ALGEBRAIC NUMBER THEORY

HOMEWORK 2

(1) Show that the ideal $(2, 1+\sqrt{-5}\,)$ equals the $\mathbb{Z}$-module $[2, 1+\sqrt{-5}\,]$.

(2) Show that the $\mathbb{Z}$-module $M = [2, 1+3\sqrt{-5}\,]$ has norm 6, and that $MM' = 2[1, 3\sqrt{-5}\,]$.

(3) Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Prove Fermat's little theorem: $\alpha^{N\mathfrak{p}} \equiv \alpha \bmod \mathfrak{p}$ for all $\alpha \in \mathcal{O}_K$. (Hint: transfer the proof from elementary number theory to $\mathcal{O}_K$.)

(4) Let m be a squarefree integer and p a prime number with $(\frac{m}{p}) = -1$. Derive the congruence $(a+b\sqrt{m}\,)^p \equiv a - b\sqrt{m}$ for $a, b \in \mathbb{Z}$. What happens if $(\frac{m}{p}) = +1$?

(5) Let $K = \mathbb{Q}(\sqrt{m}\,)$ be a quadratic number field, where m is squarefree. Prove the following:
   - If $m \equiv 2 \bmod 4$ then $2\mathcal{O}_K = (2, \sqrt{m}\,)^2$.
   - If $m \equiv 3 \bmod 4$ then $2\mathcal{O}_K = (2, 1+\sqrt{m}\,)^2$.
   - If $m \equiv 1 \bmod 8$ then $2\mathcal{O}_K = \mathfrak{a}\mathfrak{a}'$, where $\mathfrak{a} = (2, \frac{1+\sqrt{m}}{2}\,)$ and $\mathfrak{a} \neq \mathfrak{a}'$.
   - If $m \equiv 5 \bmod 8$ then $2\mathcal{O}_K$ is prime.