Math 4720/5210 # Homework #3 **Due: Mon., Feb. 12^{th}, 2024**

#1 Gaussian Integers 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 $0 \neq n \in \mathbb{Z}$. Notice if n properly factors in $\mathbb{Z}$, then it also properly factors in $\mathbb{Z}[i]$. However, the converse does not necessarily hold (for example, $5 = (1 + 2i)(1 - 2i)$ is a proper factorization on $\mathbb{Z}[i]$ but 5 is irreducible in $\mathbb{Z}$). 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) Run through the standard argument showing that elements of norm 1 are units and vice-versa. Then use that to identify the units of the Gaussian integers (i.e., $\mathbb{Z}[i]^\times$).

(b) Show that π is a Gauss prime iff $\bar{\pi}$ is a Gauss prime. [*Note:* Prime = irreducible since $\mathbb{Z}[i]$ is a UFD.]

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

(d) Let p be a positive prime (integer). Show that either p is a Gauss prime or $p = \pi\bar{\pi}$ for some Gauss prime π.
Hint: If p properly factors, what do norms tell us?

(e) Let p be any 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: 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 (so π is not a unit – thus $N(\pi) > 1$). By part (b), we also know $\bar{\pi}$ is also Gauss prime. Consider $\pi\bar{\pi} = N(\pi) \in \mathbb{Z}_{>1}$. Either $N(\pi)$ is a prime integer (done) or it properly factors in $\mathbb{Z}$ (and thus also in $\mathbb{Z}[i]$), say $N(\pi) = AB$ for some $A, B \in \mathbb{Z}_{>1}$. Considering part (a), A and B are definitely not units in $\mathbb{Z}[i]$. Now A and B can be factored into irreducibles in $\mathbb{Z}[i]$ (since it is a UFD). However, $\pi\bar{\pi}$ is already a factorization into irreducibles. Therefore, A and B cannot be properly factored in $\mathbb{Z}[i]$ (otherwise AB would have more irreducible factors than the factorization $\pi\bar{\pi}$ does). Thus A and B do not properly factor in $\mathbb{Z}$ (i.e., they are prime integers). Finally, by uniqueness of factorizations, either π is an associate of A and $\bar{\pi}$ of B or vice-versa. WLOG assume the former. Recalling that associates share the same norms as do conjugates: $A^2 = N(A) = N(\pi) = N(\bar{\pi}) = N(B) = B^2$ (i.e., $N(\pi)$ is the square of a prime integer).

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

proof: In a PID, an ideal (r) is maximal (i.e., the associated quotient ring is a field) if and only if r is irreducible (=prime). Therefore, since $\mathbb{Z}[i]$ is a PID, p is a Gauss prime exactly when $\mathbb{Z}[i]/(p)$ is a field. Since $\mathbb{Z}[i]\big/(p) \cong \mathbb{Z}[x]\big/(p, x^2+1) \cong \mathbb{Z}_p[x]\big/(x^2+1)$, we have $\mathbb{Z}[i]/(p)$ is a field if and only if $\mathbb{Z}_p[x]/(x^2 + 1)$ is a field (i.e., $(x^2 + 1)$ is maximal in $\mathbb{Z}_p[x]$). But $\mathbb{Z}_p[x]$ is also a PID, so this is true if and only if $x^2 + 1$ 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: Apply the lemma and keep in mind (when working over a field): quadratics are irreducible iff they have no roots.

Lemma: Let p be an odd prime (integer). Then $a \in \mathbb{Z}$ 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: Since p is odd, $-1 \neq 1 \pmod{p}$. If a is a solution (i.e., $a^2 = -1 \bmod p$), then the order of a is not 1 or 2. However, $a^4 = (-1)^2 = 1 \pmod{p}$. Thus the order of a is 4. Conversely, if a has order 4, then $a^4 = 1 \pmod{p}$. Therefore, a is a root of $x^4 - 1 = (x^2 - 1)(x^2 + 1)$ in $\mathbb{Z}_p[x]$. But a has order 4, so $a^2 \neq 1 \pmod{p}$. This means that a is not a root of $x^2 - 1$. Therefore, a must be a root of $x^2 + 1$ (i.e., $a^2 + 1 = 0 \bmod p$). Thus $a^2 = -1 \pmod{p}$.

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, $p = 1 \neq 3 \pmod{4}$.

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 have proven the following theorem...

Theorem: Let p be a positive 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 $3 + i$ is not 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 $\mathbb{Z}[i]$.

#2 Euclid's Revenge! 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).

Note: I would like you to practice doing this by hand, but this can be very tedious. If you would like to check your work with software, Maple can be coaxed into doing these calculations. Alternatively, I have written some Sage demos which can automate this calculation: https://www.BillCookMath.com/sage

Specifically, https://www.BillCookMath.com/sage/algebra/Euclidean_algorithm-poly.html is what we want here.

(b) Let $I = (x^3 - 2x^2 + 1)$. Is $x^2 - x - 3 + I$ 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 $I = (x^3 - 2x^2 + 1)$. Is $x^2 - 1 + I$ 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?).

#3 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 $\mathbb{Z}[x]$

#4 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 $a, b, c \in \mathbb{Q}$).