1. Let A be a Dedekind domain with field of fractions Q and let $\mathfrak{p} \lhd A$ be a prime ideal. Define the *localization at* $\mathfrak{p}$ by
$$A_{\mathfrak{p}} = \left\{ \frac{a}{q} \colon a \in A, q \in A \smallsetminus \mathfrak{p} \right\}.$$
   a) Show that $A_{\mathfrak{p}}$ is a subring of Q.
   b) Let $\mathfrak{a}_{\mathfrak{p}} \lhd A_{\mathfrak{p}}$ an ideal. Show that $\mathfrak{a} = \mathfrak{a}_{\mathfrak{p}} \cap A$ is an ideal in A satisfying $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{a}.A_{\mathfrak{p}}$.
   c) Let $\mathfrak{q} \lhd A$ coprime to $\mathfrak{p}$. Show that $\mathfrak{q}.A_{\mathfrak{p}} = A_{\mathfrak{p}}$.
   d) Let $\mathfrak{m}_{\mathfrak{p}} = \mathfrak{p}.A_{\mathfrak{p}}$ and let $\mathfrak{a}_{\mathfrak{p}} \lhd A_{\mathfrak{p}}$ be a non-zero proper ideal. Show that there exists $v \in \mathbb{N}$ such that $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}^v$. In particular, $\mathfrak{m}_{\mathfrak{p}}$ is the unique maximal ideal in $A_{\mathfrak{p}}$.
   e) Show that $\mathfrak{m}_{\mathfrak{p}}$ is principal.
   Hint: Let $x \in \mathfrak{p} \smallsetminus \mathfrak{p}^2$ and show that $\mathfrak{m}_{\mathfrak{p}} = x.A_{\mathfrak{p}}$.
   f) Show that $A/\mathfrak{p} \cong A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$.
2. Let $K/\mathbb{Q}$ be a number field and let Δ_K be the discriminant of the maximal order in K. Prove that $\Delta_K \equiv 0, 1 \mod 4$.
Hint: Let $\mathcal{B} = (\omega_1, \ldots, \omega_d)$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$ and let $(\sigma_1, \ldots, \sigma_d)$ be an enumeration of $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. Write $\det(\sigma_j \omega_i) = P - N$, where P is the sum running over even and N is the sum running over odd permutations. Then
$$\Delta_K = (P - N)^2 = (P + N)^2 - 4PN.$$
Show that $P + N$ and PN are contained in $\mathbb{Z}$ by showing that they are algebraic integers contained in $\mathbb{Q}$. For the latter, you might want to consider the Galois closure L/K of K.
3. The goal of this exercice is to state and to give a proof of the Quadratic reciprocity law. For this we will need to first define the Legendre symbol.
$$\left(\frac{\cdot}{p} \right) \colon (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{C}$$
is defined by $\left(\frac{a}{p}\right) = 1$ if $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a square and $\left(\frac{a}{p}\right) = -1$ if $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a nonsquare.
   a) Prove that the Legendre symbol is the unique non-trivial real character on $(\mathbb{Z}/p\mathbb{Z})^\times$.
   b) Prove that
$$\left(\frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \mod p \text{ for } a \in (\mathbb{Z}/p\mathbb{Z})^\times$$
   Conclude that -1 is a square mod p if and only if $p \equiv 1 \mod 4$.

Now we wish to prove the Quadratic reciprocity law which states that for distinct odd primes p, q we have
$$\left(\frac{p}{q} \right) \left(\frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

We will work through the sixth published proof of Gauss of this result. For this we define the quadratic Gauss sum. Let ζ_p be a primitive p-th root of unity. We define

$$\tau = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) \zeta_p^a$$

c) Prove that $\tau^2 = (-1)^{\frac{p-1}{2}} p$
Hint:

$$\tau^2 = \sum_{a,b \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{ab}{p}\right) \zeta_p^{a+b}$$

and change variables $b = ac$.

d) Prove that the ideal $(q, \tau) \lhd \mathbb{Z}[\zeta_p]$ equals $\mathbb{Z}[\zeta_p]$.
Hint: $\tau^2 \in (q, \tau)$.

e) Prove that

$$\tau^{q-1} \equiv \left(\frac{q}{p}\right) \mod q\mathbb{Z}[\zeta_p].$$

Hint: Expand τ^q and note that for $0 \leqslant k_1, \ldots, k_r \leqslant q$ we have that

$$q \left| \frac{q!}{k_1! \cdots k_r!} \right.$$

unless there is $1 \leqslant i \leqslant r$ such that $k_i = q$.

f) Use (c) and (e) to conclude the proof of the Quadratic reciprocity law.