December 1, 2025

Problem Set 11

Exercise 1. Find the smallest positive integer x such that:

$$(a)\quad \begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 5 \pmod 7. \end{cases} \qquad (b)\quad \begin{cases} x \equiv 1 \pmod{17} \\ x \equiv 1 \pmod{20} \\ x \equiv 1 \pmod{29}. \end{cases} \qquad (c)\quad \begin{cases} x \equiv 0 \pmod{11} \\ x \equiv 0 \pmod{13} \\ x \equiv 1 \pmod 2. \end{cases}$$

Exercise 2.
Show that the system of congruences

$$\begin{cases} x \equiv 4 \pmod 6 \\ x \equiv 2 \pmod 4 \\ x \equiv 5 \pmod{15}. \end{cases}$$

has no solution.

Exercise 3. Let $d_1, d_2, \ldots, d_n$ be the integers ≥ 2. Find the conditions on $d_1, d_2, \ldots, d_n$ so that the ring $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$ contains nilpotent elements.

(a) What are the nilpotent elements in the ring $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$?

(b) Let p_1, p_2, p_3 be distinct primes and $d = p_1^2 p_2^2 p_3^2$. Show that the rings $\mathbb{Z}/d\mathbb{Z}$ and $\mathbb{Z}/p_1p_2\mathbb{Z} \times \mathbb{Z}/p_2p_3\mathbb{Z} \times \mathbb{Z}/p_1p_3\mathbb{Z}$ are non-isomorphic. Use three methods: the nilpotent elements, the units and the characteristic of the two rings.

(c) Show that the rings $\mathbb{Z}/1260\mathbb{Z}$ and $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ are not isomorphic.

(d) Decompose $\mathbb{Z}/1260\mathbb{Z}$ as a direct product of rings with the maximal number of factors.

Remark: The exercises (c) and (d) show that we cannot replace the condition "pairwise coprime" by "coprime" in the Chinese remainder theorem.

Exercise 4. Recall that if K is a field, the polynomial ring $K[X]$ is a Euclidean domain: for two polynomials $P, Q \in K[X]$ with $\deg Q \geq 1$ there exist polynomials $D, R \in K[X]$ such that $P = QD + R$ where either $R = 0$, or $\deg(R) < \deg(Q)$. Use the Euclidean algorithm in $K[X]$ to find F, the *monic* (with dominant coefficient equal to 1) greatest common divisor of the given polynomials P and Q. Then use Bezout's theorem to express F in the form $F = aP + bQ$, where $a, b \in K[X]$.
(In parts (c) and (d) the notation $[a]_d$ stands for the congruence class of $a \pmod d$ in $\mathbb{Z}/d\mathbb{Z}$)

(a) $P = X^4 - 5X^2 + 4$ and $Q = X^2 - 3X + 2$, $K = \mathbb{Q}$

(b) $P = X^4 - 3X^3 + 3X^2 - X$ and $Q = 5X^2 - 2X - 3$, $K = \mathbb{Q}$

(c) $Q = X^2 + [2]_3$ and $P = X^3 + X + [1]_3$, $K = \mathbb{Z}/3\mathbb{Z}$

(d) $P = X^3 + [2]_5 X + [2]_5$ and $Q = X^3 + X^2 - [1]_5$, $K = \mathbb{Z}/5\mathbb{Z}$