In-Class Problems Week 10, Fri.

Problem 1.
Find the inverse of 17 modulo 29 in the interval [1..28].

Problem 2.
Find

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

Problem 3. **(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:* $10 \equiv 1 \pmod{9}$.

(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.

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

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

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

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).

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)?