

Discrete Structures. CSCI-150. Spring 2016.

Homework 9.

Due Wed. Apr. 13, 2016.

Problem 1

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 (Graded)

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 (Graded)

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

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.

Problem 5 (Graded)

Let $A = \{1, 2, 3\}$, $B = \{0, 1\}$, and $C = \{x, y, z\}$.

Determine what the following sets are (list their elements):

- (a) $A \cap B$, (b) $B \cup A$, (c) $A \setminus B$, (d) $(B \cap \mathbb{Z}) \setminus A$, (e) $(A \cup C) \setminus B$,
(f) $A \times B$, (g) $B \times B$, (h) $A \times B \times C$, (i) C^3 ,
(j) $\mathcal{P}(C)$. (k) $\mathcal{P}(B^2)$.

Problem 6

Let $S = \{a, b\}$.

Prove or disprove:

- (a) $a \in S$, (b) $a \in \mathcal{P}(S)$, (c) $\{a\} \subseteq S$, (d) $\{a\} \in \mathcal{P}(S)$,
(e) $\emptyset \in S$, (f) $\emptyset \subseteq S$, (g) $\emptyset \in \mathcal{P}(S)$, (h) $\emptyset \subseteq \mathcal{P}(S)$

For the proofs, writing one short sentence for each question will be sufficient, if your argument is to the point and captures the main idea why the statement is true or false.

Problem 7 (Graded)

Prove the inclusion-exclusion formula (it's an extension of the subtraction rule)

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| \\ &\quad - |A \cap B| - |A \cap C| - |B \cap C| \\ &\quad + |A \cap B \cap C|. \end{aligned}$$

To do the proof, let's denote $X = A \cup B$, then

$$|(A \cup B) \cup C| = |X \cup C|,$$

and we can apply the usual subtraction rule (you will have to apply it twice).