Math 542 - Assignment 2 - PIDs and Euclidean domains

Assume that R is a PID.

(1) Show that if $d = gcd(a, b)$ then

$$(d) = (a, b)$$

where $(a, b) = Ra + Rb = \{ra + sb \mid r, s \in R\}$.

Note: This implies that there is some $r, s \in R$ such that $d = ra + sb$.

(2) Show that if $e = lcm(a, b)$ then $(e) = (a) \cap (b)$.

(3) Suppose $p \in R$ is not a unit. We call p **irreducible** if whenever $p = ab$ then either a or b is a unit. What are the irreducible elements of $\mathbb{Z}$? of $F[x]$?

(4) Prove that if p is irreducible and $p \mid ab$ then either $p \mid a$ or $p \mid b$.

Note: Using this lemma we can prove that any $r \in R$ has the form $r = p_1 p_2 \cdots p_k$ where each p_i is irreducible.

(5) Using the note from the previous problem find a nice formula for lcm and gcd of $a, b \in R$ in terms of the irreducibles of a and b.

Assume that R is an integral domain.

(6) A norm on R is a function N which assigns to each nonzero $a \in R$ a nonnegative integer $N(a) \in \mathbb{R}$. We say that an integral domain R is a **Euclidean domain** if it has a norm that satisifes the following condition: If $a, b \in R$ with $b \neq 0$ then there exists elements $q, r \in R$ so that $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$. We as that q is the quotient and r is the remainder. Clearly $\mathbb{Z}$ is a Euclidean domain with $N(a) = |a|$. Show that $F[x]$ is a Euclidean domain with N given by the degree of the polynomial.

(7) $(*)$ (Honors) Show that any Euclidean domain is a PID.

(8) The nice thing about Euclidean domains is that we have a *Euclidean algorithm* to find r, s such that $ra + sb = gcd(a, b)$. You have probably seen examples of this algorithm in $\mathbb{Z}$ (if not then refer to wikipedia for example). Apply the same algorithm in $F[x]$ to the polynomials $x^2 - 1$ and $x^2 + 2x + 1$.