Staff Solutions to In-Class Problems Week 6, Mon.

Staff Note: Number Theory: Modular Arithmetic, Ch. 8.5–8.9

Problem 1.

Find

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

Solution. Its remainder is 7.

Following the General Principle of Remainder Arithmetic from Section 8.7, 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 (1) equals the remainder on division by 14 of

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

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

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

and therefore

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

Finally,

\[
\begin{align*}
\text{rem}(13^1, 14) &= 13 \\
\text{rem}(13^2, 14) &= 1,
\end{align*}
\]
so \[ \text{rem}(13^{3456789}, 14) = \text{rem}(13 \cdot (13^2)^{34567878/2}, 14) = \text{rem}(13 \cdot 13^{34567878/2}, 14) = 13. \]

Therefore, the number (2) 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 2.
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

\[
\begin{align*}
    x &\equiv m \mod a, \\
    x &\equiv n \mod b. 
\end{align*}
\]

Moreover, \(x\) is unique up to congruence modulo \(ab\), namely, if \(x'\) also satisfies (3) and (4), then

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

(a) Prove that for any \(m, n\), there is some \(x\) satisfying (3) and (4).

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

\[
me_a + ne_b = \begin{cases} 
m \cdot 1 + n \cdot 0 = m \mod a \\\nm \cdot 0 + n \cdot 1 = n \mod b. \end{cases}
\]

(b) Prove that

\[ [x \equiv 0 \mod a \text{ AND } x \equiv 0 \mod b] \impliedby x \equiv 0 \mod ab. \]

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 8.4.1, \(ab \mid x\), that is, \(x \equiv 0 \mod ab\).

(c) Conclude that

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

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

Solution. \((x' - x)\) is \(\equiv 0 \mod a\) by (3) and \(\equiv 0 \mod b\) by (4), 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 (3) and (4), 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 8.61 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

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

So in particular,

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

Problem 3.

Definition. The set, $P$, of integer polynomials can be defined recursively:

**Base cases:**

- the identity function, $\text{Id}_\mathbb{Z}(x) := x$ is in $P$.
- for any integer, $m$, the constant function, $c_m(x) := m$ is in $P$.

**Constructor cases.** If $r, s \in P$, then $r + s$ and $r \cdot s \in P$.

(a) Using the recursive definition of integer polynomials given above, prove by structural induction that for all $q \in P$,

$$j \equiv k \pmod{n} \quad \text{IMPLIES} \quad q(j) \equiv q(k) \pmod{n},$$

for all integers $j, k, n$ where $n > 1$.

Be sure to clearly state and label your Induction Hypothesis, Base case(s), and Constructor step.

Solution. The proof is by structural induction on the definition of $P$. The hypothesis $H(q)$ is:

$$H(q) := [j \equiv k \pmod{n} \quad \text{IMPLIES} \quad q(j) \equiv q(k) \pmod{n},$$

for all $j, k, n \in \mathbb{Z}$, where $n > 1$.

**Base cases:**

Case: $(q = \text{Id}_{\mathbb{Z}})$. 

H(q) holds because if \( j \equiv k \pmod{n} \), then

\[
q(j) := \text{Id}_\mathbb{Z}(j) \\
= j \\
\equiv k \pmod{n} \\
= \text{Id}_\mathbb{Z}(k) \\
= q(k),
\]

so \( q(j) \equiv q(k) \pmod{n} \), as required.

**Case:** \( (q = c_m) \). \( H(c_m) \) holds because \( c_m(j) = c_m(k) \), and therefore certainly \( c_m(j) \equiv c_m(k) \pmod{n} \).

**Constructor cases:**

We may assume by structural induction that \( H(r) \) and \( H(s) \) both hold.

**Case:** \( (q = r + s) \). To show \( H(q) \), suppose \( j \equiv k \pmod{n} \). Since \( H(r) \) holds, we have that \( r(j) \equiv r(k) \pmod{n} \). Likewise, \( s(j) \equiv s(k) \pmod{n} \). So

\[
r(j) + s(k) \equiv r(j) + s(k) \pmod{n}.
\]

by additivity of congruences Lemma 8.6.4(8.7), that is, \( q(j) \equiv q(k) \pmod{n} \), as required.

**Case:** \( (q = r \cdot s) \). The proof in this case is the same as the previous with “+” replacing “.”

**STAFF NOTE:** The values of polynomial \( p(n) := n^2 + n + 41 \) are prime for all the integers from 0 to 39 (see Section 1.1). Well, \( p \) didn’t work, but are there any other polynomials whose values are always prime? No way! In fact, we’ll prove a much stronger claim.

(b) We’ll say that \( q \) produces multiples if, for every integer greater than one in the range of \( q \), there are infinitely many different multiples of that integer in the range. For example, if \( q(4) = 7 \) and \( q \) produces multiples, then there are infinitely many different multiples of 7 in the range of \( q \).

Prove that if \( q \) has positive degree and positive leading coefficient, then \( q \) produces multiples. You may assume that every such polynomial is strictly increasing for large arguments.

**Hint:** Observe that all the elements in the sequence

\[
q(k), q(k + v), q(k + 2v), q(k + 3v), \ldots,
\]

are congruent modulo \( v \). Then let \( v = q(k) \).

**Solution.** For any \( k \in \mathbb{Z} \) and \( v > 1 \)

\[
k \equiv k + v \equiv k + 2v \equiv k + 3v \ldots \pmod{v},
\]

by definition of \( \equiv \pmod{v} \). Now part (a) implies that each of the elements in the sequence

\[
q(k), q(k + v), q(k + 2v), q(k + 3v), \ldots
\]

is \( \equiv q(k) \pmod{v} \).

If \( 1 < v \in \text{range}(q) \), then \( v = q(k) \) for some integer \( k \) and

\[
q(k) \equiv 0 \pmod{v}.
\]
So all the elements in the sequence (5) are multiples of \( v \).

Since \( q(k) \) is strictly increasing\(^1\) for \( k \geq b \) for some bound, \( b > 0 \), all the elements in the sequence are different after a certain point (no later than after \( (b/2) \) elements). So there are arbitrarily large multiples of \( v \) in the range of \( q \). Since \( v > 1 \) was an arbitrary element, we conclude there are infinitely many multiples of every element \( v > 1 \) in the range of \( q \). That is, \( q \) produces multiples. \( \blacksquare \)

Part (b) implies that an integer polynomial with positive leading coefficient and degree has infinitely many nonprimes in its range. This fact no longer holds true for multivariate polynomials. An amazing consequence of Matiyasevich’s [31] solution to Hilbert’s Tenth Problem is that multivariate polynomials can be understood as general purpose programs for generating sets of integers. If a set of nonnegative integers can be generated by any program, then it equals the set of nonnegative integers in the range of a multivariate integer polynomial! In particular, there is an integer polynomial \( p(x_1, \ldots, x_7) \) whose nonnegative values as \( x_1, \ldots, x_7 \) range over \( \mathbb{N} \) are precisely the set of all prime numbers!

\(^1\)We’ll prove this and similar “growth rate” facts about polynomials and other functions in Chapter 13.