Homework 1

Deadline: Wednesday, October 30 at 14:00.

Please submit your solutions either on paper at the beginning of the practicals or as a pdf-file in the SIS using the Study group roster (Studijní mezivýsledky) application. A maximum of 5 points can be awarded for each task. The solution to each problem must be explained. Everything that is not immediately obvious needs to be proved or quoted from lecture notes.

1. Calculate inverse 2024^{-1} in the field $\mathbb{Z}_{3733}$.

2. Using Euclid's algorithm find a pair of polynomials $u, v \in \mathbb{Z}_3[x]$ (i.e. computing modulo 3) such that $u(x^3 + 1) + v(x^2 - x) = 1$.

3. Calculate $17^{19^{777}} \bmod 70$.

4. Find all $x \in \mathbb{Z}$ satisfying all congruences
$$x \equiv -1 \pmod 7, \quad x \equiv 7 \pmod 8, \quad x \equiv 3 \pmod 9$$

5. Find all $x \in \mathbb{Z}$ satisfying $x^2 \equiv 1 \pmod{70}$.