1. Show that the equation $x^3 - 3x + 4 = 0$ has a unique solution in $\mathbb{Z}_7$, but no solutions in $\mathbb{Z}_5$ or in $\mathbb{Z}_3$. How many are there in $\mathbb{Z}_2$?

2. Use Hensel's lemma to show that if p is a prime and $(n, p) = 1$, then the homomorphism $1 + p\mathbb{Z}_p \to 1 + p\mathbb{Z}_p$, $x \mapsto x^n$, is bijective.

3. Use Hensel's lemma to show that if p is an odd prime, then an element $\alpha \in \mathbb{Z}_p^\times$ lies in $(\mathbb{Z}_p^\times)^p$ if and only if $\alpha \bmod p^2\mathbb{Z}_p \in ((\mathbb{Z}/p^2\mathbb{Z})^\times)^p$. What happens when $p = 2$?

4. Let K be a number field, and let E/K be a Galois extension. Let $\mathfrak{q}$ be a non-zero prime ideal of $\mathcal{O}_E$ lying above the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Let $E^D \subset E$ denote the fixed field of $D_{\mathfrak{q}/\mathfrak{p}}$ and E^I the fixed field of $I_{\mathfrak{q}/\mathfrak{p}}$ in E. Let $\mathfrak{q}^D = \mathfrak{q} \cap E^D$ and $\mathfrak{q}^I = \mathfrak{q} \cap E^I$. Thus we have a tower of extensions $E/E^I/E^D/K$ corresponding to the tower of primes $\mathfrak{q}/\mathfrak{q}^I/\mathfrak{q}^D/\mathfrak{p}$.

   (a) Show that $\mathfrak{q}^I$ is totally ramified in E/E^I (i.e. $e_{\mathfrak{q}/\mathfrak{q}^I} = [E : E^I]$); that $\mathfrak{q}^D$ is totally inert in E^I/E^D (i.e. $f_{\mathfrak{q}^I/\mathfrak{q}^D} = [E^I : E^D]$); and that $\mathfrak{q}$ is the unique prime ideal of E lying above $\mathfrak{q}^D$.

   (b) For any intermediate extension $E/L/K$, let $\mathfrak{q}_L = \mathfrak{q} \cap L$. Show that if $e_{\mathfrak{q}_L/\mathfrak{p}} = f_{\mathfrak{q}_L/\mathfrak{p}} = 1$ then $L \subset E^D$; that if $e_{\mathfrak{q}_L/\mathfrak{p}} = 1$ then $L \subset E^I$; and that if $\mathfrak{q}$ is the only prime ideal of $\mathcal{O}_E$ lying above $\mathfrak{q}_L$, then $E^D \subset L$.

5. Let K be a number field, let E/K be a finite extension, and let $E/L_1/K$ and $E/L_2/K$ be intermediate fields.

   (a) Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$ which is unramified in L_1 and L_2. Show that $\mathfrak{p}$ is unramified in the compositum $L_1 \cdot L_2$.

   (b) Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$ which splits completely in L_1 and L_2. Show that $\mathfrak{p}$ splits completely in the compositum $L_1 \cdot L_2$.

6. Find an example of a number field $K/\mathbb{Q}$ with the following property: for each prime number p, $p\mathcal{O}_K$ is divisible by an even number of prime ideals $\mathfrak{p} \subset \mathcal{O}_K$. (Hint: Try a compositum of quadratic fields.)

7. Let $\overline{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$. Recall that if $K/\mathbb{Q}_p$ is a finite extension contained inside $\overline{\mathbb{Q}}_p$, then there is a canonical valuation $v_K : K^\times \to \mathbb{Z}$ satisfying $v_K|_{\mathbb{Q}_p} = e_{K/\mathbb{Q}_p} v_{\mathbb{Q}_p}$.

   (a) Show that there is a unique map $v : \overline{\mathbb{Q}}_p^\times \to \mathbb{Q}$ satisfying $v|_K = e_{K/\mathbb{Q}_p}^{-1} v_K$ for each finite extension $K/\mathbb{Q}_p$ contained inside $\overline{\mathbb{Q}}_p$.

(b) Show that $v : \overline{\mathbb{Q}}_p^\times \to \mathbb{Q}$ is surjective and satisfies $v(xy) = v(x) + v(y)$ and $v(x+y) \geq \min(v(x), v(y))$ for all $x, y \in \overline{\mathbb{Q}}_p$ with $xy(x+y) \neq 0$.

(c) Define a metric on $\overline{\mathbb{Q}}_p$ by the formula $d(x,y) = 2^{-v(x-y)}$ when $x \neq y$. Decide whether $\overline{\mathbb{Q}}_p$ is complete.

8. (Krasner's lemma) Let K be a finite extension of $\mathbb{Q}_p$, let E/K be a finite Galois extension with valuation $v_E : E^\times \to \mathbb{Z}$, and let $x, y \in E$. Let $y_1, \ldots, y_n$ be the Galois conjugates of y over K. Show that if $v_E(x-y) > v_E(x-y_i)$ for each $i = 2, \ldots, n$, then $K(x) \supset K(y)$.

9. (a) Let K be a finite extension of $\mathbb{Q}_p$, and let A denote the integral closure of $\mathbb{Z}_p$ in K. Let $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X]$ be a monic, irreducible polynomial, and let E/K denote the splitting field of $f(X)$. Let $\alpha \in E$ be a root of $f(X)$. Show that there exists $N \geq 1$ such that if $g(X) = X^n + b_1 X^{n-1} + \cdots + b_n \in A[X]$ satisfies $v_K(a_i - b_i) \geq N$ for each $i = 1, \ldots, n$, then $g(X)$ is irreducible and there exists a root $\beta \in E$ of $g(X)$ such that $K(\alpha) = K(\beta)$.

(b) Deduce that for each $n \geq 1$, there exist only finitely many isomorphism classes of extension $K/\mathbb{Q}_p$ with $[K : \mathbb{Q}_p] = n$. (Hint: A is compact.)

10. Let $f(X) = 5!(1 + X + X^2/2! + \cdots + X^5/5!) \in \mathbb{Z}[X]$.

(a) Draw the Newton polygon of $f(X)$ over $\mathbb{Q}_p$ for each $p = 2, 3, 5$.

(b) Conclude that $f(X)$ is irreducible over $\mathbb{Q}$ and the Galois group of its splitting field is S_5.