Algebra II

# Exercises for week 11

**Problem 1.** Find a number $x \in \{1, \ldots, 273\}$ that would give remainder 1 modulo 3, remainder 2 modulo 7 and remainder 4 modulo 13.

**Problem 2.** Let $a_1, \ldots, a_n, d \in \mathbb{Z}$. Prove that the equation

$$a_1 x_1 + \cdots + a_n x_n = d$$

has an integer solution if and only if gcd of $a_1, \ldots, a_n$ divides $d$.

**Problem 3.** Find all involutions in the group $\mathbb{Z}_n$. Involutions are elements of order 2.

**Problem 4.** Solve in $\mathbb{Z}$ the equation $x^2 \equiv -17 \pmod{182}$. (Yes, CRT is handy here!)

**Problem 5** (Secret sharing, from David Stanovský)**.** To open a Very Important Safe, we need a secret nonnegative integer $s$. We have a huge prime $q$ (where $q > s$; to be exact, we choose $q$ first and then pick $s$ uniformly randomly from $\{0, 1, 2, \ldots, q-1\}$), we choose randomly (uniformly, independently) $m$ numbers $a_1, \ldots, a_m$ from $\mathbb{Z}_q$ and construct the polynomial $f(x) = a_m x^m + \cdots + a_1 x + s$.

There are $n$ bankers, call them $1, \ldots, n$. We tell banker $i$ the value $f(i)$ (modulo $q$), the number $q$ and the degree of $f$ (and nothing else). Prove that

1. Any group of $m+1$ bankers calculate $s$ and open the safe on the first try.
2. Any group of $m$ bankers can't use their information to do better than guess $s$ randomly from $\{0, \ldots, q-1\}$.