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 $d(a) = d(1)$.

Solution. Since $d(1) \leq d(1 \cdot a) = d(a)$, the first part is obvious. Assume $d(1) = d(a)$. Then, division algorithm says we can write $1 = qa + r$ for some $q, r \in A$ with $d(r) < d(a) = d(1)$ or $r = 0$. Since for any non-zero r, we have seen that $d(1) \leq d(r)$ and thus r must be zero. So, $1 = qa$ and then a is a unit. If a is a unit, we have $ax = 1$ for some x and so $d(a) \leq d(ax) = d(1) \leq d(a)$. So, $d(a) = d(1)$. □

(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.

Solution. We first show that $\phi(a) \leq \phi(ax)$ for all $x \neq 0$. This is obvious, since $\{axy | y \neq 0\} \subset \{ay | y \neq 0\}$ and so the minimum of $d(axy)$ is greater than or equal to the minimum of $d(ay)$.
Next, we show that division algorithm can be done with ϕ. Let $a \neq 0$ and choose an x so that $\phi(a) = d(ax)$. If $b \in A$, we can divide by ax to get $b = qax + r$ with $d(r) < d(ax) = \phi(a)$. Then, $b = (qx)a + r$ as desired. □

(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 $\text{lcm}(a, b)$ exists in A

for any two non-zero elements a, b. Further, show that $\gcd(a,b)\operatorname{lcm}(a,b) = ab$.

Solution. Consider $I = \{ra + sb | r, s \in A\}$. Easy to show that I is an ideal and thus $I = dA$ for some $d \in A$, clearly non-zero. I claim, $d = \gcd(a,b)$. Since $a, b \in dA$, we can write $a = pd, b = qd$ and thus $d|a, d|b$. If $c|a, c|b$, then since $d = ra + sb$ for some $r, s \in A$, we see that $c|d$.
Similarly, let $J = aA \cap bA$. Again, easy to show that it is an ideal and then $J = lA$ for some $l \in A$. I will leave you to check that $l = \operatorname{lcm}(a,b)$. The last part I leave you to check (and is easy). □

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

Solution. Let $P = pA$ be a non-zero prime ideal, so that p is a prime element. If $P \subset Q$, $Q \neq A$ an ideal, we have $Q = qA$ for some q and q is not a unit. Since $p \in P \subset Q$, we see that $q|p$ and since p is a prime, we see that $p = qu$, where u is a unit. Then $Q = P$, proving maximality of P. □

(c) Let K be the fraction field of A and let $x \in K$. Assume we have an equation, $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ where $a_i \in A$. Show that $x \in A$.

Solution. Since $x \in K$, we can write $x = a/b$, $a, b \in A, B \neq 0$. If $a = 0$, $x = 0$, so we may as well assume $a \neq 0$. If $d = \gcd(a,b)$, then $a = da', b = db'$ and thus $x = a/b = a'/b'$. So, we may assume $\gcd(a,b) = 1$.
Now, multiply our equation by b^n to get,

$$a^n + a_1a^{n-1}b + a_2a^{n-2}b^2 + \cdots + a_nb^n = 0.$$

Since all terms except the first have a b in them, we see that $b|a^n$. But, $\gcd(a,b) = 1$, and so this can happen only if b is a unit. Then $x = a/b \in A$. □

(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.

Solution. This is identical to the argument for Gaussian integers. First note that $\phi(x) \geq 1$ for any $x \in A - \{0\}$ and

$\phi(xy) = \phi(x)\phi(y)$, which easily shows the first condition is satisfied.
For division algorithm, we procced as we did in class. Let $x = a + b\sqrt{-2} \neq 0$ and $y = c + d + \sqrt{-2}$. We wish to find $q, r \in A$ so that $y = qx + r$ with $\phi(r) < \phi(x)$. Let $X = a^2 + 2b^2 = x(a - b\sqrt{-2})$ and $Y = y(a - b\sqrt{-2})$. Write $Y = P + Q\sqrt{-2}$. Since X is a non-zero integer, by the usual division algorithm, we can write $P = q_1X + r_1, Q = q_2X + r_2$, with $|r_i| \leq X/2$. Thus, $Y = (q_1 + q_2\sqrt{-2})X + (r_1 + r_2\sqrt{-2})$. Since both X, Y are multiples of $a - b\sqrt{-2}$, we see that $r_1 + r_2\sqrt{-2} = w(a - b\sqrt{-2})$ for some $w \in A$. Then, we have $y = (q_1 + q_2\sqrt{-2})x + w$, by cancelling $a - b\sqrt{-2}$. Finally, we have $\phi(w)X = r_1^2 + 2r_2^2 \leq X^2/4 + 2X^2/4 = 3/4X^2 < X^2$. So, $\phi(w) < X = \phi(x)$ which proves what we want. □

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

Solution. By the first problem in this set, the only units $u \in A$ are the ones with $\phi(u) = \phi(1) = 1$ and it is immediate that the only units are ± 1.
11 is not a prime, since $3 + \sqrt{-2}$ divides it. $(11 = (3 + \sqrt{-2})(3 - \sqrt{-2}))$
17 is not a prime since $17 = 9 + 8 = (3 + 2\sqrt{-2})(3 - 2\sqrt{-2})$.
The case of 13 is coveredd in the next problem. □

(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 $4^n \equiv 1 \mod p$.

Solution. If $p \in \mathbb{Z}$ is a prime but not a prime in A, take a prime factor $a + b\sqrt{-2}$. Then, $b \neq 0$, since if it is , we write $p = a(c + d\sqrt{-2})$ and then $p = ac$. But $a \neq \pm 1$ and so this means $a = p$ and so p is a prime in A. If $b \neq 0$, it is clear that $a - b\sqrt{-2}$ is a prime different from $a + b\sqrt{-2}$ and $a + b\sqrt{-2}$ also divides p, so $(a + b\sqrt{-2})(a = b\sqrt{-2}) = a^2 + 2b^2$ divides p and thus must be p. So, we get $p = a^2 + 2b^2$. This implies in $\mathbb{F}_p$, $a^2 + 2b^2 = 0$ and $a, b \neq 0$. This says $(a/b)^2 = -2$. So, $(-2)^{\frac{p-1}{2}} = (a/b)^{p-1} = 1$. Since $p = 4n + 1$, we get $(-2)^{2n} = 4^n = 1$.

For $p = 13 = 4 \times 3 + 1$, we look at 4^3 modulo 13. I will leave you to check that $4^3 \equiv -1 \bmod 13$ and thus 13 is a prime in A. $\square$

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

Solution. $4 - 3i = -i(3 + 4i)$ and since i is a unit, we see that the gcd is just $3 + 4i$ (or $4 - 3i$). $\square$

(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 $(a^2 + b^2)(c^2 + d^2) = A^2 + B^2$.)

Solution. If we have $N = a^2 + b^2$, let $d = \gcd(a, b)$. Then, $a = a_1 d, b = b_1 d$ and so, $N = d^2(a_1^2 + b_1^2)$. Thus, we see that such integers are precisely the ones got as $a_1^2 + b_1^2$ with gcd 1 and multiplied by any square. So, if we understand numbers of the form $a^2 + b^2$ with $\gcd(a, b) = 1$, we know all the others are got by just multiplying these by squares. So, we study the ones with gcd 1.
If a prime p divides $a^2 + b^2$ since p can not divide a, b, we see that in $\mathbb{F}_p$, -1 is a square. This immediately says that either $p = 2$ or $p \equiv 1 \bmod 4$. Thus, $a^2 + b^2 = 2^n p_1 p_2 \cdots p_m$ for primes $p_i \equiv 1 \bmod 4$.
Since $2 = 1^2 + 1^2$ and any p of the above form can be written as sum of two squares, by the hint any such number is a sum of squares. So, we see that $N = d^2 2^n P$ where P is a product of primes which are congruent to 1 modulo 4. $\square$

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

Solution. We imitate Euclid's proof of infinitude of primes. Assume there are only finitely many such primes, say $p_1, \ldots, p_m$. Then, $\prod p_i \equiv 1 \bmod 4$ if m is even and $\equiv 3 \bmod 4$ if m is odd. If m is even, take $N = \prod p_i + 2$ and if odd take $N = \prod p_i + 4$. So, $N \equiv 3 \bmod 4$. Notice that $N > 1$ and so not a unit and let p be a prime factor. Since N is odd, p is odd. If $p \equiv \bmod 3$, then $p \neq p_i$ for any i

and thus we have found a new prime of the desired kind. So, $p \equiv 1 \bmod 4$. Then $N = \prod p \equiv 1 \bmod 4$ a contradiction to the choice $N \equiv 3 \bmod 4$. $\square$

(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.)

Solution. Let ϕ be an Euclidean function.

We start with a matrix $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, A)$. We are allowed to multiply a row (or column) by some element of A and add to the other row (or column). First, let us assume that $a \neq 0$. Then, we can write $b = qa + r$ and so multiplying the first column by q and subtracting from the second column, we can replace b by r. If $r \neq 0$, $\phi(r) < \phi(a)$. Now, we can add a suitable multiple of the second column to the first to replace a by an s, and again if $s \neq 0, \phi(s) < \phi(r)$. Clearly, this can not go on forever and so by this procedure, we can make the first row to be $(a, 0)$ or $(0, a)$. But, this is the first row of a determinant one matrix implies, a is a unit and then by doing the operation twice, we can make $a = 1$. Again, one can make a column operations to get X to look like $\begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix}$. The determinant condition forces $d = 1$. Now, multiply the first row by c and subtract from the second to convert the matrix to identity. $\square$

(6) Let $K = \mathbb{F}_{11}$ field with 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.

Solution. If $x^2 + 1$ is not irreducible, then since its degree is 2, the only way it can factorize is $x^2 + 1 = (x - a)(x - b)$. This says, $a^2 + 1 = 0$. So, $\mathrm{ord}(a) = 4$ in $\mathbb{F}_{11}^*$, which is a group of order 10 and can not have an element of order 4. Thus, being a PID, $(x^2+1)A$ is a maximal ideal and thus L is a field. Any element in L is the image of some polynomial $P(x) \in A$. By division algorithm, we can write $P(x) = q(x)(x^2+1) + r(x)$, where $\deg r < 2$. Since $P(x) \equiv r(x)$ in $\mathbb{F}_{11}$, we see that any element in L is the image of a polynomial of degree at most one. So, as a $\mathbb{F}_{11}$ vector space, L is generated by images of $1, x$. I will leave you to check that these are linearly independent and thus L is a vector space of dimension 2 and so has $11 \times 11 = 121$ elements. $\square$

(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.

Solution. The idea is exactly as before. If it is not irreducible, it has a root a. We complete squares to get $(a+\frac{1}{2})^2 + (4-\frac{1}{4}) = 0$. (Notice the fractions make sense in $\mathbb{F}_{11}$, since 2 is a unit. Let $b = a + \frac{1}{2}$. $\frac{1}{4} = 3$ and thus, we get $b^2+1 = 0$, again $\operatorname{ord}(b) = 4$, which is impossible. M has 1221 elements is now clear. $\square$

(c) Show that L is isomorphic to M.

Solution. The idea is exactly same. If we change variables $y = x + \frac{1}{2}$, then $x^2+x+4 = y^2+1$. The change of variable gives an automorphism of A. In other words, consider the map $\theta : \mathbb{F}_{11}[y] \to \mathbb{F}_{11}[x]$, given by $\theta(P(y)) = P(x+\frac{1}{2})$. This is an automorphism. $\theta(y^2+1) = x^2+x+4$ and so $L = \mathbb{F}_{11}[y]/(y^2+1) \cong \mathbb{F}_{11}[x]/(x^2+x+4) = M$ $\square$