Errata

O autor erroneamente disse que não se sabe nada para o caso $r_{\mathrm{an}}(E) > 1$. Isso é verdade para a conjectura "*forte*" de Birch e Swinnerton-Dyer, que dá uma fórmula para o coeficiente líder de $L_E(s)$ em termos do grupo de Tate-Shafarevich de E (este que não se sabe sequer ser finito para $r_{\mathrm{an}}(E) > 1$!). Para a conjectura BSD "*fraca*", que é o enunciado em questão é, como foi dito, **fácil** de calcular a L-função de E e checá-lo, mesmo para curvas elípticas de posto algébrico maior que 1:

`http://www.lmfdb.org/EllipticCurve/Q/389/a/1`

Peço desculpas por um erro tão trivial (que, honestamente, não sei como não percebi!).

A Conjectura BSD: mistérios de um milhão de dólares

Eduardo Rocha Walchek

Seminário de Coisas Legais

11 de outubro de 2019

Introdução: contando pontos em curvas algébricas

Uma **curva algébrica plana** sobre $\mathbb{Q}$ é um conjunto de pontos que satisfazem uma equação polinomial $f(x, y) = 0$, com $f \in \mathbb{Q}[x, y]$.

Cada curva possui um inteiro não-negativo intrínseco a ela chamado **gênero**.

Pergunta: quantos pontos uma curva irredutível $\mathcal{C}$ de gênero g possui?

- $g = 0$: se $\mathcal{C} \neq \emptyset$, $\mathcal{C}$ é parametrizável (exceto por finitos pontos):

$$\begin{aligned} \mathbb{Q} &\hookrightarrow \mathcal{C} \\ t &\mapsto \left(\frac{p_1(t)}{q_1(t)}, \frac{p_2(t)}{q_2(t)} \right) \end{aligned}$$

  Portanto, *infinitos pontos*.

- $g \geqslant 2$: (Faltings) $\mathcal{C}$ possui apenas *finitos pontos* (não-trivial!).

Introdução: contando pontos em curvas algébricas

E $g = 1$? Finitos? Infinitos? Ambos?

A curva $\mathcal{C}: y^2 = x^3 + k$ possui

- nenhum ponto, para $k = -5$;
- 1 ponto, para $k = -1$;
- 2 pontos, para $k = 16$;
- 5 pontos, para $k = 1$;
- infinitos pontos, para $k = -2$!

As curvas de gênero 1, como as acima, são as **curvas elípticas**.

Quantos pontos uma curva elíptica possui? Difícil de dizer, em geral.

A **Conjectura de Birch e Swinnerton-Dyer (BSD)** responde esta a pergunta de maneira simples.

Introdução: contando pontos em curvas algébricas

Peter Swinnerton-Dyer (1927-2018) e Bryan Birch (1931-)

A conjectura BSD conecta o número de pontos numa curva elíptica E (difícil de computar) ao comportamento de uma função complexa associada a E num certo ponto (fácil de computar).

Em 2000, o Clay Mathematics Institute anunciou um prêmio de 1 milhão de dólares para a primeira solução correta da conjectura. A descrição oficial do problema pode ser acessada em

`https://www.claymath.org/sites/default/files/birchswin.pdf`

Por que a conjectura BSD é tão interessante?

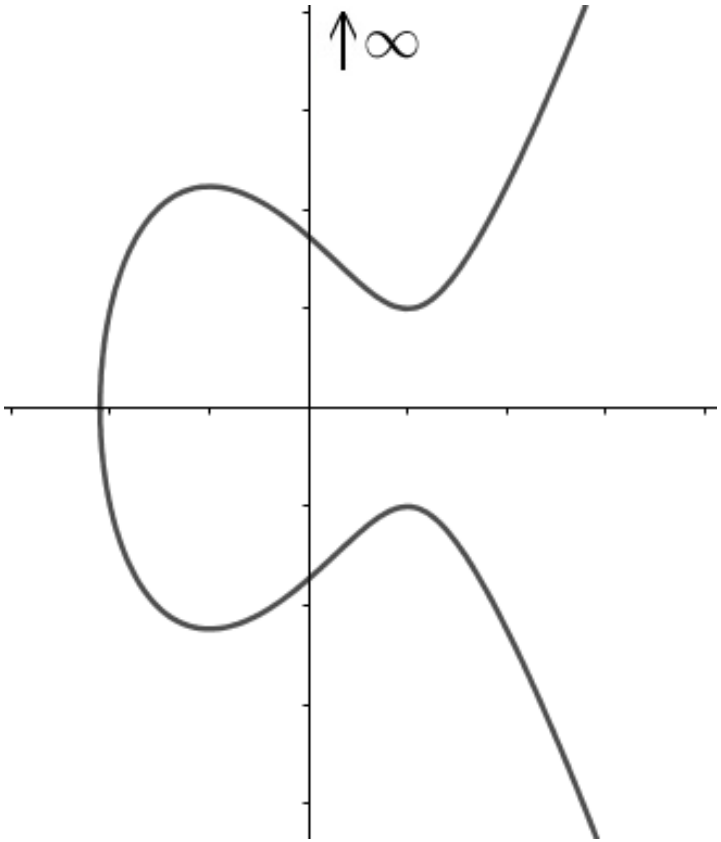
- 1 milhão de dólares!
- Solução de outros problemas em aberto (e.g. problema do número congruente);
- Esclarecimento de diversos mistérios que frustram nossas tentativas de entender as curvas elípticas.

Curvas elípticas

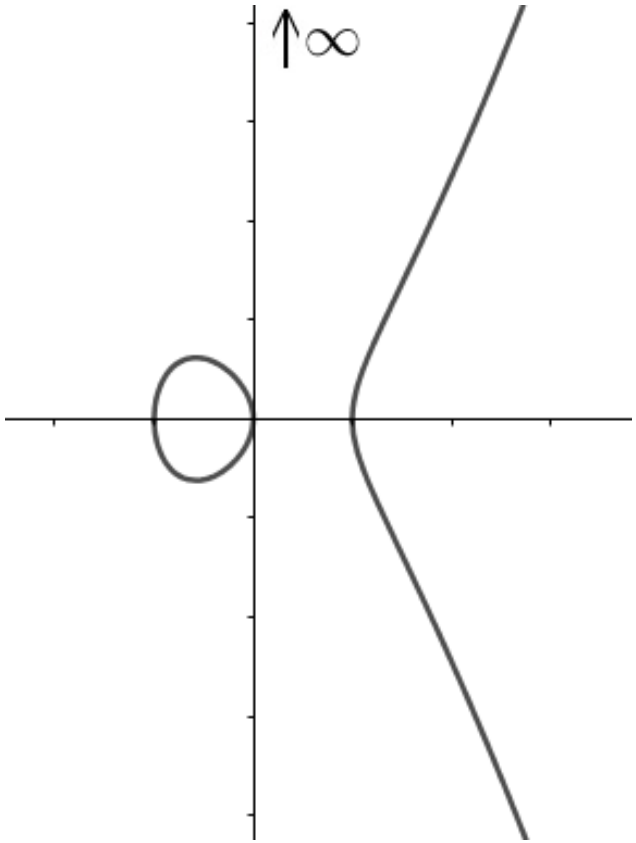
Uma **curva elíptica** sobre $\mathbb{Q}$ é uma curva dada por uma equação da forma

$$y^2 = f(x)$$

onde $f(x)$ é um polinômio cúbico com as 3 raízes distintas.



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



$y^2 = x^3 - x$

O que as curvas elípticas têm de tão especial?

Curvas elípticas são grupos abelianos!

Grupos abelianos

Definição (Grupo Abeliano)

Um conjunto G com uma operação $+$ é um **grupo abeliano** *se valem:*

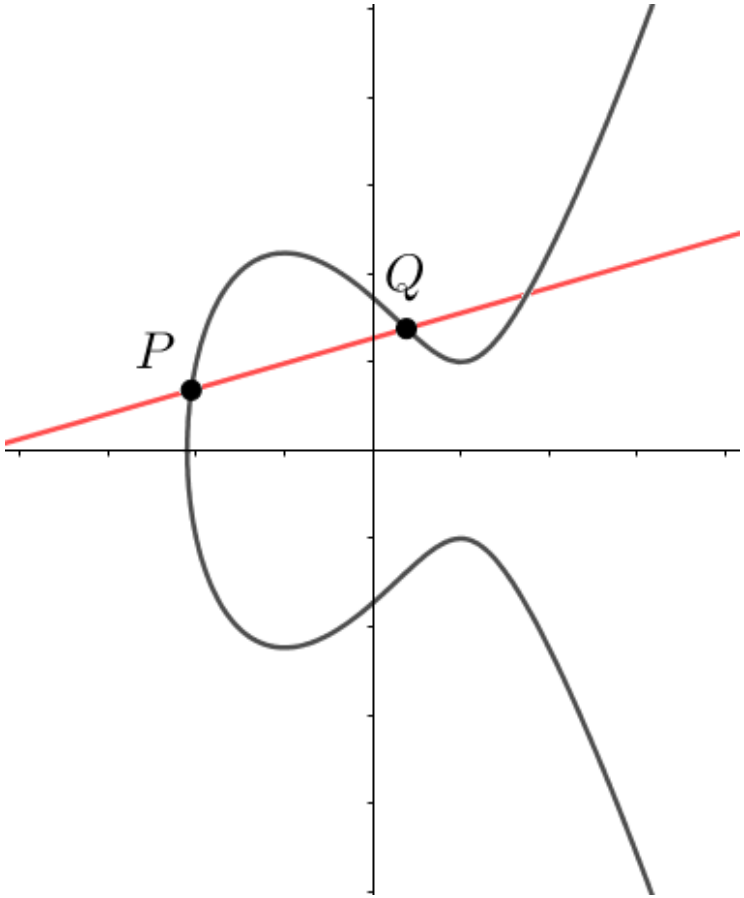
- Associatividade: $a + (b + c) = (a + b) + c$;
- Comutatividade: $a + b = b + a$;
- Elemento neutro: *existe* $0 \in G$ *tal que* $a + 0 = 0$;
- Elemento inverso: *para cada* $a \in G$, *existe* $b \in G$ *tal que* $a + b = 0$.

O que acontece se somamos $a \in G$ consigo mesmo várias vezes?

- ou obtemos $na \doteq \underbrace{a + \cdots + a}_{n} = \infty$ para algum n (dizemos que a é de ordem finita (n), ou de **torção**),
- ou obtemos infinitos pontos distintos a, $2a$, $3a$... (a tem ordem infinita)

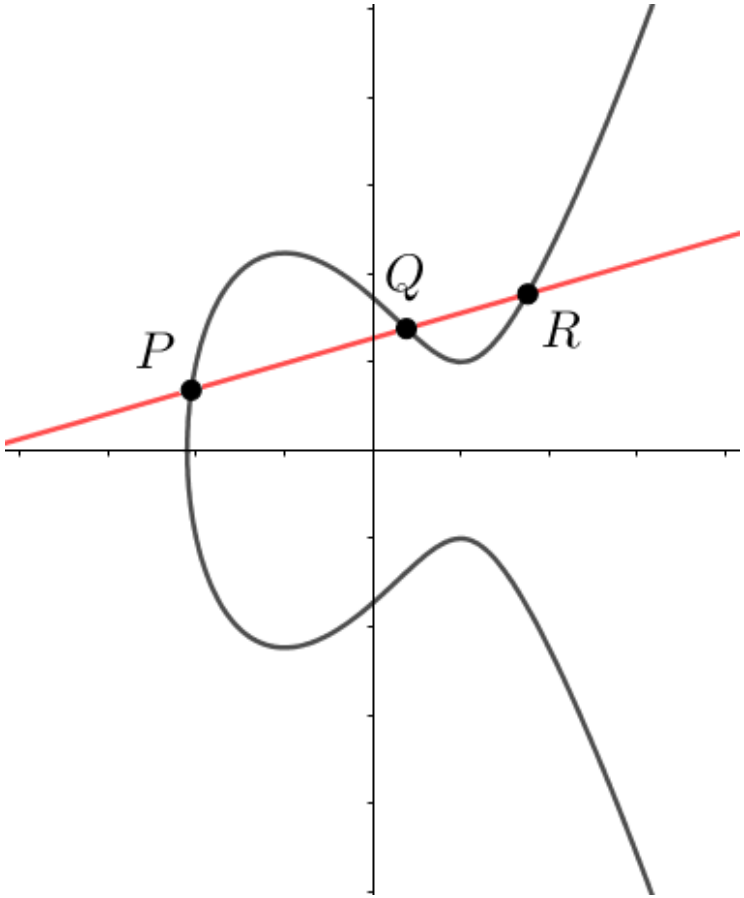
A lei de soma na curva elíptica

P, Q e R são colineares $\implies P + Q + R = \infty \ (= 0_E)$



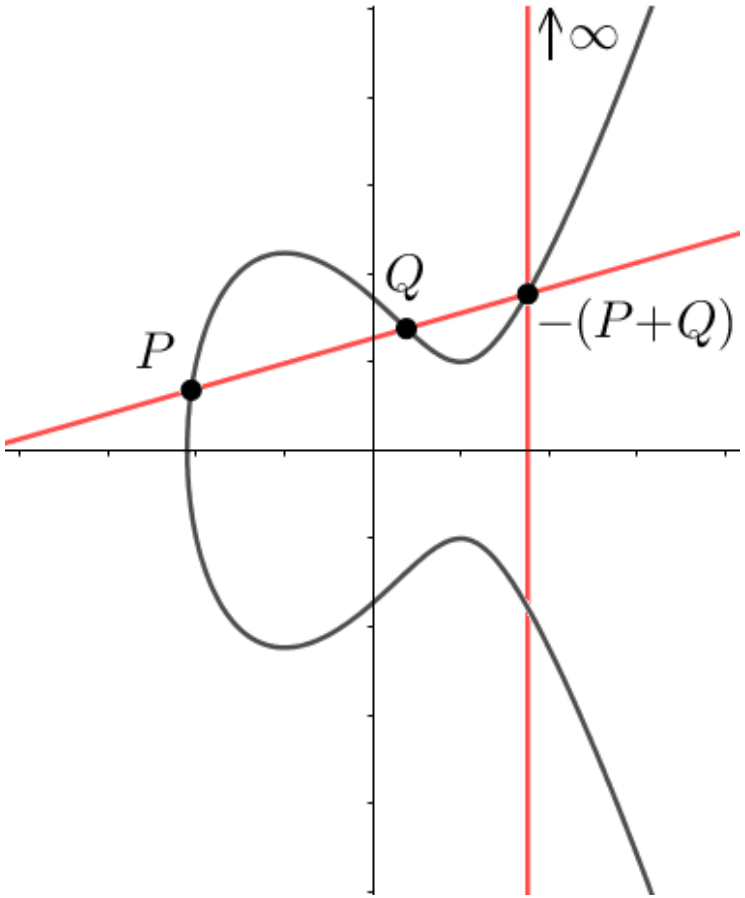
A lei de soma na curva elíptica

P, Q e R são colineares $\implies P + Q + R = \infty \ (= 0_E)$



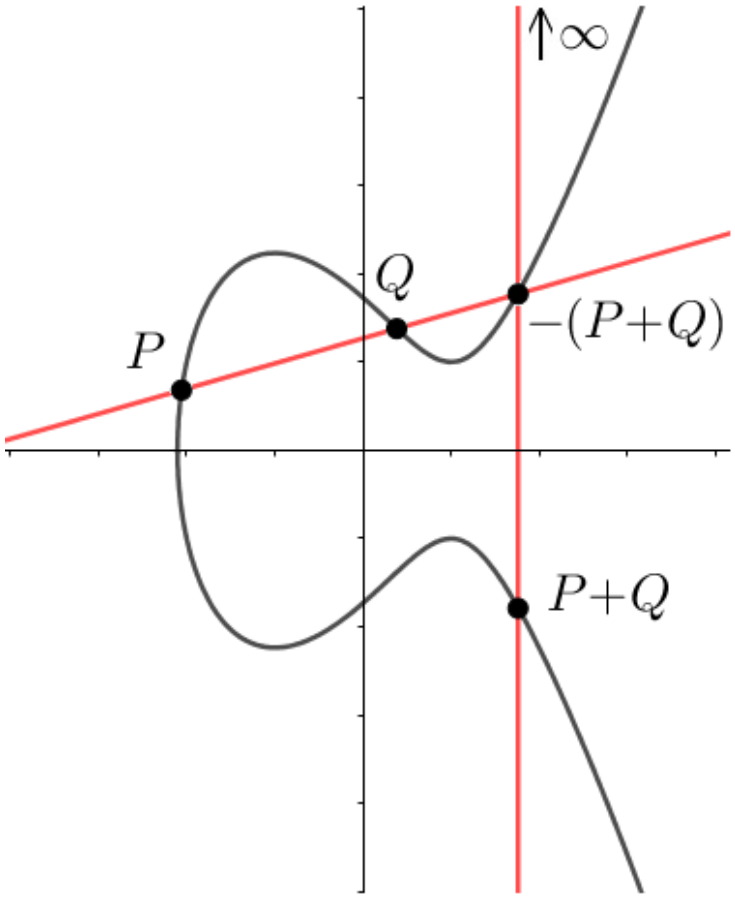
A lei de soma na curva elíptica

P, Q e R são colineares $\Longrightarrow$ $P + Q + R = \infty \ (= 0_E)$



A lei de soma na curva elíptica

P, Q e R são colineares $\Longrightarrow$ $P + Q + R = \infty \ (= 0_E)$



Curvas elípticas como grupos abelianos

Teorema (Mordell-Weil, 1922)

Uma curva elíptica $E/\mathbb{Q}$, como um grupo abeliano, é finitamente gerada.

Em outras palavras,

$$E = \mathbb{Z}^{r_{\mathrm{alg}}(E)} + E_{\mathrm{tor}},$$

onde $r_{\mathrm{alg}}(E) \in \mathbb{Z}_{\geqslant 0}$ é chamado **posto algébrico** de E e E_{tor} é o subgrupo (finito) dos pontos de torção.

Pergunta: Quais dos possíveis $r_{\mathrm{alg}}(E)$ e E_{tor} são realizados?

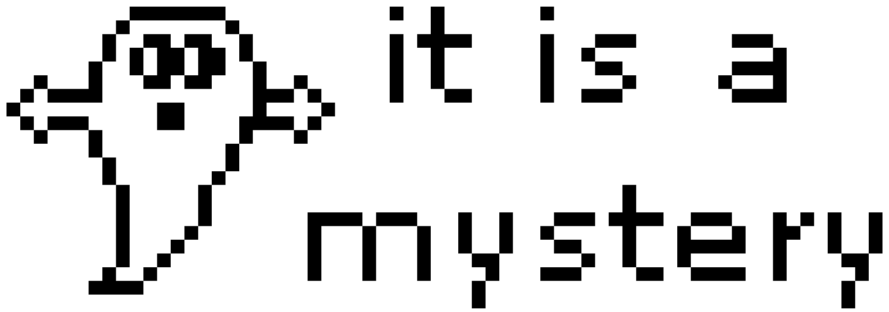
Teorema (Mazur, 1978)

E_{tor} *é um dos seguintes 15 grupos:*

- $\mathbb{Z}/N\mathbb{Z}$, *para* $1 \leqslant N \leqslant 10$ *ou* $N = 12$ *(pula o 11!);*
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, *para* $1 \leqslant N \leqslant 4$.

E o posto algébrico?

Pode ser qualquer inteiro não-negativo? Pode ser arbitrariamente grande? O conjunto dos possíveis postos algébricos é limitado? Pra cada possibilidade existem infinitas curvas elípticas com tal posto algébrico? Existe algum jeito fácil de calculá-lo?



Quão alto pode ser o posto algébrico?

O maior posto conhecido atualmente é $\geqslant 28$ (Elkies, 2006):

$$y^2 = x^3 - \frac{3}{4}x^2 - \frac{1}{2}\ 4013552483115105317006641641867708 5$$
$$5018604606243579130 03\ x + \frac{1}{4}\ 13792644718012222586813194 2$$
$$7615628814994237774372767214450640331851677577949289737 17$$

(e nem se sabe se é exatamente 28!)

A estratégia para achar curvas com posto algébrico alto é construir, usando heurísticas, curvas elípticas que potencialmente tenham muitos pontos de ordem infinita independentes.

Pergunta: como saber se um ponto é de ordem infinita?

Teorema (Nagell-Lutz (fraco), 1935)

Se $(x, y) \in E$ é de torção, então $x, y \in \mathbb{Z}$.

O que conjecturamos sobre o posto algébrico?

Quanto mais alto o posto algébrico, menos curvas elípticas existem. A existência de muitos pontos independentes de ordem infinita é uma condição *muito restritiva*.

Conjectura ("folclórica")

50% das curvas elípticas sobre $\mathbb{Q}$ *têm* $r_{\mathrm{alg}}(E) = 0$, *50% têm* $r_{\mathrm{alg}}(E) = 1$ *e 0% têm* $r_{\mathrm{alg}}(E) \geqslant 2$.

Tradicionalmente, acredita-se que o posto algébrico poderia ser arbitrariamente alto. Porém, heurísticas recentes (B. Poonen *et. al.*, 2018) sugerem que apenas **finitas** curvas elípticas têm posto algébrico $\geqslant 21$ (!)

Voltando ao problema de contar pontos, $r_{\mathrm{alg}}(E) > 0$ é equivalente a E ter infinitos pontos. Se a conjectura "folclórica" for verdadeira, o caso $g = 1$ é o meio-termo entre os casos $g < 1$ (infinitos) e $g > 1$ (finitos)!

Contando soluções módulo p

É sempre possível fazer uma mudança de coordenadas tal que os coeficientes de uma curva elíptica E sejam inteiros. Logo, podemos olhar para as soluções da equação de E *módulo um primo* p.

Em $\mathbb{Z}/p\mathbb{Z}$, metade dos elementos não-nulos são quadrados. Logo, esperamos encontrar p soluções para a equação de E módulo p. Mas isto não é o que acontece em geral.

Exemplo. A curva elíptica $E\colon y^2 = x^3 - 27x - 54$ tem apenas 5 soluções módulo 11, a saber $(\overline{0}, \pm\overline{1})$, $(\overline{4}, \pm\overline{1})$ e $(\overline{6}, \overline{0})$.

Para cada p primo, denotamos a diferença entre o número esperado e o número real de soluções da equação de E módulo p por

$$a_p(E) \doteq p - \#\{\text{soluções de } E \text{ módulo } p\}$$

L-função de um curva elíptica

Estendemos o coeficiente a_p para todo n fazendo:

$$a_{p^e}(E) \doteq p^e - \#\{\text{soluções de } E \text{ módulo } p^e\} \qquad a_1(E) \doteq 1$$

$$a_{mn}(E) \doteq a_m(E)a_n(E), \text{ com } \operatorname{mdc}(m,n) = 1$$

Definimos a L-**função** de E por

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s}, \qquad \operatorname{Re}(s) > 2$$

Um importante resultado (Teorema da Modularidade) afirma que $L_E(s)$ possui uma extensão analítica para todo o plano complexo. Em particular, $L_E(s)$ está defina em $s = 1$ (mas **não** é dada pela série neste ponto!).

A ordem de $L_E(s)$ em $s = 1$ é o **posto analítico** de E, denotado $r_{\text{an}}(E)$. Existem algoritmos para calculá-la com a precisão que se queira!

Enfim, a Conjectura BSD

Conjectura (BSD, 1965). Para toda curva elíptica $E/\mathbb{Q}$, $r_{\mathrm{an}}(E) = r_{\mathrm{alg}}(E)$.

Em particular, E tem infinitos pontos se, e somente se, $L_E(1) = 0$.

O mais próximo que chegamos desta conjectura até hoje é:

Teorema (Kolyvagin-Rubin, 1989-1991)

Se $r_{\mathrm{an}}(E) \leqslant 1$, então E satisfaz BSD.

Conj. folclórica + Kolyvagin-Rubin = BSD para 100% das curvas elípticas!

Aplicações da Conjectura BSD

Solução de outros problemas em aberto:

Alguns problemas em aberto dependem de saber calcular posto algébrico de curvas elípticas. Se temos BSD, temos um jeito fácil de calculá-lo e os problemas estão resolvidos!

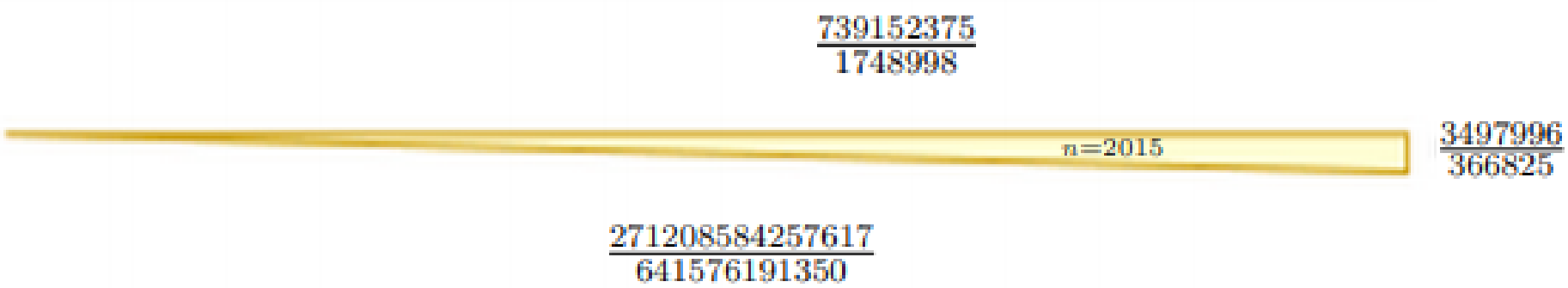
Exemplo: Problema do Número Congruente

Problema do Número Congruente

Um inteiro n é **congruente** se existe um triângulo retângulo com lados racionais e área n.

Pergunta. Quais são os números congruentes?

Existe um teorema (Tunnell, 1983) que nos permite dizer quando um número não é congruente, mas é difícil saber quando um número *é* congruente:



Fun fact: 2019 não é congruente!

Problema do Número Congruente

E o que isso tem a ver com curvas elípticas?

Considere a curva elíptica $E_n : y^2 = x^3 - n^2 x$. Pontos desta curva nos dão triângulos retângulos que atestam a congruência de n:

$$(x, y) \in E_n,\ x, y > 0, \implies \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y} \right) \text{ retângulo de área } n$$

E triângulos que atestam a congruência de n nos dão pontos de E_n:

$$(a, b, c) \text{ retângulo de área } n \implies \left(\frac{nb}{c - a}, \frac{2n^2}{c - a} \right) \in E_n$$

Note que o ponto acima tem coordenadas não-inteiras. Pelo teorema de Nagell-Lutz, este ponto é de ordem infinita. Logo,

$$n \text{ é congruente se, e somente se, } r_{\text{alg}}(E_n) > 0.$$

Aplicações da Conjectura BSD

Desvendar a estrutura das curvas elípticas:

Como já foi dito, BSD nos dá um jeito simples de capturar a propriedade mais evasiva das curvas elípticas, o posto algébrico. Para entender a importância disso, precisamos saber qual é o estado da arte:

- Não há algoritmo que calcule o posto algébrico para qualquer curva elíptica (há um algoritmo, mas não sabe se ele sempre termina);
- Achar os pontos de torção é relativamente fácil (Nagell-Lutz), mas, pontos de ordem infinita, nem sempre: A curva elíptica $y^2 = x^3 + 877x$, de posto 1, parece simples, mas o gerador mais "simples" encontrado para ela é um ponto com abscissa

$$\frac{3754945281271621931055040699420927923462 01}{6215987776871505425463220780697238044100}$$

Conhecendo o posto algébrico, podemos não só calcular quantos pontos existem na curva, mas *achá-los todos!* (com algoritmos que terminam!)

... e daí?

Por que entender curvas elípticas?

- Curvas elípticas são legais! (motivo necessário e suficiente);
- Curvas elípticas aparecem onde menos se espera (vide o *Último Teorema de Fermat*, cuja prova se baseia em construir, a partir de uma hipotética solução da equação de Fermat, uma curva elíptica que contradiria o Teorema da Modularidade);
- Curvas elípticas são úteis em criptografia: chaves de mesmo nível de segurança em ECC precisam de 10x menos bits que em RSA. Buscam-se curvas elípticas E em que o problema do logaritmo discreto é difícil de resolver (se P e Q são pontos que satisfazem a equação de E módulo p primo são tais que $P = kQ$, determine k), como as curvas elípticas com posto alto;
- Novamente, curvas elípticas são legais!

Referências

- F. Diamond, J. Shurman, *A First Course in Modular Forms*, Springer, 2005.
- A. Dujella, *History of elliptic curves rank records*, `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`
- J. Park, B. Poonen, J. Voight, M. Wood, *A heuristic for boundeness of ranks of elliptic curves*, arXiv:1602.01431, 2018.
- J. Silverman, *The Arithmetic of Elliptic Curves (GTM 106)*, Springer, 1986.
- J. Silverman, T. Tate, *Rational Points on Elliptic Curves*, Springer, 1992.
- J. Star, *Elliptic Curves and The Congruent Number Problem*, `https://scholarship.claremont.edu/cmc_theses/1120/`
- W. Stein, *The Birch and Swinnerton-Dyer Conjecture, a computational approach*, `https://williamstein.org/books/bsd/bsd.pdf`, 2016.
- J. Tunnell, *A Classical Diophantine Problem and Modular Forms of Weight 3/2*, Inv. Math. **72** (2): 323–334, 1983.
- L. Washington, *Elliptic Curves, Number Theory and Cryptography*, CRC Press, 2008.