Question 1
A *Euclidean domain* is an integral domain \( R \) which admits a function \( d : R - \{0\} \to \mathbb{N} \) such that:

1. For all nonzero \( a, b \in R \), \( d(a) \leq d(ab) \)
2. For all \( a, b \in R \) with \( b \neq 0 \), there exist elements \( q, r \in R \) satisfying \( a = qb + r \) and either \( r = 0 \) or \( d(r) < d(b) \)

We have seen that \( \mathbb{Z} \) is a Euclidean domain with \( d(n) = |n| \), and \( F[x] \) is one with \( d(f(x)) = \deg(f) \).

Recall that for an arbitrary ring \( R \), we say that a nonzero, nonunit \( p \in R \) is *irreducible* if its only divisors are the units and its associates. We say that \( R \) is a unique factorization domain (UFD) if every nonzero \( a \in R \) admits a unique (up to units) factorization into irreducibles.

For this workshop, fix a Euclidean domain \( R \) with associated Euclidean function \( d \).

(a) Given a nonzero, nonunit element \( b \in R \), prove that \( d(a) < d(ab) \) for every nonzero \( a \in R \).

(b) Given nonzero \( a, b \in R \), set \( I = I_{a,b} = \{ax + by | x, y \in R \} \) (the set of \( R \)-linear combinations of \( a \) and \( b \)). Prove that \( I \) is nonempty, and moreover contains elements other than 0.

(c) Choose \( c \in I \) minimizing the function \( d \). Show that any common divisor \( d \) of \( a \) and \( b \) must also divide \( c \). (We call \( c \) a GCD of \( a \) and \( b \). It is unique up to multiplication by a unit).

(d) Show that if \( p \in R \) is irreducible, and \( p \) divides the product \( ab \), then \( p \) divides \( a \) or \( p \) divides \( b \).

Here’s an outline of how the proof should go:

1. Suppose \( p \) does not divide \( a \). Let \( c \) be a GCD of \( p \) and \( a \) (see part c)). Conclude from c) that \( c \) divides \( p \).
2. Write \( p = ck \). Use the irreducibility of \( p \) to show that one of \( c, k \) must be a unit. Then use the assumption that \( p \) doesn’t divide \( a \) to show that \( c \) must be the unit.
3. Show that \( 1 \in I_{a,p} \).
4. Show that \( p \) divides \( b \).

(e) Show that \( R \) is a UFD. Hence all Euclidean domains are also UFDs.