Discrete Structures. CSCI-150. Spring 2015.

Homework 8. Due Fri. Apr 17, 2015.

Problem 1 (Graded)

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

(a) 37, (b) 66, (c) -17, (d) -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

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,

$$a_0 = 172, \quad a_1 = 61,$$

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.

Problem 5

Repeat the task from the previous problem for numbers

$$a_0 = 800, \quad a_1 = 33.$$

Problem 6 (Graded)

Prove that

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

You are allowed to use a calculator only for computing multiplication, division, addition, and subtraction. Particularly, not allowed to use the power function.

Problem 7

Prove or disprove

$$3^{23} + 3 \equiv 5^{37} - 4 \pmod{7}.$$

Problem 8

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.

Problem 9

Prove that if x is a multiplicative inverse of a modulo n, that is

$$x \cdot a \equiv 1 \pmod{n},$$

then $x + n$ is also a multiplicative inverse.

Then, prove that there are infinitely many multiplicative inverses of a modulo n.