MATH 4576 Rings and Fields

Additional exercises 1

(1) Let $R = \mathbb{Z}[\sqrt{2}] = \{\, m + n\sqrt{2} \mid m, n \in \mathbb{Z} \,\}$.
Set $\delta(m + n\sqrt{2}) = |m^2 - 2n^2|$.

(a) Prove that R is a Euclidean domain with respect to the function δ.

(b) Prove that $a \in R$ is a unit if and only if $\delta(a) = 1$.

(c) Prove that any irreducible element from R divides a prime integer.

(d) Prove that an odd prime integer p is an irreducible element of R if and only if $p \equiv \pm 1 \pmod 8$. (*Use the result of the next exercise.*)

(e) Deduce a criterion for the equation $x^2 - 2y^2 = p$, where p is a prime number, to have an integral solution.

(2) Let p be an odd prime number and K be an extension of the field Z_p such that the polynomial $x^4 + 1$ has a root θ in K.

(a) Prove that $(\theta + \theta^{-1})^2 = 2$.

(b) Prove that

$$\theta^p = \begin{cases} \theta & \text{if } p \equiv 1 \pmod 8, \\ -\theta^{-1} & \text{if } p \equiv 3 \pmod 8, \\ -\theta & \text{if } p \equiv 5 \pmod 8, \\ \theta^{-1} & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

(c) Deduce that

if $p \equiv \pm 1 \pmod 8$, then $2^{(p-1)/2} \equiv 1 \pmod p$,

if $p \equiv \pm 3 \pmod 8$, then $2^{(p-1)/2} \equiv -1 \pmod p$.

Hint: $2^{(p-1)/2} = \dfrac{(\theta + \theta^{-1})^p}{\theta + \theta^{-1}}$ (in the field K).

(d) Deduce that the congruence $x^2 \equiv 2 \pmod p$ has a solution if and only if $p \equiv \pm 1 \pmod 8$.