Number Theory

Lectured by Meng T. Heang

June 18, 2022

Chapter 1

Quadratic Ring

The motivation of this comes from the fact that solving equations like $x^n + y^n = z^n$ is rather hard. For example, case $n = 2$, the equation becomes

$$z^2 = x^2 + y^2 = (x + \mathrm{i}y)(x - \mathrm{i}y)$$

so we need a language to say that $(x + \mathrm{i}y)$ is a divisor of z^2, I guess. And here comes the

Definition 1.1. For any square-free (not a perfect square) integer d, we define

$$\mathbb{Z}[\sqrt{d}] := \{x + y\sqrt{d} \ : \ x, y \in \mathbb{Q}\}.$$

In $\mathbb{Z}[\sqrt{d}]$, we define the usual addition and multiplication as follow: for $a + b\sqrt{d},\ x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, then

$$(a + b\sqrt{d}) + (x + y\sqrt{d}) = (a + x) + (b + y)\sqrt{d}$$

and

$$(a + b\sqrt{d})(x + y\sqrt{d}) = (ax + byd) + (ay + bx)\sqrt{d}$$