Discrete Structures. CSCI-150. Summer 2015.

Homework 9. Due Mon. Jul. 6, 2015.

Problem 1 (Graded)

Prove that

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

Prove or disprove:

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

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 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 $k \in \mathbb{Z}$ and the remainder $r \in \{1, 2, 3, 4\}$.

Also don't forget that

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

Problem 3

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 4

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 5 (Graded)

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) $\varnothing \in S$, (f) $\varnothing \subseteq S$, (g) $\varnothing \in \mathcal{P}(S)$, (h) $\varnothing \subseteq \mathcal{P}(S)$

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 6

Prove that the subset relation is transitive, that is, show that

$$\text{if} \quad A \subseteq B \text{ and } B \subseteq C \quad \text{then} \quad A \subseteq C.$$

Please base your proof on the definition of the subset. Just drawing a diagram would not be a real full proof.

Many other relations have this transitivity property, for example the relation “less” ($<$) is transitive, because if $a < b$ and $b < c$ then it means that $a < c$. The equality relation ($=$) is transitive as well. However, what’s about the relation “not-equals” ($\neq$), is it transitive?