HOMEWORK 7, DUE THU APR 1ST

All solutions should be with proofs, you may quote from the book or from previous home works

(1) Let A be a Euclidean ring with a Euclidean function d.
   (a) Show that $d(1) \leq d(a)$ for any $a \in A$ and a is a unit if and only if $d(a) = d(1)$.

   (b) Now assume the function d above only satisfies the second condition (division algorithm) not necessarily the first ($d(a) \leq d(ax)$). Then, show that $\phi(a) = \min\{d(ax) | x \neq 0\}$ satisfies both the conditions and thus the ring is an Euclidean domain.

(2) Let A be a principal ideal domain. (There are PIDs which are not Euclidean domains.)
   (a) If $a, b \in A$, both non-zero, as usual we can define their greatest common divisor and least common multiple (lcm for short). Show that $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ exists in A for any two non-zero elements a, b. Further, show that $\gcd(a, b) \operatorname{lcm}(a, b) = ab$.

   (b) Show that any non-zero prime ideal is maximal.

   (c) Let K be the fraction field of A and let $x \in K$. Assume we have an equation, $x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$ where $a_i \in A$. Show that $x \in A$.

(3) Let $A = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} | a, b \in \mathbb{Z}\}$.
   (a) Show that $\phi : A - \{0\} \to \mathbb{N}$, given by $\phi(a + b\sqrt{-2}) = a^2 + 2b^2$ is a Euclidean function, so that A is a Euclidean domain.

   (b) Decide whether $11, 13$ and/or 17 are primes in A.

   (c) Let p be a prime such that $p = 1 + 4n$, n a positive integer. Show that p is not a prime in A only if $4^n \equiv 1 \bmod p$.

(4) Let $A = \mathbb{Z}[i]$, the ring of Gaussian integers.
   (a) Find $\gcd(3+4i, 4-3i)$.

   (b) Find all positive integers which can be written as a sum of two squares of integers. (Hint: If a, b, c, d are integers, then there exists integers A, B such that $(a^2+b^2)(c^2+d^2) = A^2+B^2$.)

   (c) Show that there are infinitely many primes of the form $4n+3$, $n \in \mathbb{N}$.

(5) Let A be a Euclidean domain. As usual, we have $G = SL(2, A)$, the set of 2×2 matrices over A with determinant one. We have a subgroup of G generated by matrices of the form $E = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ and E^T, the transpose of E, where $a \in A$ varies, called the subgroup of elementary matrices and denoted by $E_2(A)$. Show that $E_2(A) = G$. (You probably realize elements E, E^T correspond to row and column operations. The result is valid for $n \times n$ matrices for any n.)

(6) Let $K = \mathbb{F}_{11}$ the field of 11 elements and $A = K[x]$, polynomial ring over K.
   (a) Show that x^2+1 is prime (also called *irreducible*) in A and $L = A/(x^2+1)A$ is a field with 121 elements.

   (b) Show that x^2+x+4 is irreducible in A and thus $M = A/(x^2+x+4)A$ is also a field with 121 elements.

   (c) Show that L is isomorphic to M.