Math 676, Homework 3 (Part 2)

(Here is one more problem.)

11. [Splitting of Prime Ideals in Quadratic Fields] Consider a quadratic field $K = \mathbb{Q}(\sqrt{m})$ with m squarefree. The ring of integers is $O_K = \mathbb{Z}[1, \sqrt{m}]$ and discriminant $\Delta_K = 4m$ if $m \equiv 2, 3 \pmod{4}$, and $O_K = \mathbb{Z}[1, \frac{1+\sqrt{m}}{2}]$ and absolute discriminant $\Delta_K = m$ if $m \equiv 1 (\text{mod } 4)$. Let p be a rational prime.

(a) Show that if $p|m$ then $(p)O_K = (p, \sqrt{m})^2$.

(b) Show that if p is odd, and $p \nmid \Delta_K$, then

$$(p)O_K = \begin{cases} (p, n+\sqrt{m},)(p, n-\sqrt{m}) & \text{if } n^2 \equiv m \pmod{p}. \\ (p)O_K & \text{If } x^2 \equiv m (\text{mod } p) \text{ is unsolvable.} \end{cases}$$

(c) Show that if $p = 2$ and $2 \nmid m$, then

$$(2)O_K = \begin{cases} (2, 1+\sqrt{m})^2 & m \equiv 3 \pmod{4}. \\ (2, \frac{1+\sqrt{m}}{2})(2, \frac{1-\sqrt{m}}{2}) & \text{if } m \equiv 1 \pmod{8}. \\ (2)O_K & \text{If } m \equiv 5 \pmod{8} \end{cases}$$

[Hint: Write the ring of integers as $\mathbb{Z}[\alpha]$ for the given α above and use the criterion on factoring $f(x) \pmod{p}$.]