Fall 2021 – Math 328K – 55385

Homework 7

due Thursday, October 21, 14:00

Problem 1. Use the Chinese Remainder Theorem and Hensel's Lemma to find all solutions of the following polynomial equations.

a) $x^2 + x + 34 = 0$ in $\mathbb{Z}/81\mathbb{Z}$

b) $x^2 + x + 47 = 0$ in $\mathbb{Z}/2401\mathbb{Z}$

c) $x^6 - 2x^5 - 35 = 0$ in $\mathbb{Z}/6125\mathbb{Z}$

Problem 2. Find all solutions $x \in \mathbb{Z}$ of the following systems of congruences

a)

$$\begin{aligned} x &\equiv 4 \pmod{11} \\ x &\equiv 3 \pmod{17} \end{aligned}$$

b)

$$\begin{aligned} 2x &\equiv 3 \pmod{5} \\ 5x &\equiv 2 \pmod{6} \\ 3x &\equiv 4 \pmod{7} \\ x &\equiv 5 \pmod{8} \end{aligned}$$

Problem 3. Show that for any $n \in \mathbb{Z}_+$ there are n consecutive integers

$$a, a+1, \ldots, a+(n-1)$$

such that each of them is divisible by a perfect square (an integer of the form x^2, where x is an integer greater than 1).

Hint: Find an integer a such that $a + (i-1)$ is divisible by p_i^2 where p_i is the i-th prime number, for all $i \in \{1, \ldots, n\}$. That is, a is divisible by 4, $a+1$ is divisible by 9, $a+2$ is divisible by 25, etc.

Problem 4. Let $a, b \in \mathbb{Z}$ be coprime. Show that for every $c \in \mathbb{Z}$ there exists $n \in \mathbb{Z}$ such that

$$(an + b, c) = 1.$$

Hint: use the Chinese Remainder Theorem to find n such that $(an+b) \bmod p = 1 \bmod p$ for every prime factor p of c that does not divide a.

Problem 5. The goal of this problem is to prove a generalization of the Chinese Remainder Theorem for integers which are not pairwise coprime.

a) Let m_1, m_2 be any integers greater than 1, and set $M = \operatorname{lcm}(m_1, m_2)$ and $m = \gcd(m_1, m_2)$. Show that the map

$$\begin{aligned} f\colon \quad \mathbb{Z}/M\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \\ a \bmod M &\mapsto (a \bmod m_1, a \bmod m_2) \end{aligned}$$

is well–defined and injective. Show that its image is

$$f(\mathbb{Z}/M\mathbb{Z}) = \{(x_1, x_2) \mid x_1 \bmod m = x_2 \bmod m\}.$$

b) *(optional)* Let $m_1, \ldots, m_n$ be integers greater than 1 and let M be the least common multiple of all of them. Show that the map

$$\begin{aligned} \mathbb{Z}/M\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \\ a \bmod M &\mapsto (a \bmod m_1, \ldots, a \bmod m_n) \end{aligned}$$

is well–defined and injective, and that its image is

$$\{(x_1, \ldots, x_n) \mid x_i \bmod m_{ij} = x_j \bmod m_{ij} \text{ for all } 1 \le i, j \le n\},$$

where $m_{ij} = \gcd(m_i, m_j)$.

Hint: use part a) and induction.