Algebraic Number Theory

Vinesh Ramgi

January 18, 2019

Abstract

What did the number theorist say as he drowned?

Log, log, log, log....

For an up to date version of this pdf, check my GitHub :)

https://github.com/vrvinny/algebraic_nt

Contents

1 Introduction/Review

1.1 Introduction

This is the study of certain rings, numbers called algebraic integers, e.g.

- Quadratic rings $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$
- Cyclotomic rings $\mathbb{Z}[\zeta_n] \implies y = e^{2\pi\imath/n}$
- $\mathbb{Z}[z\sqrt{2}] = \{x + y^3\sqrt{2} + z^3\sqrt{z}^2\}$ $x, y, z \in \mathbb{Z}$

Defintion 1.1. *A Diophantine equation is an equation of the form* $f(x_1, \ldots, x_n) = 0$ *where* f *is a polynomial with coefficients in* $\mathbb{Z}$

We'll usually be interested in solution in integers (or maybe rational numbers), for example, Pell's equation- $x^2 - dy^2 = 1$, or $N(A) = n$ where $A = x + y\alpha$, $\alpha = \{\sqrt{d}, \frac{1+\sqrt{d}}{2}\}$.

In general Diophantine equations are hard, Matiyasevich's theorem shows Diophantine equations are as hard as any mathematical question. Inspite of this, there are some Diophantine eqations for which we have methods for solving, e.g. *What are the integer solutions of* $x^3 = y^2 + y = y(y+1)$?.

Since $y, y+1$ are both coprime and their product is a cube, both y and $y+1$ are a cube which implies $y = 0, -1$. So we have two solutions, $(0, 0), (0, -1)$. To do this we used this lemma:

Lemma 1.2. *Descent Lemma*

Let R *be a ring be a unique factorisation domain. Suppose* $a, b, c \in R$ *and* $a^n = bc$*. If* b, c *are coprime in* R *then* $b = u^{rn}$, $c = vs^n$ *where* u, v *are units in* R*.*

Another example, $x^3 = y^2 + 1$:

Problem, $y^2 + 1$ doesn't factorise in $\mathbb{Z}$ but it does factorise in $\mathbb{Z}[i] \implies x^3 = (y+i)(y-i)$. We want to use the Descent lemma to solve the equation.

- $\mathbb{Z}[i]$ is a unique factorisation domain
- Are $y + i$ and $y - i$ coprime in $\mathbb{Z}[i]$?

Suppose $p \in \mathbb{Z}[i]$ is an irreducible common factor of $y+i$, $y-i$. If $p|y+i$ and $p|y-i \implies p|(y+i) - (y-i) \implies p|2i$. This means the norms also divide each other, $N(p)|N(2i) \implies N(p)|4$.

$N(p) \neq \pm 1$ because p isn't a unit, therefore, $2|N(p)|N(y+i) \implies N(y+i) = y^2 + 1 = x^3$, so $2|x^3$.

Since 2 is a prime, $2|x \implies x^3 \equiv 0 \pmod{8}$. This implies $y^2 + 1 \equiv 0 \pmod{8}$

y	$y^2 \mod 8$
0	0
± 1	1
± 2	4
± 3	1
4	0

Since the equation has no solutions, $y^2 + 1 \equiv 0 \pmod{8}$ has no solutions.
So $y + i, y - i$ are coprime in $\mathbb{Z}[i]$.