Math 620: Algebraic Number Theory

David Zhu

August 26, 2025

Started with Calabi's computation of $\zeta(1)$ and $\zeta(2)$ with an ingenious integral and change of variables.

1 Algebraic Numbers, Algebraic Integers

Theorem 1.1 (Liouville Theorem)**.** If x is a irrational number of degree n over the rationals, then there exists a constant c such that

$$|x - \frac{p}{q}| > \frac{c}{q^n}$$

for all $p, q > 0$.

The remark is algebraic numbers are harder to estimate with rationals with small denominators.

Example 1.1.1. The real number

$$\alpha = \sum_{n=0}^{\infty} 10^{-n!}$$

is transcendental.

One can show the example is indeed transcendental because it violates the bound of Theorem 1.1.

Theorem 1.2 (Apery, $\sim$ 1980)**.** The real number

$$\zeta(3) = \sum_{n=1}^{\infty} n^{-3}$$

is irrational.

Theorem 1.3 (Thue-Siegel-Roth)**.** Suppose α is algebraic and irrational, $\epsilon > 0$. Then, there is $c(x, \alpha)$ such that

$$|\alpha - \frac{p}{q}| > \frac{c(x, \alpha)}{q^{2+\epsilon}}$$

with $q > 0$.

Note that the proof is not effective.

1.1 Continued Fractions

Theorem 1.4. Quadratic irrationals are characterized by having infinite conitnued fractions that are evetually periodic.

Theorem 1.5 (Hurwitz)**.** If α is irrational, then there are infinitely many $\frac{p}{q}$

$$|\alpha - \frac{p}{q}| < \frac{p}{\sqrt{5}q^2}$$

Moreover, $\sqrt{5}$ is the best bound.

Remark 1.5.1. The 'Lagrange Spectrum' says something about how difficult to approximate an irrational by rationals. The are related to the constant $\sqrt{5}$ appearing in Theorem 1.5.

Definition 1.5.1. The **Markov triple** is a triple (m, n, p) such that

$$m^2 + n^2 + p^2 = 3mnp$$

A **Markov number** is any number appearing in a Markov triple.

These Markov triples are related to algebraic geometry of $K3$ surfaces.

2 Integrality

Definition 2.0.1. Suppose $A \leq R$ are commutative rings. An $x \in R$ is **integral** over A if satisfies a monic polynomial with coefficients in A.

Example 2.0.1. $R := F[u, v]/(v^2 - (u^2 + au + b))$ defines an elliptic curve, and R is integral over $F[u]$.

Note that given a ring extension $A \to B$, elements in B integral over A forma subring of B.

Definition 2.0.2. Given a ring extension $A \to B$, the integral closure of A with respect to the extension is the subring of B that contains the integral elements over A.

Definition 2.0.3. A **number field** is a finite extension of $\mathbb{Q}$.

By the primitive element theorem, we know every nymber field is of the form $\mathbb{Q}[u]$ for some primitive u.

Example 2.0.2. A **Kummer extension** is a number field of the form

$$\mathbb{Q}[x]$$

where $x^n - a = 0$ for some $a \in \mathbb{Q}$.

Theorem 2.1 (Kronecker-Weber)**.** The abelian number fields over the rationals are subfields of the cyclotomic number fields $\mathbb{Q}(\zeta_n)$.

Definition 2.1.1. The **ring of integers** $\mathcal{O}_K$ associated to a number field K is the integral closure of $\mathbb{Z}$ in K. Alternatively, it is the subring of all algebraic integers in K.