Discrete Structures. CSCI-150. Summer 2015.

Homework 8. Due Thr. Jul. 2, 2015.

Problem 1

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

(a) 38, (b) 66, (c) 67, (d) -3, (e) -17, (f) -18.

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

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)

Problem 4 (Graded)

Given two numbers,

$$a_0 = 191, \quad a_1 = 125,$$

write out the execution of the extended Euclidean algorithm. Find $a_k = \gcd(a_0, a_1)$ and Bezout's coefficients x_k and y_k, i.e. the numbers such that the following equation is satisfied:

$$x_k a_0 + y_k a_1 = \gcd(a_0, a_1)$$

If the multiplicative inverse of a_1 modulo a_0 exists, find such a number and show why it is a multiplicative inverse. Otherwise, prove that it does not exist.