Problem (Problem 1)**:** Let $a_1, \dots, a_n \in \mathbb{R}$. Suppose that for each $i \in \{1, \dots, n\}$, we are given $m_i \geqslant 0$ and $m+1$ numbers $b_{i0}, \dots, b_{im_i} \in \mathbb{R}$. Use the Chinese Remainder Theorem to show that there exists a polynomial $f(x) \in \mathbb{R}[x]$ such that

$$\begin{aligned} f(a_i) &= b_{i0} \\ f'(a_i) &= b_{i1} \\ &\vdots \\ f^{(m_i)} &= b_{im_i}. \end{aligned}$$

Solution: We observe that if we take

$$f(x) = q_{01}(x)(x - a_1) + b_{10},$$

then

$$f'(x) = q_{01}(x) + q_{01}'(x)(x - a_1),$$

so that

$$f'(a_1) = q_{01}(a_1)$$

and

$$f'(x) = q_{11}(x)(x - a_1) + b_{11},$$

meaning

$$f(x) = (q_{11}(x)(x - a_1) + b_{11})(x - a_1) + b_{10}.$$

Inductively, we thus desire a solution to the system of congruences

$$\begin{aligned} f(x) &\equiv b_{10} + b_{11}(x - a_1) + \cdots + b_{1m_1}(x - a_1)^{m_1 - 1} \bmod (x - a_1)^{m_1} \\ &\equiv b_{20} + b_{21}(x - a_2) + \cdots + b_{2m_2}(x - a_2)^{m_2 - 1} \bmod (x - a_2)^{m_2} \\ &\vdots \\ &\equiv b_{n0} + b_{n1}(x - a_n) + \cdots + b_{nm_n}(x - a_n)^{m_n - 1} \bmod (x - a_n)^{m_n}. \end{aligned}$$

Since the family of ideals $\left\{\left((x - a_1)^{m_1}\right), \dots, \left((x - a_n)^{m_n}\right)\right\}$ are pairwise coprime, as the corresponding family of principal ideals $\{(x - a_1), \dots, (x - a_n)\}$ are pairwise coprime, the Chinese Remainder Theorem implies that some $f(x) \in \mathbb{R}[x]$ satisfies this system of congruences.

Problem (Problem 3)**:** Let R be a commutative ring with 1. A prime ideal $P \subseteq R$ is called minimal if there is no prime ideal $P' \subseteq R$ with $P' \subsetneq P$. Prove the existence of minimal prime ideals by applying Zorn's Lemma.

Solution: We know that R has at least one maximal ideal, and since maximal ideals are prime, we let $M \subseteq R$ be a maximal ideal, and define

$$\mathcal{P} = \left\{ P \subseteq R \,\middle|\, P \subseteq M, P \text{ is a prime ideal} \right\}$$

to be a partially ordered set ordered by containment — i.e., $P_1 \preceq P_2$ if $P_1 \supseteq P_2$. Notice that $\mathcal{P}$ is nonempty, as M is prime in R and $M \subseteq M$. Next, if $\{P_i\}_{i \in I} = \mathcal{C} \subseteq \mathcal{P}$ is a chain, we set

$$P = \bigcap_{i \in I} P_i.$$

We claim that P is prime. Let $ab \in P$; then, $ab \in P_i$ for all $i \in I$. We claim that this implies that either $a \in P_i$ for all i or $b \in P_i$ for all i. If not, then there would be some index j such that both a and b are not in P_i for all $i \geq j$. This would imply that for all $i \geq j$, $ab \notin P_i$, as each of the P_i are prime. Thus, it must be the case that either $a \in P$ or $b \in P$.

Since $\mathcal{P}$ is a nonempty partially ordered set (by containment) where every chain has an upper bound, $\mathcal{P}$ has a "maximal" (with respect to containment, so minimal) element.

Problem (Problem 4)**:**

(a) Let R, S be commutative rings with 1, and let $f\colon R \to S$ be a ring homomorphism such that $f(1_R) = 1_S$. Show that for any prime ideal $P \subseteq S$, the preimage $f^{-1}(P)$ is a prime ideal of R.

(b) Give an example of a ring homomorphism $f\colon R \to S$ with $f(1_R) = 1_S$ and a maximal ideal $M \subseteq S$ such that $f^{-1}(M)$ is not a maximal ideal of R.

Solution:

(a) Let $a, b \in R$ be such that $ab \in f^{-1}(P)$. Then, by definition of preimage, we have that $f(ab) \in P$, and since f is a ring homomorphism, $f(a)f(b) \in P$. Since P is prime, we have $f(a) \in P$ or $f(b) \in P$, so by the definition of preimage, we must have either $a \in f^{-1}(P)$ or $b \in f^{-1}(P)$. Thus, $f^{-1}(P)$ is prime.

(b) Let $R = \mathbb{Z}$ and $S = \mathbb{Q}$, with $f\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$ being the natural inclusion. Since $\mathbb{Q}$ is a field, the only maximal ideal of $\mathbb{Q}$ is $\{0\}$, but $\{0\} = f^{-1}(\{0\})$ is not maximal in $\mathbb{Z}$ since there are other proper ideals in $\mathbb{Z}$.

Problem (Problem 6)**:** Let $R = \mathbb{C}[x, y]$ be the ring of polynomials in two variables over the field of complex numbers. Let J be the ideal of R generated by $x + y^2$ and $y + x^2 + 2xy^2 + y^4$. The goal of this problem is to compute the quotient R/J, and conclude that J is a maximal ideal. For this, we set I to be the ideal generated by $x + y^2$ and use the Third Isomorphism Theorem.

(a) Consider the ring homomorphism $f\colon \mathbb{C}[x, y] \to \mathbb{C}[y]$ given by $f(x) = -y^2$ and $f(y) = y$. Show that f is surjective, and that $\ker(f) = I$.

(b) By the Third Isomorphism Theorem, $R/J \cong (R/I)/(J/I)$. Observe that this identifies J/I with $f(J)$, and compute $f(J)$ explicitly. Then, compute $R/J \cong \mathbb{C}[y]/f(J)$, and conclude that J is a maximal ideal.

Solution:

(a) We consider the identification $\mathbb{C}[x, y] \cong (\mathbb{C}[y])[x]$, and perform Euclidean division by $x + y^2$ in x, which is well-defined as $x + y^2$ is monic in x. Therefore, we get that for any $p(x, y) \in \mathbb{C}[x, y]$, we have

$$p(x, y) = q(x, y)\left(x + y^2\right) + r(x, y),$$

where since $\deg_x(r) < 1$, we have $r(x, y) \equiv r(y)$. Via the properties of the division algorithm, we observe that if we map $p(x, y) \mapsto r(y)$, then this map is well-defined, as any two such $r_1(y)$ and $r_2(y)$ that satisfy the division algorithm must have the same degree in x, which is zero, hence are equal to each other, and surjective with kernel $\left(x + y^2\right)$.

Notice then that $x \mapsto -y^2$, as $x = (1)\left(x + y^2\right) - y^2$, and $y \mapsto y$, as $y = (0)\left(x + y^2\right) + y$, implying that the map $p(x, y) \mapsto r(y)$ is exactly the map f.

(b) Observe that J is the ideal consisting of all polynomials of the form

$$p(x, y) = a(x, y)\left(x + y^2\right) + b(x, y)\left(y + x^2 + 2xy^2 + y^4\right)$$

By performing division with respect to $x + y^2$, we find that

$$\begin{aligned} p(x, y) &= \left(a(x, y) + b(x, y)\left(x + y^2\right)\right)\left(x + y^2\right) + y\left(q(x, y)\left(x + y^2\right) + r(y)\right) \\ &= \ell(x, y)\left(x + y^2\right) + yk(y), \end{aligned}$$

meaning that $f(J)$ can be expressed as

$$f(J) = \{yk(y) \mid k \in \mathbb{C}[y]\}.$$

Now, by performing division in $\mathbb{C}[y]$ by y, we find that for any $r(y) \in \mathbb{C}[y]$,

$$r(y) = yk(y) + c,$$

where $c \in \mathbb{C}$. Thus, $R/J \cong (R/I)/(J/I) \cong \mathbb{C}$, implying that J is maximal.