December 2, 2024

Problem Set 11 Solutions

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

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

Solution 1. (a) By the Chinese remainder theorem, there exists a unique solution of these congruences modulo $2 \cdot 3 \cdot 5 \cdot 7 = 210$.
Using the method of consecutive solution of congruences, we have: $x \equiv 0(\mod 2)$ and $x \equiv 2(\mod 3)$ implies $x \equiv 2(\mod 6)$. Note that it is enough for us to find any one solution (for example $x \equiv 8(\mod 6)$ would also work). We proceed with the next congruence. Since 6 and 5 are coprime, we need to solve the equation $2 + 6t = 4 + 5s$, or $6t - 5s = 2$. We find a solution $t = s = 2$, and $x = 2 + 6t \equiv 14(\mod 30)$. Finally, with the last congruence this gives $5 + 7t = 14 + 30s$. We obtain $30s - 7t = -9$. It is easy to guess for example $s = -1, t = -3$, and then $x \equiv -30 + 14 \equiv -16(\mod 210)$. Then the smallest positive integer that solves the system is $-16 + 210 = 194$.

(b) This system is easier than it seems. Note that 1 satisfies all three congruences and is the smallest possible positive integer, so it is the solution.

(c) The numbers 11, 13 and 2 are mutually prime, and the product $11 \cdot 13 = 143$ is an odd number, therefore it satisfies all the congruences. This is also the smallest positive integer with this property.

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.

Solution 2.
If there exist a solution x, then we have in particular $x = 4 + 6k = 5 + 15l$, where k and l are integers. Then $1 = 6k - 15l$, which is impossible because the left hand side is not divisible by 3. Therefore the system has no solution.

Exercise 3. Let $d_1, d_2, \ldots, d_n$ be the integers ≥ 2. Recall that an element a in a ring A is nilpotent $a \neq 0$ and there exists $k \in \mathbb{N}$ such that $a^k = 0 \in A$. 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 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.

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

Solution 3. First let us consider the ring $\mathbb{Z}/d\mathbb{Z}$ for $d \geq 2$. We will show that it has a nontrivial nilpotent element if and only if d is divisible by a square of a prime. Indeed, suppose that $d = p^2 m$, where $m \in \mathbb{Z}_+$. Then $pm \cdot pm = p^2 m^2 \equiv 0(\mod d)$. On the other hand, suppose that the prime factorization of d is square-free: $d = p_1 p_2 \ldots p_k$. Then d divides a^k if and only if d divides a, which means that $a \equiv 0(\mod d)$.
Now for the ring $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$ to have nontrivial nilpotent elements it is necessary and sufficient that at least one of $d_1, d_2, \ldots, d_n$ would be divisible by a square of a prime. Then if $t \in \mathbb{Z}/d_i\mathbb{Z}$ is nilpotent, so that $t^k = 0 \in \mathbb{Z}/d_i\mathbb{Z}$, then $(0, \ldots t, \ldots 0)^k = 0 \in \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$.

(a) The nilpotent elements in this ring are $(0,0,2)$, $(0,0,4)$, $(0,0,6)$.

(b) For questions (b) and (c) we can use the statement proven in class: $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z}$ if and only if $\gcd(n,m) = 1$. However, in these exercises we want to compare the number of nilpotent and invertible elements and the characteristics of the two rings.
The ring $\mathbb{Z}/d\mathbb{Z}$ contains nontrivial nilpotent elements, for example $x = p_1p_2p_3$: $x^2 \equiv 0(\mod d)$. However, the ring $\mathbb{Z}/p_1p_2\mathbb{Z}\times\mathbb{Z}/p_2p_3\mathbb{Z}\times\mathbb{Z}/p_1p_3\mathbb{Z}$ contains no nilpotent elements because none of the rings $\mathbb{Z}/p_1p_2\mathbb{Z}$, $\mathbb{Z}/p_2p_3\mathbb{Z}$, $\mathbb{Z}/p_1p_3\mathbb{Z}$ does. One can also compare the number of units: We have $\phi(d) = (p_1^2 - p_1)(p_2^2 - p_2)(p_3^2 - p_3)$ in the ring $\mathbb{Z}/d\mathbb{Z}$, and $\phi(p_1p_2)\phi(p_2p_3)\phi(p_1p_3) = (p_1-1)^2(p_2-1)^2(p_3-1)^2$ units in the ring $\mathbb{Z}/p_1p_2\mathbb{Z}$, $\mathbb{Z}/p_2p_3\mathbb{Z}$, $\mathbb{Z}/p_1p_3\mathbb{Z}$. Clearly, $\phi(d) > \phi(p_1p_2)\phi(p_2p_3)\phi(p_1p_3)$. To compare the characteristic of the rings, we compute $\tau(\mathbb{Z}/d\mathbb{Z}) = d = p_1^2p_2^2p_3^2$, and $\tau(\mathbb{Z}/p_1p_2\mathbb{Z} \times \mathbb{Z}/p_2p_3\mathbb{Z} \times \mathbb{Z}/p_1p_3\mathbb{Z}) = lcm(p_1p_2, p_2p_3, p_3p_1) = p_1p_2p_3 = \sqrt{d}$.

(c) We have $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$. The ring $\mathbb{Z}/1260\mathbb{Z}$ contains nontrivial nilpotent elements, for example $210 = 2 \cdot 3 \cdot 5 \cdot 7$: we have $210^2 = 44100 = 35 \cdot 1260$. But the direct product ring $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ has no nilpotent elements, because each of 14, 30, 3 is square-free. Therefore the rings cannot be isomorphic.
Alternatively, we can compare the characteristic of the rings. We have $\mathrm{char}(\mathbb{Z}/1260\mathbb{Z}) = 1260$. For the direct product of rings, we have $\mathrm{char}(\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) = \mathrm{lcm}(14, 30, 3) = 210$. Since the rings have different characteristics, they are not isomorphic.

(d) By the Chinese remainder theorem, if a set of integers $d_1, d_2, \ldots, d_n$ are pairwise mutually prime, then there is a ring isomorphism

$$\mathbb{Z}/(d_1 \ldots d_n)\mathbb{Z} \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}.$$

In our case, we have

$$\mathbb{Z}/1260\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z},$$

this is the maximal number of factors that correspond to mutually pairwise prime integers.

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 (mod)d in $\mathbb{Z}/d\mathbb{Z}$)

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

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

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

(d) $P = X^3 + [2]_5X + [2]_5, Q = X^3 + X^2 - [1]_5$, $K = \mathbb{Z}/5\mathbb{Z}$

Solution 4. (a) We have

$$X^4 - 5X^2 + 4 = (X^2 - 3X + 2) \cdot (X^2 + 3X + 2) + 0,$$

so $\gcd(P, Q) = Q = X^2 - 3X + 2$.

As Bézout coefficients we have:

$$X^2 - 3X + 2 = 0 \cdot (X^4 - 5X^2 + 4) + 1 \cdot (X^2 - 3X + 2).$$

(b) We have

$$X^4 - 3X^3 + 3X^2 - X = (5X^2 - 2X - 3) \cdot \left(\frac{X^2}{5} - \frac{13X}{25} + \frac{64}{125}\right) + \left(-\frac{192X}{125} + \frac{192}{125}\right).$$

The Euclidean algorithm terminates in the next step:

$$5X^2 - 2X - 3 = \left(-\frac{192X}{125} + \frac{192}{125}\right) \cdot \left(-\frac{625X}{192} - \frac{125}{64}\right) + 0$$

Hence the monic representative for $\gcd(P, Q)$ is

$$-\frac{125}{192} \cdot \left(-\frac{192X}{125} + \frac{192}{125}\right) = X - 1.$$

As Bézout coefficients we have:

$$\begin{aligned} X-1 &= -\frac{125}{192}\cdot\left((X^4-3X^3+3X^2-X)-(5X^2-2X-3)\cdot\left(\frac{X^2}{5}-\frac{13X}{25}+\frac{64}{125}\right)\right) \\ &= \left(-\frac{125}{192}\right)\cdot(X^4-3X^3+3X^2-X)+\left(\frac{25X^2}{192}-\frac{65X}{192}+\frac{64}{192}\right)\cdot(5X^2-2X-3). \end{aligned}$$

(c) We use the Euclidean algorithm to find $\gcd(P(X),Q(X))$ where $P(X)=X^3+X+[1]_3$ and $Q(X)=X^2+[2]_3$. By the Euclidean division of $P(X)$ by $Q(X)$ we have:

$$(X^3+X+[1]_3)=(X^2+[2]_3)\cdot X+([2]_3X+[1]_3),$$

and so $S_1(X)=X$ et $R_1(X)=[2]_3X+[1]_3$. Since $R_1(X)$ is nonzero, we divide $Q(X)$ by $R_1(X)$:

$$X^2+[2]_3=([2]_3X+[1]_3)\cdot([2]_3X+[2]_3)+[0]_3,$$

therefore $S_2(X)=[2]_3X+[2]_3$ et $R_2(X)=[0]_3$. Since $R_2(X)$ is a zero polynomial, the algorithm terminates.

The last nonzero remainder is $R_1(X)=[2]_3X+[1]_3$. To obtain a monic polynomial, we multiply it by $[2]_3$ which gives $X+[2]_3$. So $\gcd(P(X),Q(X))=X+[2]_3$.

The Bezout's theorem gives: $X+[2]_3=[2]_3\cdot((X^3+X+[1]_3)-X\cdot(X^2+[2]_3))=[2]_3\cdot(X^3+X+[1]_3)+X\cdot(X^2+[2]_3)$.

(d) We use the Euclidean algorithm to find $\gcd(P(X),Q(X))$ where $P(X)=X^3+[2]_5X+[2]_5$ and $Q(X)=X^3+X^2+[4]_5$. By the Euclidean division of $P(X)$ by $Q(X)$ we have:

$$X^3+[2]_5X+[2]_5=(X^3+X^2+[4]_5)\cdot[1]_5+(-X^2+[2]_5X-[2]_5),$$

and so $S_1(X)=[1]_5$ et $R_1(X)=-X^2+[2]_5X-[2]_5=[4]_5X^2+[2]_5X+[3]_5$. SInce $R_1(X)$ is nonzero, we proceed with the Euclidean division of $Q(X)$ by $R_1(X)$:

$$X^3+X^2+[4]_5=([4]_5X^2+[2]_5X+[3]_5)\cdot([4]_5X+[2]_5)+[4]_5X+[3]_5,$$

and therefore $S_2(X)=[4]_5X+[2]_5$ and $R_2(X)=[4]_5X+[3]_5$. SInce $R_2(X)$ is again nonzero, we continue with the Euclidean division of $R_1(X)$ by $R_2(X)$:

$$[4]_5X^2+[2]_5X+[3]_5=([4]_5X+[3]_5)\cdot(X+[1]_5)+[0]_5,$$

and therefore $S_3(X)=X+[1]_5$ and $R_3(X)=[0]_5$. Now $R_3(X)$ is zero, and the algorithm terminates. The last nonzero remainder is $R_2(X)=[4]_5X+[3]_5$. To obtain a monic polynomial, we multiply it by $[4]_5$ which gives $X+[2]_5$. So $\gcd(P(X),Q(X))=X+[2]_5$.

We read the Euclidean algorithm backwards to obtain the Bezout's coefficients :

$$\begin{aligned} X+[2]_5 &= [4]_5\cdot((X^3+X^2+[4]_5)-([4]_5X^2+[2]_5X+[3]_5)\cdot([4]_5X+[2]_5)) \\ &= [4]_5\cdot((X^3+X^2+[4]_5)-((X^3+[2]_5X+[2]_5)-(X^3+X^2+[4]_5))\cdot([4]_5X+[2]_5)). \end{aligned}$$