Discrete Structures. CSCI-150. Fall 2015.

Homework 7. Due Wed. Oct. 21, 2015.

Problem 1

Decide whether each of these integers is congruent to 3 modulo 7:

(a) 10, (b) -3, (c) 37, (d) 66, (e) -17, (f) -67.

Problem 2 (Graded)

In this problem, don't use a calculator. The answers can be derived without doing much computation, try to find these simple solutions.

Prove or disprove:

(a) $4 + 5 + 6 \equiv 0 \pmod 5$

(b) $55 + 56 + 7 \equiv 3 \pmod 5$

(c) $1004 + 2005 + 3006 \equiv 0 \pmod 5$

(d) $15 + 111^5 \cdot (-10) \equiv 5 \pmod{11}$

(e) $1112 \cdot 2224 \cdot 4448 + 2221 \equiv 7 \pmod{1111}$

(f) $20 \cdot 10 \cdot (-10) \cdot (-20) \equiv 13000000000 \pmod 9$

Problem 3 (Graded)

Given the following recurrently defined sequence of integers:

$$a_0 = 3,$$
$$a_n = 5a_{n-1} + 8$$

Prove by induction that all elements in this sequence are congruent to 3 modulo 4, or in other words:

$$\forall n \geq 0 : \qquad a_n \equiv 3 \pmod 4$$

Problem 4 (Graded)

We want to prove that 119 has infinitely many multiplicative inverses modulo 198.

(a) Prove that such a multiplicative inverse exists.

(b) Verify that 5 is one of them.

(c) Prove that there are infinitely many inverses. Hint: Consider the number $(5 + n \cdot 198)$

(d) **Generalize the statement:** Try to prove that for any two positive integers a and b that are relative primes, there are infinitely many multiplicative inverses of a modulo b.

Problem 5

Find the GCD of two numbers, if you know their prime factorizations:

$$2^5 \cdot 3^9 \cdot 5^{16} \cdot 11 \qquad \text{and} \qquad 2^2 \cdot 3 \cdot 5^{11} \cdot 7 \cdot 11^2 \cdot 13$$

(There is no need to do Euclid's algorithm here)