Algebra - I
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

ALGEBRA I

Gaussian integers form a Euclidean domain. The size function is defined

$$d(a + bi) = a^2 + b^2.$$

We must establish that for all $m, n \in \mathbb{Z}[i]$ there exist Gaussian integers q and r such that

$$n = qm + r,$$

with $d(r) < d(m)$.

So, what to understand this, what we do is firstly, you fix m ok. So, in the complex plane, you can think of m as a vector. So, you have 0 and then, you have a vector m . To the complex number m and you can think of you can draw a vector from 0 to m ok and consider the lattice L equal to qm where q belongs to the Gaussian integers ok. Another way of think of this lattice is you consider the vector m and then, you consider the vector im, and the lattice L can be written as $am + bim$ where a and b are inside just because every q in the Gaussian integers of the form $a + bi$.

Now, I claim that for every $n \in Z[i]$, there exists $q \in Z[i]$ such that $d(n - qm) < d(m)$. In fact, I claim that every complex number inside a square lies inside one of the squares of the lattice L. So, every point in the complex plane lies inside one of these squares.

So, these are points in L and each point in a square of size so, what is the size here? The size here is $\sqrt{d(m)}$. Now, each side, each point in a square of side $\sqrt{d(m)}$ cannot be more than a distance $\sqrt{\frac{d(m)}{2}}$.

So, what we have is that there exist $qm \in L$ such that $z - qm$ is the distance from z to qm is less than $\sqrt{\frac{d(m)}{2}}$.

So, in fact, every complex number is close enough to one of these lattice points. So, $n = qm + r$ where $d(r) < d(m)$, you can conclude that the ring of Gaussian integers is a principal ideal domain.