The Local-Global Principle and a Projective Twist on the Hasse Norm Theorem

Alan Bu
MIT PRIMES
Under the Direction of Thomas Rüd

October 15th, 2023

Diophantine Equations

Question (c. 200 A.D.)

How can you determine if an equation has a solution over the integers?

Diophantine Equations

Question (c. 200 A.D.)

How can you determine if an equation has a solution over the integers?

Example

$$\frac{x}{y+z} + \frac{y}{z+x} + \frac{z}{x+y} = 4$$

Diophantine Equations

Question (c. 200 A.D.)

How can you determine if an equation has a solution over the integers?

Example

$$\frac{x}{y+z} + \frac{y}{z+x} + \frac{z}{x+y} = 4$$

Smallest positive solution:

Diophantine Equations

Question (c. 200 A.D.)

How can you determine if an equation has a solution over the integers?

Example

$$\frac{x}{y+z} + \frac{y}{z+x} + \frac{z}{x+y} = 4$$

Smallest positive solution:

x = 154476802108746166441951315019919837485664325669565431700026634898253202035277999

y = 36875131794129999827197811565225474825492979968971970996283137471637224634055579

z = 43736126779286972578612526023713901528165375581616136186214379933784234677720 36

Using Parity

Example

$$x^2 + x^3 + 2y = 3$$

Figure 1: Gauss, 1801

Using Parity

Example

$$x^2 + x^3 + 2y = 3$$

$$\overbrace{x^2}^{\text{odd}} + \overbrace{x^3}^{\text{odd}} + \overbrace{2y}^{\text{even}} \quad \text{or} \quad \overbrace{x^2}^{\text{even}} + \overbrace{x^3}^{\text{even}} + \overbrace{2y}^{\text{even}}$$

Figure 1: Gauss, 1801

Using Parity

Example

$$x^2 + x^3 + 2y = 3$$

$$\overbrace{x^2}^{\text{odd}} + \overbrace{x^3}^{\text{odd}} + \overbrace{2y}^{\text{even}} \quad \text{or} \quad \overbrace{x^2}^{\text{even}} + \overbrace{x^3}^{\text{even}} + \overbrace{2y}^{\text{even}}$$

This is never an odd number!

Question

Does this approach always work?

Figure 1: Gauss, 1801

Modular Reduction

Example

$$x^2 + y^2 + z^2 = 1007:$$

Modular Reduction

Example

$$x^2 + y^2 + z^2 = 1007:$$

Another Idea

Parity is characterizing numbers by their remainders after division by 2. What if we try another divisor?

Modular Reduction

Example

$$x^2 + y^2 + z^2 = 1007:$$

Another Idea

Parity is characterizing numbers by their remainders after division by 2. What if we try another divisor?

$x \pmod 8$	0	1	2	3	4	5	6	7
$x^2 \pmod 8$	0	1	4	1	0	1	4	1

Modular Reduction

Example

$$x^2 + y^2 + z^2 = 1007:$$

Another Idea

Parity is characterizing numbers by their remainders after division by 2. What if we try another divisor?

$x \pmod 8$	0	1	2	3	4	5	6	7
$x^2 \pmod 8$	0	1	4	1	0	1	4	1

$\Rightarrow$ $x^2 + y^2 + z^2 \not\equiv 7 \pmod 8$

Modular Reduction

Example

$$x^2 + y^2 + z^2 = 1007:$$

Another Idea

Parity is characterizing numbers by their remainders after division by 2. What if we try another divisor?

$x \pmod 8$	0	1	2	3	4	5	6	7
$x^2 \pmod 8$	0	1	4	1	0	1	4	1

$\Rightarrow$ $x^2 + y^2 + z^2 \not\equiv 7 \pmod 8$

Thus we have no integer solutions!

What did we learn?

- $x^2 + x^3 + 2y = 3$

What did we learn?

- $x^2 + x^3 + 2y = 3$

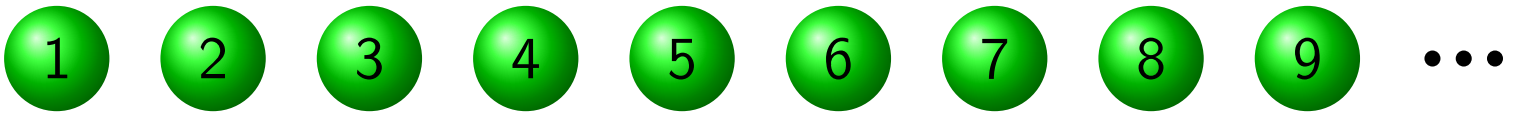
- $x^2 + y^2 + z^2 = 1007$

What did we learn?

- $x^2 + x^3 + 2y = 3$

- $x^2 + y^2 + z^2 = 1007$

- $3x^3 + 4y^3 + 5z^3 = 0$?



What did we learn?

Definition

A diophantine equation has a **local solution** if it has a solution modulo every n and over the real numbers and a **global solution** if it has a solution over the integers.

Remark

If the equation fails modulo some n, then it has no local solution, and thus no global solution either. But if it succeeds modulo every n, does it imply that there is a global solution too?

Helmut Hasse

Question (Hasse Principle)

Local $\Longrightarrow$ Global?

Figure 2: Hasse, 1921

Helmut Hasse

Question (Hasse Principle)

$$\text{Local} \stackrel{?}{\Longrightarrow} \text{Global?}$$

Theorem (Hasse, 1921)

The local-global principle holds for homogeneous polynomial equations of degree 2 over arbitrarily many variables.

Figure 2: Hasse, 1921

Helmut Hasse

Question (Hasse Principle)

Local $\Longrightarrow$ Global?

Theorem (Hasse, 1921)

The local-global principle holds for homogeneous polynomial equations of degree 2 over arbitrarily many variables.

Counterexample (Selmer, 1951)

The equation $3x^3 + 4y^3 + 5z^3 = 0$ always has a local solution, yet has no global solution.

Figure 2: Hasse, 1921

Tate-Shafarevich Group

Remark

The Tate-Shafarevich group $Ш(A/K)$ measures the degree of failure of the local-global principle for some equation.

$$3x^3 + 4y^3 + 5z^3 = 0 \text{ (Selmer, 1951)}$$
$$x^4 \quad 17z^2 = 2y^2 \text{ (Carl-Erik Lind, 1940)}$$

Figure 3: Tate, 1959

Tate-Shafarevich Group

Remark

The Tate-Shafarevich group $Ш(A/K)$ measures the degree of failure of the local-global principle for some equation.

$$3x^3 + 4y^3 + 5z^3 = 0 \text{ (Selmer, 1951)}$$
$$x^4 \quad 17z^2 = 2y^2 \text{ (Carl-Erik Lind, 1940)}$$

Open Question

Over what equations does the local-global principle hold?

Figure 3: Tate, 1959

Number Fields

Definition

A *number field* is a number system which contains the rational numbers adjoined together with the roots of some polynomial.

Number Fields

Definition

A *number field* is a number system which contains the rational numbers adjoined together with the roots of some polynomial.

Examples

(Gaussian Numbers) $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$

Number Fields

Definition

A *number field* is a number system which contains the rational numbers adjoined together with the roots of some polynomial.

Examples

(Gaussian Numbers) $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$

Hasse Norm Theorem

Definition

Each number field K comes equipped with a *norm* N, that maps elements of the field to rational numbers.

Hasse Norm Theorem

Definition

Each number field K comes equipped with a *norm* N, that maps elements of the field to rational numbers.

Theorem (Hasse Norm Theorem)

If N is a norm function on a cyclic Galois number field, then $\boxed{N(x) = c}$ satisfies the local-global principle where c is a fixed rational number.

Hasse Norm Theorem

Definition

Each number field K comes equipped with a *norm* N, that maps elements of the field to rational numbers.

Theorem (Hasse Norm Theorem)

If N is a norm function on a cyclic Galois number field, then $\boxed{N(x) = c}$ satisfies the local-global principle where c is a fixed rational number.

This theorem allows us to tackle higher degree functions. Although it is very rare for any given function to be a norm of a cyclic Galois number field, it is a step in the right direction.

Hasse Norm Theorem

Example

In the Gaussian rationals, $N(a + bi) = (a + bi)(a \quad bi) = a^2 + b^2$, which is the square of the complex magnitude. This implies that $a^2 + b^2 = 7$ satisfies the Hasse principle.

Hasse Norm Theorem

Example

In the Gaussian rationals, $N(a + bi) = (a + bi)(a \quad bi) = a^2 + b^2$, which is the square of the complex magnitude. This implies that $a^2 + b^2 = 7$ satisfies the Hasse principle.

Remark

The Hasse Norm theorem is dependent the cyclic condition. For example, $N(x) = 25$ in $\mathbb{Q}(\sqrt{13}; \sqrt{17})$ has a local solution but no global solution.

Our Research

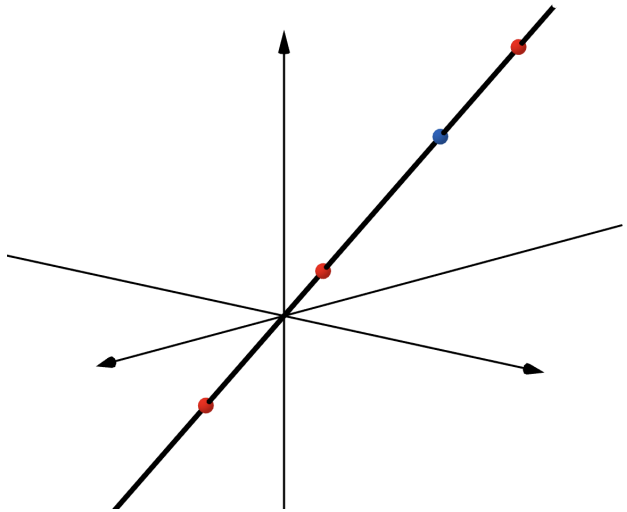
Problem

When does the local-global principle hold for $\frac{N_1(x)}{N_2(y)} = c$? Is the local-global principle in both $N_1; N_2$ enough to imply that it holds for $\frac{N_1(x)}{N_2(y)}$? What about the other direction?

Our research

Problem

More generally, we can define a projective ratio of n terms to be an n-tuple which can be freely scaled by a constant factor. For example, the ratio $(4;2;6)$ would be equal to $(2;1;3)$ (similarly to how $\frac{4}{6} = \frac{2}{3}$). When does the projective ratio of norms $N_1;N_2;:::;N_n$ satisfy the local-global principle?

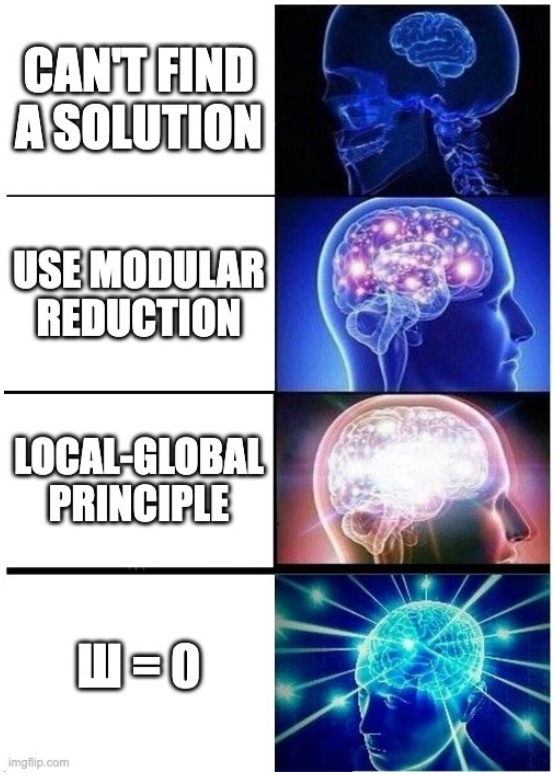


Summary

Gauss's modular reduction method gives an easy approach to prove that a diophantine equation has no solutions.

Hasse shows that sometimes, a local solution is enough to imply a global solution, but Selmer shows that this doesn't hold in general.

The Hasse Norm theorem allows us to find higher-degree functions that satisfy the Hasse principle.



Summary of our research

The Hasse principle in $\frac{N_1(x)}{N_2(y)}$ does not transfer to N_1 or N_2.

In our paper, we develop a Sagemath program for Tate-Shafarevich group calculation.

If the smallest field containing $N_1; N_2$ has squarefree degree, then Hasse principle in $N_1; N_2$ together implies the Hasse principle in $\frac{N_1(x)}{N_2(y)}$.

The size of the relevant Tate-Shafarevich groups is used to study elliptic curves.

Acknowledgements

Dr. Thomas Rüd

Dr. Tanya Khovanova

MIT PRIMES

References

[1] Helmut Hasse. "Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol". In: *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* 1931 (1931), pp. 64–69.

[2] Pei-Xin Liang et al. "On Tamagawa numbers of CM tori". In: *arXiv preprint arXiv:2109.04121* (2021).

[3] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Springer Science & Business Media, 2013.