Solving Fermat Type Equations by Modular Approach

Yasemin Kara

Boğaziçi University

May 25, 2021

Solving Fermat Type Equations by Modular Approach

Yasemin Kara

Boğaziçi University

May 25, 2021

Diophantine Equations

Diophantine Equation: an indeterminate polynomial equation with integral coefficients for which integral solutions are sought

- $ax + by = c$: linear equation
- $y^2 = x^3 + ax + b$: elliptic curve
- $x^n + y^n + z^n = 0$: Fermat's equation
- $Ax^n + By^n + Cz^n = 0$: generalized Fermat's Equation
- $x^p + y^q + z^r = 0$: Fermat's equation with signature (p, q, r)

Fermat's Last Theorem

- **Fermat's Last Theorem:** The equation $x^n + y^n + z^n = 0$, where x, y, z and n are integers, has no non-trivial solutions ($xyz \neq 0$) for $n > 2$.

- It is sufficient to consider cases $n = 4$ and n is an odd prime.

- $n = 4$: Fermat
  $p = 3, 5, 7$: Euler, Legendre, Dirichlet, Gauss, Lamé

- p is regular prime i.e. $p \nmid h(\mathbb{Q}(\zeta_p))$, $\zeta_p = e^{2\pi i/p}$: Kummer

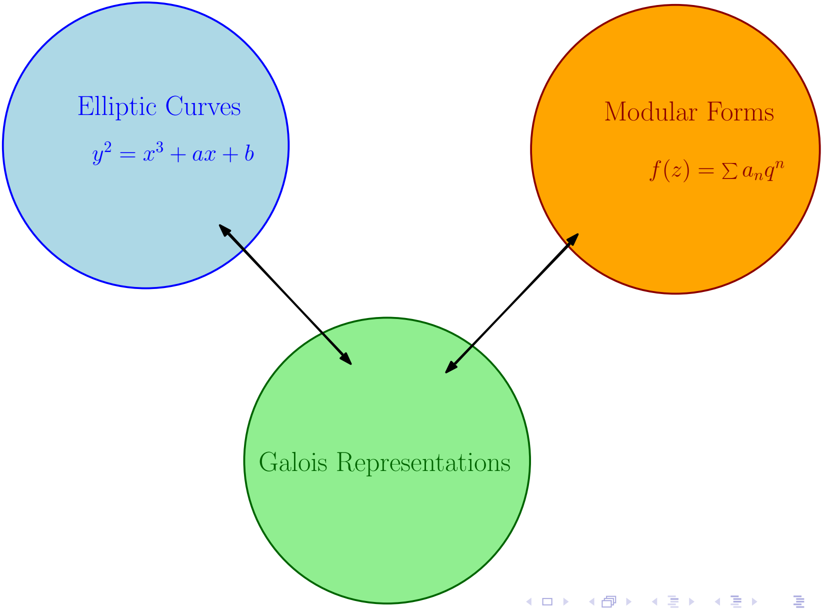
Theorem (Wiles, Taylor, 1995)

Let $p \geq 3$ be a prime. Then $x^p + y^p + z^p = 0$ has no non-trivial integer solutions.

Modular approach

- Find an elliptic curve associated to a putative solution
- Show that this elliptic curve has properties contradicting to each other
    1. Modularity theorem (Wiles, Taylor-Wiles)
    2. Irreducibility of Galois representations (Mazur)
    3. Level lowering theorem (Ribet)

Comparing Different Worlds

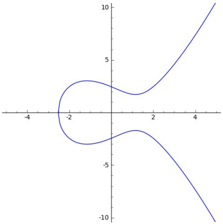


Elliptic curves

Definition

An elliptic curve E over a field K is a smooth, projective algebraic curve of genus one, on which there is a specified point $\mathcal{O}$. The point $\mathcal{O}$ is called point at infinity.

- Given by $y^2 = x^3 + ax + b$, where a, b are in K if $\mathrm{char}(K) \neq 2, 3$.
- $E(K) = \{(x, y) \in K^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$.
- No cusp or self-intersection, $E : y^2 = x^3 - 4x + 6$ over $\mathbb{R}$



Elliptic curves mod p

- Given E, we can reduce it modulo p.
- Then we say E has good reduction at p if the reduced curve $\tilde{E}$ is smooth.
- We say E has bad reduction at p if the reduced curve $\tilde{E}$ is singular.
- There can be only finitely many bad primes. The conductor of E, denoted by N_E, is an invariant of E which encodes the bad primes.

Example

$E : y^2 = x^3 - x + 1$, find solutions mod 3.
$E(\mathbb{F}_3) = \{(0,1),(0,2),(1,1),(1,2),(2,1),(2,2)\}$. Note that point at ∞ is always in the set of solutions, $|E(\mathbb{F}_3)| = 7$.

- We can do this modulo many other primes p.
  Say N_p is the number of solutions mod p.

p	3	5	7	11	13	17	19	29	31	37	41
N_p	7	8	12	10	19	14	22	37	35	36	51

- Number of solutions increase as p increases.

Definition

For an elliptic curve E, define $a_p = p + 1 - N_p$.

- Can we predict a_p?
- For example, for $E : y^2 = x^3 - x + 1$ we have

p	3	5	7	11	13	17	19	29	31	37	41
N_p	7	8	12	10	19	14	22	37	35	36	51
a_p	-3	-2	-4	2	-5	4	-2	-7	-3	2	-9

Modular Forms

- A modular form of weight $2k$ wrt $\mathrm{SL}_2(\mathbb{Z})$ is a holomorphic function on the upper half plane satisfying :

$$f(\frac{az+b}{cz+d}) = (cz+d)^{2k} f(z), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

  and a growth condition.

- **newform of level N**: a special kind of modular form for the group $\Gamma_0(N)$.

- Modular forms have power series representations i.e. they can be written as $\sum_{n=0}^{\infty} c_n q^n$ where $q = e^{2\pi i}$.

- Let E/K be an elliptic curve and $m \in \mathbb{Z}$ with $m \geq 1$. The m-torsion subgroup of E, denoted by $E[m]$, is the set of points of E of order m,

$$E[m] = \{P \in E(K) : [m]P = O\}.$$

- $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ if $char(\overline{K}) = 0$.

- Let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. For an elliptic curve E/K,

$$\overline{\rho}_{E,p} : G_K \longrightarrow \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

denotes the mod p Galois representation of E.

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

Three main ingredients:

- Modularity Thm: Every elliptic curve over $\mathbb{Q}$ is associated to a rational newform of level N i.e.
  there is a newform $f(z) = \sum_{n=1}^{\infty} c_n q^n$ such that
  $c_l = a_l(E) = l + 1 - |E(\mathbb{F}_l)|$.
- Mazur's Thm: If E is an elliptic curve over $\mathbb{Q}$ with full two torsion then E doesn't have any p isogenies for $p \geq 5$ (irreducibility of Galois representations attached to the elliptic curve for each p)
- Ribet's Thm: Sometimes it is possible, due to Ribet's work, to replace f by another newform of smaller level if we have modularity of E and irreducibility of mod p Galois representations.

Basic sketch

- Suppose (a, b, c) is a solution.
  Scale a, b and c so that they become coprime integers.

- Attach the Frey elliptic curve to this solution:

$$E : y^2 = x(x - a^p)(x + b^p).$$

- Let $\bar{\rho}_{E,p}$ be its mod p Galois representation.

- $\bar{\rho}_{E,p}$ is irreducible by Mazur[1978] and modular by Wiles[1995].
- Apply Ribet's level lowering theorem[1990] and conclude that $\bar{\rho}_{E,p}$ arises from a weight 2 newform f of level 2.
- There are no such newforms at this level, so we get a contradiction.
- Hence, the equation $x^p + y^p + z^p = 0$ does not have any solutions.

Fermat equation over higher degree number fields

- K: a number field
- $\mathcal{O}_K$: its ring of integers and p be a prime.
- We refer the equation

$$a^p + b^p + c^p = 0, \quad a, b, c \in \mathcal{O}_K$$

as the *Fermat equation over K* with the exponent p.

Conjecture (Asymptotic Fermat Conjecture)

Let K be a number field such that $\zeta_3 \notin K$. There is a constant B_K depending only on K such that for any prime $p > B_K$, all solutions to the Fermat equation are trivial i.e. $abc = 0$.

- treat the Fermat equation with fixed exponent p as a curve and determine the points of low degree (i.e. points defined over number fields of low degree) on the Fermat curve

  For $p = 3, 5, 7$ and 11, Gross and Rohrlich (78) determined the solutions to $x^p + y^p + z^p = 0$ over all number fields K of degree $\leq (p-1)/2$.

- try to use modular approach

Theorem (Jarvis and Meekin, 2004)

The Fermat equation $x^n + y^n = z^n$ has no solutions $x, y, z \in \mathbb{Q}(\sqrt{2})$ with $xyz \neq 0$ and $n \geq 4$.

Example (Serre and Mazur)

- Consider the equation

$$x^p + y^p + L^r z^p = 0,$$

where $L = 1$ or an odd prime and $0 < r < p$, $p \neq L$, $p \geq 5$ prime.

- Assume $(x, y, z) \in \mathbb{Z}^3$ is a non-trivial solution and $gcd(x, y, Lz) = 1$.

- Let $(A, B, C) = (x^p, y^p, L^r z^p)$, $A \equiv -1 \pmod 4$ and $2|B$.

- $E : Y^2 = X(X - A)(X + B)$ (Frey curve)

- Mazur, Wiles, Ribet $\implies$ $E \sim f$ and f newform of weight 2 and level $N = 2L$

- If $L = 1$, then $N = 2$ (the FLT case). Since there are no newforms of weight 2 and level 2, there are no non-trivial solutions for $L = 1$.

- There are no newforms of weight 2 and levels $6, 10, 22$, i.e. there are non non-trivial solutions for $L = 3, 5, 11$.

- There are newforms of weight 2 and level $2L$ for $L = 7, 13, 17, \ldots$

- We need to study the relationship between E and f where f has a q-expansion

$$f = q + \sum_{n=1}^{\infty} c_n q^n$$

.

- Let $K_f = \mathbb{Q}(c_1, c_2, \dots)$. K_f is totally real and actually c_n belongs to the ring of integers $\mathcal{O}$ of K_f.

Definition

*A newform f is **irrational** if $K_f \neq \mathbb{Q}$ and **rational** if $K_f = \mathbb{Q}$.*

- It can be shown that if f is irrational,then the exponent p is bounded for non-trivial solutions to $x^p + y^p + L^r z^p = 0$, e.g. this is the case when $L = 37$.

- There is a rational f corresponding to E for the remaining $L = 7, 13, 17, 19, 23, \ldots$.
- **Eichler-Shimura Relation:** A rational weight 2, level N newform f corresponds to an isogeny class of elliptic curves E' defined over $\mathbb{Q}$ of conductor N.
- Actually, this case also can be reduced to the case in which E' is isogenous to an elliptic curve with full 2-torsion.
- **Question:** What are the odd primes L for which there is an elliptic curve E' over $\mathbb{Q}$ with full 2-torsion and conductor $2L$?

Lemma

Let L be an odd prime. Then there is an elliptic curve E' over $\mathbb{Q}$ with full 2-torsion and conductor $2L$ if and only if L is a Mersenne or a Fermat prime and $L \geq 31$.

Proof.

E' has a model

$$E' : y^2 = x(x-a)(x+b)$$

where $a, b \in \mathbb{Z}$, $ab(a+b) \neq 0$, and $\Delta_{E'} = 16a^2b^2(a+b)^2$. We can choose a, b so that the model is minimal away from 2. Hence,

$$a^2b^2(a+b)^2 = 2^u L^v$$

for some nonnegative integers u, v. Then we obtain

$$a = \pm 2^{u_1} L^{v_1}, \quad b = \pm 2^{u_2} L^{v_2}, \quad a+b = \pm 2^{u_3} L^{v_3}$$

It follows that L is a Mersenne or a Fermat prime and $L \geq 31$. □

Theorem (Serre and Mazur)

Let L be an odd prime. Suppose $L < 31$, or L is neither a Mersenne nor a Fermat prime. Then there is a constant C_L s.t.for all primes $p > C_L$ the only solutions $(x, y, z) \in \mathbb{Z}^3$ to the equation $x^p + y^p + L^r z^p = 0$ are the trivial ones satisfying $xyz = 0$.

Summary

- The equation

$$\pm 2^{u_1} L^{v_1} \pm 2^{u_2} L^{v_2} = \pm 2^{u_3} L^{v_3}$$

  is called an S-unit equation with $S = \{2, L\}$.
- It is possible to relate non-trivial solutions to Fermat type equations to solutions of certain S-unit equations.

S-unit Equation

- K: a number field, $\mathcal{O}_K$: its ring of integers
  S: finite set of prime ideals of $\mathcal{O}_K$
- S-integers in K:

$$\mathcal{O}_S = \{\alpha \in K^* : v_{\mathfrak{P}}(\alpha) \geq 0 \text{ for all } \mathfrak{P} \notin S\}$$

- S-units in K:

$$\mathcal{O}_S^* = \{\alpha \in K^* : v_{\mathfrak{P}}(\alpha) = 0 \text{ for all } \mathfrak{P} \notin S\}$$

- The S-unit equation is

$$\lambda + \mu = 1, \quad \lambda, \mu \in \mathcal{O}_S^*$$

Examples of S-units

- $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, and $S = \{2\}$.

  $\mathcal{O}_S = \{\pm 2^r m : m \in \mathbb{Z},\ r \in \mathbb{Z}\},\ \ \mathcal{O}_S^* = \{\pm 2^r : r \in \mathbb{Z}\}$

  S-unit equation solutions : $(1/2, 1/2), (2, -1), (-1, 2)$

- $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, and $S = \{2, L\}$.

  $\mathcal{O}_S = \{\pm 2^r L^s m : m \in \mathbb{Z},\ r, s \in \mathbb{Z}\},$

  $\mathcal{O}_S^* = \{\pm 2^r L^s : r, s \in \mathbb{Z}\}$

- $K = \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_K = \{a(\frac{1+\sqrt{5}}{2}) + b : a, b \in \mathbb{Z}\}$, and $S = \{\emptyset\}$.

  $\mathcal{O}_S^* = \{\pm(\frac{1+\sqrt{5}}{2})^r : r \in \mathbb{Z}\}$,

  S-unit equation solutions : $(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2})$

- $K = \mathbb{Q}(\sqrt{5})$ and $S = \{2\mathcal{O}_K\}$

  $\mathcal{O}_S^* = \{\pm 2^r(\frac{1+\sqrt{5}}{2})^s : r, s \in \mathbb{Z}\}$,

Conjecture (Asymptotic Fermat Conjecture)

Let K be a number field such that $\zeta_3 \notin K$. There is a constant B_K depending only on K such that for any prime $p > B_K$, all solutions to the Fermat equation are trivial i.e. $abc = 0$.

Theorem (Freitas and Siksek, 2015)

Let K be a totally real field. The asymptotic Fermat's last theorem holds for K satisfying some explicitly given, algorithmically testable criterion.

- In particular, they show that the criterion in the above theorem is satisfied by $K = \mathbb{Q}(\sqrt{d})$ for a subset of $d \geq 2$ having density $5/6$ among the squarefree positive integers. This density becomes 1 if "Eichler-Shimura conjecture" is assumed.
- Şengün and Siksek[2018] proved the asymptotic Fermat's Last Theorem holds for any number field K by assuming "modularity".

Assumptions

- **K: totally real number field**
  (I)An "Eichler-Shimura" Conjecture over K: Let K be a totally real field. Let $\mathfrak{f}$ be a Hilbert newform of level $\mathcal{N}$ and parallel weight 2 and with rational eigenvalues. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same L-function as $\mathfrak{f}$.

Assumptions

- **K: a general number field**

(I) Serre's modularity Conjecture over K: This associates a totally odd, continuous, finite flat, absolutely irreducible 2 dimensional mod p representation of $\mathrm{Gal}(\overline{K}/K)$ a cuspform of parallel weight 2 whose level is equal to the prime-to-p part of the Artin conductor of the representation.

(II) An "Eichler-Shimura" Conjecture over K: This associates to a weight 2 cuspform with rational Hecke eigenvalues either an elliptic curve or a "fake elliptic curve".

We call (I) and (II) together as "modularity".

Our results

- K: a number field
  $\mathcal{O}_K$: its ring of integers and p be a prime.

- **generalized Fermat equation:**

  $$Ax^p + By^p + Cz^p = 0 \text{ where } A, B, C \text{ are odd integers}$$

  i.e. if $\mathfrak{P}$ is a prime of $\mathcal{O}_K$ lying over 2, then $\mathfrak{P} \nmid ABC$.

- Our main theorem depends on the "modularity" conjecture since the analogues of modularity theorem have not been proven yet in general.

Our results

Main Theorem (K., Ozman)

K: a number field satisfying the "modularity"

$\mathcal{O}_S^*$: the set of S-units of K,
S: set of primes dividing $2ABC$

S-unit equation: $\lambda + \mu = 1, \qquad \lambda, \mu \in \mathcal{O}_S^*$

Suppose that for every solution (λ, μ) to the S-unit equation, there is some $\mathfrak{P} \in U$ that satisfies

$$max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\} \leq 4v_{\mathfrak{P}}(2).$$

Then there is a constant $\mathcal{B} = \mathcal{B}(K, A, B, C)$ such that the generalized Fermat equation with exponent p and coefficients A, B, C does not have non-trivial solutions with $p > \mathcal{B}$.

Existence and Density Theorems

Density Theorem (K., Ozman)

Assuming the "modularity", the asymptotic Fermat's Last Theorem holds for 5/6 of the imaginary quadratic number fields.

Theorem 1 (K., Ozman)

$K = \mathbb{Q}(\sqrt{-d})$, and $-d \equiv 2, 3 \pmod 4$

$q \geq 29$: prime, and $q \equiv 5 \pmod 8$ and $\left(\frac{-d}{q}\right) = -1$

Assume the "modularity".

Then there exists a constant depending on K and q, namely $B_{K,q}$, such that for all $p > B_{K,q}$ the Fermat equation $x^p + y^p + q^r z^p = 0$ doesn't have any non-trivial solutions.

Theorem 2 (K., Ozman)

$K = \mathbb{Q}(\sqrt{-d})$ and $d \equiv 7 \pmod 8, d \equiv 5 \pmod 6$ and $d \not\equiv 7 \pmod{14}$

Assume the “modularity”.

Then there exists a constant depending on K, namely B_K, such that for all $p > B_K$ the Fermat equation $x^p + y^p + z^p = 0$ doesn't have any nontrivial solutions.

Comparing the two density results

Density Theorem (Freitas,Siksek)

Assuming the "Eichler-Shimura", the asymptotic Fermat's Last Theorem holds for a set of real quadratic fields of density 1.

Density Theorem (K., Ozman)

Assuming the "modularity", the asymptotic Fermat's Last Theorem holds for 5/6 of the imaginary quadratic number fields.

What is the reason for the disparity?

- Because the conclusion of the Eichler-Shimura conjecture over real quadratic fields is stronger than the conclusions of the E-S over imaginary quad. fields

Comparing the two density results

- **K:real quadratic field**

  a rational weight 2 Hilbert eigenform $\mathfrak{f}$ over K corresponds to an ell. curve E/K

- **K: imag. quad. field**

  a rational weight 2 Bianchi eigenform over K corresponds to either an ell. curve E/K or a fake ell. curve A/K (an abelian surface whose endomorphism alg. is an indefinite division quaternion algebra)
- If 2 splits or ramifies in K, then we can eliminate the fake ell. curve case

- If 2 is inert in $\mathbb{Q}(\sqrt{-d})$ i.e. $-d \equiv 5 \pmod 8$, we cannot eliminate fake ell. curves

- This is exactly 1/6 of all imag. quad.fields.

Idea behind the proof

- attach the Frey curve
- enough of modularity, irreducibility and level lowering known for totally real fields and assume "modularity" for a general number field
- get newform of weight 2 and some level $\mathcal{N}$
- there are newforms at the level $\mathcal{N}$, so no contradiction yet
- for p sufficiently large, we can get E' with full 2-torsion and good reduction outside the prime factors of $\mathcal{N}$
- parametrize such elliptic curves with the solution of S-unit equation and get a contradiction by using the valuation condition on S-units

Sketch of the proof

- Let $G_K = \mathrm{Gal}(\bar{K}/K)$ be the absolute Galois group of K. For an elliptic curve E/K,

$$\bar{\rho}_{E,p} : G_K \longrightarrow \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

denotes the mod p Galois representation of E.

- Let (a, b, c) be a solution of the Fermat equation.

- Attach the Frey curve

$$E : y^2 = x(x - Aa^p)(x + Bb^p).$$

- Compute the discriminant Δ_E and the j-invariant of j_E of the Frey elliptic curve.

- **Irreducibility of Galois representations**: If p is large enough, then $\bar{\rho}_{E,p}$ is irreducible.

- **Modularity:** modularity conjecture from Langlands programme

- **Level lowering:**
  - There is a non-trivial weight 2 new complex eigenform $\mathfrak{f}$ which has an associated elliptic curve $E_{\mathfrak{f}}/K$ of conductor $\mathfrak{N}'$ dividing $\mathfrak{N}$ with $\bar{\rho}_{E,p} \sim \bar{\rho}_{E_{\mathfrak{f}},p}$.

  - There is an elliptic curve E'/K where E' has full 2-torsion with $\bar{\rho}_{E,p} \sim \bar{\rho}_{E,p}$.

Elliptic Curves with full 2-torsion and solutions to the S-unit equation

- $\mathfrak{S}_S$: the set of all elliptic curves over K with full 2-torsion and potentially good outside S
- $E_1 \sim E_2$ on $\mathfrak{S}_S$: E_1 and E_2 are isomorphic $\bar{K}$
- $\Delta_S = \{(\lambda, \mu) : \lambda + \mu = 1,\ \lambda, \mu \in \mathcal{O}_S^*\}$
- $\mathfrak{S}_3$, the symmetric group on 3 letters, acts on Δ_S.
- There is a bijection between $\mathfrak{S}_3 \setminus \Delta_S$ and $\mathfrak{S}_S / \sim$
- The orbit of (λ, μ) is sent to the class of the Legendre elliptic curve $y^2 = x(x-1)(x-\lambda)$.

Proof of the Main Theorem

- Let K be a number field satisfying Conjectures and S, U, V be the sets we defined before with $U \neq \emptyset$.
- Let (a, b, c) be a non-trivial solution to the Fermat equation.
- For the solution above, attach the Frey curve
- Apply level lowering and obtain an elliptic curve E'/K having full 2-torsion and potentially good reduction away form S with j-invariant j' satisfying $v_{\mathfrak{P}}(j') < 0$ for all $\mathfrak{P} \in U$.
- We can express j' in terms of λ and μ and by using the condition

$$max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\} \leq 4v_{\mathfrak{P}}(2)$$

we deduce that $v_{\mathfrak{P}}(j') > 0$, contradiction.

Signature $(p, p, 2)$

- We consider the equation $x^p + y^p = z^2$ over number fields K.
- The strategy is the same, we apply the modular approach.
- The Frey curve attached to $x^p + y^p = z^2$ is not "symmetric".

$$E : y^2 = x(x - Aa^p)(x + Bb^p) \text{ for the Fermat equation.}$$

$$E = E_{a,b,c} : Y^2 = X^3 + 4cX^2 + 4a^pX.$$

for the equation $x^p + y^p = z^2$.

- Solving the S-unit equation over K is not enough but we need to solve them over some extensions L of K.

Our Result

Theorem (Isik, K., Ozman)

K:a totally real number field with narrow class number $h_K^+ = 1$,

$L = K(\sqrt{a})$ for each $a \in K(S_K, 2)$,

S_K-unit equation: $\lambda + \mu = 1, \qquad \lambda, \mu \in \mathcal{O}_{S_K}^*$,

Suppose that for every solution (λ, μ) to the S_K-unit equation, there is some $\mathfrak{P} \in T_K$ that satisfies

$$\max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\} \leq 4v_{\mathfrak{P}}(2)$$

.

Suppose also that for each L, for every solution (λ, μ) to the S_L-unit equation, there is some $\mathfrak{P}' \in T_L$ that satisfies

$$\max\{|v_{\mathfrak{P}'}(\lambda)|, |v_{\mathfrak{P}'}(\mu)|\} \leq 4v_{\mathfrak{P}'}(2)$$

Theorem

Then there is a constant B_K -depending only on K- such that for $p > B_K$, the equation $x^p + y^p = z^2$ has no solution $(a, b, c) \in W_K$.

W_K: the set of $(a, b, c) \in \mathcal{O}_K$ such that $a^p + b^p = c^2$ with $\mathfrak{P} | b$ for every $\mathfrak{P} \in T_K$

In this case we say that asymptotic Fermat's Last Theorem holds for W_K.

Thank you!