M2P4 Rings and Fields
Problem Sheet 5.

1. Let p be an odd prime number. You are given the following fact: there exists an integer x such that $x^2 \equiv -2 \bmod p$ if and only if $p \equiv 1$ or $3 \bmod 8$. Using this fact, prove that there are integers x, y such that $p = x^2 + 2y^2$ if and only if $p \equiv 1$ or $3 \bmod 8$.

2. Let $R = \mathbb{Z}/3[x]$ and let I be the principal ideal $(x^2 + 1)R$.
(1) Show that R/I is a field of 9 elements. (You may quote any results from lectures which you need.)
(2) Let F^* be the multiplicative group consisting of the non-zero elements of R/I. Prove that F^* is cyclic.

3. Let $R = \mathbb{Z}[i]$.
(1) Show that $3R$ and $(3 + 2i)R$ are maximal ideals of R.

(2) How many elements have the fields $R/3R$ and $R/(3 + 2i)R$?

4. (1) List the irreducible cubic polynomials in $\mathbb{Z}/2[x]$.
(2) List the irreducible monic quadratic polynomials in $\mathbb{Z}/3[x]$.
Explain briefly how you obtained your answers.

5. Let R be an integral domain. An ideal P of R is said to be a prime ideal of R if $P \neq R$ and, whenever $rs \in P$ for some $r, s \in R$, then either $r \in P$ or $s \in P$.
(1) Show that if p is a prime number, then $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

(2) Let I be an ideal of R. Prove that the factor ring R/I is an integral domain if and only if I is a prime ideal.