MAT 347
Factorization in the Gaussian integers
January 14, 2020

We know that $\mathbb{Z}[i]$ is a Euclidean domain (see homework), hence a PID, hence a UFD. Thus prime and irreducible mean the same thing in $\mathbb{Z}[i]$. We want to list all irreducibles in $\mathbb{Z}[i]$. In the process, we will solve some diophantine equations.

Given $\alpha = x + iy \in \mathbb{Z}[i]$, we define $\overline{\alpha} := x - iy$ and $N(\alpha) = \alpha\overline{\alpha} = x^2 + y^2 \in \mathbb{Z}_{\geq 0}$. Note that the map $\alpha \mapsto \overline{\alpha}$ is a *ring homomorphism*. Therefore $N(\alpha\beta) = N(\alpha)N(\beta)$. (See Example 9 in Alfonso's notes.)

1 Setting up the problem

1. Let $\alpha \in \mathbb{Z}[i]$. Prove that α is a unit iff $N(\alpha) = 1$.

2. Let $\alpha, \beta \in \mathbb{Z}[i]$. Prove that if $\alpha|\beta \in \mathbb{Z}[i]$ then $N(\alpha)|N(\beta)$ in $\mathbb{Z}$.

3. Let $\pi \in \mathbb{Z}[i]$. Prove that if $N(\pi)$ is irreducible in $\mathbb{Z}$ then π is irreducible in $\mathbb{Z}[i]$.

4. Let $p \in \mathbb{Z}$ be a prime number (i.e., an irreducible/prime element that is positive). Prove that the following three conditions are equivalent:

   (a) p is not irreducible in $\mathbb{Z}[i]$.

   (b) There exists $\alpha \in \mathbb{Z}[i]$ such that $N(\alpha) = p$.

   (c) The equation $x^2 + y^2 = p$ has integer solutions x, y.

5. Let $p \in \mathbb{Z}$ be a prime number. How many irreducibles in $\mathbb{Z}[i]$ of norm p can there be, up to associates? (There are three possible cases.)

6. Let $\pi \in \mathbb{Z}[i]$. Prove that if π is irreducible in $\mathbb{Z}[i]$ then there exists some prime number p such that $\pi|p$ in $\mathbb{Z}[i]$.

   Hint: Show that the ideal $(\pi) \cap \mathbb{Z} \lhd \mathbb{Z}$ is prime and not equal to (0).

   Alternative hint: without ideals, try to use a factorization of $N(\pi)$ inside $\mathbb{Z}$...

The above results together show that, in order to find all irreducibles in $\mathbb{Z}[i]$, all we need to do is find how each prime number p factors in $\mathbb{Z}[i]$. Make sure you understand this before moving on.

2 The three cases

7. Let n be an integer. Assume that $n \equiv 3 \pmod 4$. Show that the equation $x^2+y^2=n$ does not have any integer solutions.

   Hint: Assume it does and reduce the equation mod 4.

8. Is 2 irreducible in $\mathbb{Z}[i]$?

9. Let p be an odd prime number in $\mathbb{Z}$. Prove that there exists $m \in \mathbb{Z}$ such that $p|m^2+1$ iff $p \equiv 1 \pmod 4$.

   Hint: Translate the condition $p|m^2+1$ into a condition in the group $(\mathbb{Z}/p\mathbb{Z})^\times$. Remember what you know about that group.

10. Let $p \in \mathbb{Z}$ be a prime number such that $p \equiv 1 \pmod 4$. Prove that p is not prime in $\mathbb{Z}[i]$.

    Hint: $m^2+1=(m+i)(m-i)$.

3 Summary

11. Let $p \in \mathbb{Z}$ be a prime number. How many irreducibles with norm p are there in $\mathbb{Z}[i]$, up to associates? How many irreducibles with norm p^2 are there in $\mathbb{Z}[i]$, up to associates?

    Note: Your answer will depend on p.

12. Let $p \in \mathbb{Z}$ be a prime number. Does the equation $x^2+y^2=p$ have integer solutions (x,y)? If so, how many?

    Note: Your answer will depend on p.

13. Let n be a positive integer. Does the equation $x^2+y^2=n$ have integer solutions? If so, how many?

    Note: Your answer will depend on n. *Hint:* use the existence and uniqueness of factorizations into irreducibles in the UFD $\mathbb{Z}[i]$ and that the norm N is multiplicative. If you get stuck, first try $n=2^k$ of 3^k or 5^k.

14. Find all integer solutions to the equation $x^2+y^2=585$.