不定方程相关理论及其应用

郑欢誉

2024 年 12 月 28 日

开题报告目录

Contents of Thesis Proposal

开题报告目录

Contents of Thesis Proposal

开题报告目录

Contents of Thesis Proposal

研究背景和意义

Research Background & Significance

$$x^n + y^n = z^n$$

1637 *Pierre de Fermat*：提出猜想

1839 $n = 3, 4, 5, 7$，无穷递降

1847 ***Ernst Kummer*：唯一分解，理想**；n 正规素数（不整除 $\mathbb{Q}(\zeta_n)$ 的类数）

1994 *Andrew Wiles*，模形式和椭圆曲线

文献调研

Literature Research

$x^n + y^n = z^n$ no integer solution (x, y, z) for $2 < n$

$\overset{\textit{analysis}}{\Longrightarrow}$ suffices to consider situation where $n = p$ odd prime & x, y, z coprime

$\overset{\textit{in } \mathbb{Q}(\zeta_p)}{\Longrightarrow}$ $(x + y)(x + \zeta_p y) \cdots (x + \zeta_p^{p-1} y) = z^p$ $\Leftarrow$ decomposition in $\mathbb{Z}[\zeta_p]$

文献调研

Literature Research

"to what extend unique factorization fails or holds in number fields?"

factorization with respect to what subring? $\Longrightarrow$ ring of integers

recovering unique factorization $\Longrightarrow$ ideal

a way to measure by how much unique factorization fails? $\Longrightarrow$ class number

simplifying how prime acts $\Longrightarrow$ regular primes

the structure of the group of units in the ring of integers? $\Longrightarrow$ unit theorem

文献调研

Literature Research

"to what extend unique factorization fails or holds in number fields?"

factorization with respect to what subring? $\Longrightarrow$ ring of integers

recovering unique factorization $\Longrightarrow$ ideal

a way to measure by how much unique factorization fails? $\Longrightarrow$ class number

simplifying how prime acts $\Longrightarrow$ regular primes

the structure of the group of units in the ring of integers? $\Longrightarrow$ unit theorem

文献调研

Literature Research

"to what extend unique factorization fails or holds in number fields?"

factorization with respect to what subring? $\Longrightarrow$ ring of integers

recovering unique factorization $\Longrightarrow$ ideal

a way to measure by how much unique factorization fails? $\Longrightarrow$ class number

simplifying how prime acts $\Longrightarrow$ regular primes

the structure of the group of units in the ring of integers? $\Longrightarrow$ unit theorem

文献调研

Literature Research

"to what extend unique factorization fails or holds in number fields?"

factorization with respect to what subring? $\Longrightarrow$ ring of integers

recovering unique factorization $\Longrightarrow$ ideal

a way to measure by how much unique factorization fails? $\Longrightarrow$ class number

simplifying how prime acts $\Longrightarrow$ regular primes

the structure of the group of units in the ring of integers? $\Longrightarrow$ unit theorem

文献调研

Literature Research

"to what extend unique factorization fails or holds in number fields?"

factorization with respect to what subring? $\Longrightarrow$ ring of integers
recovering unique factorization $\Longrightarrow$ ideal
a way to measure by how much unique factorization fails? $\Longrightarrow$ class number
simplifying how prime acts $\Longrightarrow$ regular primes
the structure of the group of units in the ring of integers? $\Longrightarrow$ unit theorem

文献调研

Literature Research

Kummer: splits the problem (regular cases) into

x, y, z all coprime with p v.s. exactly one divisible by p

$$\prod_{i=0}^{p-1}\langle x+\zeta_p^i y\rangle = \langle z\rangle^p \quad | \quad \prod_{i=0}^{p-1}\langle x+\zeta_p^i y\rangle = I^{pm}\langle z_0\rangle^p$$

文献调研

Literature Research

FLT & ABC conjecture:

(ABC conjecture): $\forall \epsilon > 0$, $\exists$ constant k_ϵ s.t. for any coprime integers a, b, c satisfying $a + b = c$,

$$c \leq k_\epsilon \left(\prod_{p \text{ prime},\, p \mid abc} p \right)^{1+\epsilon}$$

- ABC $\Longrightarrow$ FLT (Goldfeld, 1999)
- improvements on subexponential ABC (Hector, 2024)

文献调研

Literature Research

Asymptotic Fermat's Last Theorem:

(Asymptotic FLT): K a number field, there is a bound B_K, depending only on the field K, such that for all prime exponents $p > B_K$, there is no nontrivial solution to

$$x^p + y^p + z^p = 0$$

- established the asymptotic Fermat's Last Theorem for many infinite families of number fields via class field theory (Freitas, 2020)

文献调研

Literature Research

Formalization (Riccardo, 2024):

```
variable {p : ℕ+} {K : Type*} [Field K] [NumberField K]
  [IsCyclotomicExtension {p} ℚ K]

variable {ζ : K} (hζ : IsPrimitiveRoot ζ p)

def IsRegularNumber (n : ℕ) [hn : Fact (0 < n)] : Prop :=
  n.Coprime <| Fintype.card <| ClassGroup (𝓞 <| CyclotomicField ⟨n, hn.1⟩ ℚ)

def IsRegularPrime (p : ℕ) [Fact p.Prime] : Prop := IsRegularNumber p

theorem flt_regular {p : ℕ} [Fact p.Prime] (hreg : IsRegularPrime p) (hodd : p ≠ 2) :
FermatLastTheoremFor p := sorry
```

研究方案和进度安排

Research Scheme & Scheduling

1-2 月 代数数论和交换代数（*Ian&Tall*，*Ash*，*Milne*，*Matsumura*）
理解掌握 *Kummer* 关于正规素数情况的证明

2-3 月 通过 *Hector* 和 *Andrew* 的工作学习费马大定理与 *ABC* 猜想间的关联
利用类域论拓展性地了解渐进费马大定理

3-4 月 形式化相关工作


1896
XI'AN JIAOTONG UNIVERSITY