

Discrete Structures. CSCI-150. Fall 2015.

Homework 8.

Due Wed. Oct. 28, 2015.

Problem 1 (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.

Prove or disprove

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

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

Problem 2

Prove that

$$\begin{aligned} 112^{112} &\equiv 114^{114} \pmod{113} \\ 771^{78} \cdot 222^{444} + 121^{85} &\equiv 5 \pmod{11} \\ 17^{170} + 1 &\equiv 0 \pmod{50} \end{aligned}$$

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

Prove the following statements:

- (a) if a is odd then $a^4 \equiv 1 \pmod{4}$,
- (b) if 5 does not divide a , then $a^4 \equiv 1 \pmod{5}$.

Hint: If a is not divisible by 5 then it's representable as $a = 5k + r$, where k is an integer and the remainder r can be equal to 1, 2, 3, or 4.

Also don't forget that

$$(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

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 the numbers

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

Problem 6 (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.