MATEMÁTICA UNIVERSITÁRIA
no. 20/21 – junho/dezembro 1996 – pp. 3-16

A Conjetura de Catalan

Paulo Ribenboin

A conjetura de Catalan é de enunciado muito simples. Os objetivos deste artigo são:

1. Descrever os métodos usados para tentar resolvê-la.

2. Explicar porque a conjetura, além de desafiadora, é natural.

Terei sido bem sucedido se você também achá-la bonita. Com uma única exceção, ao longo deste artigo referências tomarão o lugar de demonstrações.

1 O problema

Vou considerar sequências de inteiros e fazer algumas perguntas. Em primeiro lugar, consideremos a sequência de todos os quadrados e cubos:

$$4, 8, 9, 16, 25, 27, 36, 49, 64, 81, 100, \ldots .$$

Nela observamos que 8 e 9 são os únicos números consecutivos. O primeiro problema é: existem outros pares de inteiros consecutivos nesta sequência? Quantos? Finitos? Infinitos?

Posso também considerar a sequência de todas as potências inteiras, que inclui 5^as, 7^as, 11^as ... potências (note que potências com expoentes pares são quadrados, potências com expoentes múltiplos de 3 são cubos, etc). A mesma questão se aplica: existem potências consecutivas além de 8 e 9? Outra pergunta natural é: existem três inteiros consecutivos que são potências perfeitas?

Como potências crescem muito rapidamente, listas de potências são forçosamente muito limitadas; além de 8 e 9, até hoje não foram detectadas outras potências consecutivas. Devemos levar em conta este fato, mas por outro lado temos que ser cuidadosos antes de tirar conclusões.

Note, por exemplo, que 10% dos naturais até 100 são quadrados, 1% são quadrados até 10.000, até 1.000.000 apenas 1 em 1000 são quadrados, e assim por diante. Apesar desta crescente rarefação de quadrados, Lagrange provou que todo número natural pode ser escrito como soma de no máximo 4 quadrados. É como se os quadrados estivessem ocupando posições estratégicas. Nosso problema, é claro, é diferente.

Perguntas análogas podem ser feitas a respeito da sequência de potências de dois inteiros a e b com $1 < a < b$. Por exemplo, se $a = 2$ e $b = 3$, temos a sequência

$$4, 8, 9, 16, 27, 32, 64, 81, \ldots$$

Quantos pares de inteiros consecutivos existem nestas sequências?

Como outro exemplo, seja E um conjunto não vazio e finito de números primos, e $E^\times$ o conjunto de todos os números naturais cujos fatores primos pertencem a E. Quantos pares de inteiros consecutivos aparecem em $E^\times$?

Todos os problemas enunciados acima podem ser facilmente expressos na linguagem de equações diofantinas. O primeiro é equivalente a achar as soluções, em números naturais, das equações

$$x^2 - y^3 = 1, \quad x^3 - y^2 = 1.$$

O problema a respeito de potências arbitrárias é expresso pela equação diofantina exponencial

$$x^u - y^v = 1$$

onde buscamos soluções inteiras x, y maiores que 1. Finalmente, o problema para a sequência $E^\times$ é descrito pela simples equação

$$x - y = 1$$

mas aqui as soluções devem estar em $E^\times$.

Em 1844, Catalan conjeturou que 8 e 9 são os únicos inteiros consecutivos que são potências perfeitas. Esta conjetura está em aberto até hoje, apesar dos avanços que serão descritos.

2 Relação com outros problemas

Quero agora convencê-lo que os problemas vistos anteriormente fazem parte de uma grande classe de perguntas interessantes e bem conhecidas, para que você não ache que o problema de Catalan é irrelevante para uma melhor compreensão dos números inteiros.

Seja P um conjunto de números inteiros; quando conveniente, vamos assumir que $0 \in P$. Vou agora descrever problemas de adição e subtração.

Problemas de adição

Seja $P + P = \{p + p' \mid p, p' \in P\}$, e para $n \geq 1$ seja $nP = \{p_1 + p_2 + \cdots + p_n : \text{cada } p_i \in P\}$. Seja $\langle P \rangle = \bigcup_{n \geq 1} nP$. Podemos estudar os conjuntos nP e $\langle P \rangle$, e compará-los com os números naturais ou com algum subconjunto destes. As perguntas usuais são: existe n tal que $nP =$? Será que $\langle P \rangle =$?

Podemos formular questões análogas de um ponto de vista assintótico. Existe k_0 tal que

$$\{k \in \quad | k \geq k_0\} \subseteq nP \quad \text{ou} \quad \{k \in \quad | \, k \geq k_0\} \subseteq \langle P \rangle \; ?$$

Nestas situações, pode-se achar k_0 efetivamente?

Problemas de subtração

Aqui o problema é identificar o conjunto $P - P = \{p_1 - p_2 \mid p_1, p_2 \in P\}$. Mais precisamente, se $n \in P - P$, queremos determinar o conjunto $\{(p, p') \in P \times P \mid n = p - p'\}$ ou, pelo menos, achar cotas para o número de elementos deste conjunto.

Em alguns casos as respostas a estas perguntas são dadas assintoticamente, e podem ser de grande dificuldade.

Vamos agora dar exemplos específicos destas situações.

1. Números primos

Seja P o conjunto dos números primos, Mais geralmente, para $k \geq 1$, seja P_k o conjunto de todos os inteiros da forma $p_1^{e_1} \ldots p_n^{e_n}$ onde $0 < e_1 + \cdots e_n \leq k$. Os elementos de P_k são chamados de quase-k-primos. Em particular, temos $P_1 = P$.

Problema de adição: a conjetura de Goldbach. A famosa conjetura de Goldbach diz que

$$\{2n \mid n \geq 2\} \subset P + P$$

ou, equivalentemente,

$$\{n \mid n \geq 6\} = P + P + P \ .$$

Em meu livro sobre números primos (ver referências), descrevi os principais resultados obtidos no estudo da conjetura de Goldbach. Por exemplo, Vinogradov provou que

$$\{n \mid n \text{ é ímpar }, n > 3^{3^{15}}\} \subset P + P + P \ .$$

Schnirelman mostrou que existe s_0 tal que

$$\{n \mid n \geq 2\} = \bigcup_{k=1}^{s_0} kP \ ,$$

e Riesel e Vaughn mostraram que pode-se supor $s_0 = 19$.

Ao permitir o uso de quase-primos, temos o resultado pioneiro de Brun:

$$\{n \mid n \geq 4\} = P_9 + P_9 \ .$$

O melhor resultado conhecido é devido a Chen:

$$\{n \mid n \geq 4\} = P + P_2 \ .$$

Problemas de subtração: A conjetura de Polignac e a conjetura dos primos gemeos. A conjetura de Polignac, ainda em aberto, diz que todo número par pode ser escrito como a diferença de dois primos, ou seja,

$$\{2k \mid k \geq 1\} = P - P \ .$$

A conjetura dos primos gemeos diz que existem infinitos primos p tais que $p + 2$ também é primo. Em outras palavras, pode-se escrever 2 de infinitas maneiras distintas na forma $2 = p - p'$ onde p, p' são primos. Esta conjetura também está em aberto.

Para cada $N > 1$, seja $\pi_2(N)$ o número de primos $p \geq N$ tais que $p + 2$ também é primo. Podemos então enunciar a conjetura dos primos gemeos na seguinte versão quantitativa:

$$\pi_2(N) \sim \frac{N}{(\log N)^2} \ ,$$

ou seja, o quociente das duas expressões acima tem limite 1 quando $N \to \infty$.

Brun mostrou que

$$\sum \frac{1}{p} < \infty$$

(soma sobre todos os primos p tais que $p+2$ também é primo), donde se segue que os primos gemeos são bem raros. Note que $\sum \frac{1}{p} = \infty$ (soma sobre todos os primos), como mostrado por Euler.

2. Potências e números poderosos

Seja P o conjunto de todas as potências perfeitas e Q o conjunto de todos os números poderosos (isto é, números n tais que se um primo p divide n então p^2 divide n). É imediato que $Q = \{a^2b^3 \mid a, b \geq 1\}$.

Problemas de adição: Um problema interessante a respeito de $P + P$ é descrever $(P + P) \cap P$; em outras palavras, o estudo das soluções de $x^l + y^m = z^n$ para l, m, n fixos ou variáveis. Em particular, tem-se estudado a equação $x^n + y^n = z^n$ (a equação de Fermat) por mais de três séculos. Este problema acaba de ser resolvido por A. Wiles (com a colaboração de R. Taylor), que mostrou que se $n \geq 3$ e x, y, z são números naturais tais que $x^n + y^n = z^n$ então $xyz = 0$.

Para $n = 2$ a situação é bem diferente. Sabe-se há muito que existem infinitas triplas (x, y, z) de inteiros relativamente primos tais que $x^2 + y^2 = z^2$ (ditas triplas pitagóricas). Um resultado semelhante foi recentemente obtido por Elkies: existem infinitas quartas potências que são somas de três quartas potências.

Outro famoso problema de adição é devido a Waring. Dado $k \geq 2$, existe um inteiro $G(k) > 1$ tal que todo número natural suficientemente grande é a soma de no máximo $G(k)$ k-ésimas potências? Similarmente, existe um inteiro $g(k) > 1$ tal que todo número natural é a soma de no máximo $g(k)$ k-ésimas potências?

Como já mencionei anteriormente, Lagrange provou que $g(2) = 4$, e Gauss provou que $G(2) = 4$ mostrando que existem infinitos números racionais que não são somas de 3 quadrados.

Hilbert mostrou que $g(k)$ existe para todo $k \geq 2$. O problema então passou a ser o cálculo exato de $g(k)$ e $G(k)$. Davenport mostrou que $g(4) = 19$. A solução completa para quartas potências foi dada recentemente por Balasubramanian, Deshouillers e Dress: $G(4) = 16$. Ou seja, todos os inteiros suficientemente grandes podem ser escritos como uma

soma de 16 quartas potências; existem infinitos inteiros que não são somas de 15 quartas potências, e todos os inteiros podem ser escritos como soma de no máximo 19 quartas potências.

Outros resultados sobre o problema de Waring podem ser encontrados em meu livro sobre números primos.

Nem todo número natural pode ser escrito como soma de dois números poderosos. De fato,

$$\lim_{N\to\infty} \frac{\#\{n \in Q+Q \mid n \geq N\}}{N} = 0 \, .$$

No entanto, Heath-Brown mostrou que todo número natural suficientemente grande é soma de no máximo três números poderosos.

Problemas de subtração: Aqui considero em primeiro lugar números poderosos. Por $1 \in_\infty Q - Q$ quero dizer que 1 pode ser escrito como a diferença de números poderosos de infinitas maneiras; em outras palavras, existem infinitos pares de números poderosos consecutivos. De fato, a equação $x^2 - 8y^2 = 1$ tem infinitas soluções, donde x^2 e $8y^2$ são números poderosos consecutivos. Com a mesma notação, Mollin e McDaniel mostraram que $n \in_\infty Q - Q$ para todo $n \geq 2$.

Erdös conjeturou que não existem três números poderosos consecutivos. Granville mostrou como deduzir, a partir desta conjetura, o teorema de Adleman, Heath-Brown & Fouvry: existem infinitos primos p tais que se x, y, z são números naturais satisfazendo $x^p + y^p = z^p$ então $p \mid xyz$. Apesar da recente prova do último teorema de Fermat, a relação entre este teorema e números poderosos ainda é intrigante.

A pergunta análoga para potências é a conjetura de Catalan: se $1 = p - p'$ com $p, p' \in P$ então $p = 9$ e $p' = 8$. Pillai conjeturou que para todo $k > 1$ existem apenas finitos pares de potências (p, p') tais que $k = p - p'$. Esta conjetura pode ser expressa em termos da sequência

$$z_1 < z_2 < z_3 < \ldots$$

das potências, na forma

$$\lim_{i\to\infty} (z_{i+1} - z_i) = \infty \, .$$

No momento adequado, vou lidar com três potências consecutivas.

Interlúdio

Tendo explicado a significância da conjetura de Catalan em relação a outros problemas conhecidos e importantes, acho que posso contar com seu interesse. Vou agora descrever as numerosas tentativas que foram feitas para resolver o problema.

Se temos um problema e não é possível resolvê-lo imediatamente, é prudente estimar sua dificuldade analisando alguns casos especiais. Isto, é claro, pode não ser suficiente. Uma análise cuidadosa dos sucessos obtidos nestas situações especiais leva a métodos mais sistemáticos e abrangentes; para a conjetura de Catalan isto envolve números algébricos e, em última análise, congruências. No entanto, ficará claro mais tarde que a própria natureza destes belos métodos não os torna capazes de cobrir todas as possibilidades.

O que fazer então? A intuição sobre a progressiva rarefação das potências indica que métodos analíticos devem ser capazes de detectar se existem soluções com números arbitrariamente grandes. Seja paciente, até que eu explique como a teoria de equações diofantinas forneceu os métodos mais bem sucedidos para atacar nosso problema.

3 Casos especiais

O primeiro resultado conhecido relacionado aos problemas de Catalan e outros análogos data de aproxiamadamente 1320, e é devido a Levi ben Gerson (Leo Hebraeus), famoso astrônomo da época. Ele provou que se as únicas potências de 2 e 3 consecutivas são 8 e 9. Hoje isto é um exercício trivial com congruências.

Euler provou que se $x^2 - y^3 = \pm 1$ então $x = 3$ e $y = 2$. A idéia da prova de que $x^2 - y^3 = -1$ não tem solução em inteiros $x, y > 1$ é a seguinte. Se $x^2 - y^3 = -1$ então $y^3 = x^2 + 1 = (x + i)(x - i)$, onde $i^2 = -1$. De resultados elementares da aritmética de inteiros gaussianos, já conhecidos por Euler, segue-se que $x + i = \alpha(a + bi)^3$, onde a, b são inteiros e $\alpha = \pm 1$ ou $\pm i$, donde $x - i = \overline{\alpha}(a - bi)^3$ com $\overline{\alpha} = \pm 1$ ou $\pm i$, respectivamente. Logo $2i = \alpha(a+bi)^3 - \overline{\alpha}(a - bi)^3$, e um cálculo simples mostra que isto é impossível. Deve-se notar o uso de inteiros gaussianos neste argumento.

Esta idéia, convenientemente modificada, é encontrada no estudo de

outros casos particulares. Por exemplo, para mostrar que $x^m - y^n = 1$ não tem solução é suficiente considerar a mesma equação com expoentes primos; de fato, se p e q são primos com $m = pm'$ e $n = qn'$ então $x^m - y^n = 1$ pode ser escrita como $(x^{m'})^p - (y^{n'})^q = 1$.

Se p, q são primos ímpares, $x, y \neq 0$ e $x^p - y^q = 1$ então $y^q = x^p - 1 = (x-1)\left(\frac{x^p-1}{x-1}\right)$. Como $\text{mdc}(x-1, \frac{x^p-1}{x-1}) = 1$ ou p, temos dois casos:

$$\begin{cases} x-1 &= r^q \\ \frac{x^p-1}{x-1} &= r'^q \end{cases}$$

com $\text{mdc}(r, r') = 1$ e $rr' = y$, ou

$$\begin{cases} x-1 &= p^{q-1}r^q \\ \frac{x^p-1}{x-1} &= pr'^q \end{cases}$$

onde $\text{mdc}(r, r') = 1$ e $prr' = y$, de vez que p^2 não divide $\frac{x^p-1}{x-1}$.

De $x^p = y^q+1 = (y+1)\left(\frac{y^q+1}{y+1}\right)$ obtem-se expressões análogas para $y+1$ e $\frac{y^q+1}{y+1}$, em dois casos distintos. Existem também expressões similares para $x^2 - y^q = 1$, onde q é um primo ímpar.

O próximo caso especial é o das equações $x^2 - y^q = 1$ e $x^p - y^2 = 1$, onde p e q são primos ímpares maiores que 3. Uma destas não ofereceu dificuldades, e foi resolvida por Lebesgue em 1850, apenas seis anos após Catalan fazer sua conjetura, enquanto a outra, apesar de várias tentativas, só foi resolvida 120 anos depois por Ko em 1964. Qual é qual? Esta é uma questão apropriada para enfatizar o fato de que duas equações diofantinas podem ser muito parecidas, mas resolvê-las pode requerer métodos com níveis de dificuldade bem distintos.

Lebesgue provou , usando uma variante do método de Euler, que $x^p - y^2 = 1$ (p primo ≥ 5) tem apenas a solução trivial. A prova de Ko de que $x^2 - y^q = 1$ (q primo ≥ 5) tem apenas a solução trivial foi muito mais difícil. Mais tarde Chein usou resultados de Størmer e Nagell, do começo deste século, para dar uma prova engenhosa e muito mais curta do teorema de Ko em apenas três páginas! Matemáticos não devem desistir de substituir demonstrações longas e difíceis (que podem refletir apenas a falta de uma compreensão completa) por outras – eventualmente engenhosas – curtas e elegantes. [Não generalize o que acabo

de dizer para a recente prova do último teorema de Fermat, nem conclua que acredito que uma prova em 3 páginas poderia ser encontrada, e muito menos em uma margem ...]

As equações $x^3 - y^q = 1$ e $x^p - y^3 = 1$, onde p e q são primos ímpares maiores que 3, levam ao estudo das equações

$$x^2 + x + 1 = y^q \quad \text{ou} \quad x^2 + x + 1 = 3y^q \, .$$

Nagell mostrou que estas possuem apenas a solução trivial, supondo que as soluções de

$$x^3 - 3xy^2 + y^3 = 1$$

fossem apenas as já conhecidas $(x, y) = (1, 0), (0, 1), (1, 3), (2, -1), (-3, 2)$ e $(-1, -1)$. Foi difícil provar esta última afirmação; Ljungreen conseguiu fazê-lo em 1942, com uma análise precisa do grupo de unidades em um determinado corpo cúbico.

Gosto de chamar a atenção para o fato de que ninguém teve coragem de atacar a equação $x^p - y^q = 1$, onde $\min(p, q) \geq 5$, usando métodos especiais.

4 Métodos algébricos

O objetivo dos métodos que dependem fortemente da aritmética de corpos de números algébricos é tratar, simultaneamente, de grandes classes de expoentes, usando frequentemente as idéias de congruências, unidades e classes de ideais.

Antes vou mencionar algumas outras condições que implicam que a única solução não trivial de $x^u - y^v = 1$ $(u, v \geq 2)$ é $x = 3$, $y = 2$, $u = 2$ e $v = 3$, ou seja, $9 - 8 = 1$. São elas:

a. Se p, q, l são primos e $l^p - y^q = \pm 1$ então $l = 3$, $p = 2$, $y = 2$ e $q = 3$.

b. Se $x, y \geq 2$ e $x^y - y^x = 1$ então $x = 3$ e $y = 2$.

c. As únicas potências consecutivas de inteiros consecutivos são 8 e 9; em outras palavras, $x^m - y^n = 1$ e $\mid x - y \mid = 1$ implica $x = 3$, $y = 2$, $m = 2$ e $n = 3$.

A prova de **c.** requer um fato aritmético interessante e bem conhecido sobre os divisores primos de expressões da forma $x^m - 1$.

Cassels deu uma prova notável do seguinte resultado: se $x^p - y^q = 1$ com p, q primos então p divide y e q divide x. Segue-se que, dos dois casos

do resultado de Euler visto na seção anterior, apenas o segundo pode acontecer; então $x-1=p^{q-1}r^q$, $\frac{x^p-1}{x-1}=pr'^q$ e também $y+1=q^{p-1}s^p$, $\frac{y^q+1}{y+1}=qs'^p$.

Pode-se perguntar qual a importância do resultado de Cassels. Sem saber se existem x, y tais que $x^p-y^q=1$, como usar o fato de que $p \mid y$ e $q \mid x$? Surpresa! Hyyrö (em finlandês) e Makowski provaram que não existem três potências consecutivas usando este resultado. Parece haver uma uma regra informal que toda apresentação deve conter pelo menos uma prova, e escolho esta por sua notável simplicidade.

Se $x^p<y^q<z^r$ são potências perfeitas, com expoentes que podem ser supostos primos, $y^q-x^p=1$, $z^r-y^q=1$, o resultado de Cassels implica que $q \mid x$ e $q \mid z$. Logo $q \mid x^p$ e $q \mid z^r$, donde q divide $z^r-x^p=2$, e segue-se que $q=2$ e $z^r-y^2=1$. Pelo resultado de Lebesgue isto é impossível; contradição e fim da demonstração.

O teorema de Cassels implica que se $x^p-y^q=1$ então x, y são de uma forma especial, a saber, $x=1+p^{q-1}r^q$, $y=-1+q^{p-1}s^q$, assim como $\frac{x^p-1}{x-1}$ e $\frac{y^q+1}{y+1}$ também são de forma especial. Hyyrö explorou esta idéia introduzindo outras restrições que devem ser satisfeitas por x e y. Essencialmente, ele seguiu Wieferich e Inkeri ao relacionar o problema às congruências obtidas por Wieferich para o último teorema de Fermat. Vou agora explicar os resultados pertinentes de Inkeri, que seguem a linha da pesquisa de Hyyrö.

Seja p um primo ímpar e $H(-p)$ o número de classe do corpo $\mathbf{Q}(\sqrt{-p})$. Um dos resultados de Inkeri é: seja $p>3$, $p \equiv 3 \pmod 4$, $q>3$ um primo que não divide $H(-p)$ e tal que $p^{q-1} \not\equiv 1 \pmod{q^2}$. Então $x^p-y^q=1$ tem apenas a solução trivial.

Inkeri deu um critério análogo para $q \equiv 3 \pmod 4$ e um outro mais forte para o caso em que $p \equiv 3 \pmod 4$ e $q \equiv 3 \pmod 4$, todos complementados de maneira mais precisa em casos especiais.

Estes resultados são interessantes na prática por dois motivos. Em primeiro lugar é relativamente fácil calcular o número de classe de um corpo quadrático imaginário e checar se ele é divisível por um primo dado. Por outro lado, já foi observado que $p^{p-1} \equiv 1 \pmod{q^2}$ (a assim chamada congruência de Wieferich de base p) ocorre muito raramente. Este critério e outros semelhantes permitem decidir, através de cálculos, para quantos pares de expoentes (p, q) a equação correspondente admite apenas a solução trivial.

Mas mesmo pares pequenos como $(7, 5)$ não podem ser tratados com este critério. De fato, $7 \equiv 3 \pmod 4$, 5 não divide $H(-7) = 1$ e no entanto $7^4 \equiv 1 \pmod{5^2}$.

Para cobrir mais casos, Inkeri considerou também corpos ciclotômicos. Seja h_p o número de classe do corpo ciclotômico $\mathbf{Q}(\sqrt{\zeta_p})$, onde ζ_p é uma raiz p-ésima primitiva de 1. Inkeri mostrou que se $x^p - y^q = 1$ tem solução não trivial então:

a. Se p não divide h_q então $q^{p-1} \equiv 1 \pmod{p^2}$.

b. Se q não divide h_p então $p^{q-1} \equiv 1 \pmod{q^2}$.

Em particular as equações $x^5 - y^7 = \pm 1$ admitem apenas soluções triviais. De fato, 5 não divide h_7 e 7 não divide h_5, mas $5^6 \not\equiv 1 \pmod{7^2}$.

Em um artigo posterior com Aaltonen, muitos outros pares de expoentes foram eliminados por este método, através do cálculo de números de classe e congruências de Wieferich.

Mignotte, levando adiante estes cálculos, mostrou (com o uso de um lema não publicado de W. Schwarz) que se $\min(p, q) \leq 10.640$ então $x^p - y^q = 1$ tem apenas a solução trivial. Esta é, por enquanto, a última palavra sobre o assunto.

5 Métodos analíticos

Quero enfatizar um ponto óbvio, que tem estado implícito. Até agora temos considerado três tipos de equações:

I. $a^u - b^v = 1$, onde a e b são inteiros distintos fixos e maiores que 1.

II. $x^m - y^n = 1$, onde m e n são inteiros distintos fixos e maiores que 1.

III. $x^u - y^v = 1$.

É conveniente discutir cada uma destas isoladamente.

I. Equação $\mathbf{a^u - b^v = 1}$

O resultado principal é devido a LeVecque, que mostrou que existe no máximo um par (u, v) com $u, v \geq 2$ tal que $a^u - b^v = 1$. Cassels deu um algoritmo que permite achar, caso exista, a solução hipotética. Para $(a, b) \neq (3, 2)$ o algoritmo – até agora – não achou nenhuma solução!

Gostaria de considerar uma variante desta equação, que já foi mencionada no início deste artigo. Seja $E = \{p_1, \ldots, p_s\}$ um conjunto de primos e $k \geq 1$. Thue provou que existe uma constante efetivamente

calculável $C > 0$ tal que se

$$p_1^{n_1} p_2^{n_2} \dots p_s^{n_s} - p_1^{m_1} p_2^{m_2} \dots p_s^{m_s} = k$$

com inteiros $n_i, m_i \geq 0$ então $n_i, m_i < C$ para todo $i = 1, 2, \dots, s$.

Os casos especiais $k = 1, 2$ já tinham sido provados anteriormente por Størmer por um método muito interessante, envolvendo propriedades de divisibilidade de têrmos de sequências linearmente recorrentes de ordem 2 (ou seja, análogas às sequências de Lucas e Fibonacci).

II. Equação $x^m - y^n = 1$

Siegel trabalhou com uma equação mais geral. De seu resultado principal, segue que se $\max(m, n) \geq 3$ e a, b, k são inteiros dados então $ax^m - by^n = k$ tem apenas um número finito de soluções inteiras. Este resultado não inclui nenhuma cota para o número de soluções e, forçosamente, para a ordem de grandeza das mesmas.

A grande descoberta de Baker, que lhe valeu uma medalha Fields, foi um novo método para gerar cotas efetivas para as soluções de vários tipos de equações diofantinas. No caso em questão, as estimativas de Baker mostram que se $m, n \geq 2$ e $x^m - y^n = 1$ então $|x|, |y| < \exp\exp((3m)^{10} n^{10n^3} |k|^{n^2})$ (e uma cota similar trocando m e n). O cálculo desta cota depende de estimativas de cotas inferiores para certas formas lineares em logaritmos e envolve uma exponenciação dupla, resultando assim em números muito, muito grandes.

Deve-se também mencionar que para o número de pares (m, n) tais que $x^m - y^n = 1$ tem solução não trivial tem-se a cota $\exp(632 m^2 n^2)$, devida a Hyyrö.

Menor que a de Baker, mas maior que 0 – é o que se espera de uma cota para o número de soluções! Boa evidência para esta conjetura vem de um teorema de densidade que provei usando um teorema de Schinzel e Tijdeman: dados inteiros não nulos a, b, k seja, para cada $N > 0$, $\alpha(N)$ o número de pares (m, n) com $2 \leq m, n \leq N$ tais que a equação $ax^m - by^n = k$ não tenha soluções em inteiros positivos. Então $\lim_{N \to \infty} \frac{\alpha(N)}{N^2} = 1$.

III. Equação $x^u - y^v = 1$

É hora de enunciar o principal resultado obtido até agora sobre a conjetura de Catalan: existe uma constante C tal que se p, q são primos e x, y são inteiros tais que $x^u - y^v = 1$ então $p, q < C$. Este resultado

é devido a Tijdeman (1976), que usou duas vezes as desigualdades de Baker de um modo original e inovativo.

Levando em conta o resultado efetivo de Baker para a equação (II), segue-se que existe uma constante $T > 0$ tal que se $x^p - y^q = 1$ com p, q primos e $x, y \geq 1$ então $x, y, p, q < T$. Langevin conjeturou que pode-se supor $T = \exp\exp\exp\exp(730)$, um número além da minha imaginação; só de pensar nele, fico com dor de cabeça.

Este teorema ainda não é suficiente para determinar se a conjetura de Catalan é verdadeira, mas mostra que ela é decidível em um número finito de etapas. Teoricamente (e praticamente, em princípio) é suficiente tomar, consecutivamente, todas as quádruplas (x, y, p, q) até a cota T e checar se $x^p - y^q = 1$.

A busca de formas mais apuradas das desigualdades de Baker em conexão com a equação de Catalan levou Mignotte, por um lado, e Glass (e seus colaboradores), por outro, a uma corrida para diminuir a cota dos expoentes. Agora já se sabe que se $x^p - y^q = 1$ então $\max(p, q) \leq 10^{35}$.

Assim, sabemos que a conjetura de Catalan é decidível, mas não quando ela será decidida.

6 Conclusão

Mais uma vez, um problema de aparência inocente sobre números naturais mostrou ser um desafio até para os melhores matemáticos.

Um estudo cuidadoso dos esforços para resolver este problema pode ser comparado, como disse no prefácio de meu livro, a uma viagem através de uma bela paisagem matemática. Uma estrada sinuosa com lindas flores a serem colhidas. Um pico distante, que parece não mais estar fora de alcance.

7 Referências

Para provas, observações e detalhes a respeito da conjetura de Catalan, pode-se consultar meu livro, que contém uma bibliografia bem completa: P. Ribenboin, **Catalan's conjecture**, Academic Press, Boston, 1994.

Anteriormente, publiquei um apanhado sobre o problema: P. Ribenboin, *Consecutive powers*, Expositiones Mathematicae 2 (1984), 193-221.

Há vários preprints recentes de A. W. Glass et al., W. Mignotte e W. Schwarz sobre desenvolvimentos na linha dos critérios de K. Inkeri e os cálculos pertinentes, alguns dos quais ainda não foram publicados.

Os resultados sobre números primos podem ser achados, por exemplo, em meu livro: P. Ribenboin, **The book of prime number records**, Springer-Verlag, New York (primeira edição 1987; segunda edição 1989; terceira edição 1995). Veja também a edição resumida em francês: P. Ribenboin, **Les nombres premiers: mystères et records**, Presses Universitaires de France, Paris, 1994.

(Tradução de Michel Spira)