The Catalan's Conjecture and a Ribenboim's book

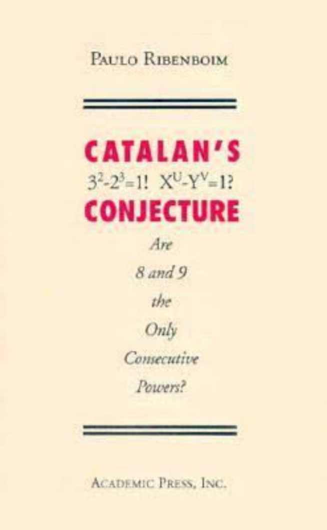
Gabriel Araujo Guedes

Universidade Federal Rural de Pernambuco

October 26, 2018

Abstract

In this lecture we will talk about the Catalan conjecture, the solution of this problem due to Preda Mihailescu, also as one of Ribenboim's books was the main reference on this subject for a long time and we'll conclude with some recent developments in the area.


Paulo Ribenboim
CATALAN'S
$3^2-2^3=1!$ $X^U-Y^V=1?$
CONJECTURE
Are
8 and 9
the
Only
Consecutive
Powers?
Academic Press, Inc.

On 1844, it was published on Crelle's Journal the following small note, of Eugene Catalan:

> *"Je vous prie, Monsieur, de vouloir bien énoncer, dans votre recueil, le théorème suivant, que je crois vrai, bien que je n'aie pas encore réussi à le démontrer complètement: d'autres seront peut-être plus heureux: Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être des puissances exactes; autrement dit: l' équation $x^u - y^v = 1$, dans làquelle les inconnues sont entières et positives, n'admèt qu'une seule solution?"*

But in fact Catalan never published any concrete result about his conjecture.

On 1844, it was published on Crelle's Journal the following small note, of Eugene Catalan:

> *"Je vous prie, Monsieur, de vouloir bien énoncer, dans votre recueil, le théorème suivant, que je crois vrai, bien que je n'aie pas encore réussi à le démontrer complètement: d'autres seront peut-être plus heureux: Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être des puissances exactes; autrement dit: l' équation* $x^u - y^v = 1$ *, dans làquelle les inconnues sont entières et positives, n'admèt qu'une seule solution?"*

But in fact Catalan never published any concrete result about his conjecture.

Even Exponents

It's easy to see that you only have to prove this conjecture for exponents being prime numbers, that is, $x^p - y^q = 1$, where p and q are prime numbers.

Lebesgue Theorem

On 1850, only six year after the establishment of this conjecture, the French mathematician Victor Amedèe Lebesgue (not the famous one), demonstrated that the equation $x^p - y^2 = 1$, does not have any solution for $p > 2$.

Idea of the Proof

The idea of the proof is factor the equation $x^p = y^2 + 1$, as $x^p = (y + i) \cdot (y - i)$ in $\mathbb{Z}[i]$ and make arithmetic on this domain to obtain a contradiction.

Even Exponents

It's easy to see that you only have to prove this conjecture for exponents being prime numbers, that is, $x^p - y^q = 1$, where p and q are prime numbers.

Lebesgue Theorem

On 1850, only six year after the establishment of this conjecture, the French mathematician Victor Amedèe Lebesgue (not the famous one), demonstrated that the equation $x^p - y^2 = 1$, does not have any solution for $p > 2$.

Idea of the Proof

The idea of the proof is factor the equation $x^p = y^2 + 1$, as $x^p = (y + i) \cdot (y - i)$ in $\mathbb{Z}[i]$ and make arithmetic on this domain to obtain a contradiction.

p=2 and q=3

An old result of Euler: The unique solutions of $x^2 - y^3 = 1$ in $\mathbb{Z}^*$ are $(\pm 3, 2)$. The proof uses the method of *descenso infinito* of Fermat.

Ko Chao, p=2 and q>3

If $q \geq 5$ is prime, then the equation $x^2 = y^q + 1$, does not have solutions on $\mathbb{Z}^*$.

p=2 and q=3

An old result of Euler: The unique solutions of $x^2 - y^3 = 1$ in $\mathbb{Z}^*$ are $(\pm 3, 2)$. The proof uses the method of *descenso infinito* of Fermat.

Ko Chao, p=2 and q>3

If $q \geq 5$ is prime, then the equation $x^2 = y^q + 1$, does not have solutions on $\mathbb{Z}^*$.

A brief sketch

Based on some elementary arithmetic manipulation we can show that $(s, 1)$ and $(x, y^{\frac{q-1}{2}})$ are roots of the same Pell equation

$$W^2 - yZ^2 = 1$$

and work with congruence we find $y = 0$, it achieves a contradiction.

Elementary different of easy

One of the most strongest result on Catalan conjecture till the Preda Mihailescu answer, is Cassels' theorem which has an elementary (but not easy) proof having intricated calculations. It needed to be someone like Cassels to believe that the calculation would go to anywhere.

Theorem (Cassels Theorem)

Let p, q be odd primes and $x > 0$ and $y > 0$ be integers such that $x^p - y^q = 1$. Then p divides y and q divides x.

Elementary different of easy

One of the most strongest result on Catalan conjecture till the Preda Mihailescu answer, is Cassels' theorem which has an elementary (but not easy) proof having intricated calculations. It needed to be someone like Cassels to believe that the calculation would go to anywhere.

Theorem (Cassels Theorem)

Let p, q be odd primes and $x > 0$ and $y > 0$ be integers such that $x^p - y^q = 1$. Then p divides y and q divides x.

Corollary

Let p, q be odd primes and $x > 0$ and $y > 0$ integers such that $x^p - y^q = 1$ then $x - 1 = p^{q-1}a^q$, $\dfrac{x^p - 1}{x - 1} = pb^q$, $y = pab$. With $gcd(a, b) = 1$ and $p \nmid b$.

Upper Bounds

Someone could ask: Is it possible to find an upper bound for the number of solutions for this equation? The Answer is: Yes, but... By using the Alan Baker theory of linear forms in logarithms, to the catalan equation, R. Tijdeman was able to determine an effective computable upper bounds. But as Tauno Metsankyla said in his expository article "These constant are astronomical, cryptographically locked for practical purposes."

$$|x|, |y| < 10^{10^{10^{120}}}$$

what are not in the book?

This Ribenboim's book made an overview of the state of the art concerning the problem till 1994. Only in 2002 Preda Mihailescu, an unknown mathematician, gave a proof of the problem. He used a huge machinery of algebraic number fields, cyclotomic units on numbers fields, Galois modules, rational points on curves and so one. For more detailed reference you can see my master thesis (in Portuguese) or Rene Schoof's book.

What come next?

Now I'm going to exhibit a quick panorama of current research. Or try to answer: What the researchers are doing after the new ideas introduced by Mihailescu?

Pillai Equation

The natural question is the Pillai conjecture: Fixed a integer C, the equation $x^m - y^n = C$, has finite many solutions in integers (x, y, m, n) with $(m, n) \neq (2, 2)$.

We don't know very much on this problem, because some parts of Mihailescu theory are very sensitive for modifications, even if you try simple modification. Also you can use the Tidjeman theory to give upper bounds for the number of solutions to these equations too. But the comment of Tauno Metsankyla, is true again.

What about Function fields?

Probably the other natural question is if the Catalan Equation can be solved in function fields. But this question is not attractive. M. B. Nathanson proved that:

Theorem (Nathanson)

Let F be a field of characteristic not dividing v. If $u > 2$ and $v > 2$, the equation $x^u - y^v = 1$ with $x, y \in F(X)$ implies that x and y are constants.

Nagell-Ljunggren Equation

NL Equation

If x, y are non-zero integers; p, q are odd primes and $e \in \{0, 1\}$ the equation $\dfrac{x^p - 1}{x - 1} = p^e \cdot y^q$ has no solution in integers.

For this equation, the machinery of ciclotomics units of Mihailescu, is more adaptive, and a lot of partial results are obtained in recent years.

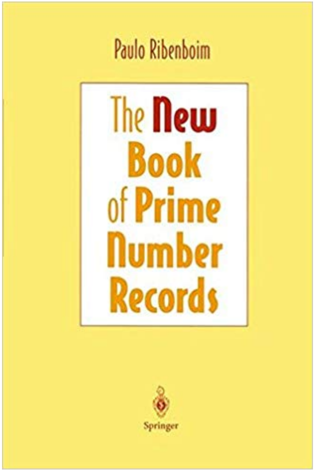


Figure: A delightful read

Problems that I spent a time

This book is very interesting it was written in a non-technical way. It presents a lot of exciting results and open problems. The first problem that I've spent a time was:

Yet another Erdös' Conjecture

Let the series

$$S = \sum_{n=1}^{\infty} (-1)^{n+1} \cdot \frac{n}{p_n}$$

Where p_n is the nth prime. S is convergent?

This kind of problem is deceitful. Because it looks like a simple one, but it is difficult. Erdös in the lecture that he proposed this problem, he told something like: "A proof of it is hopeless. The series are completely random."

What did we do?

Maria Eulalia and I in a joint work :

• We realized that almost nothing is known about alternating series;

• We did a huge review of old results and we proved some new ones;

• We did a review of the notion of convergence for alternanting double series, in the sense of Pringsheim, diagonally, Sigma convergence and clarifying some parts;

• Did we solve the problem? See soon.

The second problem:Topologies on Integers

On this Ribenboim's Book, he gave 10 proves of the existence of infinite many primes. One of them is Furstenberg proof, from 1955. In the demonstration it's defined a topology τ_f where the opens are defined as $Na, b = \{an + b \ : \ n \in \mathbb{Z}\}$. This topology is Hausdorff, but totally disconnected. In 1959, Golomb defined a new topology τ_G where the opens are defined
$Na, b = \{an + b \ : \ n \in \mathbb{Z}^+ \text{ and } gcd(a, b) = 1\}$. Thus τ_G it is Hausdorff and connected. Furthermore Dirichlet theorem on primes in arithmetic progression is equivalent to P, the set of prime numbers is dense in τ_G.

In 1966, Kirch defined a another new topology τ_k where the opens were defined

$$Na, b = \{an+b \ : \ n \in \mathbb{Z}^+, \ gcd(a, b) = 1, \ a > b \text{ and } a \ squarefree \ \}$$

it's not hard to prove that τ_k is locally connected but not regular. Working with my student Marcos Sobral, we realized that these researcher are sieving the opens of Furstenberg topology to obtain coarsers topologies. With the conditions of you can proof that P is infinite and the restriction are on a, b.
Then we define a topology τ_S with the opens like in the Kirch topology with the extra restriction of the primes in factorization of a are of the form $4k + 1$. By doing that, we proved some properties on this topology.

Another point of View

It's easy to see a natural bijection of the opens of τ_F and the points (a, b) of the lattices $\mathbb{Z}^2$. From this we can "measure" how τ_G is coarser than τ_F. This is equivalent to the classical result of count points visible from origin in Analytic Number Theory. That is, if you are attributing 1 to τ_F then to τ_G we obtain $\frac{6}{\pi^2}$. In other words, τ_G is approximately 40% coarser than τ_F. With the same technique we can proof that τ_K is 60% coarser.

Um Final em português

• Eu sou especialista em geometria algébrica, mas especificamente em geometria enumerativa de variedades projetivas simpléticas.
• Porém gosto muito de teoria dos números. De falar de matemática, de escrever, de conversar.
• Então se você ta procurando alguém para conversar, trocar uma ideia, qualquer coisa do tipo. Me manda um e-mail, um zap, me procura no facebook, no instagram...
• Atualmente tenho interesse em um monte de coisas: Problemas de soma zero, polinômios de permutação, polinômios de Ulam, conjectura de sendov...

Reference

1. G.A. GUEDES, **Sobre a Demonstração da Conjectura de Catalan**, 2009. UFMG/CNPQ.
2. R. SCHOOF, **Catalan's conjecture.** Springer, 2010.
3. Y. BILU, et al. **The problem of Catalan**. Springer, 2014.
4. T. METSÄNKYLÄ, **Catalan's conjecture: another old Diophantine problem solved**. Bulletin of the American Mathematical Society, v. 41, n. 1, p. 43-57, 2004.
5. T. SHOREY; R. TIJDEMAN, **Exponential diophantine equations**. Cambridge, 1986.

Reference

1. G.A. GUEDES, **Sobre a Demonstração da Conjectura de Catalan**, 2009. UFMG/CNPQ.
2. R. SCHOOF, **Catalan's conjecture.** Springer, 2010.
3. Y. BILU, et al. **The problem of Catalan**. Springer, 2014.
4. T. METSÄNKYLÄ, **Catalan's conjecture: another old Diophantine problem solved**. Bulletin of the American Mathematical Society, v. 41, n. 1, p. 43-57, 2004.
5. T. SHOREY; R. TIJDEMAN, **Exponential diophantine equations**. Cambridge, 1986.

Reference

1. G.A. GUEDES, **Sobre a Demonstração da Conjectura de Catalan**, 2009. UFMG/CNPQ.
2. R. SCHOOF, **Catalan's conjecture.** Springer, 2010.
3. Y. BILU, et al. **The problem of Catalan**. Springer, 2014.
4. T. METSÄNKYLÄ, **Catalan's conjecture: another old Diophantine problem solved**. Bulletin of the American Mathematical Society, v. 41, n. 1, p. 43-57, 2004.
5. T. SHOREY; R. TIJDEMAN, **Exponential diophantine equations**. Cambridge, 1986.

Reference

1. G.A. GUEDES, **Sobre a Demonstração da Conjectura de Catalan**, 2009. UFMG/CNPQ.
2. R. SCHOOF, **Catalan's conjecture.** Springer, 2010.
3. Y. BILU, et al. **The problem of Catalan**. Springer, 2014.
4. T. METSÄNKYLÄ, **Catalan's conjecture: another old Diophantine problem solved**. Bulletin of the American Mathematical Society, v. 41, n. 1, p. 43-57, 2004.
5. T. SHOREY; R. TIJDEMAN, **Exponential diophantine equations**. Cambridge, 1986.

Reference

1. G.A. GUEDES, **Sobre a Demonstração da Conjectura de Catalan**, 2009. UFMG/CNPQ.
2. R. SCHOOF, **Catalan's conjecture.** Springer, 2010.
3. Y. BILU, et al. **The problem of Catalan**. Springer, 2014.
4. T. METSÄNKYLÄ, **Catalan's conjecture: another old Diophantine problem solved**. Bulletin of the American Mathematical Society, v. 41, n. 1, p. 43-57, 2004.
5. T. SHOREY; R. TIJDEMAN, **Exponential diophantine equations**. Cambridge, 1986.