Geometry of numbers and quadratic forms

Exercise 1. [Sums of two squares] Let Σ_2 be the set of integers of the form a^2+b^2 with $a, b \in \mathbb{Z}$.

1. Show that Σ_2 is stable by multiplication.
2. Let p be a prime such that $p \equiv 3 \bmod 4$. Show that if p divides a^2+b^2 then p^2 divides a^2+b^2.
3. Let p be a prime such that $p \equiv 1 \bmod 4$ and $u \in \mathbb{Z}$ such that $u^2 \equiv -1 \bmod p$. Let $L = \{(a,b) \in \mathbb{Z}^2 \mid b \equiv ua \bmod p\}$.
   (a) Show that L is a sublattice of $\mathbb{Z}^2$.
   (b) Show that if $(a,b) \in L$ then $p \mid a^2+b^2$.
   (c) Use Minkowski's theorem to prove that there exists $(a,b) \in L$ such that $p = a^2+b^2$.

   Remark : We have obtained a new proof of the fact that $p \equiv 1 \bmod 4$ splits in $\mathbb{Q}(\sqrt{-1})$.
4. Describe the elements of Σ_2.

Exercise 2. [Legendre's theorem] We are going to show Legendre's theorem : Let a, b, c be coprime positive squarefree integers. The quadratic form $q(x,y,z) = ax^2+by^2-cz^2$ represents 0 (non-trivially) if and only if bc, ac, and $-ab$ are quadratic residues modulo a, b and c respectively.

1. Show that the condition on Legendre symbols is necessary.
2. We now assume that the condition is satisfied, and let $u, v, w \in \mathbb{Z}$ such that

$$u^2 \equiv bc \bmod a, \quad v^2 \equiv ac \bmod b, \quad w^2 \equiv -ab \bmod c.$$

   (a) Let $L = \{(x,y,z) \in \mathbb{Z}^3 \mid uy \equiv cz \bmod a, vz \equiv -ax \bmod b, wx \equiv -by \bmod c\}$. Show that L is a sublattice of $\mathbb{Z}^3$. What is its covolume ?
   (b) Apply Minkowski's theorem to $C = \{(x,y,z) \in \mathbb{R}^3 \mid 0 \leq ax^2+by^2-cz^2 \leq R\}$ for a well-chosen R and show that there exists $(x,y,z) \neq (0,0,0)$ in $\mathbb{Z}^3$ such that $q(x,y,z) = 0$ (*Hint :* The volume of C is $\frac{4\pi}{3}\sqrt{\frac{R^3}{abc}}$).

Exercise 3. [Negative discriminant]

1. Let $K = \mathbb{Q}(\sqrt{-23})$.
   (a) Let $I = \left(3, \frac{1+\sqrt{-23}}{2}\right)$ and $J = \left(13, \frac{1+\sqrt{-23}}{2}+4\right)$. Do I and J belong to the same class in $\mathcal{C}\ell(\mathcal{O}_K)$?
   (b) Show that $\mathcal{C}\ell(\mathcal{O}_K) \simeq \mathbb{Z}/3\mathbb{Z}$.
2. Compute $\mathcal{C}\ell(\mathcal{O}_{\mathbb{Q}(\sqrt{-84})})$.

Exercise 4. [Square discriminant] Let $k \in \mathbb{Z}$, $D = k^2$ and $q(x,y) = ax^2+bxy+cy^2$ a quadratic form with discriminant D.

1. Give a non-zero solution of $q(x,y)=0$.
2. Prove that $q \sim (0,k,c')$ for some $c' \in \{0,\dots,k-1\}$.
3. Prove that c' is determined by q up to proper equivalence.

Exercise 5. [Lagrange's theorem]

1. Let p be a prime number and D a quadratic residue modulo $4p$. Show that, up to equivalence, there exists a unique quadratic form of discriminant D that represents p.
2. Conversely, show that if there is a quadratic form with discriminant D that represents p then D is a square modulo $4p$.
3. What are the prime numbers of the form x^2+5y^2 ?

Exercise 6. [Positive discriminant] Show that, up to equivalence, there is a unique quadratic form of discriminant D for $D=5$ and $D=8$.

Exercise 7. [Trivial class groups]

1. Let $K=\mathbb{Q}(\alpha)$, with $\alpha^3-\alpha-1=0$. Show, using Minkowski's bound, that $\mathcal{C}\ell(\mathcal{O}_K)$ is trivial.
2. Let $K=\mathbb{Q}(\sqrt{-65})$. Show that $\mathcal{C}\ell(\mathcal{O}_K)\simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.
3. Show that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is principal for $d\in\{-163,-67,-43,-19,-11,-7,-3,-2,-1,2,3,5,13\}$.