

Números congruente e a Conjectura BSD

Izabella Calais Fernandes

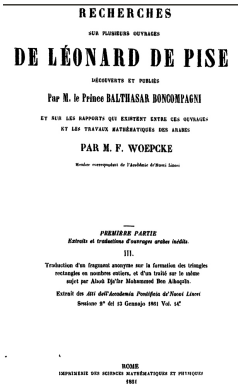
Orientador: Prof. Dr. Tiago Jardim da Fonseca

19 de Agosto de 2025



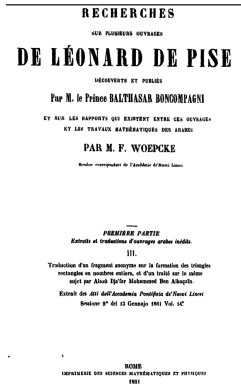
O problema dos números congruentes

- Artigo do historiador matemático **Franz Woepcke**, publicado em 1861.
- Um tratado do século IX atribuído ao matemático árabe **Aboû Dja'far**.



O problema dos números congruentes

- Artigo do historiador matemático **Franz Woepcke**, publicado em 1861.
- Um tratado do século IX atribuído ao matemático árabe **Aboû Dja'far**.



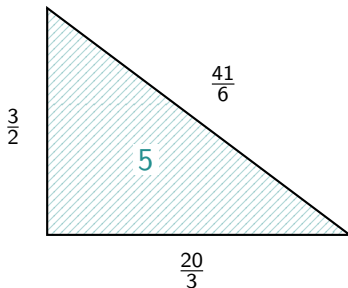
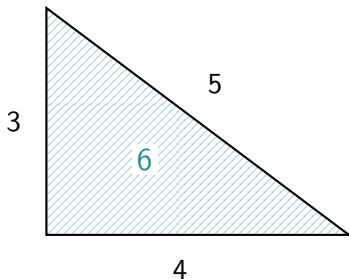
Definição

Um número $n \in \mathbb{Z}$ é chamado **congruente** se é a área de algum triângulo retângulo com lados racionais.

Exemplos de números congruentes

Os primeiros exemplos de números congruentes descobertos foram:

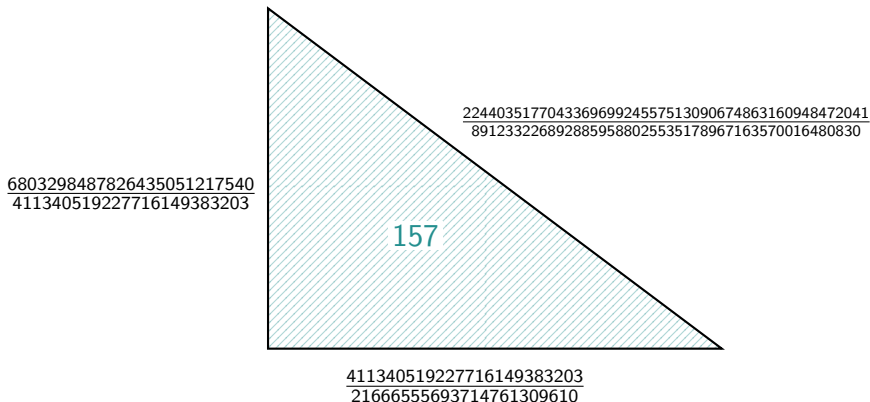
- Menor n com lados inteiros;
- Menor número congruente;



Ambos podem ser verificados com uma conta simples.

Exemplos de números congruentes

- Mas as coisas podem ficar difíceis rapidamente.



Este exemplo foi computado por D. Zagier em 1990.

Um número não congruente

Exemplo (Fermat, 1640)

1 não é um número congruente.

- Provado por Fermat utilizando o que foi posteriormente chamado de *método da descida infinita*.

Um número não congruente

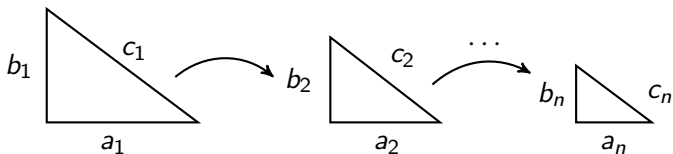
Exemplo (Fermat, 1640)

1 não é um número congruente.

- Provado por Fermat utilizando o que foi posteriormente chamado de *método da descida infinita*.

Ideia: Segue por contradição.

Se 1 é congruente, então existe um triângulo retângulo com lados inteiros cuja a área é um *quadrado perfeito*.



Reformulando o problema

O problema dos números congruentes pode ser reformulado como a busca por soluções racionais das equações

$$a^2 + b^2 = c^2 \quad \text{e} \quad \frac{ab}{2} = n, \quad n \in \mathbb{N}.$$

Seja $c = t + a$. Então, a equação $a^2 + b^2 = (t + a)^2$ implica:

$$2at = b^2 - t^2.$$

Substituindo $a = \frac{2n}{b}$ e multiplicando ambos os lados por $\frac{b^3}{t^3}$, obtemos:

$$\frac{4n^4}{t^2} = \left(\frac{bn}{t}\right)^3 - \frac{n^2bn}{t}.$$

Agora, definindo $y = \frac{2n^2}{t}$ e $x = \frac{bn}{t}$, obtemos a curva elíptica:

$$E_n : y^2 = x^3 - n^2x.$$

Problema dos números congruentes

A busca por soluções racionais das equações

$$a^2 + b^2 = c^2 \quad \text{e} \quad \frac{ab}{2} = n, \quad n \in \mathbb{N}.$$

Dessa maneira, podemos reformular o problema por:

Problema de Curvas elípticas

Se n é congruente, então existe um ponto racional (x, y) e $y \neq 0$ sob a curva elíptica

$$E_n : y^2 = x^3 - n^2x.$$

Proposição

Para $n > 0$, existe uma correspondência biunívoca entre os seguintes dois conjuntos:

$$\{(a, b, c) : a^2 + b^2 = c^2, \frac{ab}{2} = n\} \leftrightarrow \{(x, y) : y^2 = x^3 - n^2x, y \neq 0\}.$$

As correspondências inversas entre esses conjuntos são dadas por:

$$(a, b, c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a} \right), (x, y) \mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y} \right).$$

Definição

De maneira geral, uma **curva elíptica** complexa é uma curva algébrica plana determinada por uma equação da forma

$$E : y^2 = x^3 + ax + b, \text{ com } a, b \in \mathbb{Q} \text{ e } \Delta = 4a^3 + 27b^2 \neq 0.$$

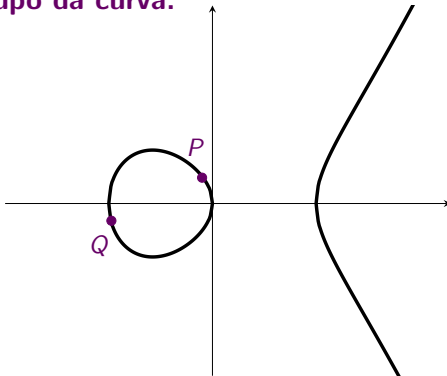
Curvas Elípticas

Definição

De maneira geral, uma **curva elíptica** complexa é uma curva algébrica plana determinada por uma equação da forma

$$E : y^2 = x^3 + ax + b, \text{ com } a, b \in \mathbb{Q} \text{ e } \Delta = 4a^3 + 27b^2 \neq 0.$$

■ A lei de grupo da curva:



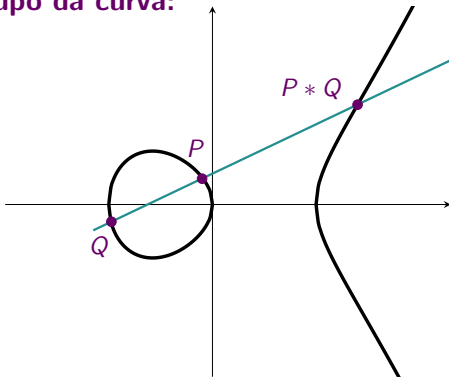
Curvas Elípticas

Definição

De maneira geral, uma **curva elíptica** complexa é uma curva algébrica plana determinada por uma equação da forma

$$E : y^2 = x^3 + ax + b, \text{ com } a, b \in \mathbb{Q} \text{ e } \Delta = 4a^3 + 27b^2 \neq 0.$$

■ A lei de grupo da curva:



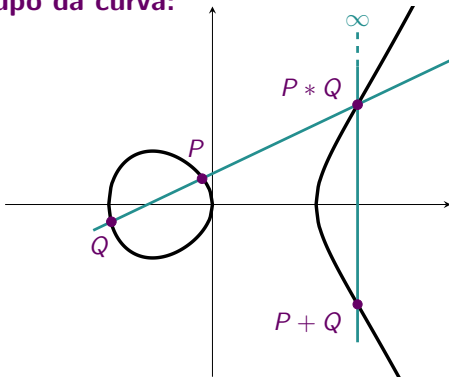
Curvas Elípticas

Definição

De maneira geral, uma **curva elíptica** complexa é uma curva algébrica plana determinada por uma equação da forma

$$E : y^2 = x^3 + ax + b, \text{ com } a, b \in \mathbb{Q} \text{ e } \Delta = 4a^3 + 27b^2 \neq 0.$$

■ A lei de grupo da curva:



Re-formulando o problema

Teorema (Mordell, 1922)

Seja E uma curva elíptica complexa. Então, o conjunto $E(\mathbb{Q})$ dos pontos racionais de E , com a operação de soma de pontos, é um grupo abeliano finitamente gerado. Isto é,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r,$$

onde $E(\mathbb{Q})_{\text{tor}}$ é o subgrupo finito dos pontos de torção de $E(\mathbb{Q})$ e $r \geq 0$ é chamado de *posto* da curva elíptica.

Re-formulando o problema

Teorema (Mordell, 1922)

Seja E uma curva elíptica complexa. Então, o conjunto $E(\mathbb{Q})$ dos pontos racionais de E , com a operação de soma de pontos, é um grupo abeliano finitamente gerado. Isto é,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r,$$

onde $E(\mathbb{Q})_{\text{tor}}$ é o subgrupo finito dos pontos de torção de $E(\mathbb{Q})$ e $r \geq 0$ é chamado de *posto* da curva elíptica.

Proposição

n é um número congruente se, e somente se, $E_n(\mathbb{Q})$ tem posto $r \neq 0$.

As dificuldades do posto

- A decomposição via o Teorema de Mordell é uma tarefa difícil e computacionalmente custosa.
- Dificuldade algébrica: a estrutura do grupo.
- Dificuldade computacional: Dada uma curva elíptica $y^2 = x^3 + bx$ é necessário estudar os divisores de b .
- Podemos encontrar curvas de posto 0, 1, 2, 3 ou 4 de maneira relativamente fácil.
- Encontrar curvas de posto muito grande é difícil. Ainda é uma **questão em aberto** se existem curvas de posto arbitrariamente grande.

Exemplificando a dificuldade do posto

Até 2015, para curvas $y^2 = x^3 + bx$, o maior posto conhecido era 14, associado a curva:

$$y^2 = x^3 + 402599774387690701016910427272483x,$$

onde

$$b = 32 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 37 \cdot 59 \cdot 71 \cdot 73 \cdot 97 \cdot 127 \cdot 139 \cdot 151 \cdot 263 \cdot 313 \cdot 443 \cdot 733.$$

Exemplo creditado a [Mark Watkins](#).

Exemplificando a dificuldade do posto

Até 2015, para curvas $y^2 = x^3 + bx$, o maior posto conhecido era 14, associado a curva:

$$y^2 = x^3 + 402599774387690701016910427272483x,$$

onde

$$b = 32 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 37 \cdot 59 \cdot 71 \cdot 73 \cdot 97 \cdot 127 \cdot 139 \cdot 151 \cdot 263 \cdot 313 \cdot 443 \cdot 733.$$

Exemplo creditado a [Mark Watkins](#).

Em 2006, [Noam Elkies](#) construiu uma curva de posto 28:

$$y^2 + xy + y = x^3 - x^2 + bx + c,$$

onde

$$b = -20067762415575526585033208209338542750930230312178956502$$

$$c = 34481611795030556467032985690390720374855944359319180361266 \\ 008296291939448732243429.$$

Uma curva elíptica que tem no **mínimo** posto 29.

NEW RANK RECORDS FOR ELLIPTIC CURVES HAVING RATIONAL
TORSION

NOAM D. ELKIES AND ZEV KLAGSBRUN

ABSTRACT. We present rank-record breaking elliptic curves having torsion subgroups $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, and $\mathbb{Z}/7\mathbb{Z}$.

Figura: Artigo de 2024, N. ELKIES e Z. KLAGSBRUN

Função L-Hasse-Weil

Seja $s \in \mathbb{C}$, definimos a **função L-Hasse-Weil** por

$$L(E, s) = \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E/\mathbb{F}_p; p^{-s})}$$

Função L-Hasse-Weil

Seja $s \in \mathbb{C}$, definimos a **função L-Hasse-Weil** por

$$L(E, s) = \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E/\mathbb{F}_p; p^{-s})}$$

Conjectura (Birch e Swinnerton-Dyer)

Seja E uma curva elíptica definida sobre $\mathbb{Q}$, e seja $L(E, s)$ a função L de Hasse-Weil. Então,

$$\operatorname{ord}_{s=1} L(E, s) = r.$$

- É um dos *Problemas do Milênio* estabelecido pelo [Clay Mathematics Institute](#).

E os números congruentes?

Teorema (Tunnell, 1983)

Seja $n \in \mathbb{N}$.

- Se n é ímpar, defina:

$$A = \# \{ (x, y, z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2 \} ,$$

$$B = \# \{ (x, y, z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2 \} .$$

- Se n é par, defina:

$$C = \# \{ (x, y, z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 8z^2 \} ,$$

$$D = \# \{ (x, y, z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 32z^2 \} .$$

Sendo assim,

- Se n é um número congruente, então:

se n é ímpar, então $A = 2B$, se n é par, então $C = 2D$.

E os números congruentes?

Teorema (Tunnell, 1983)

Seja $n \in \mathbb{N}$.

- Se n é ímpar, defina:

$$A = \# \{ (x, y, z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2 \},$$

$$B = \# \{ (x, y, z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2 \}.$$

- Se n é par, defina:

$$C = \# \{ (x, y, z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 8z^2 \},$$

$$D = \# \{ (x, y, z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 32z^2 \}.$$

Sendo assim,

- Se n é um número congruente, então:

se n é ímpar, então $A = 2B$, se n é par, então $C = 2D$.

- É condicional a conjectura BSD.

Exemplos da aplicação

Exemplo

Para $n = 1$ e $n = 3$, temos que o número de soluções inteiras positivas das equações que definem os conjuntos A e B é 2 em ambos os casos, ou seja, $A = B = 2$.

Dessa maneira como a condição $A = 2B$ não é satisfeita, pelo critério de Tunnell, podemos concluir que $n = 1$ e $n = 3$ não são números congruentes.

Exemplo (Aplicação da volta do teorema de Tunnell)

Queremos mostrar que todo inteiro positivo livre de quadrados com $n \equiv 5, 6, 7 \pmod{8}$ é um número congruente (assumindo a forma fraca da conjectura de Birch e Swinnerton-Dyer).

A volta do teorema de Tunnell

Exemplo (Aplicação da volta do teorema de Tunnell)

Segundo o teorema de Tunnell:

- Se $n \equiv 5$ ou $7 \pmod{8}$, devemos verificar se $A = 2B$;
 - Se $n \equiv 6 \pmod{8}$, devemos verificar se $C = 2D$.
- i) No primeiro caso, observamos que não existem soluções inteiras (x, y) para a congruência $x^2 + 2y^2 \equiv 5 \pmod{8}$ nem para $x^2 + 2y^2 \equiv 7 \pmod{8}$. Isso implica que $A = B = 0$, e portanto $A = 2B = 0$.
- ii) No segundo caso, para $n \equiv 6 \pmod{8}$, temos $\frac{n}{2} \equiv 3 \pmod{4}$. Mas, como não existe $x \in \mathbb{Z}$ tal que $x^2 \equiv 3 \pmod{4}$, concluímos que também não há soluções para as equações que definem C e D . Logo, $C = D = 0$, e temos $C = 2D$.

Muito Obrigada!

