MAT 347
Factorization in the Gaussian integers
January 23, 2015

We have proven that $\mathbb{Z}[i]$ is a Euclidean domain, hence a PID, hence a UFD. Hence 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.

Recall that given $\alpha = x+iy \in \mathbb{Z}[i]$, we define $\overline{\alpha} := x-iy$ and $N(\alpha) = \alpha\overline{\alpha} = x^2+y^2 \in \mathbb{Z}$.

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 prime in $\mathbb{Z}$ then π is irreducible in $\mathbb{Z}[i]$.
4. Let $p \in \mathbb{Z}$ be irreducible in $\mathbb{Z}$. 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 be a prime in $\mathbb{Z}$. How many irreducibles in $\mathbb{Z}[i]$ of norm p may there be? (There are three possible answers.)
6. Let $\pi \in \mathbb{Z}[i]$. Prove that if π is irreducible in $\mathbb{Z}[i]$ then there exists some p irreducible in $\mathbb{Z}$ such that $\pi|p$ in $\mathbb{Z}[i]$.

   Hint: Show that the ideal $(\pi) \cap \mathbb{Z} \trianglelefteq \mathbb{Z}$ is prime.

The above results together suggest that, in order to find all irreducibles in $\mathbb{Z}[i]$, all we need to do is find how each irreducible in 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 $n \equiv 3 (\text{mod } 4)$. 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 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 $(\mathbb{Z}/\mathbb{Z}p)^{\times}$. Remember what you know about that group.

10. Let p a prime in $\mathbb{Z}$ 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 be a prime in $\mathbb{Z}$. How many irreducibles with norm p are there in $\mathbb{Z}[i]$? How many irreducibles with norm p^2 are there in $\mathbb{Z}[i]$?

    Note: Your answer will depend on p.

12. Let p be a prime in $\mathbb{Z}$. 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.

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