In-Class Problems Week 6, Mon.

4

8×5

Problem 1.
Find

2^1 2^2 2^3 13

$$\text{remainder}\left(9876^{3456789}\left(9^{99}\right)^{5555} - 6789^{3414259},\ 14\right). \tag{1}$$

2 4 8

2 3 9 $6^{3456789}$ 11^{414259}

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

$$x \equiv m \bmod a, \tag{2}$$
$$x \equiv n \bmod b. \tag{3}$$

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

$$x' \equiv x \bmod ab.$$

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

$x = m b^{-1} b + n a^{-1} a$

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

(b) Prove that

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

(c) Conclude that

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

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

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

$e_{a_1} := \prod_{i=2}^{n} a_i a_i^{-1}$

$x = \cancel{\Sigma} \, e_{a_1}$

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.

(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. Let $v = q(k)$.

(a) $C_m(i) \equiv C_m(j)$, $Id(i) \equiv Id(j)$

Hypo: $j \equiv k \Rightarrow q_1(j) \equiv q_1(k)$ $q_2(i) \equiv q_2(j)$

Cons: $(q_1 + q_2)(i) \equiv (q_1 + q_2)(k)$

$(q_1 \cdot q_2)(i) \equiv (q_1 \cdot q_2)\ k$