Discrete Structures. CSCI-150. Summer 2016.

Homework 9. Due Thr. Jul. 7, 2016.

Problem 1 (Graded)

Prove or disprove

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

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

$$1{,}000{,}001^{999{,}999} \equiv 1 \pmod{1{,}000{,}000}$$

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

Problem 2

Prove that

$$112^{112} \equiv 114^{114} \pmod{113}$$

$$771^{78} \cdot 222^{444} + 121^{85} \equiv 5 \pmod{11}$$

$$17^{170} + 1 \equiv 0 \pmod{50}$$

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

Problem 3 (Graded)

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

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

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