1) [10 points] Find the remainder of $493438 + 76584576 \cdot 47300272^{1000}$ when divided by 5.

Solution. We have:

$$\begin{aligned} 493438 &\equiv 3 \pmod 5, \\ 76584576 &\equiv 1 \pmod 5, \\ 47300272 &\equiv 2 \pmod 5. \end{aligned}$$

Also note that

$$2^2 = 4 \equiv -1 \Longrightarrow 2^{1000} \equiv \left(2^2\right)^{500} \equiv (-1)^{500} = 1 \pmod 5.$$

Hence:

$$493438 + 76584576 \cdot 47300272^{1000} \equiv 3 + 1 \cdot 2^{1000} \equiv 3 + 1 \cdot 1 = 4 \pmod 5.$$

□

2) [10 points] Let $n \in \mathbb{Z}$. Prove that $(n, n+1) = 1$.

[**Note:** This was a HW problem.]

Proof. If $d \mid n$ and $d \mid (n+1)$, then $d \mid (n+1) - n = 1$, by the Basic Lemma, and thus the only common divisors are ± 1, and the GCD is 1.

[Alternatively, one can also do it using the "converse" of Bezout's Theorem for when we get 1 as a linear combination: we have that

$$1 = 1 \cdot (n+1) + (-1) \cdot n.$$

So, we get $(n, n+1) = 1$.]

□

3) [10 points] Find all $x \in \mathbb{Z}$ satisfying [simultaneously]:

$$x \equiv 1 \pmod{7},$$
$$x \equiv 4 \pmod{11}.$$

If there is no such x, simply justify why.

Solution. The first congruence gives $x = 7k+1$. Substituting in the second we get $7k+1 \equiv 4 \pmod{11}$, or $7k \equiv 3 \pmod{11}$. Now $2 \cdot 11 + (-3) \cdot 7 = 1$. So, $k \equiv -9 \equiv 2 \pmod{11}$, i.e., $k = 2 + 11l$ for $l \in \mathbb{Z}$.

Thus, $x = 7k + 1 = 7(2 + 11l) + 1 = 15 + 77l$, for $l \in \mathbb{Z}$. □

4) [10 points] Prove that the only subring of $\mathbb{F}_p$ [i.e., of $\mathbb{Z}/p\mathbb{Z}$] is itself.

[**Note:** It was a HW problem that the only subring of $\mathbb{Z}$ was itself. This is similar.]

Proof. Let S be a subring of $\mathbb{F}_p$. Then, $1 \in S$ by definition of subring. Since S is closed under addition, we have that $2 = 1 + 1$, $3 = 2 + 1$, ..., $p = (p - 1) + 1 = 0$, are all in S. But these are all the elements of $\mathbb{F}_p$, so $S = \mathbb{F}_p$.

Since S was an arbitrary subring, $\mathbb{F}_p$ itself is the only subring.

□

5) Below are the factorization of $f, g \in \mathbb{F}_3[x]$ into distinct irreducibles.

$$f = x \cdot (x + 1)^3 \cdot (x^2 + 1) \cdot (x^2 + x + 2)^4$$
$$g = 2 \cdot x^2 \cdot (x + 2)^2 \cdot (x^2 + 1)^3 \cdot (x^2 + x + 2)$$

(a) [4 points] Does $g \mid f$? [*Justify!*]

Solution. No, since the power of the irreducible x dividing g [namely, 2] is greater than the power of x dividing f [namely, 1]. □

(b) [3 points] Give the factorization of the $\gcd(f, g)$.

Solution.

$$(f, g) = x \cdot (x^2 + 1) \cdot (x^2 + x + 2).$$

□

(c) [3 points] Give the factorization of $\operatorname{lcm}(f, g)$.

Solution.

$$[f, g] = x^2 \cdot (x + 1)^3 \cdot (x + 2)^2 \cdot (x^2 + 1)^3 \cdot (x^2 + x + 2)^4.$$

□

6) Examples:

(a) [5 points] Give an example of an *infinite* commutative ring which is *not* a domain.

Solution. We have that $\mathbb{I}_4 = \mathbb{Z}/4\mathbb{Z}$ is not a domain, so $\mathbb{I}_4[x]$ is not a domain, and, as any polynomial ring, it's infinite. $\square$

(b) [5 points] Give an example of a field properly containing $\mathbb{R}$ [i.e., contains $\mathbb{R}$ but it is not $\mathbb{R}$ itself], but not containing $\mathbb{C}$. [Note that this excludes $\mathbb{C}$ itself.]

Solution. $\mathbb{R}(x)$ works. $\square$

7) Determine if the polynomials below are irreducible or not in the corresponding polynomial ring. *Justify each answer!*

(a) [3 points] $f = x^{2018} - x + 2018$ in $\mathbb{R}[x]$.

Solution. It's *reducible*, as it's degree is greater than 2 [as we are in $\mathbb{R}[x]$]. $\square$

(b) [3 points] $f = x + \pi$ in $\mathbb{C}[x]$.

Solution. Since it has degree 1, it is irreducible. $\square$

(c) [3 points] $f = x^7 + 110x^5 + x^2 + 97x$ in $\mathbb{F}_{521}[x]$.

Solution. Reducible, as x is a proper factor. $\square$

(d) [3 points] $f = 3x^7 + 6x^6 - 9x^4 + 120x^3 - 15x + 2$ in $\mathbb{Q}[x]$.

Solution. Irreducible, by the inverse Eisenstein's Criterion. $\square$

(e) [4 points] $f = 64x^3 - 3x^2 + 32x + 30001$ in $\mathbb{Q}[x]$.

Solution. Reducing modulo 3, we get $\bar{f} = x^3 + 2x + 1$. Now $\bar{f}(0) = \bar{f}(1) = \bar{f}(2) = 1$. Since $\deg(\bar{f}) = 3$ and it has no roots, $\bar{f}$ is irreducible, and hence f is irreducible. $\square$

(f) [4 points] $f = x^3 + 2x^2 - 2x - 1$ in $\mathbb{Q}[x]$.

Solution. By the rational root test, the only possible roots are ± 1. Since $f(1) = 0$, f is reducible. $\square$

8) Let $\sigma, \tau \in S_9$ be given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 5 & 4 & 3 & 9 & 2 & 8 & 6 \end{pmatrix} \quad \text{and} \quad \tau = (1\ 3\ 8)(2\ 4\ 5\ 9).$$

(a) [3 points] Write the *complete* factorization of σ into disjoint cycles.

Solution. $\sigma = (1\,7\,2)(3\,5)(4)(6\,9)(8)$. □

(b) [3 points] Compute σ^{-1}. [Your answer can be in any form.]

Solution. $\sigma = (2\,7\,1)(5\,3)(4)(9\,6)(8)$, or

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 5 & 4 & 3 & 9 & 1 & 8 & 6 \end{pmatrix}$$

□

(c) [3 points] Compute $\tau\sigma$. [Your answer can be in any form.]

Solution. $\tau\sigma = (1\,7\,4\,5\,8)(2\,3\,9\,6)$, or

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 9 & 5 & 8 & 2 & 4 & 1 & 6 \end{pmatrix}$$

□

(d) [3 points] Compute $\sigma\tau\sigma^{-1}$. [Your answer can be in any form.]

Solution. $\sigma\tau\sigma^{-1} = (7\,5\,8)(1\,4\,3\,6)$. □

(e) [3 points] Write τ as a product of transpositions.

Solution. $\tau = (1\,8)(1\,3)(2\,9)(2\,5)(2\,4)$. □

(f) [2 points] Compute $\text{sign}(\tau)$.

Solution. Using the number of transpositions: $\text{sign}(\tau) = (-1)^5 = -1$.
[Alternatively, noticing that the complete decomposition of τ is $\tau = (1\ 3\ 8)(2\ 4\ 5\ 9)(6)(7)$, the definition gives us $\text{sign}(\tau) = (-1)^{9-4} = (-1)^5 = -1$.] □

(g) [3 points] Compute $|\tau|$ (the order of τ in S_n).

Solution. $|\tau| = \text{lcm}(3, 4) = 12$. □