Discrete Structures. CSCI-150. Spring 2014.

Homework 8. Due Fri. Apr 4, 2014.

Problem 1

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

(a) 37

(b) 66

(c) -17

(d) -67

Problem 2

Prove that

$$24^{31} \equiv 23^{32} \pmod{19}.$$

Problem 3

Given two numbers,

$$a_0 = 250, \quad a_1 = 149,$$

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:

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

If it's possible, find the multiplicative inverse of a_1 modulo a_0.

Problem 4

Repeat the task from the problem 3 for numbers

$$a_0 = 8000, \quad a_1 = 7001.$$

Problem 5

Verify that $p = 17$, $q = 13$, $e = 5$, and $d = 77$ are valid parameters for RSA encryption and decryption.

Encrypt the following two-blocks message $M = (115,\ 209)$.

The encrypted message should be equal to $C = (098,\ 014)$. Decrypt it back.