Math for CS 2015/2019 solutions to “In-Class Problems Week 6, Mon. (Session 13)”

https://github.com/spamegg1

October 26, 2022

Contents

1 Problem 1

Find remainder$(9876^{3456789}(9^{99})^{5555} - 6789^{3414259}, 14)$.

Proof. By doing some calculations we see that:

$$9876 = 14 \cdot 705 + 6$$
$$6789 = 14 \cdot 484 + 13$$

So $9876 \equiv 6 \mod 14$ and $6789 \equiv 13 \mod 14$.

Now we explore the powers of these numbers. We see that:

$$6^2 \equiv 8 \mod 14$$
$$6^3 \equiv 6 \mod 14$$
$$6^4 \equiv 8 \mod 14$$

We see that for all positive integers n, $6^{2n+1} \equiv 6 \mod 14$ and $6^{2n} \equiv 8 \mod 14$; therefore it follows $9876^{2n+1} \equiv 6 \mod 14$ and $9876^{2n} \equiv 8 \mod 14$.

Similarly:

$$\begin{gathered} 13^2 \equiv 1 \mod 14 \\ 13^3 \equiv 13 \mod 14 \\ 13^4 \equiv 1 \mod 14 \end{gathered}$$

We see that for all positive integers n, $13^{2n+1} \equiv 13 \mod 14$ and $13^{2n} \equiv 1 \mod 14$; therefore it follows $6789^{2n+1} \equiv 13 \mod 14$ and $6789^{2n} \equiv 1 \mod 14$.

Similarly:

$$\begin{gathered} 9^2 \equiv 11 \mod 14 \\ 9^3 \equiv 1 \mod 14 \\ 9^4 \equiv 9 \mod 14 \\ 9^5 \equiv 11 \mod 14 \\ 9^6 \equiv 1 \mod 14 \end{gathered}$$

So we see that for all positive integers n, $9^{3n} \equiv 1 \mod 14$, $9^{3n+1} \equiv 9 \mod 14$ and $9^{3n+2} \equiv 11 \mod 14$.

Putting these together we get

$$9876^{3456789^{549945}} - 6789^{3414259} \equiv (6)(1) - 13 \equiv 7 \mod 14$$

So the remainder is 7. □

2 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

$$x \equiv m \mod a \qquad (2)$$

$$x \equiv n \mod b \qquad (3)$$

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

$$x' \equiv x \mod ab$$

2.1 (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 $x = me_a + ne_b$.

Proof. 1. Since a and b are relatively prime, there exists b^{-1} such that $b^{-1} \cdot b \equiv 1 \mod a$. Define $e_a ::= b^{-1}b$.

So $e_a \equiv 1 \mod a$ and $e_a \equiv 0 \mod b$.

2. Since a and b are relatively prime, there exists a^{-1} such that $a^{-1} \cdot a \equiv 1 \mod b$. Define $e_b ::= a^{-1}a$.

So $e_b \equiv 1 \mod b$ and $e_b \equiv 0 \mod a$.

3. Define $x = me_a + ne_b$. Then

$$x = me_a + ne_b \equiv m \cdot 1 + n \cdot 0 \equiv m \mod a$$
$$x = me_a + ne_b \equiv m \cdot 0 + n \cdot 1 \equiv n \mod b$$

□

2.2 (b)

Prove that $[x \equiv 0 \mod a$ AND $x \equiv 0 \mod b]$ implies $x \equiv 0 \mod ab$.

Proof. 1. Assume $x \equiv 0 \mod a$ and $x \equiv 0 \mod b$.

2. There exist integers j, k such that $x = ja$ and $x = kb$.

3. So $ja = kb$ therefore a divides kb.

4. Since a and b are relatively prime, $a \nmid b$, therefore by (3) $a \mid k$.

5. By (4) there exists an integer i such that $k = ai$.

6. By (5) and (2) $x = aib$. Therefore $x \equiv 0 \mod ab$. □

2.3 (c)

Prove that $[x \equiv x' \mod a$ AND $x \equiv x' \mod b]$ implies $x \equiv x' \mod ab$.

Proof. 1. Assume $x \equiv x' \mod a$ and $x \equiv x' \mod b$.

2. There exist integers j, k such that $x = ja + x'$ and $x = kb + x'$.

3. So $ja = kb$ therefore a divides kb.

4. Since a and b are relatively prime, $a \nmid b$, therefore by (3) $a \mid k$.

5. By (4) there exists an integer i such that $k = ai$.

6. By (5) and (2) $x = aib + x'$. Therefore $x \equiv x' \mod ab$. □

2.4 (d)

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

Proof. We proved the existence of x in part (a). We proved the uniqueness (up to congruence $\mod ab$) of x in part (c). Therefore we proved the Chinese Remainder Theorem. □

2.5 (e)

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

Proof. 1. Assume $x \equiv x' \mod ab$. So $x - x'$ is divisible by ab. There exists an integer k such that $x - x' = abk$.

2. By (1) $x - x' = a(bk)$ so $x - x'$ is divisible by a, therefore $x \equiv x' \mod a$.

3. Similarly $x \equiv x' \mod b$. □

3 Problem 3

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

Base cases:

the identity function, $\mathrm{Id}_{\mathbb{Z}}(x) ::= x$ 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 $r \cdot s \in P$.

3.1 (a)

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

$$j \equiv k \mod n \text{ IMPLIES } q(j) \equiv q(k) \mod n, \qquad (4)$$

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.

Proof. **Base Cases.**

First up is the case when $q = \mathrm{Id}_{\mathbb{Z}}$.

Assume $j \equiv k \mod n$. Then $\mathrm{Id}_{\mathbb{Z}}(j) = j \equiv k = \mathrm{Id}_{\mathbb{Z}}(k) \mod n$. So (4) is true for $q = \mathrm{Id}_{\mathbb{Z}}$.

Next are the cases when $q = c_m$ for some integer m.

Assume $j \equiv k \mod n$. Then $c_m(j) = m \equiv m = c_m(k) \mod n$. So (4) is true for $q = c_m$.

Constructor Cases. Assume $r, s \in P$ and r, s satisfy (4). We need to show $r + s$ and $r \cdot s$ satisfy (4).

Induction Hypothesis. $j \equiv k \mod n$ IMPLIES $r(j) \equiv r(k) \mod n$

and $j \equiv k \mod n$ IMPLIES $s(j) \equiv s(k) \mod n$.

1. Assume $j \equiv k \mod n$.

2. Then by Induction Hypothesis $r(j) \equiv r(k) \mod n$ and $s(j) \equiv s(k) \mod n$.

3. Adding the two statements from (2) we get $r(j) + s(j) \equiv r(k) + s(k) \mod n$. (We are using the fact that if $x \equiv y \mod z$ and $t \equiv w \mod z$ then $x + t \equiv y + w \mod z$.)

Therefore $r + s$ satisfies (4).

4. Multiplying the two statements from (2) we get $r(j) \cdot s(j) \equiv r(k) \cdot s(k) \mod n$. (We are using the fact that if $x \equiv y \mod z$ and $t \equiv w \mod z$ then $x \cdot t \equiv y \cdot w \mod z$.)

Therefore $r \cdot s$ satisfies (4).

By Structural Induction, every $q \in P$ satisfies (4). □

3.2 (b)

(b) We'll say that q produces multiples if, for every integer greater than 1 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. Let $v = q(k)$.

Proof. 1. Assume q has positive degree and positive leading coefficient. In other words, there exist integers $n, q_n, \ldots, q_0$ such that $n > 0$ and $q_n > 0$ and

$$q(x) = q_n x^n + \ldots + q_1 x + q_0$$

2. Also assume q is strictly increasing for large arguments.

3. Assume $v > 1$ is an integer in the range of q. That is, there exists an integer k such that $q(k) = v$.

We want to show that there exist infinitely many integers in the range of q that are multiples of v.

4. For all integers m, $k \equiv k + mv \pmod v$.

5. By part (a) and (4), for all integers m, $q(k) \equiv q(k + mv) \pmod v$.

6. But $v = q(k)$ so $q(k) \equiv 0 \pmod v$, therefore $q(k+mv) \equiv 0 \pmod v$. In other words, for all integers m, $q(k + mv)$ is a multiple of v.

7. So it looks like by (6) there are infinitely many multiples of v in the range of q, but we still need to show that these multiples are different from each other, so that there can be infinitely many of them. In other words we need to show that the set

$$q_v ::= \{q(k + mv) \mid m \in \mathbb{Z}\}$$

is an infinite set.

8. The set q_v is infinite by our assumption in (2). □