Discrete Structures. CSCI-150. Fall 2014.

Homework 10. Due Mon. Nov 17, 2014.

Problem 1 (Graded)

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 2 (Graded)

Prove that

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

Problem 3 (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 it's possible, find the multiplicative inverse of a_1 modulo a_0.

Problem 4

Repeat the task from the problem 3 for numbers

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

Problem 5 (Graded)

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 6

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.