On the solutions of a class of generalized Fermat equations signature $(2, 2n, 3)$

Gökhan SOYDAN

Department of Mathematics, Bursa Uludağ University
Bursa-TÜRKİYE

Workshop on Diophantine Equations and Algebraic Equations, May 2-3, 2023
Department of Mathematics, Savoie Mont Blanc University
Chambery-FRANCE

(This is joint work with Karolina Chałupka and Andrzej Dąbrowski)

Table of contents

1. Who is Diophantus?

- Diophantus, the "father of algebra", is the best known his book Arithmetica, work on the solution of algebraic equations and the theory of numbers.

1. Who is Diophantus?

- Diophantus, the "father of algebra", is the best known his book Arithmetica, work on the solution of algebraic equations and the theory of numbers.

- Diophantus did his work in the great city of Alexandria. At this time, Alexandria was the center of mathematical learning. The period from 250 BCE (before christian era) to 350 CE (christian era) in Alexandria is known as the Silver Age, also the Later Alexandrian Age.

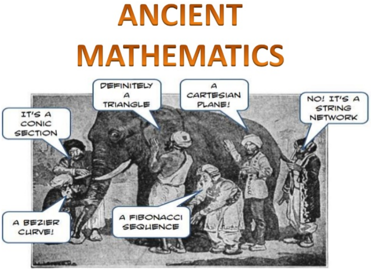
- This was a time when mathematicians were discovering many ideas that led to our current conception of mathematics. The era is considered silver because it came after the Golden age, a time of great development in the field of mathematics.

1. Who is Diophantus?

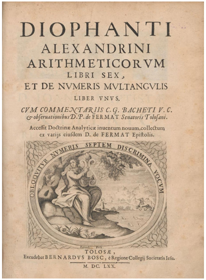
- This was a time when mathematicians were discovering many ideas that led to our current conception of mathematics. The era is considered silver because it came after the Golden age, a time of great development in the field of mathematics.

- This Golden Age encompasses the lifetime of Euclid. The quality of mathematics from this period was an inspiration for the axiomatic methods of today's mathematics.

- While it is known that Diophantus lived in the Silver age, it is hard to pinpoint the exact years in which he lived. While many references to the work of Diophantus have been made, Diophantus himself made few references to other mathematicians' work, thus making the process of determining the time that he lived more difficult.



- Arithmetica is a collection of 150 problems that give approximate solutions to equations up to degree three. Arithmetica also contains equations that deal with indeterminate equations. These equations deal with the theory of numbers.



- The original Arithmetica is believed to have comprised 13 books, but surviving Greek manuscripts contain only six.

- The original Arithmetica is believed to have comprised 13 books, but surviving Greek manuscripts contain only six.
- The others are considered lost works. It is possible that these books were lost in a fire that occured not long after Diophantus finished Arithmetica.

2. What is a Diophantine equation?

- We call a Diophantine equation an equation of the form

$$f(x_1, x_2, ..., x_n) = 0, \tag{1}$$

where f is an $n-$ variable function with $n \geq 2$. If f is a polynomial with integer coefficients, then (1) is an algebraic Diophantine equation.

2. What is a Diophantine equation?

- We call a Diophantine equation an equation of the form

$$f(x_1, x_2, ..., x_n) = 0, \tag{1}$$

where f is an $n-$ variable function with $n \geq 2$. If f is a polynomial with integer coefficients, then (1) is an algebraic Diophantine equation.

- An n-tuple $(x_1, x_2, ..., x_n) \in \mathbb{Z}^n$ satisfying (1) is called a solution to equation (1). An equation having one or more solutions is called solvable.

- Concerning a Diophantine equation three basic problems arise:

2. What is a Diophantine equation?

- Concerning a Diophantine equation three basic problems arise:

Problem 1

Is the equation solvable?

- Concerning a Diophantine equation three basic problems arise:

Problem 1

Is the equation solvable?

Problem 2

If it is solvable, is the number of its solutions finite or infinite?

- Concerning a Diophantine equation three basic problems arise:

Problem 1

Is the equation solvable?

Problem 2

If it is solvable, is the number of its solutions finite or infinite?

Problem 3

If it is solvable, determine all of its solutions.

2. What is a Diophantine equation?

- Among the 23 problems posed by David Hilbert in 1900, the 10 th Problem concerned Diophantine equations. Hilbert asked if there is an universal method for solving all Diophantine equations. Here we reformulate it:

2. What is a Diophantine equation?

- Among the 23 problems posed by David Hilbert in 1900, the 10 th Problem concerned Diophantine equations. Hilbert asked if there is an universal method for solving all Diophantine equations. Here we reformulate it:

Problem 4 (Hilbert's 10 th Problem)

Given a Diophantine equation with any number of unknown quantities and with integer coefficients. To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in integers.

2. What is a Diophantine equation?

- Among the 23 problems posed by David Hilbert in 1900, the 10 th Problem concerned Diophantine equations. Hilbert asked if there is an universal method for solving all Diophantine equations. Here we reformulate it:

Problem 4 (Hilbert's 10 th Problem)

Given a Diophantine equation with any number of unknown quantities and with integer coefficients. To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in integers.

- In 1970, Y. Matiyasevich gave a negative solution to Hilbert's 10 th Problem. His result is the following.

Theorem 5 (Y. Matiyasevich)

There is no algorithm which, for a given arbitrary Diophantine equation, would tell whether the equation has an integer solution or not.

2. What is a Diophantine equation?

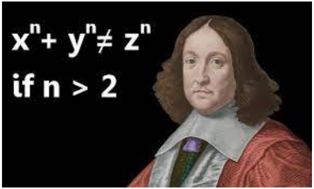
2. What is a Diophantine equation?

Remark 1 (Open Problem)

For rational solutions, the analog of Hilbert's 10 th Problem is not yet solved. That is, the question whether there exist an algorithm to decide if a Diophantine equation has a rational solution or not is still open.

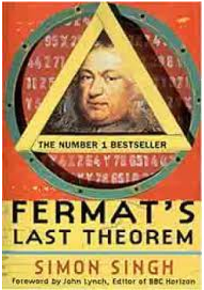
Table of contents

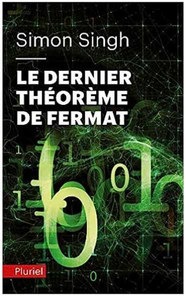
- A mathematical adventure that started with Pierre dé Fermat in 1637 and ended with Andrew Wiles in 1995:



Theorem 2 (Fermat's last theorem)

The equation $x^p + y^p = z^p$ has no solutions in non-zero integers x, y, z for $p \geq 3$.





- A generalization of Fermat's last theorem:

Conjecture 1 (Beal conjecture)

The equation $x^p + y^q = z^r$ has no solutions in non-zero mutually coprime integers x, y, z for $p, q, r \geq 3$.

2. Introduction and Motivation

- A generalization of Fermat's last theorem:

Conjecture 1 (Beal conjecture)

The equation $x^p + y^q = z^r$ has no solutions in non-zero mutually coprime integers x, y, z for $p, q, r \geq 3$.

- Andrew Beal is a Dallas banker who has a general interest in mathematics.

- A generalization of Fermat's last theorem:

Conjecture 1 (Beal conjecture)

The equation $x^p + y^q = z^r$ has no solutions in non-zero mutually coprime integers x, y, z for $p, q, r \geq 3$.

- Andrew Beal is a Dallas banker who has a general interest in mathematics.
- Beal has personally funded a standing prize of $ 1 million USD for its proof or disproof.

- For given positive integers p, q, r satisfying $1/p + 1/q + 1/r < 1$, the generalized Fermat equation

$$Ax^p + By^q = Cz^r \tag{2}$$

has only finitely many primitive integer solutions [Darmon & Granville, 1997].

- For given positive integers p, q, r satisfying $1/p + 1/q + 1/r < 1$, the generalized Fermat equation

$$Ax^p + By^q = Cz^r \tag{2}$$

has only finitely many primitive integer solutions [Darmon & Granville, 1997].

- $A = B = C = 1$ and $(p, q, r) = (n, n, n)$: Fermat's equation
- $A = B = C = 1$ and $y = 1$: Catalan's equation

the case $1/p + 1/q + 1/r = 1$

$(p, q, r) \in \{(2, 6, 3), (2, 4, 4), (3, 3, 3), (4, 4, 2), \ (2, 3, 6)\}$: Each case corresponds to an elliptic curve of rank 0.

the case $1/p + 1/q + 1/r = 1$

$(p, q, r) \in \{(2, 6, 3), (2, 4, 4), (3, 3, 3), (4, 4, 2), (2, 3, 6)\}$: Each case corresponds to an elliptic curve of rank 0.

the case $(p, q, r) = (3, 3, 3)$ and $(A, B, C) = (1, 1, 1)$

Now we consider the equation $x^3 + y^3 = z^3$. The transformation

$$x = \frac{6}{X} + \frac{Y}{6X}, \; y = \frac{6}{X} - \frac{Y}{6X}$$

yields the elliptic curve

$$Y^2 = X^3 - 432.$$

All rational solutions of the above curve are $(X, Y) = (12, 36), (12, 36)$ and $\mathcal{O}$. But none of them does not give any solution to the original equation.

the case $1/p + 1/q + 1/r > 1$

$(p, q, r) \in \{(2, 2, r), (2, q, 2), (2, 3, 3), (2, 3, 4), (2, 4, 3), (2, 3, 5)\}$: No solution or infinitely many solutions.

the case $1/p + 1/q + 1/r > 1$

$(p, q, r) \in \{(2, 2, r), (2, q, 2), (2, 3, 3), (2, 3, 4), (2, 4, 3), (2, 3, 5)\}$: No solution or infinitely many solutions.

the case $(A, B, C) = (1, 1, 1)$ and $(p, q, r) = (2, 2, 2)$

This case corresponds to the equation $x^2 + y^2 = z^2$, which has infinitely many solutions.

five small solutions

$1^n + 2^3 = 3^2$,
$2^5 + 7^2 = 3^4$,
$7^3 + 13^2 = 2^9$,
$2^7 + 17^3 = 71^2$,
$3^5 + 11^4 = 122^2$.
(Blair Kelly, Reese Scott and Benne de Weger all found these examples independently.)

five large solutions

$17^7 + 76271^3 = 21063928^2$,
$1414^3 + 2213459^2 = 65^7$,
$9262^3 + 15312283^2 = 113^7$,
$43^8 + 96222^3 = 30042907^2$,
$33^8 + 1549034^2 = 15613^3$.
(Beukers and Zagier have found these examples.)

- Now, we go back to the case $1/p + 1/q + 1/r < 1$ for the generalized Fermat equation
$$Ax^p + By^q = Cz^r.$$

2. Introduction and Motivation

- Now, we go back to the case $1/p + 1/q + 1/r < 1$ for the generalized Fermat equation
$$Ax^p + By^q = Cz^r.$$

- Modern techniques coming from Galois representations and modular forms:
  1. Methods of Frey–Helle-gouarch curves and variants of Ribet's level-lowering theorem.
  2. The modularity of elliptic curves or abelian varieties over the rationals or totally real number fields.

2. Introduction and Motivation

- Now, we go back to the case $1/p + 1/q + 1/r < 1$ for the generalized Fermat equation
$$Ax^p + By^q = Cz^r.$$

- Modern techniques coming from Galois representations and modular forms:
  1. Methods of Frey–Helle-gouarch curves and variants of Ribet's level-lowering theorem.
  2. The modularity of elliptic curves or abelian varieties over the rationals or totally real number fields.

- Modern techniques allow to give partial (sometimes complete) results concerning the set of solutions to generalized Fermat equation (usually, when a radical of ABC is small).

2. Introduction and Motivation

- Now, we go back to the case $1/p + 1/q + 1/r < 1$ for the generalized Fermat equation
$$Ax^p + By^q = Cz^r.$$

- Modern techniques coming from Galois representations and modular forms:
  1. Methods of Frey–Helle-gouarch curves and variants of Ribet's level-lowering theorem.
  2. The modularity of elliptic curves or abelian varieties over the rationals or totally real number fields.
- Modern techniques allow to give partial (sometimes complete) results concerning the set of solutions to generalized Fermat equation (usually, when a radical of ABC is small).
- At least when (p, q, r) is of the type (n, n, n), $(n, n, 2)$, $(n, n, 3)$, $(2n, 2n, 5)$, $(2, 4, n)$, $(2, 6, n)$, $(2, n, 4)$, $(2, n, 6)$, $(3, 3, p)$, $(2, 2n, 3)$, $(2, 2n, 5)$.

2. Introduction and Motivation

- Here, note that the notation $\{p, q, r\}$ implies that all permutations of the ordered triple $\{p, q, r\}$ are taken into account.

Some known results with $(A, B, C) = (1, 1, 1)$

$\{n, n, n\}$ and $n \geq 4$: Wiles and Taylor (Fermat's last theorem).
$\{n, n, 2\}$: Darmon and Merel (for n prime ≥ 7), Poonen (for $n = 5, 6, 9$).
$\{n, n, 3\}$: Darmon and Merel (for n prime ≥ 7), Lucas (19th century) (for $n = 4$) and Poonen (for $n = 5$).
$\{3, 3, n\}$: Kraus (for $17 \leq n \leq 10000$), Bruin (for $n = 4, 5$), Chen and Siksek (for $17 \leq n \leq 10^9$), Dahmen (for $n = 7, 11, 13$).
$\{2, n, 4\}$ and $\{4, n, 4\}$: Darmon.
$\{2, 4, n\}$: Ellenberg (for prime $n \geq 211$) and Ghioca (for $n = 7$).
$\{2n, 2n, 5\}$: Bennett (for $n \geq 7$ and $n = 2$), Bruin (for $n = 3$ and $n = 5$ follows from Fermat's last theorem.)

Some known results: continued

$\{2,2n,3\}$: Chen (for n prime and $7 < n < 1000$ and $n \neq 31$), Dahmen (the case $n = 31$ and $n \equiv 5 \pmod 6$))
$\{2,2n,5\}$: Chen (for $n > 17$ prime and $n \equiv 1 \pmod 4$).
$\{2,4,6\}$: Bruin.
$\{2,4,5\}$: Bruin, $2^5 + 7^2 = 3^4$, $3^5 + 11^4 = 122^2$.
$\{2,3,9\}$: Bruin, $13^2 + 7^3 = 2^9$.
$\{2,3,8\}$: Bruin, $1^8 + 2^3 = 3^2$, $43^8 + 96222^3 = 30042907^2$, $33^8 + 1549034^2 = 15613^3$.
$\{2,3,7\}$: Poonen, Schaefer and Stoll, $1^7 + 2^3 = 3^2$, $2^7 + 17^3 = 71^2$, $17^7 + 76271^3 = 21063928^2$, $9262^3 + 15312283^2 = 113^7$.

Some known results: continued

$\{2, 2n, 3\}$: Chen (for n prime and $7 < n < 1000$ and $n \neq 31$), Dahmen (the case $n = 31$ and $n \equiv 5 \pmod 6$))
$\{2, 2n, 5\}$: Chen (for $n > 17$ prime and $n \equiv 1 \pmod 4$).
$\{2, 4, 6\}$: Bruin.
$\{2, 4, 5\}$: Bruin, $2^5 + 7^2 = 3^4$, $3^5 + 11^4 = 122^2$.
$\{2, 3, 9\}$: Bruin, $13^2 + 7^3 = 2^9$.
$\{2, 3, 8\}$: Bruin, $1^8 + 2^3 = 3^2$, $43^8 + 96222^3 = 30042907^2$, $33^8 + 1549034^2 = 15613^3$.
$\{2, 3, 7\}$: Poonen, Schaefer and Stoll, $1^7 + 2^3 = 3^2$, $2^7 + 17^3 = 71^2$, $17^7 + 76271^3 = 21063928^2$, $9262^3 + 15312283^2 = 113^7$.

- Survey papers about solving the generalized Fermat equation when $ABC = 1$: [Bennett, Chen, Dahmen, Yazdani-2015], [Bennett, Mihăilescu, Siksek- 2016].

- In this lecture, we consider the Diophantine equations

$$ax^2 + y^{2n} = 4z^3, \quad x, y, z \in \mathbb{Z},\ \gcd(x, y) = 1,\ n \in \mathbb{N}_{\geq 2}, \tag{3}$$

and

$$x^2 + ay^{2n} = 4z^3, \quad x, y, z \in \mathbb{Z},\ \gcd(x, y) = 1,\ n \in \mathbb{N}_{\geq 2}, \tag{4}$$

where the class number of $\mathbb{Q}(\sqrt{-a})$ with $a \in \{7, 11, 19, 43, 67, 163\}$ is 1.

2. Introduction and Motivation

- In this lecture, we consider the Diophantine equations

$$ax^2 + y^{2n} = 4z^3, \quad x, y, z \in \mathbb{Z},\ \gcd(x, y) = 1,\ n \in \mathbb{N}_{\geq 2}, \tag{3}$$

  and

$$x^2 + ay^{2n} = 4z^3, \quad x, y, z \in \mathbb{Z},\ \gcd(x, y) = 1,\ n \in \mathbb{N}_{\geq 2}, \tag{4}$$

  where the class number of $\mathbb{Q}(\sqrt{-a})$ with $a \in \{7, 11, 19, 43, 67, 163\}$ is 1.

- Why do we work on these equations?

- $x^2 + y^{2n} = z^3$ (Bennett, Bruin, Chen, Dahmen, Yazdani, 1999-2015). It is known that this equation has no solutions for a family of n's of natural density one.

2. Introduction and Motivation

- $x^2 + y^{2n} = z^3$ (Bennett, Bruin, Chen, Dahmen, Yazdani, 1999-2015). It is known that this equation has no solutions for a family of n's of natural density one.
- Our motivation:
  1. To extend the above results (and methods) of Bruin, Chen and Dahmen, by considering some Diophantine equations $Ax^2 + By^{2n} = Cz^3$ with (A, B, C)'s different from $(1, 1, 1)$ (assuming for simplicity that the class number of $\mathbb{Q}(\sqrt{-AB})$ is one).

2. Introduction and Motivation

- $x^2 + y^{2n} = z^3$ (Bennett, Bruin, Chen, Dahmen, Yazdani, 1999-2015). It is known that this equation has no solutions for a family of n's of natural density one.
- Our motivation:
  1. To extend the above results (and methods) of Bruin, Chen and Dahmen, by considering some Diophantine equations $Ax^2 + By^{2n} = Cz^3$ with (A, B, C)'s different from $(1, 1, 1)$ (assuming for simplicity that the class number of $\mathbb{Q}(\sqrt{-AB})$ is one).
  2. To extend our previous results about the Diophantine equation

     $$ax^2 + b^{2n} = 4y^k,\ \ k > 3 \text{ odd prime},\ \ x, y \in \mathbb{Z},\ \ n, k \in \mathbb{N},\ \ (x, y) = 1,$$

     [Dąbrowski, Günhan, Soydan-JNT-2020].

2. Introduction and Motivation

- In the above work, we suppose that $a \in \{7, 11, 19, 43, 67, 163\}$ and b is an odd prime. In the new work, we fix $k = 3$, but b is arbitrary.

- In the above work, we suppose that $a \in \{7, 11, 19, 43, 67, 163\}$ and b is an odd prime. In the new work, we fix $k = 3$, but b is arbitrary.
- Why were we unable to handle the Diophantine equations $7x^2 + y^{2n+1} = 4z^3$ and $x^2 + 7y^{2n+1} = 4z^3$?

- In the above work, we suppose that $a \in \{7, 11, 19, 43, 67, 163\}$ and b is an odd prime. In the new work, we fix $k = 3$, but b is arbitrary.
- Why were we unable to handle the Diophantine equations $7x^2 + y^{2n+1} = 4z^3$ and $x^2 + 7y^{2n+1} = 4z^3$?
    1. In 2007, Poonen, Schaefer and Stoll find the primitive integer solutions to $x^2 + y^7 = z^3$. Their method combine the modular method together with determination of rational points on certain genus-3 algebraic curves. This case (and possible generalizations to $Ax^2 + By^7 = Cz^3$) is very difficult.

- In the above work, we suppose that $a \in \{7, 11, 19, 43, 67, 163\}$ and b is an odd prime. In the new work, we fix $k = 3$, but b is arbitrary.
- Why were we unable to handle the Diophantine equations $7x^2 + y^{2n+1} = 4z^3$ and $x^2 + 7y^{2n+1} = 4z^3$?
  1. In 2007, Poonen, Schaefer and Stoll find the primitive integer solutions to $x^2 + y^7 = z^3$. Their method combine the modular method together with determination of rational points on certain genus-3 algebraic curves. This case (and possible generalizations to $Ax^2 + By^7 = Cz^3$) is very difficult.
  2. In 2020, Freitas, Naskrecki and Stoll considered a general Diophantine equation $x^2 + y^p = z^3$ (with p any prime > 7). They follow and refine the arguments of Poonen, Schaefer and Stoll by combining new ideas around the modular method with recent approaches to determination of the set of rational points on certain algebraic curves.
     As a result, they were able to find (under GRH) the complete set of solutions of the Diophantine equation $x^2 + y^p = z^3$ only for $p = 11$.

Table of contents

Theorem 3 (Chałupka, Dąbrowski, Soydan-2022)

The Diophantine equations

$$ax^2 + y^{2n} = 4z^3, \quad x, y, z \in \mathbb{Z},\ \gcd(x, y) = 1,\ n \in \mathbb{N}_{\geq 2},$$

and

$$x^2 + ay^{2n} = 4z^3, \quad x, y, z \in \mathbb{Z},\ \gcd(x, y) = 1,\ n \in \mathbb{N}_{\geq 2},$$

have no solutions where the class number of $\mathbb{Q}(\sqrt{-a})$ *with* $a \in \{11, 19, 43, 67, 163\}$ *is 1.*

Theorem 4 (Chałupka, Dąbrowski, Soydan-2022)

Let x, y, z be coprime integers such that $7x^2 + y^4 = 4z^3$. Then there are rational numbers s, t such that one of the following holds.

$$
\begin{aligned}
x = \pm&(1911s^4 + 1260ts^3 + 378t^2s^2 + 12t^3s + 7t^4) \\
&(-5078115s^8 - 11928168ts^7 - 2556036t^2s^6 - 1802808t^3s^5 \\
&- 929922t^4s^4 - 38808t^5s^3 + 46620t^6s^2 + 9912t^7s + 461t^8), \\
y = \pm&3(21s^2 - 14ts - 3t^2)(2499s^4 + 1764ts^3 + 378t^2s^2 + 84t^3s - 5t^4), \\
z = {}&6828444s^8 + 7260624ts^7 + 6223392t^2s^6 + 1728720t^3s^5 \\
&+ 156408t^4s^4 + 49392t^5s^3 + 28224t^6s^2 + 3696t^7s + 268t^8,
\end{aligned}
\tag{5}
$$

$$
\begin{aligned}
x = {} & \pm(343s^4 - 84ts^3 + 378t^2s^2 - 180t^3s + 39t^4) \\
& (1106861s^8 - 3399816ts^7 + 2284380t^2s^6 + 271656t^3s^5 \\
& - 929922t^4s^4 + 257544t^5s^3 - 52164t^6s^2 + 34776t^7s - 2115t^8), \\
y = {} & \pm 3(21s^2 - 14ts - 3t^2)(-245s^4 - 588ts^3 + 378t^2s^2 - 252t^3s + 51t^4), \\
z = {} & 643468s^8 - 1267728ts^7 + 1382976t^2s^6 - 345744t^3s^5 + 156408t^4s^4 \\
& - 246960t^5s^3 + 127008t^6s^2 - 21168t^7s + 2844t^8.
\end{aligned} \tag{6}
$$

$$
\begin{aligned}
x = & \pm(343s^4 - 84ts^3 + 378t^2s^2 - 180t^3s + 39t^4) \\
& (1106861s^8 - 3399816ts^7 + 2284380t^2s^6 + 271656t^3s^5 \\
& - 929922t^4s^4 + 257544t^5s^3 - 52164t^6s^2 + 34776t^7s - 2115t^8), \\
y = & \pm 3(21s^2 - 14ts - 3t^2)(-245s^4 - 588ts^3 + 378t^2s^2 - 252t^3s + 51t^4), \\
z = & \, 643468s^8 - 1267728ts^7 + 1382976t^2s^6 - 345744t^3s^5 + 156408t^4s^4 \\
& - 246960t^5s^3 + 127008t^6s^2 - 21168t^7s + 2844t^8.
\end{aligned} \tag{6}
$$

Theorem 5 (Chałupka, Dąbrowski, Soydan-2022)

The Diophantine equation $7x^2 + y^{2n} = 4z^3$ has no non-trivial solutions with $n = 3, 4, 5$.

Theorem 6 (Chałupka, Dąbrowski, Soydan-2022)

The Diophantine equation $7x^2 + y^{2n} = 4z^3$ *has no primitive solutions for all primes* $7 < p < 10^9$ *and* $p \neq 13$.

Theorem 6 (Chałupka, Dąbrowski, Soydan-2022)

The Diophantine equation $7x^2 + y^{2n} = 4z^3$ *has no primitive solutions for all primes* $7 < p < 10^9$ *and* $p \neq 13$.

Theorem 7 (Chałupka, Dąbrowski, Soydan-2022)

The Diophantine equation $7x^2 + y^{2n} = 4z^3$ *has no primitive solutions for a family of primes* p *satisfying:*

$$p \equiv 3 \text{ or } 55 \pmod{106} \text{ or } p \equiv 47, 65, 113, 139, 143 \text{ or } 167 \pmod{168}$$

Theorem 8 (Chałupka, Dąbrowski, Soydan-?)

Let x, y, z be coprime integers such that $x^2 + 7y^4 = 4z^3$. Then there are rational numbers s, t such that one of the following holds.

$$\begin{aligned}
x &= \pm(-s^4 - 8ts^3 + 18t^2s^2 + 24t^3s - 9t^4) \\
&\quad (-405t^8 - 108st^7 - 504s^2t^6 + 252s^3t^5 - 294s^4t^4 - 84s^5t^3 \\
&\quad - 56s^6t^2 + 4s^7t - 5s^8), \\
y &= \pm(s^2 + 3t^2)(-s^4 + 6ts^3 + 18t^2s^2 - 18t^3s - 9t^4), \\
z &= (162t^8 - 108st^7 + 252s^2t^6 + 252s^3t^5 + 84s^4t^4 - 84s^5t^3 \\
&\quad + 28s^6t^2 + 4s^7t + 2s^8),
\end{aligned} \tag{7}$$

$$
\begin{aligned}
x &= \pm(1/32)(s^4 + 21t^4)(441t^8 - 714s^4t^4 + s^8) \\
y &= (3/4)st(s^4 - 21t^4), \\
z &= (1/16)(441t^8 + 294s^4t^4 + s^8),
\end{aligned}
\tag{8}
$$

$$
\begin{aligned}
x &= \pm(1/32)(3s^4 + 7t^4)(9s^8 - 714t^4s^4 + 49t^8) \\
y &= (3/4)st(3s^4 - 7t^4), \\
z &= (1/16)(9s^8 + 294t^4s^4 + 49t^8).
\end{aligned}
\tag{9}
$$

Theorem 9 (Chałupka, Dąbrowski, Soydan-?)

Any solution to the Diophantine equation $x^2 + 7y^6 = 4z^3$ in coprime integers x, y, z is of the type

$$(x_m, y_m, z_m) = (\pm\omega_m(P)/4d_m^3, \pm\psi_m(P)/d_m, \pm\varphi_m(P)/4d_m^2)$$

for some positive integer m, where $P = (8, 20)$, φ_m, ψ_m and ω_m denote the division polynomials associated to the elliptic curve $Y^2 = X^3 - 112$, and $d_m := \gcd(\pm\omega_m(P)/4, \pm\psi_m(P), \pm\varphi_m(P)/4)$.

Theorem 10 (Chałupka, Dąbrowski, Soydan-?)

The Diophantine equation $x^2 + 7y^8 = 4z^3$ *has the following non-trivial solutions* (x, y, z)*:* $(\pm 5, \pm 1, 2)$, $(\pm 16690170427, \pm 105, 4114726)$ *and* $(\pm 165997441137915, \pm 481, 1902746962)$.

Theorem 11 (Chałupka, Dąbrowski, Soydan-?)

Assume the abc conjecture. Then for a positive proportion of primes p, all non-trivial solutions to the Diophantine equation $x^2 + 7y^{2p} = 4z^3$ in coprime integers x,y,z are given by $(x, y, z) = (\pm 5, \pm 1, 2)$.

Table of contents

- As the class number of $\mathbb{Q}(\sqrt{-a})$ with $a \in \{7, 11, 19, 43, 67, 163\}$ is 1, we have the following factorization for the left side of the eq. $ax^2 + y^{2n} = 4z^3$

$$\frac{y^n + x\sqrt{-a}}{2} \cdot \frac{y^n - x\sqrt{-a}}{2} = z^3.$$

- Now we have

$$\frac{y^n + x\sqrt{-a}}{2} = \left(\frac{u + v\sqrt{-a}}{2}\right)^3,$$

  where u, v are odd rational integers. Note that $\gcd(u, v) = 1$. Replacing x with y^n, we obtain a similar factorization for the left hand side of the other equation. Equating the real and imaginer parts, we obtain the following result.

Lemma 6 (Chałupka, Dąbrowski, Soydan-2022)

(a) Suppose that (x, y, z) *is a solution to* $ax^2 + y^{2n} = 4z^3$. *Then*

$$(x, y^n, z) = \left(\frac{v(3u^2 - av^2)}{4}, \frac{u(u^2 - 3av^2)}{4}, \frac{u^2 + av^2}{4} \right) \tag{10}$$

for some odd $u, v \in \mathbb{Z}$ *with* $\gcd(u, v) = 1$.
(b) Suppose that (x, y, z) *is a solution to* $x^2 + ay^{2n} = 4z^3$. *Then*

$$(x, y^n, z) = \left(\frac{u(u^2 - 3av^2)}{4}, \frac{v(3u^2 - av^2)}{4}, \frac{u^2 + av^2}{4} \right) \tag{11}$$

for some odd $u, v \in \mathbb{Z}$ *with* $\gcd(u, v) = 1$.

- By Lemma 6, we have $u(u^2-3av^2)=4y^n$ or $v(3u^2-av^2)=4y^n$. Now, if $a\in\{11,19,43,67,163\}$, then $u(u^2-3av^2)$ is congruent to 0 modulo 8, while $4y^n$ is congruent to 4 modulo 8, a contradiction. Similarly in the second case. So, the proof is completed.

- By Lemma 6, we have $u(u^2 - 3av^2) = 4y^n$ or $v(3u^2 - av^2) = 4y^n$. Now, if $a \in \{11, 19, 43, 67, 163\}$, then $u(u^2 - 3av^2)$ is congruent to 0 modulo 8, while $4y^n$ is congruent to 4 modulo 8, a contradiction. Similarly in the second case. So, the proof is completed.
- Hence, this lemma completes the proof of Theorem 3.

- By Lemma 6, we have $u(u^2 - 3av^2) = 4y^n$ or $v(3u^2 - av^2) = 4y^n$. Now, if $a \in \{11, 19, 43, 67, 163\}$, then $u(u^2 - 3av^2)$ is congruent to 0 modulo 8, while $4y^n$ is congruent to 4 modulo 8, a contradiction. Similarly in the second case. So, the proof is completed.
- Hence, this lemma completes the proof of Theorem 3.
- So, we only need to consider the Diophantine equations

$$7x^2 + y^{2n} = 4z^3$$

and

$$x^2 + 7y^{2n} = 4z^3.$$

- Here we consider Diophantine equation

$$7x^2 + y^4 = 4z^3.$$

By Lemma 6 (a), we have reduced the problem to solving the equation

$$4y^2 = u(u^2 - 21v^2)$$

with odd u, v and y. Since $\gcd(u, v) = 1$, we have $d = (u, u^2 - 21v^2) \mid 3$.

- Here we consider Diophantine equation

$$7x^2 + y^4 = 4z^3.$$

By Lemma 6 (a), we have reduced the problem to solving the equation

$$4y^2 = u(u^2 - 21v^2)$$

with odd u, v and y. Since $\gcd(u, v) = 1$, we have $d = (u, u^2 - 21v^2) \mid 3$.

- Since $d \mid u$, we get

$$dr(d^2r^2 - 21v^2) = 4y^2.$$

In this case, problem of solving the eq. $7x^2 + y^4 = 4z^3$ is reduced to solving the following equations

$$dX^4 - (21/d)Y^2 = CZ^2$$

where $d = 1$ or 3, $C = \pm 1$, and X, Y are odd, with $(X, Y) = 1$.

- For example consider the case $(d, C) = (3, -1)$. Hence we get the equation
$$-Z^2 + 7Y^2 = 3X^4.$$

- For example consider the case $(d, C) = (3, -1)$. Hence we get the equation
$$-Z^2 + 7Y^2 = 3X^4.$$
- Put $K = X^2$. Then we obtain
$$Z^2 + 3K^2 = 7Y^2.$$

Set $2Z \pm 3K = 7L$ and $Z \pm 2K = 7M$ with $\gcd(L, M) = 1$. So, the above equation becomes
$$L^2 + 3M^2 = Y^2.$$

After elementary steps, we get two 2-parameter families of solutions of the eq. $-Z^2 + 7Y^2 = 3X^4$. Hence the proof is completed for the Diophantine equation $7x^2 + y^4 = 4z^3$.

- Here we consider
$$7x^2 + y^6 = 4z^3.$$
The above equation corresponds to the elliptic curve (multiplying bothside by $\frac{4^2 \cdot 7^3}{y^6}$)
$$Y^2 = X^3 - 2^4 \cdot 7^3.$$

- Here we consider
$$7x^2 + y^6 = 4z^3.$$
The above equation corresponds to the elliptic curve (multiplying bothside by $\dfrac{4^2 \cdot 7^3}{y^6}$)
$$Y^2 = X^3 - 2^4 \cdot 7^3.$$

- By `MordellWeilShaInformation` subroutine of MAGMA, we see that its Mordell-Weil group is trival, which means that the Diophantine equation $7x^2 + y^6 = 4z^3$ has no solution.

- Here we consider the Diophantine equation

$$7x^2 + y^8 = 4z^3.$$

Any primitive solution of the Diophantine equation $7x^2 + y^8 = 4z^3$ satisfies, of course, the equation $7x^2 + (y^2)^4 = 4z^3$. Hence using Theorem 4, we obtain formulas describing x, y^2 and z.

- Here we consider the Diophantine equation

$$7x^2 + y^8 = 4z^3.$$

Any primitive solution of the Diophantine equation $7x^2 + y^8 = 4z^3$ satisfies, of course, the equation $7x^2 + (y^2)^4 = 4z^3$. Hence using Theorem 4, we obtain formulas describing x, y^2 and z.

- In particular we have the following formulas for y^2:

$$y^2 = \pm 3(21s^2 - 14ts - 3t^2)(2499s^4 + 1764ts^3 + 378t^2s^2 + 84t^3s - 5t^4),$$
$$y^2 = \pm 3(21s^2 - 14ts - 3t^2)(-245s^4 - 588ts^3 + 378t^2s^2 - 252t^3s + 51t^4).$$

Note that $t = 0$ implies $y = 0$.

- Therefore, nontrivial solutions correspond to affine rational points on one of the following genus two curves:

$$\mathcal{C}_1 : Y^2 = 3(21X^2 - 14X - 3)(2499X^4 + 1764X^3 + 378X^2 + 84X - 5),$$

$$\mathcal{C}_2 : Y^2 = -3(21X^2 - 14X - 3)(2499X^4 + 1764X^3 + 378X^2 + 84X - 5),$$

$$\mathcal{C}_3 : Y^2 = 3(21X^2 - 14X - 3)(-245X^4 - 588X^3 + 378X^2 - 252X + 51),$$

$$\mathcal{C}_4 : Y^2 = -3(21X^2 - 14X - 3)(-245X^4 - 588X^3 + 378X^2 - 252X + 51).$$

Definition 7

Let V be a variety defined over $\mathbb{Q}$. V is everywhere locally solvable (ELS) if the set $V(\mathbb{Q}_p)$ is nonempty for all places $p \leq \infty$ of $\mathbb{Q}$.

Definition 7

Let V be a variety defined over $\mathbb{Q}$. V is everywhere locally solvable (ELS) if the set $V(\mathbb{Q}_p)$ is nonempty for all places $p \leq \infty$ of $\mathbb{Q}$.

- ELS is necessary for existence of $\mathbb{Q}$-points, but sufficient!

Definition 7

Let V be a variety defined over $\mathbb{Q}$. V is everywhere locally solvable (ELS) if the set $V(\mathbb{Q}_p)$ is nonempty for all places $p \leq \infty$ of $\mathbb{Q}$.

- ELS is necessary for existence of $\mathbb{Q}$-points, but sufficient!
- We check that the curves $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ and $\mathcal{C}_4$ have no rational points. Indeed, the MAGMA commmand `HasPointsEverywhereLocally`$(f, 2)$ gives $\mathcal{C}_1(\mathbb{Q}_2) = \mathcal{C}_2(\mathbb{Q}_2) = \mathcal{C}_3(\mathbb{Q}_2) = \mathcal{C}_4(\mathbb{Q}_2) = \emptyset$.

Definition 7

Let V be a variety defined over $\mathbb{Q}$. V is everywhere locally solvable (ELS) if the set $V(\mathbb{Q}_p)$ is nonempty for all places $p \leq \infty$ of $\mathbb{Q}$.

- ELS is necessary for existence of $\mathbb{Q}$-points, but sufficient!
- We check that the curves $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ and $\mathcal{C}_4$ have no rational points. Indeed, the MAGMA commmand `HasPointsEverywhereLocally`$(f, 2)$ gives $\mathcal{C}_1(\mathbb{Q}_2) = \mathcal{C}_2(\mathbb{Q}_2) = \mathcal{C}_3(\mathbb{Q}_2) = \mathcal{C}_4(\mathbb{Q}_2) = \emptyset$.
- Namely, the Diophantine equation

$$7x^2 + y^8 = 4z^3$$

has no non-trivial solutions.

- Here we consider the Diophantine equation $7x^2 + y^{2n} = 4z^3$ where $n = p$ is a prime ≥ 7.

- Here we consider the Diophantine equation $7x^2 + y^{2n} = 4z^3$ where $n = p$ is a prime ≥ 7.
- By Lemma 6 (a), we have reduced the problem of solving the title equation to solving the equation $4y^p = u(u^2 - 21v^2)$ with odd u, v and y. Since $\gcd(u, v) = 1$, we have $d = \gcd(u, u^2 - 21v^2)|3$. We have two cases: $d = 1$ or $d = 3$.

- Here we consider the Diophantine equation $7x^2 + y^{2n} = 4z^3$ where $n = p$ is a prime ≥ 7.
- By Lemma 6 (a), we have reduced the problem of solving the title equation to solving the equation $4y^p = u(u^2 - 21v^2)$ with odd u, v and y. Since $\gcd(u, v) = 1$, we have $d = \gcd(u, u^2 - 21v^2)|3$. We have two cases: $d = 1$ or $d = 3$.
- (i) $d = 1$. Writing $u = \alpha^p$, $u^2 - 21v^2 = 4\beta^p$, we arrive at

$$\alpha^{2p} - 4\beta^p = 21v^2.$$

- Here we consider the Diophantine equation $7x^2 + y^{2n} = 4z^3$ where $n = p$ is a prime ≥ 7.
- By Lemma 6 (a), we have reduced the problem of solving the title equation to solving the equation $4y^p = u(u^2 - 21v^2)$ with odd u, v and y. Since $\gcd(u, v) = 1$, we have $d = \gcd(u, u^2 - 21v^2)|3$. We have two cases: $d = 1$ or $d = 3$.
- (i) $d = 1$. Writing $u = \alpha^p$, $u^2 - 21v^2 = 4\beta^p$, we arrive at

$$\alpha^{2p} - 4\beta^p = 21v^2.$$

- Here, apply the strategy of Bennett-Skinner (modular approach) [Bennett, Skinner-2004] for the above equation. Then it becomes an equation with $(p, p, 2)$ signature as follows

$$X^p - 4Y^p = 21Z^2, \; p \geq 7.$$

Elliptic curves

- Let E be an elliptic curve over $\mathbb{Q}$. By changing variables if necessary, we may assume that E is defined by

$$E : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{Z})$$

with discriminant

$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$

- If $E \;mod\; p$ is an elliptic curve (or equivalently if prime p does not divide $\Delta = \Delta_E$), then we say that E has good reduction mod p (or equivalently the elliptic curve E is then said to have good reduction at p).

Elliptic curves

- This happens for all but finitely many primes. For each such p, we have

$$a_p = p + 1 - \#E(\mathbb{F}_p).$$

By Hasse's theorem, we know that $|a_p| \leq 2\sqrt{p}$.

Elliptic curves

- This happens for all but finitely many primes. For each such p, we have

$$a_p = p + 1 - \#E(\mathbb{F}_p).$$

By Hasse's theorem, we know that $|a_p| \leq 2\sqrt{p}$.

An L function

- The L-function $L_E(s)$ of an elliptic curve $E/\mathbb{Q}$ is a function of a complex variable s that "encodes" the infinite sequence of integers a_p.

Elliptic curves

- This happens for all but finitely many primes. For each such p, we have

$$a_p = p + 1 - \#E(\mathbb{F}_p).$$

By Hasse's theorem, we know that $|a_p| \leq 2\sqrt{p}$.

An L function

- The L-function $L_E(s)$ of an elliptic curve $E/\mathbb{Q}$ is a function of a complex variable s that "encodes" the infinite sequence of integers a_p.
- For the "bad" primes that divide $\Delta(E)$, one defines a_p to be $0, 1$, or -1, depending on the type of singularity E has when reduced *mod* p.

An L function

- Define

$$L_E(s) = \prod_{bad\ p} (1 - a_p p^{-s})^{-1} \prod_{good\ p} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

An L function

- Define

$$L_E(s) = \prod_{bad\ p} (1 - a_p p^{-s})^{-1} \prod_{good\ p} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

- Since one can express

$$L_E(s) = \sum_{n=0}^{\infty} a_n n^{-s},$$

one can consider

$$f_E(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}.$$

Note that $f_E(z+1) = f_E(z)$.

Modular forms

A modular form (of weight 2 and level N) is a holomorphic function f on the upper half-plane satisfying

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$$

for all

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$$

i.e. for $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$ and $c \equiv 0 \pmod{N}$.

Modular forms

Fourier expansion: As $f(z+1) = f(z)$, we have

$$f(z) = \sum_{n=0}^{\infty} c_n q^n, \; q = e^{2\pi i z}.$$

The Modularity Theorem for Elliptic Curves

If E is an elliptic curve over $\mathbb{Q}$, then the corresponding generating series $f_E(z)$ is a modular form of weight 2 and level N, where N is the conductor of the curve E.

For the primes where there is bad reduction, the cubic $x^3 + Ax + B$ has multiple roots *mod* p. If it has a triple root, we say that E has additive reduction *mod* p. If it has a double root *mod* p, it has multiplicative reduction.

conductor of elliptic curve

The conductor of $N(E)$ is defined by

$$\prod_{bad\ p} p^{f_p}$$

where

$$f_p = \begin{cases} f_p = 1 & \text{if } E \text{ has multiplicative reduction at } p \\ f_p \geq 2 & \text{if } E \text{ has additive reduction at } p, \text{ and equals } 2 \text{ if } p \neq 2, 3. \end{cases}$$

$(n, n, 2)$ signature: Bennett-Skinner Strategy

We always assume that $n \geq 7$ is prime, and a, b, c, A, B and C are nonzero integers with Aa, Bb and Cc pairwise coprime, A and B are nth-power free, C squarefree satisfying

$$Aa^n + Bb^n = Cc^2. \tag{12}$$

We further assume that we are in one of the following situations:

(i) $abABC \equiv 1 \pmod 2$ and $b \equiv -BC \pmod 4$.

(ii) $ab \equiv 1 \pmod 2$ and either $\mathrm{ord}_2(B) = 1$ or $\mathrm{ord}_2(C) = 1$.

(iii) $ab \equiv 1 \pmod 2$, $ord_2(B) = 2$ and $C \equiv -bB/4 \pmod 4$.

(iv) $ab \equiv 1 \pmod 2$, $ord_2(B) \in \{3, 4, 5\}$ and $c \equiv C \pmod 4$.

(v) $\mathrm{ord}_2(Bb^n) \geq 6$ and $c \equiv C \pmod 4$.

$(n, n, 2)$ signature: Bennett-Skinner Strategy

In cases (i) and (ii) we consider the curve

$$E_1(a,b,c) : Y^2 = X^3 + 2cCX^2 + BCb^n X.$$

In cases (iii) and (iv) we consider

$$E_2(a,b,c) : Y^2 = X^3 + cCX^2 + \frac{BCb^n}{4} CX, \tag{13}$$

and in case (v) we consider

$$E_3(a,b,c) : Y^2 + XY = X^3 + \frac{cC-1}{4} X^2 + \frac{BCb^n}{64} X. \tag{14}$$

Theorem 8

[Bennet-Skinner, 2004] Let $i = 1, 2$ *or* 3.

(I) *The minimal discriminant of* $E_i(a, b, c)$ *is given by*

$$\Delta(E) = 2^{\delta_i} C^3 B^2 A (ab^2)^n, \tag{15}$$

where

$$\delta_i = \begin{cases} 6\,; & \text{if } i=1, \\ 0\,; & \text{if } i=2, \\ -12\,; & \text{if } i=3. \end{cases}$$

(II) *The conductor of the curve* $E_i(a, b, c)$ *is given by*

$$N(E) = 2^{\alpha} C^2 Rad(ABab), \tag{16}$$

where

Theorem (continued)

$$\alpha = \begin{cases} 5\,; \text{ if i=1, case (i)}, \\ 6\,; \text{ if i=1, case (ii)}, \\ 1\,; \text{ if i=2, case (iii),, } \mathrm{ord}_2(B) = 2 \text{ and } b \equiv -BC/4 \pmod 4, \\ 2\,; \text{ if i=2, case (iii), } \mathrm{ord}_2(B) = 2 \text{ and } b \equiv BC/4 \pmod 4, \\ 4\,; \text{ if i=2, case (iv) and } \mathrm{ord}_2(B) = 3, \\ 2\,; \text{ if i=2, case (iv) and } \mathrm{ord}_2(B) \in \{4,5\}, \\ -1\,; \text{ if i=3, case (v) and } \mathrm{ord}_2(Bb^n) = 6, \\ 0\,; \text{ if i=3, case (v) and } \mathrm{ord}_2(Bb^n) \geq 7. \end{cases}$$

Theorem (continued)

(III) Suppose that $E_i(a,b,c)$ does not have complex multiplication (This would follow if we assume that $xy \neq \pm 1$). Then $E_i \sim_p f$ for some newform f of level

$$N_n(E) = 2^{\beta} C^2 Rad(AB) \tag{17}$$

where

$$\beta = \begin{cases} \alpha; \text{cases (i)-(iv)} \\ 0\,; \ \text{case (v) and } \mathrm{ord}_2(B) \neq 0, 6, \\ 1\,; \ \text{case (v) and } \mathrm{ord}_2(B) = 0, \\ -1\,; \ \text{case (v) and } \mathrm{ord}_2(B) = 6. \end{cases}$$

(IV) The curves $E_i(a,b,c)$ have non-trivial 2-torsion.

Theorem (continued)

(V) Suppose $E(a, b, c) = E_i(a, b, c)$ is a curve associated to some solution (x, y, z) satisfying the above conditions. Suppose that F is another curve defined over $\mathbb{Q}$ such that $E \sim_p F$. Then the denominator of the j-invariant $j(F)$ is not divisible by any odd prime $q \neq p$ dividing C.

Galois respresentations

Let $E = E_i(a, b, c)$ for some $1 \leq i \leq 3$ and some primitive solution (a, b, c) to (12). We associate to the elliptic curve E a Galois representation

$$\rho_n^E : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_n).$$

This is just the representation of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on the n-torsion points $E[n]$ of the elliptic curve E, having fixed once and for all an identification of $E[n]$ with $\mathbb{F}_n^2$. We continue to make our assumptions that aA, bB and cC are pairwise coprime and that C is squarefree. Withous loss of generality we may also suppose that A and B are n-th-power free.

Proposition 12 (Bennett-Skinner,2004)

If $n \geq 7$ is a prime and if $ab \neq \pm 1$, then ρ_n^E is absolutely irreducible.

Proposition 13 (Bennett-Skinner,2004)

Suppose that $n \geq 7$ is a prime and $E = E_i(a, b, c)$ is a curve associated to a primitive solution of (12) with $ab \neq \pm 1$. Suppose further that

$$f = \sum_{m=1}^{\infty} c_m q^m (q := e^{2\pi i z})$$

is a newform of weight 2 and level $N_n(E)$ giving rise to ρ_n^E and that K_f is a number field containing the Fourier coefficients of f. If u is a prime, coprime to $nN_n(E)$, then n divides one of either

$$n \mid Norm_{K_f/\mathbb{Q}}(c_u \pm (u+1)) \quad or \quad n \mid Norm_{K_f/\mathbb{Q}}(c_u \pm 2r)$$

for some integer $r \leq \sqrt{u}$.

Proposition 14 (Bennett-Skinner,2004)

Suppose that $n \geq 7$ is a prime and $E = E_i(a, b, c)$ is the curve associated to a primitive solution of (12). *If*

$$N_n(E) = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60$$

then $ab = \pm 1$, i.e. there is no new form of weight 2 and at the above level $N_n(E)$.

- Now, we go back to the equation $X^p - 4Y^p = 21Z^2, \ p \geq 7$.
- By this strategy, this equation corresponds to a Frey elliptic curve which corresponds to the newforms of weight 2 and levels $N \in \{1764, 3528\}$.

- Now, we go back to the equation $X^p - 4Y^p = 21Z^2,\ p \geq 7$.
- By this strategy, this equation corresponds to a Frey elliptic curve which corresponds to the newforms of weight 2 and levels $N \in \{1764, 3528\}$.
- To compute systems of Hecke eigenvalues (or equivalently, Fourier coefficients) for conjugacy classes of new forms, we use LMFDB (Cremona's elliptic curve and modular form database) or MAGMA.

- Now, we go back to the equation $X^p - 4Y^p = 21Z^2,\ p \geq 7$.
- By this strategy, this equation corresponds to a Frey elliptic curve which corresponds to the newforms of weight 2 and levels $N \in \{1764, 3528\}$.
- To compute systems of Hecke eigenvalues (or equivalently, Fourier coefficients) for conjugacy classes of new forms, we use LMFDB (Cremona's elliptic curve and modular form database) or MAGMA.
- Except for the cases $p = 7, 19$ all procedures worked for eliminating newforms (HOW DO WE DO IT?).

- Now, we go back to the equation $X^p - 4Y^p = 21Z^2,\ p \geq 7$.
- By this strategy, this equation corresponds to a Frey elliptic curve which corresponds to the newforms of weight 2 and levels $N \in \{1764, 3528\}$.
- To compute systems of Hecke eigenvalues (or equivalently, Fourier coefficients) for conjugacy classes of new forms, we use LMFDB (Cremona's elliptic curve and modular form database) or MAGMA.
- Except for the cases $p = 7, 19$ all procedures worked for eliminating newforms (HOW DO WE DO IT?).
- For example, we have 13 newforms of weight 2 and level 1764, say $f_1, f_2, \cdots, f_{13}$. To eliminate f_1, we use Proposition 13. We know that $c_5(f_1) = -3$. Hence, by Proposition 13, p must divide one of 1,3,5,9. But this is impossible, because we assumed that $p \geq 7$ prime.

- For example, Proposition 13 is not usefull. What will we do?

- For example, Proposition 13 is not usefull. What will we do?
- $f_3 := q - 2q^5 - 2q^{11} \cdots$ corresponds to isogeny classe of elliptic curve $1764.c1$ (Cremona label) or $1764h1$ (LMFDB label) with non-integral j-invariant $2^{13} \cdot 3^{-5} \cdot 7^{-2}$. But this contradicts Theorem 8-(v). Hence we can eliminate this newform.

- We have the following

Proposition 15 (Chałupka, Dąbrowski, Soydan-2022)

The Diophantine equation $\alpha^{2p} - 4\beta^p = 21v^2$ has no solutions in coprime odd integers for $p \geq 11$, $p \neq 19$.

- We have the following

Proposition 15 (Chałupka, Dąbrowski, Soydan-2022)

The Diophantine equation $\alpha^{2p} - 4\beta^p = 21v^2$ has no solutions in coprime odd integers for $p \geq 11$, $p \neq 19$.

- We have an alternative plan for the case $p = 19$. We will see..

- (ii) $d = 3$. Since $v_3(u^2 - 21v^2) = 1$ we have

$$\begin{cases} u = 3^{p-1}\alpha^p \\ u^2 - 21v^2 = 12\beta^p, \end{cases}$$

with odd α, β satisfying $\gcd(\alpha, \beta) = 1$. This leads to the equation

$$3^{2p-3}\alpha^{2p} - 4\beta^p = 7v^2.$$

- (ii) $d = 3$. Since $v_3(u^2 - 21v^2) = 1$ we have

$$\begin{cases} u = 3^{p-1}\alpha^p \\ u^2 - 21v^2 = 12\beta^p, \end{cases}$$

with odd α, β satisfying $\gcd(\alpha, \beta) = 1$. This leads to the equation

$$3^{2p-3}\alpha^{2p} - 4\beta^p = 7v^2.$$

- Similar to the former equation, the above equation is reduced to the equation of signature $(p, p, 2)$. Then apply the strategy of Bennett-Skinner. So, we have the following Frey curve

$$E = E(a, b, c) : Y^2 = X^3 + 7cX^2 - 7b^pX.$$

We associate this curve the Galois representation

$$\overline{\rho}_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

is irreducible for all primes $p \geq 7$.

- We see that $\overline{\rho}_{E,p}$ arises from a cuspidal newform f of weight 2, level $N = 588$ (resp. 1176), and trivial Nebentypus character. Applying some results in [Bennett, Skinner-2004] and [Freitas, Kraus-2019] yields the following result.

- We see that $\overline{\rho}_{E,p}$ arises from a cuspidal newform f of weight 2, level $N = 588$ (resp. 1176), and trivial Nebentypus character. Applying some results in [Bennett, Skinner-2004] and [Freitas, Kraus-2019] yields the following result.

Lemma 9 (Chałupka, Dąbrowski, Soydan-2022)

Let p be a prime. Suppose that (a, b, c) is a solution in coprime odd integers to the equation $3^{2p-3}\alpha^{2p} - 4\beta^p = 7v^2$. Let $E = E(a, b, c)$ be the associated Frey type curve.

1. *If $p \geq 13$, then $\overline{\rho}_{E,p} \cong \overline{\rho}_{F,p}$ for an elliptic curve F in one of the following isogeny classes: $588C, 588E, 1176G, 1176H$.*
2. *If $p = 11$, then $\overline{\rho}_{E,p} \cong \overline{\rho}_{F,p}$ for an elliptic curve F in one of the following isogeny classes: $588C, 588E, 1176A, 1176F, 1176G, 1176H$.*

- Here we will assume that $p \geq 11$ is a prime and apply variants of the method introduced by Kraus. Kraus stated a very interesting criterion [Kraus-1998] that often allows to prove that the Diophantine equation $x^3 + y^3 = z^p$ (p an odd prime) has no primitive solutions for fixed p, and verified his criterion for all primes $17 \leq p < 10^4$.

- Here we will assume that $p \geq 11$ is a prime and apply variants of the method introduced by Kraus. Kraus stated a very interesting criterion [Kraus-1998] that often allows to prove that the Diophantine equation $x^3 + y^3 = z^p$ (p an odd prime) has no primitive solutions for fixed p, and verified his criterion for all primes $17 \leq p < 10^4$.
- Such a criterion has been formulated (and refined) in other situations.

- Here we will assume that $p \geq 11$ is a prime and apply variants of the method introduced by Kraus. Kraus stated a very interesting criterion [Kraus-1998] that often allows to prove that the Diophantine equation $x^3 + y^3 = z^p$ (p an odd prime) has no primitive solutions for fixed p, and verified his criterion for all primes $17 \leq p < 10^4$.
- Such a criterion has been formulated (and refined) in other situations.

Kraus Type Criterion

Let $q \geq 11$ be a prime number, and let $k \geq 1$ be an integer factor of $q-1$. Let $\mu_k(\mathbb{F}_q)$ denote the group of k-th roots of unity in $\mathbb{F}_q^\times$. Set

$$A_{k,q} := \{\xi \in \mu_k(\mathbb{F}_q) : \frac{1 - 2^2 3^3 \xi}{3^3 \cdot 7} \text{ is a square in } \mathbb{F}_q\}.$$

Kraus Type Criterion

For each $\xi \in A_{k,q}$, we denote by δ_ξ the least non-negative integer such that

$$\delta_\xi^2 \mod q = \frac{1 - 2^2 3^3 \xi}{3^3 \cdot 7}.$$

We associate with each $\xi \in A_{k,q}$ the following equation

$$Y^2 = X^3 + 7\delta_\xi X^2 - 7\xi X.$$

Its discriminant equals $2^4 3^{-3} 7^3 \xi^2$, so it defines an elliptic curve E_ξ over $\mathbb{F}_q$. We put $a_q(\xi) := q + 1 - \#E_\xi(\mathbb{F}_q)$.

Theorem 16 (Chałupka, Dąbrowski, Soydan-2022)

Let $p \geq 13$ be a prime (resp. $p = 11$). Suppose that for each elliptic curve

$$F \in \{588C1, 1176G1\} \qquad (\textit{resp. } F \in \{588C1, 1176A1, 1176G1\})$$

there exists a positive integer k such that the following three conditions hold

1. $q := kp + 1$ *is a prime,*
2. $a_q(F)^2 \not\equiv 4 \pmod{p}$,
3. $a_q(F)^2 \not\equiv a_q(\xi)^2 \pmod{p}$ *for all* $\xi \in A_{k,q}$.

Then the equation $3^{2p-3}x^{2p} - 4y^p = 7z^2$ has no solutions in coprime odd integers.

Corollary 17 (Chałupka, Dąbrowski, Soydan-2022)

Let $11 \leq p < 10^9$ *and* $p \neq 13, 17$ *be a prime. Then there are no triples* (x, y, z) *of coprime odd integers satisfying* $3^{2p-3}x^{2p} - 4y^p = 7z^2$.

Corollary 17 (Chałupka, Dąbrowski, Soydan-2022)

Let $11 \leq p < 10^9$ *and* $p \neq 13, 17$ *be a prime. Then there are no triples* (x, y, z) *of coprime odd integers satisfying* $3^{2p-3}x^{2p} - 4y^p = 7z^2$.

- The computations took about 270 hours (with two desktop computers).

Corollary 17 (Chałupka, Dąbrowski, Soydan-2022)

Let $11 \leq p < 10^9$ and $p \neq 13, 17$ be a prime. Then there are no triples (x, y, z) of coprime odd integers satisfying $3^{2p-3}x^{2p} - 4y^p = 7z^2$.

- The computations took about 270 hours (with two desktop computers).
- Now we consider the eq. $3^{2p-3}x^{2p} - 4y^p = 7z^2$ for the cases $p = 13$ or 17.

Corollary 17 (Chałupka, Dąbrowski, Soydan-2022)

Let $11 \leq p < 10^9$ and $p \neq 13, 17$ be a prime. Then there are no triples (x, y, z) of coprime odd integers satisfying $3^{2p-3}x^{2p} - 4y^p = 7z^2$.

- The computations took about 270 hours (with two desktop computers).
- Now we consider the eq. $3^{2p-3}x^{2p} - 4y^p = 7z^2$ for the cases $p = 13$ or 17.
- Following [Dahmen, 2011], we give a refined version of Kraus type criterion (Dahmen studied on the eq. $x^2 + y^{2n} = z^3$) and apply it succesfully in case $p = 17$:

- **A refined version of Kraus type criterion**
  (ii) $d = 3$. Since $v_3(u^2 - 21v^2) = 1$ we have

$$\begin{cases} u = 3^{p-1}\alpha^p \\ u^2 - 21v^2 = 12\beta^p. \end{cases}$$

If $3 \mid y$, then we have

$$3u = (3\alpha)^p \quad \text{and} \quad u^2 - 21v^2 = 12\beta^p$$

for some coprime odd integers u, v and coprime odd integers α, β such that $y = 3\alpha\beta$. Let $R = [\omega]$, where $\omega = \frac{1+\sqrt{21}}{2}$, be the ring of integers of the number field $\mathbb{Q}(\sqrt{21})$. Observe that R has class number one.

- **A refined version of Kraus type criterion**
  (ii) $d = 3$. Since $v_3(u^2 - 21v^2) = 1$ we have

$$\begin{cases} u = 3^{p-1}\alpha^p \\ u^2 - 21v^2 = 12\beta^p. \end{cases}$$

  If $3 \mid y$, then we have

$$3u = (3\alpha)^p \quad \text{and} \quad u^2 - 21v^2 = 12\beta^p$$

  for some coprime odd integers u, v and coprime odd integers α, β such that $y = 3\alpha\beta$. Let $R = [\omega]$, where $\omega = \frac{1+\sqrt{21}}{2}$, be the ring of integers of the number field $\mathbb{Q}(\sqrt{21})$. Observe that R has class number one.
- If we factor in R the both sides of the second equation, then we obtain

$$u + \sqrt{21}v = (3 \pm \sqrt{21})x_1^p\varepsilon \quad \text{and} \quad u - \sqrt{21}v = (3 \mp \sqrt{21})x_2^p\varepsilon^{-1},$$

  where $x_1, x_2 \in R$ and $\varepsilon \in R^*$.

- Suppose that $q = kp + 1$ is a prime that splits in R. Let $\mathfrak{q}$ be a prime in R lying above q. We have $R/\mathfrak{q} \simeq \mathbb{F}_q$. Write $\bar{x}$ for the reduction of $x \in R$ modulo $\mathfrak{q}$ and write r_{21} for $\sqrt{21}$. From the above equalities it follows that for some $\xi_0, \xi_1, \xi_2 \in \mu_k(\mathbb{F}_q)$

$$3\bar{u} = \xi_0, \quad \bar{u} + r_{21}\bar{v} = (3 \pm r_{21})\xi_1\bar{\varepsilon} \quad \text{and} \quad \bar{u} - r_{21}\bar{v} = (3 \mp r_{21})\xi_2\bar{\varepsilon}^{-1}.$$

- Suppose that $q = kp + 1$ is a prime that splits in R. Let $\mathfrak{q}$ be a prime in R lying above q. We have $R/\mathfrak{q} \simeq \mathbb{F}_q$. Write $\bar{x}$ for the reduction of $x \in R$ modulo $\mathfrak{q}$ and write r_{21} for $\sqrt{21}$. From the above equalities it follows that for some $\xi_0, \xi_1, \xi_2 \in \mu_k(\mathbb{F}_q)$

$$3\bar{u} = \xi_0, \quad \bar{u} + r_{21}\bar{v} = (3 \pm r_{21})\xi_1\bar{\varepsilon} \quad \text{and} \quad \bar{u} - r_{21}\bar{v} = (3 \mp r_{21})\xi_2\bar{\varepsilon}^{-1}.$$

- If we divide the second and the third equality by $3\bar{u}$ we obtain

$$\frac{1}{3} + r_{21}\frac{\bar{v}}{3\bar{u}} = (3 \pm r_{21})\xi_1'\bar{\varepsilon} \quad \text{and} \quad \frac{1}{3} - r_{21}\frac{\bar{v}}{3\bar{u}} = (3 \mp r_{21})\xi_2'\bar{\varepsilon}^{-1},$$

where $\xi_1' = \xi_1/\xi_0$ and $\xi_2' = \xi_2/\xi_0$.

- Suppose further that $\bar{\varepsilon_f} \in \mu_k(\mathbb{F}_q)$ for a fundamental unit $\varepsilon_f \in R^*$. Then also $\xi_1' \bar{\varepsilon}, \xi_2' \bar{\varepsilon} \in \mu_k(\mathbb{F}_q)$. Hence $\frac{\bar{v}}{3\bar{u}}$ is an element of $S_{k,q} \cup S'_{k,q}$, where

$$S_{k,q} = \left\{ \delta \in \mathbb{F}_q : \frac{1}{3 + r_{21}} \left(\frac{1}{3} + r_{21}\delta \right), \ \frac{1}{3 - r_{21}} \left(\frac{1}{3} - r_{21}\delta \right) \in \mu_k(\mathbb{F}_q) \right\},$$

$$S'_{k,q} = \left\{ \delta \in \mathbb{F}_q : \frac{1}{3 - r_{21}} \left(\frac{1}{3} + r_{21}\delta \right), \ \frac{1}{3 + r_{21}} \left(\frac{1}{3} - r_{21}\delta \right) \in \mu_k(\mathbb{F}_q) \right\}.$$

- Suppose further that $\bar{\varepsilon_f} \in \mu_k(\mathbb{F}_q)$ for a fundamental unit $\varepsilon_f \in R^*$. Then also $\xi_1' \bar{\varepsilon}, \xi_2' \bar{\varepsilon} \in \mu_k(\mathbb{F}_q)$. Hence $\frac{\bar{v}}{3\bar{u}}$ is an element of $S_{k,q} \cup S'_{k,q}$, where

$$S_{k,q} = \left\{ \delta \in \mathbb{F}_q : \frac{1}{3 + r_{21}} \left(\frac{1}{3} + r_{21}\delta \right), \ \frac{1}{3 - r_{21}} \left(\frac{1}{3} - r_{21}\delta \right) \in \mu_k(\mathbb{F}_q) \right\},$$

$$S'_{k,q} = \left\{ \delta \in \mathbb{F}_q : \frac{1}{3 - r_{21}} \left(\frac{1}{3} + r_{21}\delta \right), \ \frac{1}{3 + r_{21}} \left(\frac{1}{3} - r_{21}\delta \right) \in \mu_k(\mathbb{F}_q) \right\}.$$

- For $\delta \in S_{k,q} \cup S'_{k,q}$ we define $\xi_\delta = \frac{1 - 3^3 \cdot 7\delta^2}{3^3 2^2}$, which is an element of $\mu_k(\mathbb{F}_q)$. The equation

$$Y^2 = X^3 + 7\delta X^2 - 7\xi_\delta X$$

defines an elliptic curve E_δ over $\mathbb{F}_q$. We put
$a_q(\delta) := q + 1 - \#E_\delta(\mathbb{F}_q)$.
Then we have the following result.

Theorem 18 (Chałupka, Dąbrowski, Soydan-2022)

Let $p > 11$ be a prime. Suppose that for each elliptic curve $F \in \{588C1, 1176G1\}$ there exists a positive integer k such that the following conditions hold

1. $q := kp + 1$ *is a prime,*
2. q *splits in* $\mathbb{Z}[\frac{1+\sqrt{21}}{2}]$,
3. $q \mid \mathrm{Norm}_{\mathbb{Q}(\sqrt{21})/\mathbb{Q}((\frac{5+\sqrt{21}}{2})^k - 1)}$
4. $a_q(F)^2 \not\equiv 4 \pmod{p}$,
5. $a_q(F)^2 \not\equiv a_q(\delta)^2 \pmod{p}$ *for all* $\delta \in S_{k,q} \cup S'_{k,q}$.

Then the equation $3^{2p-3}x^{2p} - 4y^p = 7z^2$ *has no solutions in coprime odd integers.*

- Combining arguments of Theorem 16 and Theorem 18 allow us to prove the following result:

Corollary 19 (Chałupka, Dąbrowski, Soydan-2022)

The equation $3^{31}x^{34} - 4y^{34} = 7z^2$ *has no solutions in coprime odd integers.*

- Combining arguments of Theorem 16 and Theorem 18 allow us to prove the following result:

Corollary 19 (Chałupka, Dąbrowski, Soydan-2022)

The equation $3^{31}x^{34} - 4y^{34} = 7z^2$ *has no solutions in coprime odd integers.*

- The computation took about 51 hours.

- Combining arguments of Theorem 16 and Theorem 18 allow us to prove the following result:

Corollary 19 (Chałupka, Dąbrowski, Soydan-2022)

The equation $3^{31}x^{34} - 4y^{34} = 7z^2$ has no solutions in coprime odd integers.

- The computation took about 51 hours.
- Using the steps in "Kraus type criterion" and "the strategy of Bennett-Skinner" we prove the following (go back slide 67–> Prop. 15):

Proposition 20 (Chałupka, Dąbrowski, Soydan-2022)

The Diophantine equation $\alpha^{38} - 4\beta^{19} = 21v^2$ has no solution in coprime odd integers.

- Now we consider the eq. $7x^2 + y^{10} = 4z^3$. Here we apply Chabauty method.

- Now we consider the eq. $7x^2 + y^{10} = 4z^3$. Here we apply Chabauty method.
- In 1941, Claude Chabauty proved the finiteness of the number of rational points on curves of genus $g > 0$ with a jacobian of Mordell-Weil rank $< g$ over $\mathbb{Q}$.

- Now we consider the eq. $7x^2 + y^{10} = 4z^3$. Here we apply Chabauty method.
- In 1941, Claude Chabauty proved the finiteness of the number of rational points on curves of genus $g > 0$ with a jacobian of Mordell-Weil rank $< g$ over $\mathbb{Q}$.
- This is a method for finding the rational points on a curve C of genus at least 2, that applies when the Mordell-Weil group of $Jac(C)$ has rank less than the genus of C. It involves doing local calculations at some prime where C has good reduction.

- Now we consider the eq. $7x^2 + y^{10} = 4z^3$. Here we apply Chabauty method.
- In 1941, Claude Chabauty proved the finiteness of the number of rational points on curves of genus $g > 0$ with a jacobian of Mordell-Weil rank $< g$ over $\mathbb{Q}$.
- This is a method for finding the rational points on a curve C of genus at least 2, that applies when the Mordell-Weil group of $Jac(C)$ has rank less than the genus of C. It involves doing local calculations at some prime where C has good reduction.
- Here we consider the Diophantine equations

$$\alpha^{2p} - 4\beta^p = 21v^2$$

and

$$3^{2p-3}\alpha^{2p} - 4\beta^p = 7v^2$$

with $p = 5$.

- Then these Diophantine equations transform to the curves

$$\mathcal{C}_1 : Y^2 = 84X^5 + 21$$

and

$$\mathcal{C}_2 : Y^2 = 28X^5 + 3^7 \times 7.$$

- Then these Diophantine equations transform to the curves

$$\mathcal{C}_1 : Y^2 = 84X^5 + 21$$

and

$$\mathcal{C}_2 : Y^2 = 28X^5 + 3^7 \times 7.$$

- Now $Jac(\mathcal{C}_i)$ $(i = 1, 2)$ have $\mathbb{Q}$-rank 0, and using Chabauty0, we obtain $\mathcal{C}_i(\mathbb{Q}) = \{\infty\}$ $(i = 1, 2)$, and the assertion follows.

- Here we discuss a few approaches to this equation and the obstacles to making them work here.

- Here we discuss a few approaches to this equation and the obstacles to making them work here.
- (i) *The modular method*. We may consider the equations

$$\alpha^{2p} - 4\beta^p = 21v^2$$

and

$$3^{2p-3}\alpha^{2p} - 4\beta^p = 7v^2$$

for $p = 7$: $X^{14} - 4Y^7 = 21Z^2$ and $3^{11}X^{14} - 4Y^7 = 7Z^2$, respectively. In both cases, we could not exclude the possibility that the Galois representation associated to the Frey type curve arises from newform with nonrational Fourier coefficients.

- (ii) *Chabauty type approach in genus* 3. The Diophantine equations from (i) lead to the genus 3 curves $\mathcal{D}_1 : y^2 = x^7 + 2^{12} \cdot 3^7 \cdot 7^7$ and $\mathcal{D}_2 : y^2 = x^7 + 2^{12} \cdot 3^{11} \cdot 7^7$, respectively. Magma calculations show that the only rational points on $\mathcal{D}_i(\mathbb{Q})$ (with bounds 10^9) are points at infinity, as expected. Magma also shows that ranks of $Jac(\mathcal{D}_i)(\mathbb{Q})$ $(i = 1, 2)$ are bounded by 1.

- There are two technical problems to use Chabauty method:

Why is the proof of Theorem 5 with $n = 7$ hard ? (the eq. $7x^2 + y^{14} = 4z^3$)

- There are two technical problems to use Chabauty method:
  1. One needs explicit rational points of infinite order (not easy to find).
  2. There is no readily available implementation of Chabauty's method for (odd degree) hyperelliptic genus 3 curves.

- There are two technical problems to use Chabauty method:
  1. One needs explicit rational points of infinite order (not easy to find).
  2. There is no readily available implementation of Chabauty's method for (odd degree) hyperelliptic genus 3 curves.
- Professor Stoll suggested to try the methods of his papers [Stoll, 2018], but we were not able to follow his advise yet.

- (iii) *Combination of the modular and Chabauty methods*. One may consider a more general Diophantine equation $7x^2 + y^7 = 4z^3$, try to follow the paper [Poonen,Schaefer,Stoll-2007], and then deduce the solutions for the original Diophantine equation. It seems a very difficult task, but maybe the only available way ...

- (iii) *Combination of the modular and Chabauty methods*. One may consider a more general Diophantine equation $7x^2 + y^7 = 4z^3$, try to follow the paper [Poonen,Schaefer,Stoll-2007], and then deduce the solutions for the original Diophantine equation. It seems a very difficult task, but maybe the only available way ...
- Hence we complete the proof of Theorem 5, namely we proved that the Diophantine equation $7x^2 + y^{2p} = 4z^3$ has no primitive solutions where $11 \leq p < 10^9$ and $p \neq 13$.

3. Methods & Sketches for proofs

Theorem 7: The Diophantine equation $7x^2 + y^{2n} = 4z^3$ has no primitive solutions for a family of primes p satisfying:

$$p \equiv 3 \text{ or } 55 \pmod{106} \text{ or } p \equiv 47, 65, 113, 139, 143 \text{ or } 167 \pmod{168}$$

Symplectic method

The symplectic method is due to Halberstadt and Kraus [Halberstadt, Kraus-2002]. The reason for the name is that the method is conceptually based on the symplectic behaviour of isomorphic Galois representations.

3. Methods & Sketches for proofs

Theorem 7: The Diophantine equation $7x^2 + y^{2n} = 4z^3$ has no primitive solutions for a family of primes p satisfying:

$$p \equiv 3 \text{ or } 55 \pmod{106} \text{ or } p \equiv 47, 65, 113, 139, 143 \text{ or } 167 \pmod{168}$$

Symplectic/anti-symplectic isomorphism

Let $p \geq 3$ be a prime. Let E and E' be elliptic curves over $\mathbb{Q}$ and write $E[p]$ and $E'[p]$ for their p-torsion modules. Write $G_{\mathbb{Q}}$ for the absolute Galois group. Let $\varphi : E[p] \to E'[p]$ be a $G_{\mathbb{Q}}$-modules isomorphism. There is an element $d(\varphi) \in \mathbb{F}_p^{\times}$ such that, for all $P, Q \in E[p]$, the Weil pairings satisfy $e_{E',p}(\varphi(P), \varphi(Q)) = e_{E,p}(P, Q)^{d(\varphi)}$. We say that φ is a *symplectic isomorphism* if $d(\varphi)$ is a square modulo p and an *anti-symplectic* otherwise. If the Galois representation $\overline{\rho}_{E,p}$ is irreducible then all $G_{\mathbb{Q}}$-isomorphisms have the same symplectic type.

3. Methods & Sketches for proofs

Theorem 7:The Diophantine equation $7x^2 + y^{2n} = 4z^3$ has no primitive solutions for a family of primes p satisfying:

$$p \equiv 3 \text{ or } 55 \pmod{106} \text{ or } p \equiv 47, 65, 113, 139, 143 \text{ or } 167 \pmod{168}$$

Application of the symplectic method

Write Δ and Δ' for minimal discriminants of E and E'. Suppose E and E' have potentially good reduction at a prime l. Set $\tilde{\Delta} = \Delta / l^{v_l(\Delta)}$ and $\tilde{\Delta}' = \Delta' / l^{v_l(\Delta')}$. Define a *semistability defect* e as the order of the group $\mathrm{Gal}(\mathbb{Q}_l^{un}(E[p])/\mathbb{Q}_l^{un})$. Define e' in the same way. Note that if $E[p] \cong E'[p]$ then $e = e'$ [Bennett, Chen, Dahmen,Yazdani-2015]. If $l \geq 5$ then e is the denominator of $v_l(\Delta)/12$ [Kraus-1990]. We apply the following criterion:

3. Methods & Sketches for proofs

Theorem 7: The Diophantine equation $7x^2 + y^{2n} = 4z^3$ has no primitive solutions for a family of primes p satisfying:

$$p \equiv 3 \text{ or } 55 \pmod{106} \text{ or } p \equiv 47, 65, 113, 139, 143 \text{ or } 167 \pmod{168}$$

Lemma 10 (Freitas, Kraus-2022)

Let $p \geq 5$ and $l \equiv 3 \pmod 4$ be prime numbers. Let E and E' be elliptic curves over $\mathbb{Q}_l$ with potentially good reduction and $e = 4$. Set

$$r = \begin{cases} 0 & \text{if } v_l(\Delta) \equiv v_l(\Delta') \pmod 4, \\ 1 & \text{otherwise}, \end{cases} \qquad t = \begin{cases} 1 & \text{if } \left(\frac{\tilde{\Delta}}{l}\right)\left(\frac{\tilde{\Delta}'}{l}\right) = -1, \\ 0 & \text{otherwise}. \end{cases}$$

Suppose that $E[p]$ and $E'[p]$ are isomorphic G_l-modules. Then

$$E[p] \text{ and } E'[p] \text{ are symplectically isomorphic } \Leftrightarrow \left(\frac{l}{p}\right)^r \left(\frac{2}{p}\right)^t = 1.$$

3. Methods & Sketches for proofs

Theorem 7: The Diophantine equation $7x^2 + y^{2n} = 4z^3$ has no primitive solutions for a family of primes p satisfying:

$$p \equiv 3 \text{ or } 55 \pmod{106} \text{ or } p \equiv 47, 65, 113, 139, 143 \text{ or } 167 \pmod{168}$$

- Using the above lemma and a result of Kraus, we can prove the following proposition:

Proposition 21 (Chałupka, Dąbrowski, Soydan-2022)

The Diophantine equation $3^{2p-3}X^{2p} - 4Y^p = 7Z^2$ has no solution in coprime odd integers for any prime $p \equiv 47, 65, 113, 139, 143$ or $167 \pmod{168}$.

A small example for symplectic method

Let (a, b, c) be a solution in coprime odd integers of the equation $3^{2p-3}\alpha^{2p} - 4\beta^p = 7v^2$. Following Bennett-Skinner (BS) strategy, we consider the following Frey type curve associated to (a, b, c)

$$E = E(a, b, c) : Y^2 = X^3 + 7cX^2 - 7b^p X. \tag{18}$$

We have $\Delta_E = 2^4 \cdot 3^{2p-3} \cdot 7^3 (ab)^{2p}$ and $N_E = 588 \cdot \prod_{l|ab} l$ (resp. $1176 \cdot \prod_{l|ab} l$) if $b \equiv 3 \pmod 4$ (resp. $b \equiv 1 \pmod 4$). Using a corollary in BS, we obtain, that the associated Galois representation

$$\overline{\rho}_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

is irreducible for all primes $p \geq 7$. From BS, we know, that $\overline{\rho}_{E,p}$ arises from a cuspidal newform f of weight 2, level $N = 588$ (resp. 1176), and trivial Nebentypus character.

A small example for symplectic method

For the level 1176, there are 15 rational-nonrational newforms. For example, the newform f_9 is given by

$$q + q^3 + 2q^5 + q^9 + 4q^{11} + 2q^{13} + 2q^{15} - 2q^{17} + 4q^{19} \cdots$$

$f_9 \in S_2(1176)$ corresponds to the isogeny class $1176I$. For each curve F in this class the semistability defect at 7 is equal 2, while the semistability defect of E at 7 equals 4. Hence from we have $\overline{\rho}_{E,p} \not\cong \overline{\rho}_{F,p}$ for $p \geq 11$.

3. Methods & Sketches for proofs

Theorem 7: The Diophantine equation $7x^2 + y^{2n} = 4z^3$ has no primitive solutions for a family of primes p satisfying:

$$p \equiv 3 \text{ or } 55 \pmod{106} \text{ or } p \equiv 47, 65, 113, 139, 143 \text{ or } 167 \pmod{168}$$

Application of quadratic reciprocity

For a given field K, let $(,)_K : K^\times \times K^\times \to \{\pm 1\}$ be the Hilbert symbol defined by

$$(A, B)_K = \begin{cases} 1 & \text{if } z^2 = Ax^2 + By^2 \text{ has a nonzero solution in } K, \\ -1 & \text{otherwise.} \end{cases}$$

Note that the Hilbert symbol is symmetric and multiplicative. We will let $(,)_q$, $(,)$ and $(,)_\infty$ to denote $(,)_{\mathbb{Q}_q}$, $(,)_{\mathbb{Q}}$ and $(,)_{\mathbb{R}}$, respectively.

Application of quadratic reciprocity

Let $A = q^\alpha u$, $B = q^\beta v$, with u, v q-adic units. If q is an odd prime, then

$$(A, B)_q = (-1)^{\alpha\beta\frac{q-1}{2}} \left(\frac{u}{q}\right)^{\beta} \left(\frac{v}{q}\right)^{\alpha},$$

and

$$(A, B)_2 = (-1)^{\frac{u-1}{2}\frac{v-1}{2}+\alpha\frac{v^2-1}{8}+\beta\frac{u^2-1}{8}}.$$

For all nonzero rationals a and b, we have

$$\prod_{q\leq\infty}(a, b)_q = 1 \tag{19}$$

We need the following Lemma:

3. Methods & Sketches for proofs

Theorem 7:The Diophantine equation $7x^2 + y^{2n} = 4z^3$ has no primitive solutions for a family of primes p satisfying:

$$p \equiv 3 \text{ or } 55 \pmod{106} \text{ or } p \equiv 47, 65, 113, 139, 143 \text{ or } 167 \pmod{168}$$

Lemma 11 (Bennett, Chen, Dahmen, Yazdani-2015)

Let r and s be nonzero rational numbers. Assume that the Diophantine equation

$$A^2 - rB^{2p} = s(C^p - B^{2p})$$

has a solution in coprime nonzero integers A, B and C, with BC odd. Then

$$(r, s(C - B^2))_2 \prod_{2<q<\infty} (r, s(C - B^2))_q = 1,$$

where the product is over all odd primes q such that $v_q(r)$ or $v_q(s)$ is odd.

3. Methods & Sketches for proofs

Theorem 7: The Diophantine equation $7x^2 + y^{2n} = 4z^3$ has no primitive solutions for a family of primes p satisfying:

$$p \equiv 3 \text{ or } 55 \pmod{106} \text{ or } p \equiv 47, 65, 113, 139, 143 \text{ or } 167 \pmod{168}$$

- Using the above lemma and modular approach, we prove the folllowing result:

Proposition 22

The Diophantine equation $3^{2p-3}X^{2p} - 4Y^p = 7Z^2$ has no solution in coprime odd integers for any prime p satisfying $p \equiv 3$ or $55 \pmod{106}$.

- Hence the proof of Theorem 7 is completed.

Table of contents

6. References

T. Andrescu, D. Andrica, I. Cucurezeanu, *An introduction to Diophantine equations, a problem base approach*, Birkhauser, 2010.

M.A. Bennett, I. Chen, S.R. Dahmen, S. Yazdani, *Generalized Fermat equations: a miscellany*, Int. J. Number Theory **11** (2015), 1-28

M.A. Bennett, P. Mihăilescu, S. Siksek, *The generalized Fermat equation*, Open Problems in Mathematics (J. F. Nash, Jr. and M. Th. Rassias eds), 173-205, Springer, New York, 2016

M.A. Bennett, C.M. Skinner, *Ternary diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56**(1) (2004), 23-54

F. Beukers, *Generalized Fermat equations*, Panaromas & Syntheses. **36**(1) (2012), 119-149.

6. References

N. Bruin, *Chabauty methods and covering techniques applied to generalised Fermat equations*, PhD Thesis, University of Leiden 1999

N. Bruin, *The Diophantine Equations* $x^2 \pm y^4 = \pm z^6$ *and* $x^2 + y^8 = z^3$, Compos. Math. **118** (1999), 305-321

N. Bruin, *Chabauty methods using elliptic curves*, J. reine angew. Math. **562** (2003), 27-49

6. References

K. Chałupka, A. Dąbrowski, G. Soydan, *On a class of generalized Fermat equations of signature* $(2, 2n, 3)$, Journal of Number Theory, Vol. 234 (2022), 153-178.

K. Chałupka, A. Dąbrowski, G. Soydan, *On a class of generalized Fermat equations of signature* $(2, 2n, 3)$, *II*, submitted.

I. Chen, *On the equation* $s^2 + y^{2p} = \alpha^3$, Math. Comput. **262** (2007), 1223-1227

I. Chen, S. Siksek, *Perfect powers expressible as sums of two cubes*, J. Algebra **322** (2009), 638-656

6. References

J. Cremona, *Elliptic Curve Data*, http://johncremona.github.io/ecdata/ and *LMFDB - The L-functions and Modular Forms Database*, http://www.lmfdb.org/ or *Elliptic curves over* $\mathbb{Q}$, http://www.lmfdb.org/EllipticCurve/Q/

A. Dąbrowski, N. Günhan, G. Soydan, *On a class of Lebesgue-Ljunggren-Nagell type equations*, J. Number Theory **215** (2020), 149-159

A. Dąbrowski, T. Jędrzejak, K. Krawciów, *Cubic forms, powers of primes and the Kraus method*, Coll. Math. **128** (2012), 35-48

S.R. Dahmen, *A refined modular approach to the Diophantine equation* $x^2 + y^{2n} = z^3$, Int. J. Number Theory **7** (2011), 1303-1316

6. References

N. Freitas, A. Kraus *On the symplectic type of isomorphism of the p-torsion of elliptic curves*, arXiv:1607.01218 (2019), 1-104 (to appear in: Memoires of the American Math. Soc.)

N. Freitas, B. Naskręcki, M. Stoll, *The generalized Fermat equation with exponents* $2, 3, n$, Compos. Math. **156** (2020), 77-113

A. Kraus *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. **69** (1990), 353-385

6. References

A. Kraus, *Sur l'equation $a^3 + b^3 = c^p$*, Experiment. Math. **7** (1998), 1-13

A. Kraus, J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259-275

B. Poonen, E.F. Schaefer, M. Stoll, *Twists of X(7) and primitive solutions to $x^2 + y^3 = z^7$*, Duke Math. J. **137** (2007), 103-158

W. Stein, *The Modular Forms Database*: http://modular.math.washington.edu/Tables/

M. Stoll, *Chabauty without the Mordell-Weil group*, In: G. Böckle, W. Decker, G. Malle (Eds.): Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory, Springer Verlag (2018), 623-663

M. Stoll, *An Explicit Theory of Heights for Hyperelliptic Jacobians of Genus Three*, In: G. Böckle, W. Decker, G. Malle (Eds.): Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory, Springer Verlag (2018), 665-739

Thank you for your attention!

Merci pour votre attention!