5/14

**keywords** = [ modular_arithmetic congruence remainder ]
Solution. We know $a \equiv b \pmod{14}$ means $14 \mid a - b$. Likewise, $a \equiv b \pmod{5}$ means $5 \mid a - b$. Also, 14 and 5 are relatively prime.

But if $m, n$, are relatively prime and $m$ and $n$ both divide $x$, then $mn \mid x$. So, applying that reasoning with $x = a - b$, $m = 14$ and $n = 5$ yields $70 \mid a - b$, 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

\begin{align*}
x &\equiv m \pmod a, \quad (4) \\
x &\equiv n \pmod b. \quad (5)
\end{align*}

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 $x = me_a + ne_b$.

COMMENTS:
- CP_chinese_remainder
- used to appear as first part of PS_Euler_function_multiplicativity
- by ARM 2/27/11; revised 3/2/11

keywords = \{ prime relatively_prime number_theory modular_arithmetic chinese_remainder remainder \}

Solution. We have by definition

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

and likewise for $e_b$. Therefore

$$me_a + ne_b = \begin{cases} m \cdot 1 + n \cdot 0 = m \pmod a \\ m \cdot 0 + n \cdot 1 = n \pmod b. \end{cases}$$

(b) Prove that

$$[x \equiv 0 \pmod a \; \text{AND} \; x \equiv 0 \pmod b] \; \text{implies} \; x \equiv 0 \pmod{ab}.$$ 

Solution. If $x \equiv 0 \pmod a$, 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, $x \equiv 0 \pmod{ab}$.

(c) Conclude that

$$[x \equiv x' \pmod a \; \text{AND} \; x \equiv x' \pmod b] \; \text{implies} \; x \equiv x' \pmod{ab}.$$ 

STAFF NOTE: If needed suggest “Look at $x' - x$.”
**Solution.** \((x' - x) \equiv 0 \mod a\) 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

\[x' \equiv x \mod ab.\]

\(\blacksquare\)

**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.

\(\blacksquare\)

**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

\[x' \equiv x \mod cd \quad \text{implies} \quad x' \equiv x \mod c.\]

So in particular,

\[x \equiv x' \mod ab \quad \text{implies} \quad [x \equiv x' \mod a \ \text{AND} \ x \equiv x' \mod b].\]

\(\blacksquare\)