Math 4010/5530 **Homework #3** **Due: Wed., Feb. 17th, 2016**

Euclidean Domain Let R be a Euclidean domain equipped with norm $\delta : R - \{0\} \to \mathbb{Z}_{\geq 0}$. Let M be the minimum value taken on by the norm (i.e. $M = \min\{\delta(r) \mid r \in R - \{0\}\}$). Show that $\delta(1) = M$. Then show that $u \in R^\times$ (u is a unit) iff $\delta(u) = M$.

Hint: For the first part and half of the "iff", the property $\delta(a) \leq \delta(ab)$ will give you what you need. For the other half of the "iff" you'll need to divide with remainder (hoping to get a remainder $r = 0$).

Gaussian Integers Recall that the Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ are a Euclidean domain when equipped with the norm:

$$N(a+bi) = (a+bi)\overline{(a+bi)} = (a+bi)(a-bi) = a^2 + b^2$$

In every Euclidean domain we have $N(z) \leq N(zw)$, but here we have something even stronger: the norm is multiplicative (i.e. $N(zw) = N(z)N(w)$). Note also that for $z = a + bi \in \mathbb{Z}[i]$, we have $\bar{z} = z$ (i.e. $a - bi = a + bi$) iff z is an integer (i.e. $z = a$). Also, it may help to note that z divides w iff $\bar{z}$ divides $\bar{w}$ (since $zk = w \iff \bar{z}\bar{k} = \bar{w}$).

Consider $n \in \mathbb{Z}$. Notice that if n factors in $\mathbb{Z}$, then n factors in $\mathbb{Z}[i]$. However, the converse does not necessarily hold (for example, $5 = (1+2i)(1-2i)$). For clarity, in what follows, when we say *prime integer* or just *prime* we mean prime in $\mathbb{Z}$ and when we say *Gauss prime* we mean prime in $\mathbb{Z}[i]$.

(a) Using the previous problem, identify $\mathbb{Z}[i]^\times$ (the units of the Gaussian integers).

(b) Show that π is a Gauss prime iff $\bar{\pi}$ is a Gauss prime.

(c) Let p be a prime (integer). Show that either p is a Gauss prime or $p = \pi\bar{\pi}$ for some Gauss prime π.
Hint: If $p = \pi\tau$, then $N(\pi)N(\tau) = N(p) = p^2$. So $N(\pi) =?$ If $N(z)$ is a prime integer, can z factor?

Lemma: If π is a Gauss prime, then $N(\pi) = \pi\bar{\pi}$ is either a prime integer or the square of a prime integer.

proof: Let π be a Gauss prime and suppose that π is not a prime integer (or an associate of a prime integer). [Note: π isn't a unit so $N(\pi) > 1$.] We already showed that $\bar{\pi}$ is also a Gauss prime. Also, by considering the units of $\mathbb{Z}[i]$, we can see that π and $\bar{\pi}$ cannot be associates (if they were, they would necessarily be associates of an integer).
Now consider the integer $N(\pi)$. Suppose that $N(\pi) = AB$ for some $A, B \in \mathbb{Z}_{\geq 0}$. Now π divides $N(\pi) = \pi\bar{\pi} = AB$ so because π is prime it must either divide A or B. WLOG assume it divides A. Next, since π divides A, $\bar{\pi}$ must divide $\bar{A} = A$ as well (integers are self-conjugate). But π and $\bar{\pi}$ are non-associate primes, thus relatively prime. Hence their product $AB = N(\pi) = \pi\bar{\pi}$ must divide A. Therefore, $B = 1$. This means $N(\pi)$ has no interesting factorizations (it's a prime integer).
Of course, if π is a Gauss prime which is an associate of a prime integer, then $\pi = up$ for some unit u and prime p. Then $N(\pi) = N(u)N(p) = 1 \cdot p^2 = p^2$.

(d) Show if $N(\pi)$ is a prime integer, then π must be a Gauss prime.

(e) Let p be a prime integer. Show that $p = \pi\bar{\pi}$ for some $\pi \in \mathbb{Z}[i]$ iff $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Lemma: Let p be an odd prime integer. Then p is a Gauss prime iff $x^2 + 1$ is irreducible in $\mathbb{Z}_p[x]$.

proof: Primes in PIDs generate maximal ideals. So p is a Gauss prime iff $\mathbb{Z}[i]/(p)$ is a field. Note that $\mathbb{Z}[i]\big/(p) \cong \mathbb{Z}[x]\big/(p, x^2+1) \cong \mathbb{Z}_p[x]\big/(x^2+1)$. So $\mathbb{Z}[i]/(p)$ is a field iff $\mathbb{Z}[x]/(x^2+1)$ is a field. This is true iff (x^2+1) is maximal in $\mathbb{Z}_2[x]$. Thus iff x^2+1 is irreducible in $\mathbb{Z}_p[x]$.

(f) Let p be a prime integer. Show that $p = \pi\bar{\pi}$ from some $\pi \in \mathbb{Z}[i]$ iff $x^2 = -1 \pmod{p}$ has an integer solution.
Hint: If $p = \pi\bar{\pi}$, then p is not a Gauss prime. Apply the lemma. Also, you need to handle the case $p = 2$ separately – the integer 2 isn't odd!

Lemma: Let p be an odd prime (integer). Show that $a \in \mathbb{Z}$ is a solution of $x^2 = -1 \pmod{p}$ iff a is an element of order 4 in $U(p) = \mathbb{Z}_p^\times$ (the group of units in $\mathbb{Z}_p$).

proof: If a is a solution then $a^2 = -1 \pmod{p}$ so the order of a isn't 1 or 2. But $a^4 = (-1)^2 = 1 \pmod{p}$ so the order of a is 4. Conversely, if a has order 4, then $a^4 = 1 \pmod{p}$. This means a is a root of the polynomial $x^4 - 1 = (x^2-1)(x^2+1)$ in $\mathbb{Z}_p[x]$. But also, a has order 4 so $a^2 \neq 1 \pmod{p}$. This means that a cannot be a root of $x^2 - 1$. Thus it is a root of x^2+1 so that $a^2+1 = 0 \pmod{p}$ (i.e. $a^2 = -1 \pmod{p}$).

Proposition: Let p be a prime integer. $x^2 = -1 \pmod{p}$ has an integer solution iff $p \neq 3 \pmod{4}$.

proof: First, any prime integer congruent to 0 or 2 (mod 4) must be even. The only such prime is $p = 2$. Notice that $1^2 = 1 = -1 \pmod{2}$. Thus we can turn our attention to odd primes. Assume p is odd.

Suppose that $x^2 = -1 \pmod{p}$ has an integer solution, say a. Then by the previous lemma $|a| = 4$ in the group $\mathbb{Z}_p^\times$. Notice that $|\mathbb{Z}_p^\times| = p-1$. So 4 divides $p-1$. Therefore, $p = 1 \pmod{4}$. [Thus $p \neq 3 \pmod{4}$ for any such prime.]

Conversely, if $p \neq 3 \pmod{4}$, then since p is odd we have that $p = 1 \pmod{4}$. Therefore, 4 divides $p-1$. The group $\mathbb{Z}_p^\times$ is cyclic (we will eventually prove that *any finite subgroup* of the group of units of a field is cyclic). Therefore, this group must have an element of order 4, say a. Therefore, by the lemma above a is an integer solution of $x^2 = -1 \pmod{p}$.

In summary, we've proven the following theorem...

Theorem: Let p be a prime integer. The following are equivalent:

- $p = \pi\overline{\pi}$ for some Gauss prime π.
- $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.
- $x^2 = -1 \pmod{p}$ has an integer solution.
- $p \neq 3 \pmod{4}$.

This theorem allows us to identify the primes in $\mathbb{Z}[i]$. Factorizations can now be accomplished by focusing on factoring (as an integer) the norm of an element and then seeing what that says about the element in $\mathbb{Z}[i]$.

Example: $6+2i = 2(3+i)$. Notice that $N(3+i) = 3^2+1^2 = 10$ so $3+i$ isn't a Gauss prime. $10 = 2 \cdot 5$. $2 = (1+i)(1-i)$ and $5 = (1+2i)(1-2i)$. Thus $(1+i)(1-i)(1+2i)(1-2i) = 2 \cdot 5 = 10 = (3+i)(3-i)$ so because $\mathbb{Z}[i]$ is a UFD, the prime factors of $3+i$ must be found among $1 \pm i$ and $1 \pm 2i$. Through trial and error we find that $3+i = (1-i)(1+2i)$. Thus $6+2i = 2(3+i) = (1+i)(1-i)(1-i)(1+2i) = (1+i)(1-i)^2(1+2i)$.

Example: $6+9i = 3(2+3i)$. Notice that $3 = 3 \pmod{4}$ so 3 is not only a prime but also a Gauss prime. Next, $N(2+3i) = 2^2+3^2 = 13$ (prime) so $2+3i$ is also a Gauss prime. Therefore, $6+9i = 3(2+3i)$ is a prime factorization.

(g) Factor 700 in $\mathbb{Z}$ and then in $\mathbb{Z}[i]$.

(h) Factor $33+77i$ in $\mathbb{Z}[i]$.

Matching Problem In the following list of rings, each ring is isomorphic to exactly one other ring on the list. Pair them up! Justify your pairings (find homorphisms and use the isomorphism theorem) and explain why non-paired rings aren't isomorphic.

- $\mathbb{Q}[x]/(x^2)$
- $\mathbb{Q}[x]/((x-1)^2)$
- $\mathbb{Q}[x]/(x^2-1)$
- $\mathbb{Q} \times \mathbb{Q}$

Page 31 #45 A quotient of $\mathbb{Q}[x]$.

(a) Find the GCD of $x^3 - 2x^2 + 1$ and $x^2 - x - 3$ in $\mathbb{Q}[x]$ and express it as a linear combination (i.e. run the Extended Euclidean Algorithm).

(b) Let $I = (x^2 - x - 3)$. Is $x^3 - 2x^2 + 1 + I$ zero, a zero divisor, or a unit in ${}^{\mathbb{Q}[x]}\!/_{I}$? Prove your result (If zero, why? If a zero divisor, what is a non-zero element that multiplied by gives zero? If a unit, what's its inverse?).

(c) Let $I = (x^2 - x - 3)$. Is $x + I$ zero, a zero divisor, or a unit in ${}^{\mathbb{Q}[x]}\!/_{I}$? Prove your result (If zero, why? If a zero divisor, what is a non-zero element that multiplied by gives zero? If a unit, what's its inverse?).

Prime, maximal, both, or neither? Identify the following ideals as prime, maximal, both, or neither.

(a) $(x^2 - 5)$ in $\mathbb{Q}[x]$

(b) $(x^2 - 5)$ in $\mathbb{R}[x]$

(c) $(x^2 + 1)$ in $\mathbb{Q}[x]$

(d) $(x^2 + 1)$ in $\mathbb{Z}[x]$

Finite Field Construct the finite field of order 9. Express $\mathbb{F}_9$ as a quotient of $\mathbb{Z}_3[x]$. You don't have to write out full addition and multiplication tables, but I do want you to compute the additive inverse, multiplication inverse, and order (in $\mathbb{F}_9^\times$) of each (non-zero) element.

A Rational Problem As in the Factorization Handout, compute the inverse of $x^2 + x + 2 + I$ in ${}^{\mathbb{Q}[x]}\!/_{I}$ where $I = (x^3 - 3)$.

Then use this result to rationalize the fraction $\dfrac{1}{2 + 3^{1/3} + 3^{2/3}}$ (i.e. write this fraction as $a + b \cdot 3^{1/3} + c \cdot 3^{2/3}$ for some $a, b, c \in \mathbb{Q}$).