

Discrete Math 2200. Problem Set 6

Due date: Thursday, October 23, in class. Late homeworks are not accepted, except for a medical or some other university approved reason.

Unless specified otherwise, the numbering of the exercises below is as in the textbook (Rosen, ed. 6). Only even numbered exercises will be graded, but I recommend you try to do all of them for practice.

Problem 1. Prove that if p is a prime number, then the only solutions of $x^2 \equiv 1 \pmod{p}$ are integers x such that $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

Problem 2. Apply the Chinese Remainder algorithm to solve the following systems of congruences (only the system in a) will be graded):

$$\text{a) } \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{4}; \\ x \equiv 3 \pmod{5} \end{cases}$$

$$\text{b) } \begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 1 \pmod{5}. \\ x \equiv 2 \pmod{7} \end{cases}$$

Problem 3. Using the Euclidean algorithm, find an inverse of 144 modulo 233.

Problem 4.

- a) Prove that $(a + 1)^n \equiv 1 \pmod{a}$, for any positive integers $a, n, a \geq 2$.
- b) ex 27/245 (Although it is an odd numbered exercise, you must turn it in, and it will be graded. At some point, you may need to use part a)).
- c) ex 28/245.