1. If p is a prime and $p \equiv 3 \pmod 4$, prove that one of the congruences $a^2 \equiv 2 \pmod p$ or $a^2 \equiv -2 \pmod p$ is solvable.

2. Prove that any two fields having exactly four elements are isomorphic.

3. Let K be a field that contians $\mathbb{I}_p$ as a subfield [e.g $K = \mathbb{I}_p(x)$]. For every positive integer n, show that the function $\varphi_n: K \longrightarrow K$, given by $\varphi(n) = a^{p^n}$ is a ring homomorphism.

4. If R and S are nonzero commutative rings, prove that

$$U(R \times S) = U(R) \times U(S)$$

where $U(R)$ is the group of units of R.

5. (a) Prove that $R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a domain.
(b) Prove that $R = \{\frac{1}{2}(a + b\sqrt{2}) : a, b \in \mathbb{Z}\}$ is not a domain.
(c) Using the fact that $\alpha = \frac{1}{2}(1 + \sqrt{-19})$ is a root of $x^2 - x + 5$, Prove that $R = \{a + \alpha b : a, b \in \mathbb{Z}\}$ is a domain.

6. Define $\mathbb{F}_4$ to be all 2×2 matrices of the form

$$\begin{bmatrix} a & b \\ b & a+b \end{bmatrix},$$

where $a, b \in \mathbb{I}_2$.

(a) Prove that $\mathbb{F}_4$ is a commutative ring under the usual matrix operations of addition and multiplication.
(b) Prove that $\mathbb{F}_4$ is a field with exactly four elements.

7. (a) If R is a domain, show that if a polynomial in $R[x]$ is a unit, then it is a nonzero constant polynomial.
(b) Show that the converse is true if R is a field.
(c) Show that $(2x+1)^2 = 1$ in $\mathbb{I}_4[x]$. Conclude that the hypothesis in (a) that R be a domain is necessary.

8. Let R be a commutative ring and let $f(x) \in R[x]$.
(a) $(x - a)^2 \mid f(x)$ then $x - a \mid f'(x)$ in $R[x]$.
(b) Prove that if $x - a \mid f(x)$ and $x - a \mid f'(x)$ then $(x - a)^2 \mid f(x)$.

9. Let R be an integral domain with quotient field F and let $p(x)$ be a monic polynomial in $R[x]$. Assume that $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are monic

polynomials in $F[x]$ of smaller degree than $p(x)$. Prove that if $a(x) \notin R[x]$, then R is not a Unique Factorization Domain. Deduce that $\mathbb{Z}\left[2\sqrt{2}\right]$ is not a UFD.

10. Show that the polynomial $(x-1)(x-2)\cdots(x-n)-1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$. [If the polynomial factors, consider the values of the factors at $x = 1,2,\ldots,n$.]