1) Remainders:

(a) [5 points] Find the remainder of 2^{87} when divided by 7.

Solution. We have that $87 = 3 + 5 \cdot 7^1 + 1 \cdot 7^2$ and $3 + 5 + 1 = 9 = 2 + 1 \cdot 7$. So,

$$2^{87} \equiv 2^{3+5+1} = 2^9 \equiv 2^{2+1} = 2^3 = 8 \equiv 1 \pmod 7.$$

□

(b) [5 points] Find the remainder of $47300272^{63745765}$ when divided by 3.

Solution. We have that

$$47300272 \equiv 4 + 7 + 3 + 0 + 0 + 2 + 7 + 2 \equiv 1 + 1 + 2 + 1 + 2 \equiv 1 \pmod 3.$$

So,

$$47300272^{63745765} \equiv 1^{63745765} \equiv 1 \pmod 3.$$

□

2) [10 points] Let $a, b, c \in \mathbb{Z} \setminus \{0\}$ and $d = \gcd(a, b)$. Prove that $\gcd(a, b, c) = \gcd(d, c)$. [**Hint:** Prove first that n is a common divisor of a, b and c iff it is a common divisor of d and c.]

Proof. Suppose $n \mid a, b, c$. In particular, $n \mid a, b$ and hence [by a result seen in class, immediate consequence of Bezout's Theorem] $n \mid d$. Also, clearly $n \mid c$, so $n \mid d, c$.
Now if $n \mid d, c$, then $n \mid d$. Since $d \mid a, b$, we also have that $n \mid a, b$. Therefore $n \mid a, b, c$.
So,

$$\{n \in \mathbb{Z} \;:\; n \mid a, b, c\} = \{n \in \mathbb{Z} \;:\; n \mid d, c\} = \gcd d, c,$$

and so

$$\gcd(a, b, c) = \max\{n \in \mathbb{Z} \;:\; n \mid a, b, c\} = \max\{n \in \mathbb{Z} \;:\; n \mid d, c\} = \gcd d, c.$$

□

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

$$\begin{aligned} 3x &\equiv 1 \pmod{7}, \\ x &\equiv 4 \pmod{11}. \end{aligned}$$

If there is no such x, simply justify why.

Solution. The second equation gives us that $x = 11k + 4$, for $k \in \mathbb{Z}$. Replacing in the first we get

$$33k + 12 \equiv 1 \pmod{7},$$

i.e.,

$$5k \equiv -11 \equiv 3 \pmod{7}.$$

Since $3 \cdot 5 = 15 \equiv 1 \pmod{7}$, multiplying by 3 we get

$$k \equiv 9 \equiv 2 \pmod{7}.$$

So, $k = 7l + 2$. Replacing in the original equation we get $x = 77l + 26$, for $l \in \mathbb{Z}$. □

4) [10 points] Let F be a field and $f, g, h \in F[x]$ with $f \mid g$. Prove that $f \mid (g + h)$ iff $f \mid h$. [**Note:** This is simply the *Basic Lemma* for polynomials.]

Proof. Let $g = q \cdot f$.
Assume that $f \mid (g + h)$. Then, $(g + h) = q' \cdot f$. So,

$$h = q' \cdot f - g = q' \cdot f - q \cdot f = (q' - q) \cdot f.$$

Since $(q' - q) \in F[x]$, we have that $f \mid h$.

Now, assume that $f \mid h$. Then, $h = q'' \cdot f$. But then,

$$(g + h) = q \cdot f + q'' \cdot f = (q + q'') \cdot f.$$

Since $(q + q'') \in F[x]$, we have that $f \mid (g + h)$.

□

5) Examples:

(a) [5 points] Give an example of an *infinite field* F such that $6 \cdot a = 0$ for all $a \in F$. [**Hint:** Can you find a finite example first?]

Solution. $\mathbb{F}_2(x)$ [or $\mathbb{F}_3(x)$]. □

(b) [5 points] Give an example of a ring R that contains $\mathbb{C}[x]$ as a *proper* subring [i.e., $\mathbb{C}[x] \subseteq R$, $\mathbb{C}[x]$ a subring of R, but $\mathbb{C}[x] \neq R$].

Solution. $\mathbb{C}[x, y]$ or $\mathbb{C}(x)$. □

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

(a) [4 points] $f = x^2 - \sqrt{7}x + 2$ in $\mathbb{R}[x]$.

Solution. We have $\Delta = (-\sqrt{7})^2 - 4 \cdot 1 \cdot 2 = -1 < 0$. So, the polynomial has no root in $\mathbb{R}$. Since the degree is 2, it is irreducible. □

(b) [4 points] $f = x^7 + \mathrm{e}\, x^5 - \pi\, x^2 + \sqrt{5}\, x + \log(2)$ in $\mathbb{C}[x]$.

Solution. Since every non-constant polynomial with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$, f has a root. Since $\deg(f) > 1$, it is reducible. □

(c) [4 points] $f = \overline{211}\, x - \overline{301}$ in $\mathbb{F}_{521}[x]$.

Solution. The polynomials has degree one, so it is irreducible. □

(d) [4 points] $f = x^7 + 4x^6 - 8x^4 + 120x^3 - 2x + 14$ in $\mathbb{Q}[x]$.

Solution. Irreducible by Eisenstein's Criterion for $p = 2$. □

(e) [5 points] $f = 4x^3 + 3x^2 - 34x + 3001$ in $\mathbb{Q}[x]$.

Solution. Reducing modulo 3 we get $\bar{f} = x^3 - x + \bar{1}$. Now, $\bar{f}(\bar{0}) = \bar{f}(\bar{1}) = \bar{f}(\bar{2}) = 1$. So, $\bar{f}$ has no roots in $\mathbb{F}_3$, and since $\deg(\bar{f}) = 3$, it is irreducible. So, f is also irreducible. □

(f) [4 points] $f = x^6 - 2x^5 + x^4 - 3x^2 + x + 2$ in $\mathbb{Q}[x]$.

Solution. Using the *Rational Root Test* we see that 1 is a root. Since $\deg(f) > 1$, it is reducible. □

7) 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) [5 points] Write the *complete* factorization of σ into disjoint cycles.

Solution.

$$\sigma = (1\ 7\ 2)(3\ 5)(4)(6\ 9)(8)$$

□

(b) [4 points] Compute σ^{-1}. [Your answer can be in any form.]

Solution.

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

□

(c) [4 points] Compute $\tau\sigma$. [Your answer can be in any form.]

Solution.

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

□

(d) [4 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) [4 points] Write τ as a product of transpositions.

Solution.

$$\tau = (1\ 8)(1\ 3)(2\ 9)(2\ 5)(2\ 4)$$

□

(f) [4 points] Compute $\text{sign}(\tau)$.

Solution. $\text{sign}(\tau) = (-1)^5 = -1$ or $\text{sign}(\tau) = (1)^{9-4} = -1$. □