1) [10 points] Find all integers x such that

$$\begin{aligned} x &\equiv 2 \pmod{9}, \\ x &\equiv 4 \pmod{11}. \end{aligned}$$

[Of course, x must satisfy *both* congruences.]

Solution. The first congruence tell us that $x = 9k + 2$ for some $k \in \mathbb{Z}$. So, we get $9k \equiv 2 \pmod{11}$. As $5\cdot 9 - 4\cdot 11 = 1$, we can multiply the congruence by 5 and get $k \equiv 10 \pmod{11}$. So, $k = 10 + 11l$ and hence $x = 92 + 99l$ for $l \in \mathbb{Z}$. □

2) [10 points] Let $a, b \in \mathbb{Z} \setminus \{0\}$ and $d = (a, b)$. Prove that $(a/d, b/d) = 1$.

Proof. By *Bezout's Theorem*, there are $r, s \in \mathbb{Z}$ such that

$$ra + sb = d.$$

Dividing by d [and noticing $a/d, b/d \in \mathbb{Z}$], we get

$$r\,\frac{a}{d} + s\,\frac{b}{d} = 1.$$

Hence, by Problem 1.56 from the book [which I did in class], we have $(a/d, b/d) = 1$. □

3) [10 points] Prove that if $x, y, z \in \mathbb{Z}$, none divisible by 3, then $x^2 + y^2 \neq z^2$.

Proof. If $a \in \mathbb{Z}$ is not divisible by 3, then $a \equiv \pm 1 \pmod{3}$. So, $a^2 \equiv 1 \pmod{1}$. Thus, $x^2 \equiv y^2 \equiv z^2 \equiv 1$. If $x^2 + y^2 = z^2$, then $x^2 + y^2 \equiv z^2 \pmod{3}$, but that would mean $1 + 1 = 2 \equiv 1 \pmod{3}$, a contradiction. □

4) [10 points] Let R be a *domain*. Prove that if $f \in U(R[x])$, then $f \in U(R)$ [i.e., f is a constant polynomial and a unit of R].

[**Note:** This was proved in class.]

Proof. Let $f \in U(R[x])$. Then, there is $g \in R[x]$ such that $fg = 1$. Thus $\deg(fg) = \deg(1) = 0$. Since R is a domain, we have that $\deg(fg) = \deg(f) + \deg(g) = 0$. So, $\deg(f) = \deg(g) = 0$ and hence $f, g \in R \setminus \{0\}$. Since $fg = 1$, we have that $f, g \in U(R)$. $\square$

5) The statements below are *false*. Give a counter example to each one.

(a) [3 points] If F is a field, and $a \in F$, then $a = -a$ only if $a = 0$.

Solution. In $\mathbb{F}_2$ we have that $-1 = 1$, but $1 \neq 0$. $\square$

(b) [3 points] If R is a ring and $f \in R[x]$, then $\deg(f^2) = 2\deg(f)$.

Solution. In $\mathbb{I}_4[x]$, we have that if $f = 2x$, then $\deg(f) = 1$. But $f^2 = 4x^2 = 0$, so $\deg(f^2) = -\infty \neq 2$. $\square$

(c) [4 points] If R is a ring and $f \in R[x]$ with $\deg(f) = n$, then f has at most n roots in R.

Solution. In $\mathbb{I}_4[x]$, we have that if $f = 2x$, then $\deg(f) = 1$ and $f(0) = f(2) = 0$, so f has 2 roots in $R = \mathbb{I}_4$. $\square$

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

(a) [3 points] $f = x^5 - 4x^4 + 10x^3 + 8x^2 - 2x + 6$ in $\mathbb{Q}[x]$.

Solution. Irreducible by the *Eisenstein's Criterion* with $p = 2$. $\square$

(b) [4 points] $f = 6666667x^3 - 33333334x + 99999991$ in $\mathbb{Q}[x]$.

Solution. Reducing modulo 3 we get $\bar{f} = x^3 - x + 1 \in \mathbb{F}_3[x]$. Now $\bar{f}(0) = \bar{f}(1) = \bar{f}(2) = 1 \neq 0$. So, $\bar{f}$ has no roots in $\mathbb{F}_3$ and since it is of degree 3, it is irreducible in $\mathbb{F}_3[x]$. So, f must be irreducible in $\mathbb{Q}[x]$. $\square$

(c) [3 points] $f = 3x^4 - 6x^3 + 9x - 1$ in $\mathbb{Q}[x]$.

Solution. Irreducible by the *Reversed Eisenstein's Criterion* with $p = 3$. $\square$

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

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

(a) [4 points] Write the *complete* factorization of σ into disjoint cycles.

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

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

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

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

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

(d) [4 points] Compute $\sigma\tau\sigma^{-1}$. [Your answer can be in any form.]

Solution. $\sigma\tau\sigma^{-1} = (5\ 9\ 8\ 7)(3\ 2\ 1\ 6)$. □

(e) [3 points] Compute $\text{sign}(\tau)$.

Solution. $\text{sign}(\tau) = (-1)^6 = 1$. □

(f) [3 points] Compute $|\tau|$.

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

8) [10 points] Let G be a group, H and K finite subgroups of G such that $(|H|, |K|) = 1$. Prove that $H \cap K = \{1\}$.

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

Proof. Let $x \in H \cap K$. Since $x \in H$, we have that $|x| \mid |H|$ by Corollary 2.85. Similarly, since $x \in K$, we have that $|x| \mid |K|$. Since $|x|$ is a common divisor of $|H|$ and $|K|$, which are relatively prime, we must have $|x| = 1$, i.e., $x = 1$. Since x was arbitrary, 1 is the only element in $H \cap K$. [Note that clearly $1 \in H \cap K$, as $1 \in H$ and $1 \in K$, since H and K are subgroups of G.] □

9) [10 points] Let G be a group and suppose that $(ab)^3 = 1$ for some $a, b \in G$. Prove that $(ba)^3 = 1$.

[**Note:** There is nothing special about the exponent 3. After you do this, you should see how to do it for any exponent.]

Proof. We have that

$$(ab)(ab)(ab) = 1.$$

Or,

$$a(ba)(ba)b = 1.$$

Multiply on the left by b, we get:

$$(ba)(ba)(ba)b = b \cdot 1 = b.$$

Now, multiply on the right by b^{-1}:

$$(ba)^3 = (ba)(ba)(ba) = 1.$$

□