EXERCISE 6 IN ALGEBRAIC NUMBER THEORY

(1) Le $(a, p) = 1$. Show that the number of solutions of the congruence $ax^2 + bx + c = 0 \mod p$ equals $1 + \left(\frac{b^2-4ac}{p}\right)$.

(2) (P) Let $K = \mathbb{Q}(i)$. Give an example each of ideals that are unramified, ramified and inert.

(3) If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $\mathfrak{o}$, then $\mathfrak{a} = \mathfrak{a}\mathcal{O} \cap \mathfrak{o}$ and $\mathfrak{a} \mid \mathfrak{b} \Longleftrightarrow \mathfrak{a}\mathcal{O} \mid \mathfrak{b}\mathcal{O}$.

(4) (P) For a number field K, the statement of Prop. (8.3) concerning the prime decomposition in the extension $K(\theta)$ holds for all prime ideals $\mathfrak{p} \nmid (\mathcal{O} : \mathfrak{o}[\theta])$.

(5) (P) Show that the class group of $\mathbb{Q}(\sqrt{-30})$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$.