1) [10 points] Find the remainder of 2^{2020} when divided by 7.

Solution. We have:

$$\begin{aligned} 2020 &= 288 \cdot 7 + 4 \\ 288 &= 41 \cdot 7 + 1 \\ 41 &= 5 \cdot 7 + 6 \\ 5 &= 0 \cdot 7 + 5. \end{aligned}$$

So, $2020 = 4 + 1 \cdot 7 + 6 \cdot 7^2 + 5 \cdot 7^3$. Then, since $2^7 \equiv 2 \pmod 7$, we have:

$$2^{2020} \equiv 2^{4+1+6+5} = 2^{16} = 2^{2+2\cdot 7} \equiv 2^{2+2} = 16 \equiv 2 \pmod 7.$$

Alternatively, since we have $2^6 \equiv 1 \pmod 7$ and $2020 = 366 \cdot 6 + 4$, we have:

$$2^{2020} = 2^{366\cdot 6+4} = (2^6)^{366} \cdot 2^4 \equiv 1^{366} \cdot 2^4 = 2^4 = 16 \equiv 2 \pmod 7.$$

□

2) [10 points] Find all $x \in \mathbb{Z}$ satisfying [simultaneously]:

$$\begin{aligned} x &\equiv 3 \pmod 5, \\ 2x &\equiv 3 \pmod 7. \end{aligned}$$

If there is no such x, simply justify why.

Solution. The first equation gives $x = 3+5n$, for $n \in Z$. Substituting in the second equation, we get $2(3+5n) \equiv 3 \pmod 7$, i.e., $10n \equiv -3 \pmod 7$, or $3n \equiv 4 \pmod 7$.

Now, we have $1 = (-2) \cdot 3 + 1 \cdot 7$, so $n \equiv -8 \equiv 6 \pmod 7$. Thus, $n = 6 + 7m$ for $m \in \mathbb{Z}$. Thus, we have $x = 3 + 5n = 3 + 5 \cdot (6 + 7m) = 33 + 35m$ for $m \in \mathbb{Z}$. □

3) [10 points] Prove that if $\gcd(r, m) = \gcd(r', m) = 1$, then $\gcd(rr', m) = 1$.

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

Proof. Suppose $\gcd(rr', m) = d \neq 1$. Then, there is some prime p prime such that $p \mid d$, and since $d \mid rr', m$, we have $p \mid rr', m$. Now, since p is prime, by Euclid's Lemma, we have $p \mid r$ or $p \mid r'$. We may assume, without loss of generality, that $p \mid r$. But then, $p \mid r, m$ and so $\gcd(rr', m) \geq p > 1$, a contradiction.

Alternatively, if $\gcd(r, m) = \gcd(r', m) = 1$, then there are $a, b, c, d \in \mathbb{Z}$ such that:

$$ar + bm = 1, \qquad cr' + dm = 1.$$

Multiplying them, we get

$$1 = (ar + bm) \cdot (cr' + dm) = ac \cdot rr' + (adr + bcr' + bdm) \cdot m.$$

Since $ac, (adr + bcr' + bdm) \in \mathbb{Z}$, we have that $\gcd(rr', m) = 1$. $\square$

4) [10 points] Let F be a field and $f(x) \in F[x]$. Prove that if $f(x^2)$ is irreducible, then so is $f(x)$.

Proof. We prove the contrapositive. Suppose that $f = g \cdot h$, with $\deg(g), \deg(h) > 0$. Then, $f(x^2) = g(x^2) \cdot h(x^2)$. Since $\deg(g(x^2)) = 2 \cdot \deg(g) > 0$ and $\deg(h(x^2)) = 2 \cdot \deg(h) > 0$, we have that $f(x^2)$ is reducible as well. $\square$

5) Suppose that F is a field, $a \in F$ and $f \in F[x]$. Prove that if $(x - a) \mid f$ and $(x - a) \mid f'$ [where f' is the *derivative* of f], then $(x - a)^2 \mid f$.

[**Note:** This was a HW problem. **Hint:** You can use the *Basic Lemma* for polynomials: Assume that $f \mid g$. Then, $f \mid (g + h)$ iff $f \mid h$.]

Proof. Since $(x - a) \mid f$, we have that $f = (x - a) \cdot g$, for some $g \in F[x]$. Then, by the product rule, we have that $f' = g + (x - a) \cdot g'$.

Now, by the Basic Lemma, since $(x - a) \mid f'$ and $(x - a) \mid (x - a) \cdot g'$, we have that $(x - a) \mid g$. So, $g = (x - a) \cdot h$, for some $h \in F[x]$ and therefore $f = (x - a) \cdot g = (x - a)^2 \cdot h$, i.e., $(x - a)^2 \mid f$. $\square$

6) Examples:

(a) [5 points] Give an example of an *infinite* field F such that for all $a \in F$, we have $2020 \cdot a = 0$.

Solution. $\mathbb{F}_2(x)$ works. $\square$

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

Solution. $(\mathbb{Z}/4\mathbb{Z})[x]$ works. $\square$

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

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

Solution. We have that $\Delta = (-2)^2 - 4 \cdot 1 \cdot 3 = -8 < 0$ [no real roots], so f is irreducible. $\square$

(b) [3 points] $f = x^{2020} - 2020$ in $\mathbb{C}[x]$.

Solution. Since $\mathbb{C}$ is algebraically closed and $\deg(f) > 1$, we have that f is reducible. $\square$

(c) [3 points] $f = 137x + 389$ in $\mathbb{F}_{521}[x]$.

Solution. Since $\deg(f) = 1$, it is irreducible. $\square$

(d) [3 points] $f = x^5 + 400x^4 - 10x^3 + 120x^2 - 3000x + 310$ in $\mathbb{Q}[x]$.

Solution. We have $310 \equiv 10 \equiv 2 \not\equiv 0 \pmod 4$, so $4 \nmid 310$. Then, by Eisenstein's Criterion for $p = 2$, we have that f is irreducible. $\square$

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

Solution. We try the rational root test. The only possible roots are ± 1. But $f(1) = 2 \neq 0$ and $f(-1) = 4 \neq 0$. So, f has no rational root. Since $\deg(f) = 3$, we get that f is irreducible. $\square$

(f) [4 points] $f = 30003x^3 - 10x^2 + 11x + 30001$ in $\mathbb{Q}[x]$.

Solution. Reducing modulo $p = 2$, we have $\bar{f} = x^3 + x + 1$. Now $\bar{f}(0) = \bar{f}(1) = 1 \neq 0$. So, $\bar{f}$ has no roots in $\mathbb{F}_2$, and since it has degree 3, it is irreducible in $\mathbb{F}_2[x]$. Thus, f is irreducible in $\mathbb{Q}[x]$. $\square$

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

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

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

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

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

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

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

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

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

Solution. $\sigma\tau\sigma^{-1} = (7\ 6\ 9\ 5)(2\ 4\ 3)$. $\square$

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

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

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

Solution. $\operatorname{sign}(\tau) = (-1)^5 = -1$ [or $\operatorname{sign}(\tau) = (-1)^{9-4} = -1$]. $\square$

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

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