Introdução à conjetura de Birch e Swinnerton-Dyer

Fabio Ferrari Ruffino

DM – UFSCar

XI Bienal de Matemática – UFSCar

1 de agosto de 2024

Equações diofantinas

- Uma *equação diofantina* é uma equação polinomial com coeficientes inteiros, cujas soluções têm que ser inteiras.

Equações diofantinas

- Uma *equação diofantina* é uma equação polinomial com coeficientes inteiros, cujas soluções têm que ser inteiras.
- Exemplos:

Equações diofantinas

- Uma *equação diofantina* é uma equação polinomial com coeficientes inteiros, cujas soluções têm que ser inteiras.
- Exemplos:
  - $x^5 - 6x^3 + x^2 + 4 = 0$; neste caso, 1 é uma solução;

Equações diofantinas

- Uma *equação diofantina* é uma equação polinomial com coeficientes inteiros, cujas soluções têm que ser inteiras.
- Exemplos:
  - $x^5 - 6x^3 + x^2 + 4 = 0$; neste caso, 1 é uma solução;
  - $x^3yz^2 - 7xy + 2z^2 - 2 = 0$; neste caso, $(0, 0, 1)$ é uma solução;

Equações diofantinas

- Uma *equação diofantina* é uma equação polinomial com coeficientes inteiros, cujas soluções têm que ser inteiras.
- Exemplos:
  - $x^5 - 6x^3 + x^2 + 4 = 0$; neste caso, 1 é uma solução;
  - $x^3yz^2 - 7xy + 2z^2 - 2 = 0$; neste caso, $(0, 0, 1)$ é uma solução;
  - ...

Equações diofantinas

- Uma *equação diofantina* é uma equação polinomial com coeficientes inteiros, cujas soluções têm que ser inteiras.
- Exemplos:
  - $x^5 - 6x^3 + x^2 + 4 = 0$; neste caso, 1 é uma solução;
  - $x^3yz^2 - 7xy + 2z^2 - 2 = 0$; neste caso, $(0, 0, 1)$ é uma solução;
  - ...
- Podemos também procurar por soluções *racionais*, de que as inteiras constituem um caso particular.

Equações diofantinas de *uma* variável

- A princípio, podemos resolver qualquer equação diofantina de uma variável.

Equações diofantinas de *uma* variável

- A princípio, podemos resolver qualquer equação diofantina de uma variável.
- Equação: $a_n x^n + \cdots + a_1 x + a_0 = 0$, sendo $a_0, \ldots, a_n \in \mathbb{Z}$.

Equações diofantinas de *uma* variável

- A princípio, podemos resolver qualquer equação diofantina de uma variável.
- Equação: $a_n x^n + \cdots + a_1 x + a_0 = 0$, sendo $a_0, \ldots, a_n \in \mathbb{Z}$.
- *Lema de Gauss:* Se $\frac{p}{q}$ for uma solução não nula e $(p, q) = 1$, então $q \mid a_n$ e $p \mid a_0$.

Equações diofantinas de *uma* variável

- A princípio, podemos resolver qualquer equação diofantina de uma variável.
- Equação: $a_n x^n + \cdots + a_1 x + a_0 = 0$, sendo $a_0, \ldots, a_n \in \mathbb{Z}$.
- *Lema de Gauss:* Se $\frac{p}{q}$ for uma solução não nula e $(p, q) = 1$, então $q \mid a_n$ e $p \mid a_0$.
- Portanto, só temos uma família *finita* de possibilidades a serem analisadas.

Equações diofantinas de *duas* variáveis

- Com duas variáveis, a situação é bem mais complicada.

Equações diofantinas de *duas* variáveis

- Com duas variáveis, a situação é bem mais complicada.
- Caso simples: equação de *primeiro* grau (dita *linear*).

Equações diofantinas de *duas* variáveis

- Com duas variáveis, a situação é bem mais complicada.
- Caso simples: equação de *primeiro* grau (dita *linear*).
- Equação: $ax + by + c = 0$, sendo $a, b, c \in \mathbb{Z}$ e $ab \neq 0$.

Equações diofantinas de *duas* variáveis

- Com duas variáveis, a situação é bem mais complicada.
- Caso simples: equação de *primeiro* grau (dita *linear*).
- Equação: $ax + by + c = 0$, sendo $a, b, c \in \mathbb{Z}$ e $ab \neq 0$.
- Soluções racionais: $\left(t, -\frac{at+c}{b}\right)$, sendo $t \in \mathbb{Q}$ qualquer.

Equações diofantinas de *duas* variáveis

- Com duas variáveis, a situação é bem mais complicada.
- Caso simples: equação de *primeiro* grau (dita *linear*).
- Equação: $ax + by + c = 0$, sendo $a, b, c \in \mathbb{Z}$ e $ab \neq 0$.
- Soluções racionais: $\left(t, -\frac{at+c}{b}\right)$, sendo $t \in \mathbb{Q}$ qualquer.
- Existem soluções inteiras se, e somente se, $d := (a, b) \mid c$.

Equações diofantinas de *duas* variáveis

- Com duas variáveis, a situação é bem mais complicada.
- Caso simples: equação de *primeiro* grau (dita *linear*).
- Equação: $ax + by + c = 0$, sendo $a, b, c \in \mathbb{Z}$ e $ab \neq 0$.
- Soluções racionais: $\left(t, -\frac{at+c}{b}\right)$, sendo $t \in \mathbb{Q}$ qualquer.
- Existem soluções inteiras se, e somente se, $d := (a, b) \mid c$.

  Neste caso, fixando $n, m \in \mathbb{Z}$, tais que $an+bm = d$, as soluções inteiras são da forma $\left(-\frac{cn+bt}{d}, \frac{-cm+at}{d}\right)$, sendo $t \in \mathbb{Z}$ qualquer.

Cônicas *vs* retas

- Caso sucessivo: equação de *segundo* grau.

Cônicas *vs* retas

- Caso sucessivo: equação de *segundo* grau.
- Equação: $ax^2 + bxy + cy^2 + dx + ey + f = 0$ de duas variáveis, sendo $a, \ldots, f \in \mathbb{Z}$ e $(a, b, c) \neq (0, 0, 0)$.

Cônicas *vs* retas

- Caso sucessivo: equação de *segundo* grau.
- Equação: $ax^2 + bxy + cy^2 + dx + ey + f = 0$ de duas variáveis, sendo $a, \ldots, f \in \mathbb{Z}$ e $(a, b, c) \neq (0, 0, 0)$.
- Temos que encontrar os pontos inteiros e racionais de uma cônica real com coeficientes inteiros.

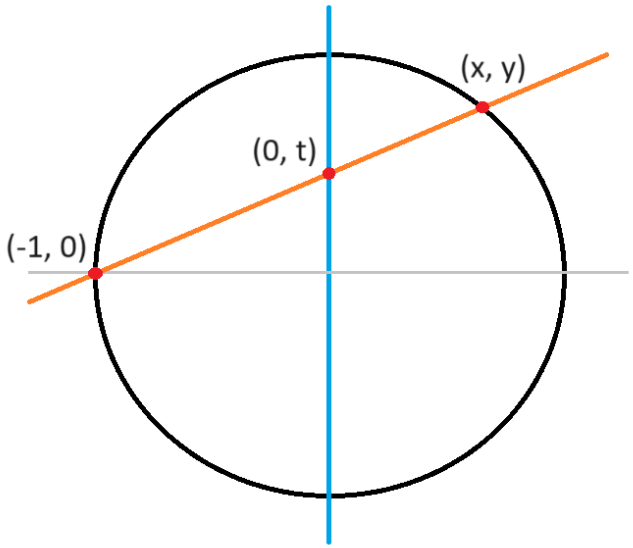
Cônicas *vs* retas

- Caso sucessivo: equação de *segundo* grau.
- Equação: $ax^2 + bxy + cy^2 + dx + ey + f = 0$ de duas variáveis, sendo $a, \ldots, f \in \mathbb{Z}$ e $(a, b, c) \neq (0, 0, 0)$.
- Temos que encontrar os pontos inteiros e racionais de uma cônica real com coeficientes inteiros.
- Se a cônica for redutível, voltamos essencialmente às equações de primeiro grau.

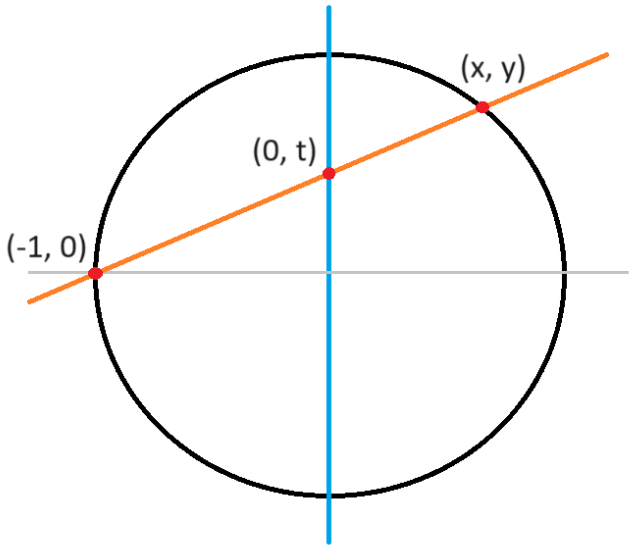
Cônicas *vs* retas

- Caso sucessivo: equação de *segundo* grau.
- Equação: $ax^2 + bxy + cy^2 + dx + ey + f = 0$ de duas variáveis, sendo $a, \ldots, f \in \mathbb{Z}$ e $(a, b, c) \neq (0, 0, 0)$.
- Temos que encontrar os pontos inteiros e racionais de uma cônica real com coeficientes inteiros.
- Se a cônica for redutível, voltamos essencialmente às equações de primeiro grau.
- Ideia: podemos "projetar" uma cônica irredutível em uma reta.

Cônicas *vs* retas

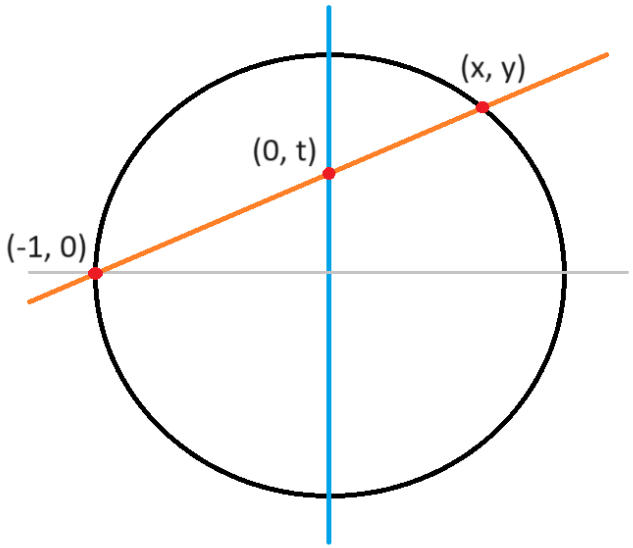


Cônicas *vs* retas



- "Projetamos" a circunferência $x^2 + y^2 - 1 = 0$ na reta $x = 0$.

Cônicas *vs* retas



- "Projetamos" a circunferência $x^2 + y^2 - 1 = 0$ na reta $x = 0$.
- $(x, y) = (\cos\theta, \sin\theta) \mapsto (0, t) = (0, \tan\frac{\theta}{2})$.

Cônicas *vs* retas

- Reciprocamente: $(0,t) \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.

Cônicas *vs* retas

- Reciprocamente: $(0,t) \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.
- O ponto $(-1,0)$ corresponde ao "ponto ao infinito" da reta.

Cônicas *vs* retas

- Reciprocamente: $(0,t) \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.
- O ponto $(-1,0)$ corresponde ao "ponto ao infinito" da reta.
- Trata-se de uma *equivalência biracional*, que respeita os pontos racionais.

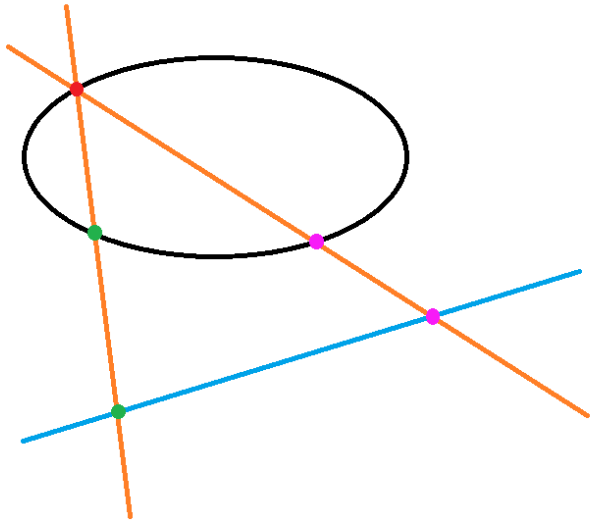
Cônicas *vs* retas

- Reciprocamente: $(0,t) \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.
- O ponto $(-1,0)$ corresponde ao "ponto ao infinito" da reta.
- Trata-se de uma *equivalência biracional*, que respeita os pontos racionais.
- Portanto, escolhendo $t \in \mathbb{Q}$, obtemos todos os pontos racionais da circunferência $x^2 + y^2 - 1 = 0$.

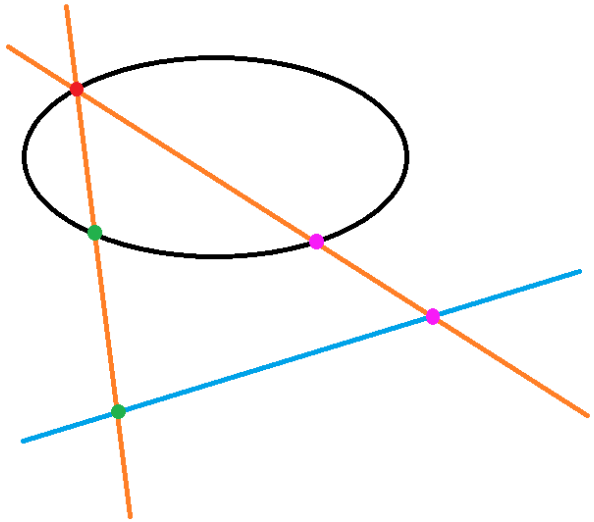
Cônicas *vs* retas

- Reciprocamente: $(0,t) \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.
- O ponto $(-1,0)$ corresponde ao "ponto ao infinito" da reta.
- Trata-se de uma *equivalência biracional*, que respeita os pontos racionais.
- Portanto, escolhendo $t \in \mathbb{Q}$, obtemos todos os pontos racionais da circunferência $x^2 + y^2 - 1 = 0$.
- O fato que os pontos racionais sejam respeitados segue do fato que $(-1,0)$ é um ponto racional.

Cônicas *vs* retas



Cônicas *vs* retas



- Em geral, fixando um ponto *racional* de uma cônica irredutível, obtemos uma equivalência biracional com uma reta, que respeita os pontos racionais.

Equações diofantinas de *duas* variáveis

- Portanto, *se houver um ponto racional*, conseguimos determiná-los todos.

Equações diofantinas de *duas* variáveis

- Portanto, *se houver um ponto racional*, conseguimos determiná-los todos.
- Pergunta: é sempre possível encontrar um ponto racional em uma cônica?

Equações diofantinas de *duas* variáveis

- Portanto, *se houver um ponto racional*, conseguimos determiná-los todos.
- Pergunta: é sempre possível encontrar um ponto racional em uma cônica?
- Resposta: não. Por exemplo, é fácil verificar que a circunferência $x^2 + y^2 - 3 = 0$ não possui pontos racionais.

Equações diofantinas de *duas* variáveis

- Portanto, *se houver um ponto racional*, conseguimos determiná-los todos.
- Pergunta: é sempre possível encontrar um ponto racional em uma cônica?
- Resposta: não. Por exemplo, é fácil verificar que a circunferência $x^2 + y^2 - 3 = 0$ não possui pontos racionais.
- Felizmente, conhecemos um método para determinar em um número finito de passos se uma cônica possui pontos racionais.

Terceiro grau

- Consideremos equações de *terceiro* grau em duas variáveis.

Terceiro grau

- Consideremos equações de *terceiro* grau em duas variáveis.
- Neste caso, *não* conhecemos uma solução geral do problema.

Terceiro grau

- Consideremos equações de *terceiro* grau em duas variáveis.
- Neste caso, *não* conhecemos uma solução geral do problema.
- Uma equação de terceiro grau representa uma *curva cúbica plana* com coeficientes inteiros.

Terceiro grau

- Consideremos equações de *terceiro* grau em duas variáveis.
- Neste caso, *não* conhecemos uma solução geral do problema.
- Uma equação de terceiro grau representa uma *curva cúbica plana* com coeficientes inteiros.
- *Não* há um método conhecido para estabelecer se uma cúbica possui pontos racionais.

Terceiro grau

- Consideremos equações de *terceiro* grau em duas variáveis.
- Neste caso, *não* conhecemos uma solução geral do problema.
- Uma equação de terceiro grau representa uma *curva cúbica plana* com coeficientes inteiros.
- *Não* há um método conhecido para estabelecer se uma cúbica possui pontos racionais.
- Trata-se de um problema aberto relevante.

Terceiro grau

- Portanto, consideramos uma curva cúbica assumindo de conhecer um ponto racional dela.

Terceiro grau

- Portanto, consideramos uma curva cúbica assumindo de conhecer um ponto racional dela.
- Neste caso, queremos encontrar todos os pontos racionais e inteiros dela.

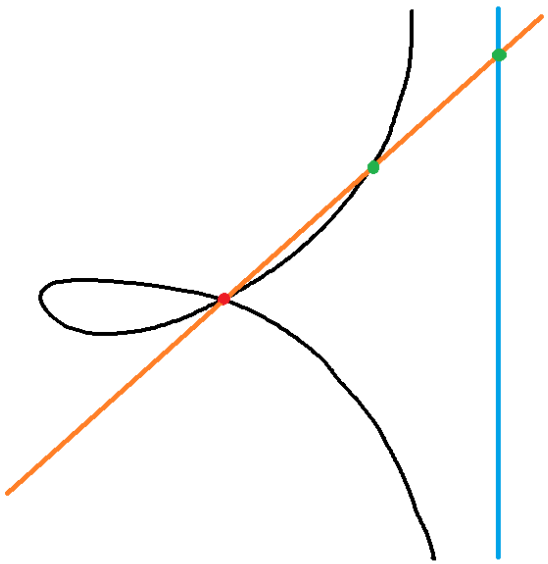
Terceiro grau

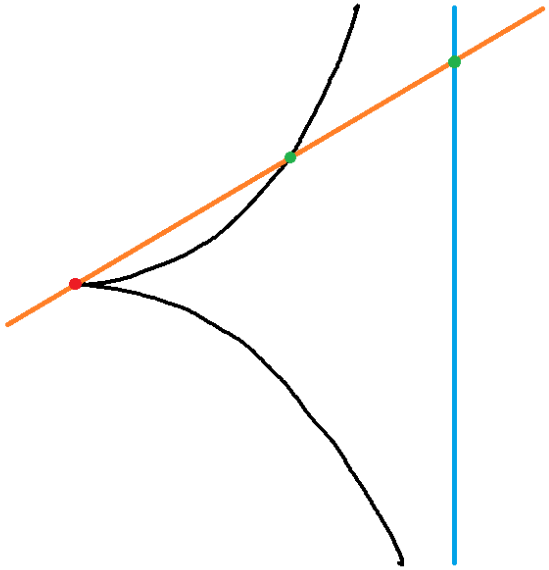
- Portanto, consideramos uma curva cúbica assumindo de conhecer um ponto racional dela.
- Neste caso, queremos encontrar todos os pontos racionais e inteiros dela.
- Uma cúbica possui no máximo *uma* singularidade (senão, haveria uma reta que intersecta a cúbica com multiplicidade 4).

Terceiro grau

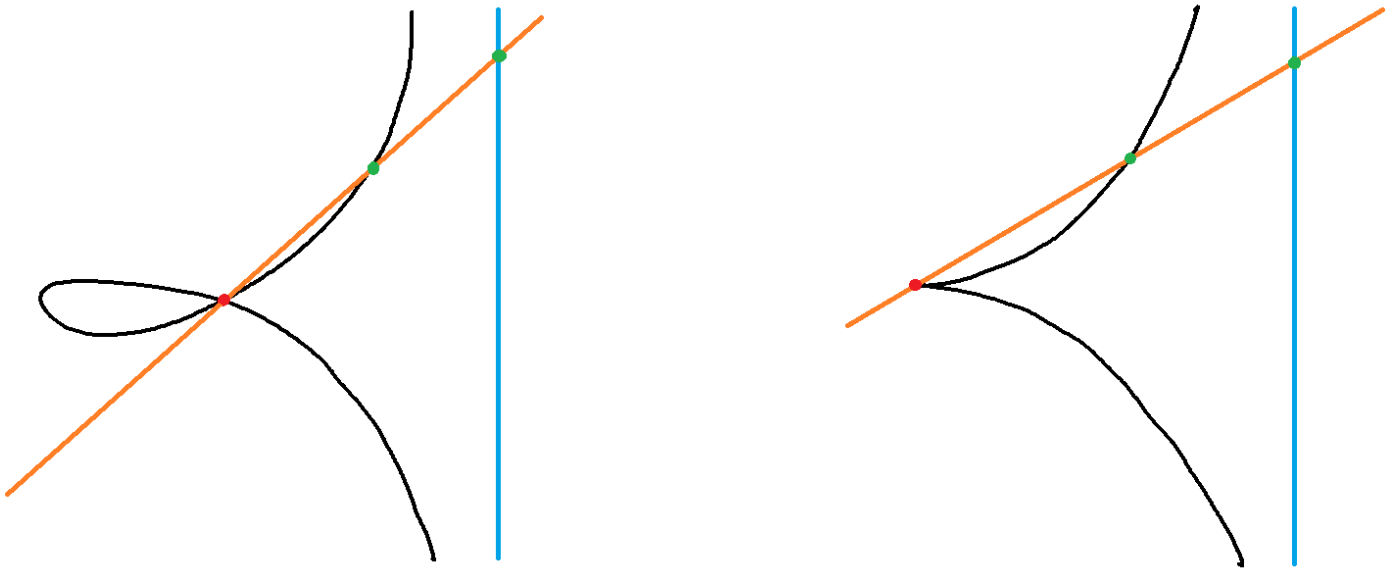
- Portanto, consideramos uma curva cúbica assumindo de conhecer um ponto racional dela.
- Neste caso, queremos encontrar todos os pontos racionais e inteiros dela.
- Uma cúbica possui no máximo *uma* singularidade (senão, haveria uma reta que intersecta a cúbica com multiplicidade 4).
- Se a cúbica for singular, podemos raciocinar como no caso das cônicas.

Cúbicas singulares



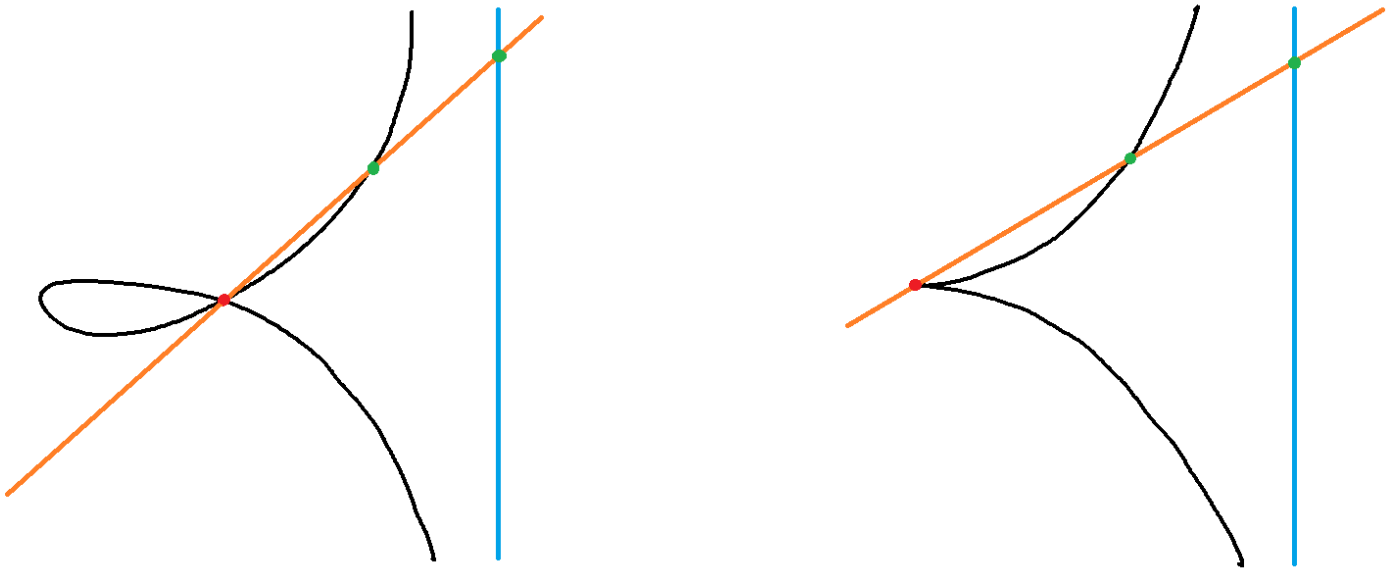


Cúbicas singulares



- Sendo os coeficientes inteiros e existindo pelo menos um ponto racional, pode-se verificar que a singularidade é necessariamente racional.

Cúbicas singulares



- Sendo os coeficientes inteiros e existindo pelo menos um ponto racional, pode-se verificar que a singularidade é necessariamente racional.
- Podemos "projetar" a cúbica singular em uma reta.

Curvas elípticas

- Portanto, o problema principal é o seguinte: dada uma cúbica *suave* com coeficientes inteiros e *um ponto racional fixado*, quais são todos os pontos racionais dela?

Curvas elípticas

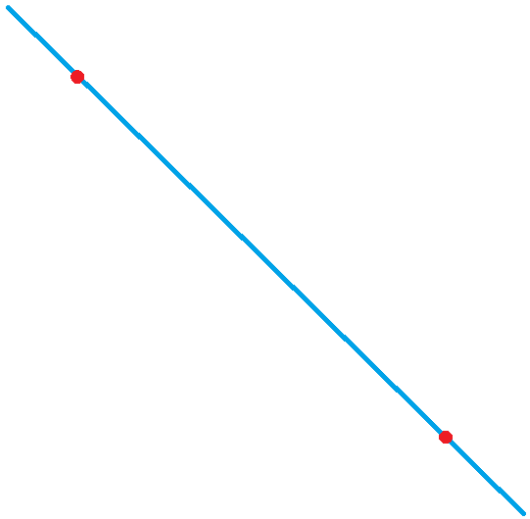
- Portanto, o problema principal é o seguinte: dada uma cúbica *suave* com coeficientes inteiros e *um ponto racional fixado*, quais são todos os pontos racionais dela?

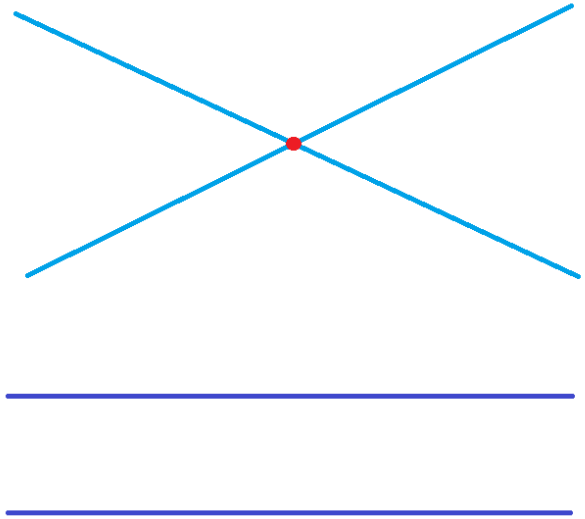
- *Definição (provisória e incompleta):* uma *curva elíptica* é uma curva plana *cúbica suave* com coeficientes inteiros e *um ponto racional fixado*.

Curvas elípticas

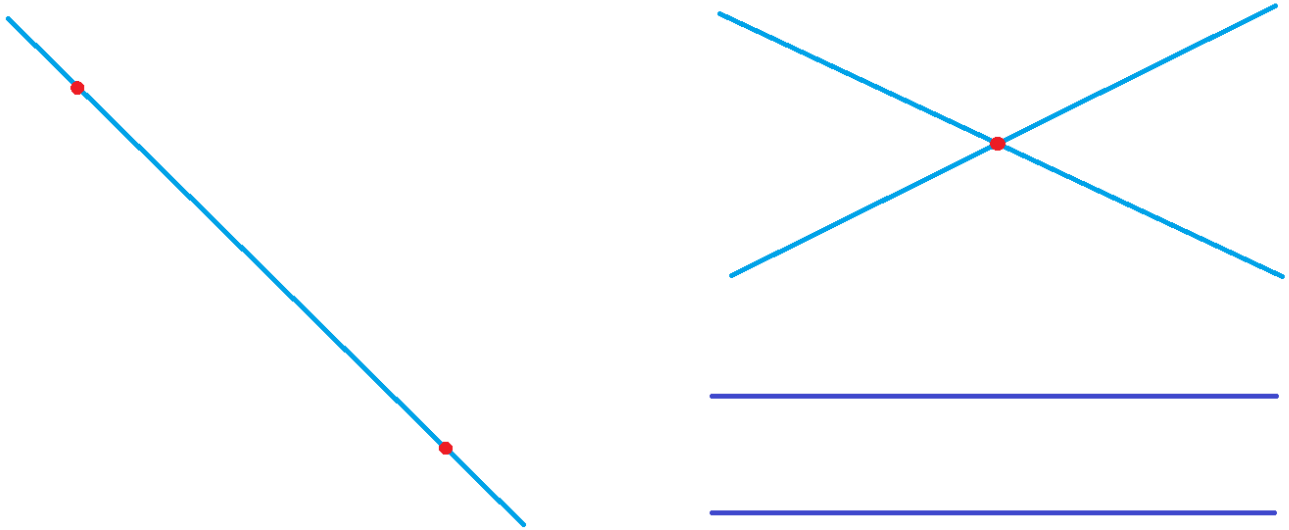
- Portanto, o problema principal é o seguinte: dada uma cúbica *suave* com coeficientes inteiros e *um ponto racional fixado*, quais são todos os pontos racionais dela?
- *Definição (provisória e incompleta):* uma *curva elíptica* é uma curva plana *cúbica suave* com coeficientes inteiros e *um ponto racional fixado*.
- Para completar esta definição (provisória), precisamos introduzir o *plano projetivo*.

Plano projetivo



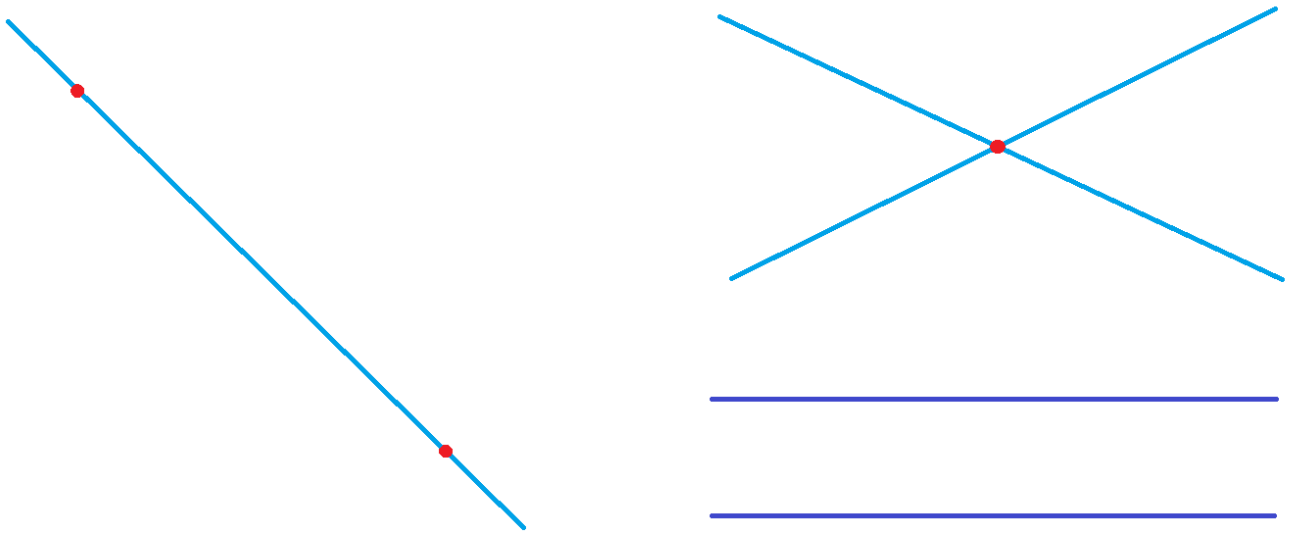


Plano projetivo



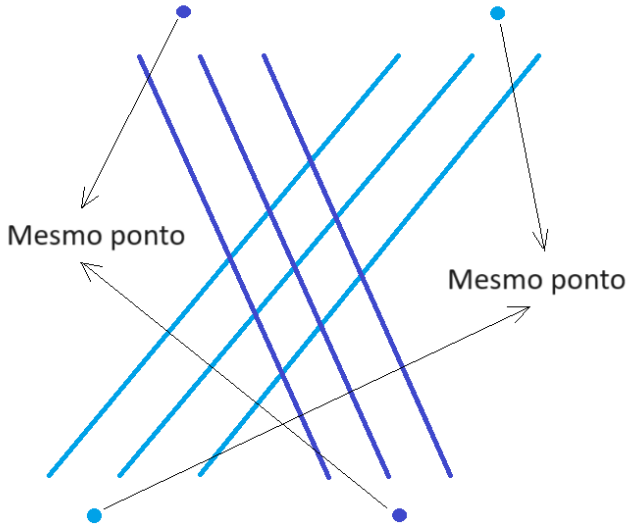
- Dois pontos distintos do plano induzem uma única reta; duas retas distintas induzem um único ponto, *exceto quando forem paralelas*.

Plano projetivo

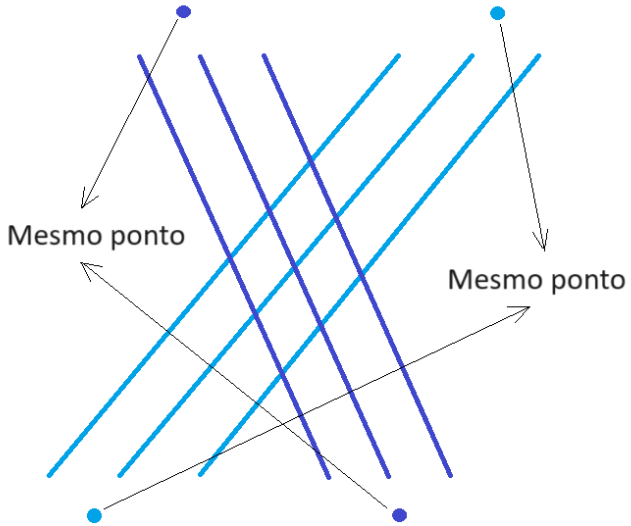


- Dois pontos distintos do plano induzem uma única reta; duas retas distintas induzem um único ponto, *exceto quando forem paralelas*.
- Para eliminar esta assimetria, acrescentamos "pontos ao infinito", que representam as possíveis direções das retas.

Plano projetivo

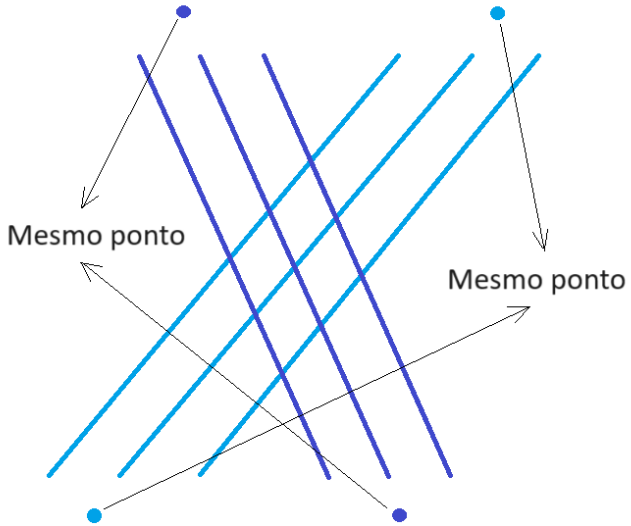


Plano projetivo



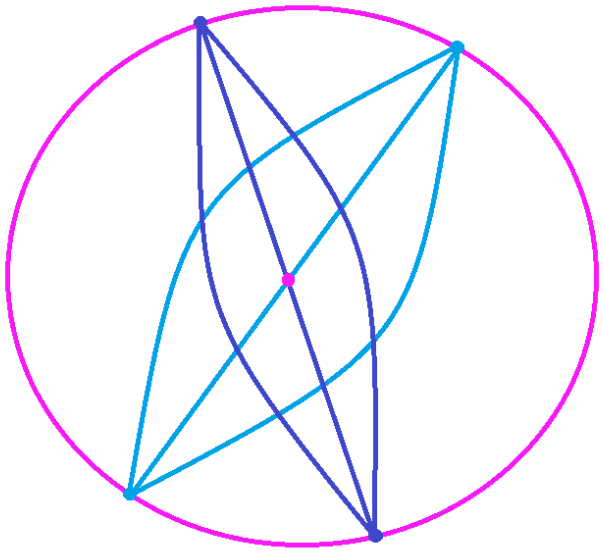
- Cada direção possível corresponde a um ponto ao infinito.

Plano projetivo

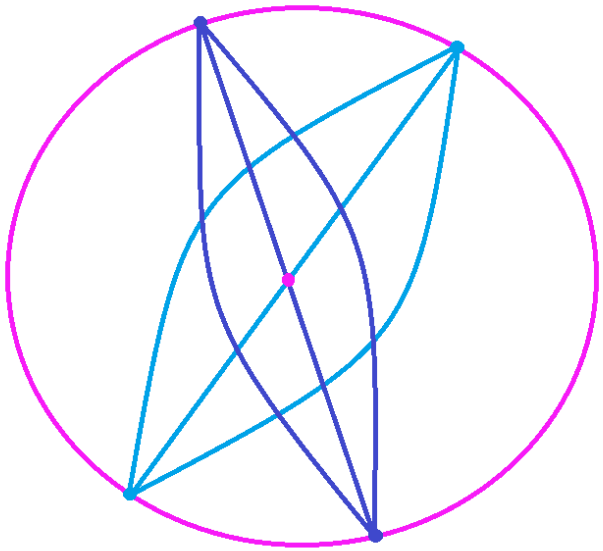


- Cada direção possível corresponde a um ponto ao infinito.
- Desta maneira, duas retas paralelas distintas se intersectam no ponto ao infinito correspondente.

Plano projetivo

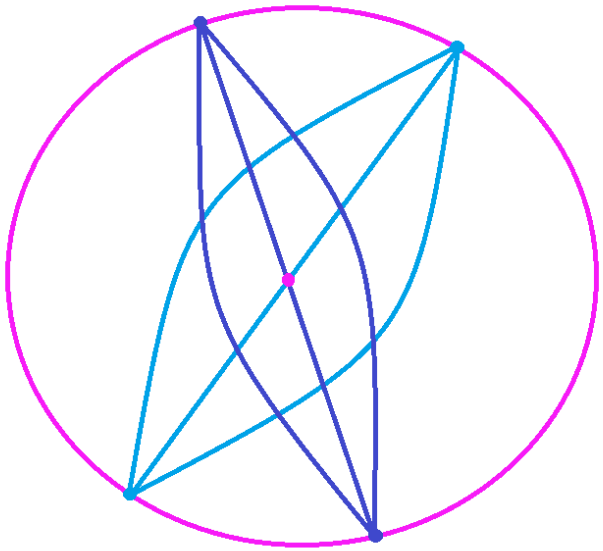


Plano projetivo



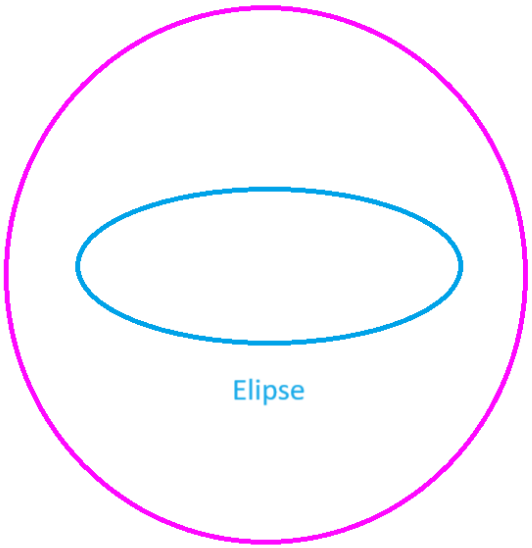
- Representamos o plano projetivo como um disco em que os pontos antipodais do bordo são identificados.

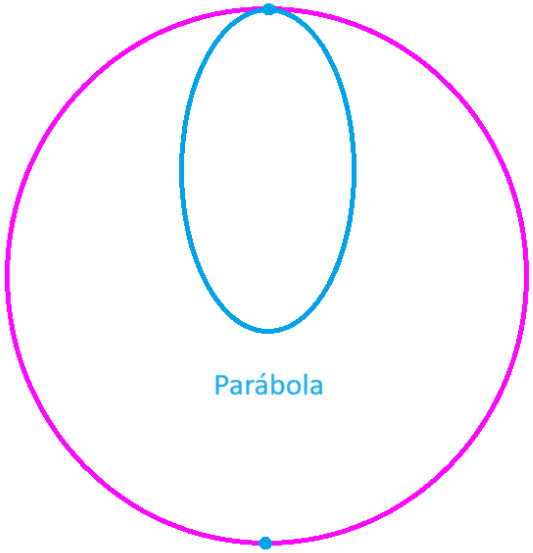
Plano projetivo

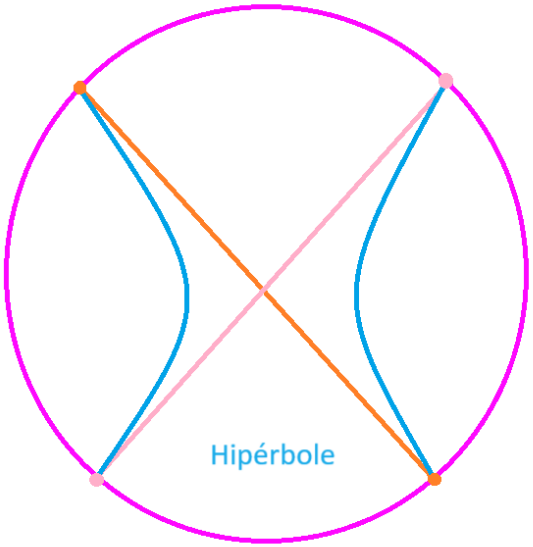


- Representamos o plano projetivo como um disco em que os pontos antipodais do bordo são identificados.
- Cada par de pontos antipodais representa uma direção.

Cônicas projetivas







Forma canônica de Weierstrass

- Em geral, uma curva algébrica no plano afim admite um *fecho projetivo*.

Forma canônica de Weierstrass

- Em geral, uma curva algébrica no plano afim admite um *fecho projetivo*.
- No caso de uma curva elíptica, podemos escolher o ponto ao infinito do eixo y como ponto racional.

Forma canônica de Weierstrass

- Em geral, uma curva algébrica no plano afim admite um *fecho projetivo*.
- No caso de uma curva elíptica, podemos escolher o ponto ao infinito do eixo y como ponto racional.
- Obtemos a seguinte *forma canônica de Weierstrass*:

$$y^2 = x^3 + ax + b.$$

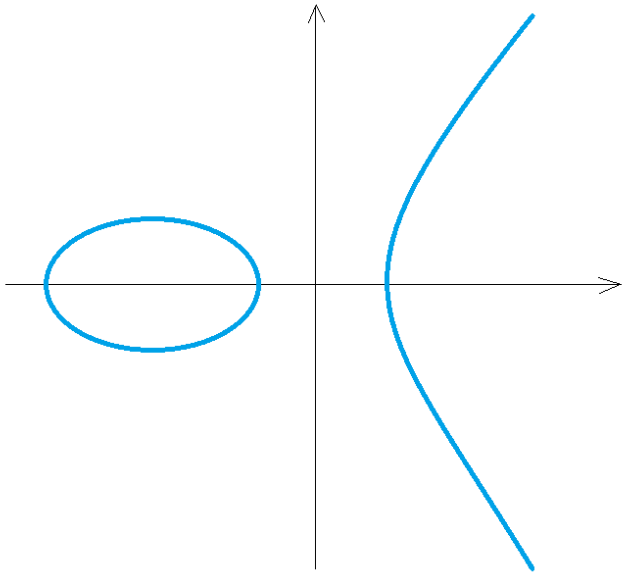
Forma canônica de Weierstrass

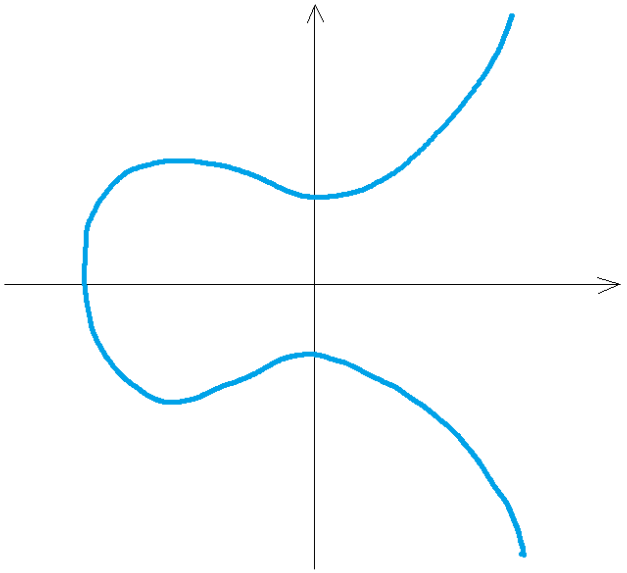
- Em geral, uma curva algébrica no plano afim admite um *fecho projetivo*.
- No caso de uma curva elíptica, podemos escolher o ponto ao infinito do eixo y como ponto racional.
- Obtemos a seguinte *forma canônica de Weierstrass*:

$$y^2 = x^3 + ax + b.$$

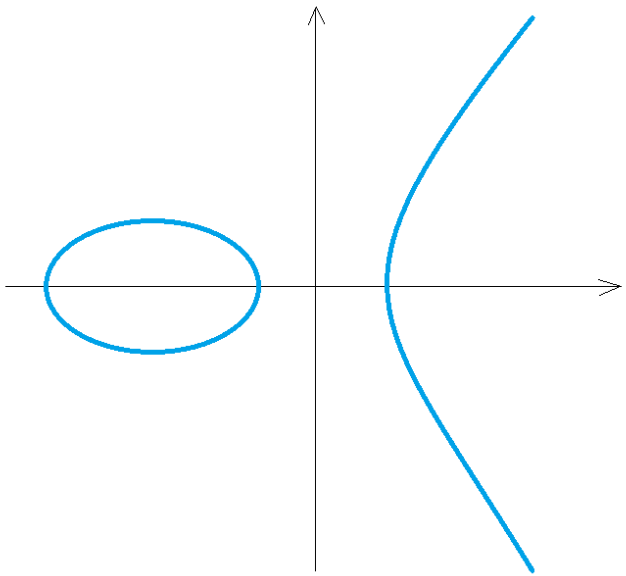
- Dependendo das raízes reais de $f(x) = x^3 + ax + b$ (uma ou três), temos duas formas possíveis.

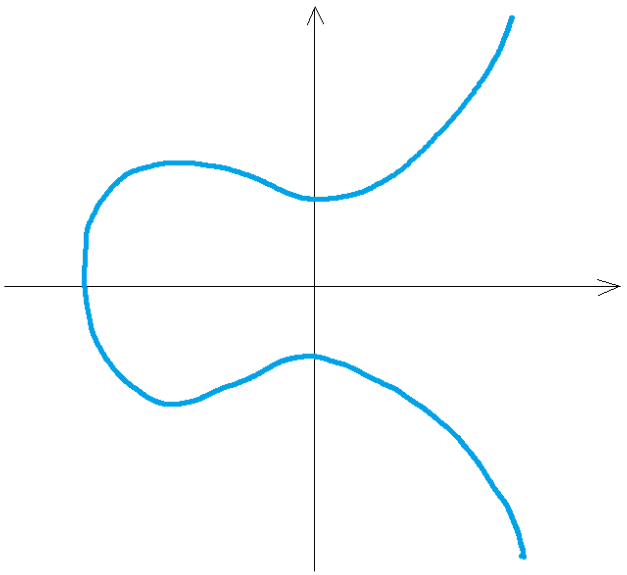
Forma canônica de Weierstrass





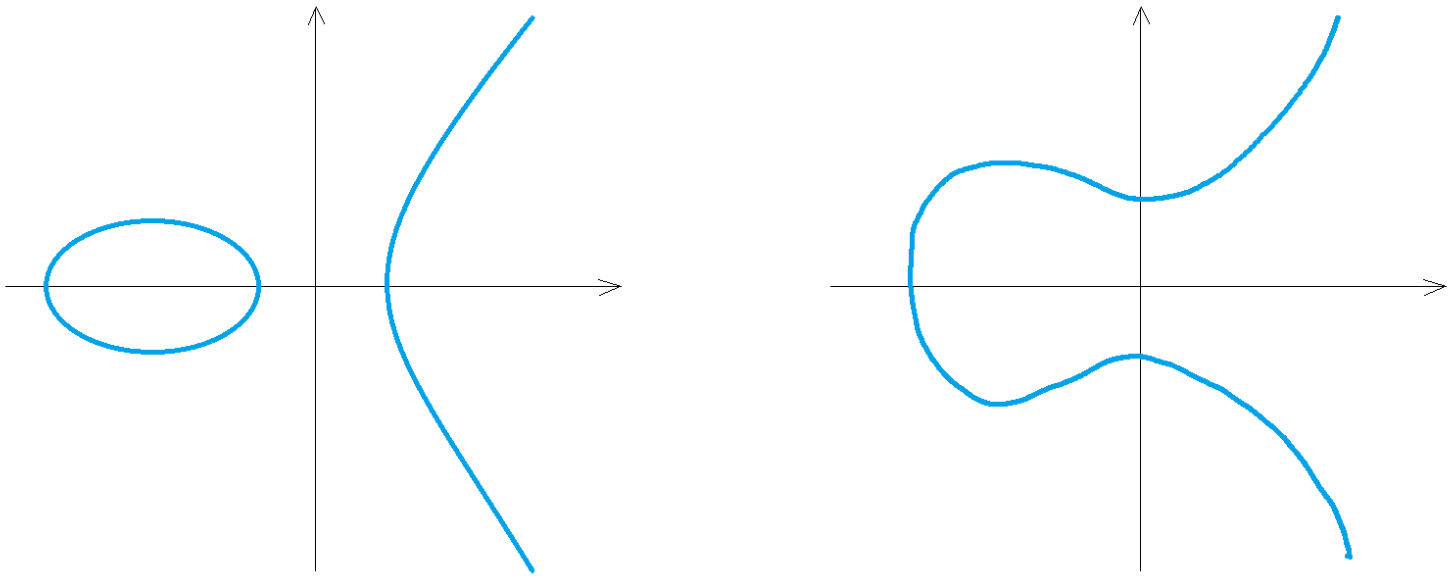
Forma canônica de Weierstrass





- *Definição (provisória):* uma *curva elíptica* é uma curva *projetiva* plana *cúbica suave* com coeficientes inteiros e *um ponto racional fixado*.

Forma canônica de Weierstrass



- *Definição (provisória):* uma *curva elíptica* é uma curva *projetiva* plana *cúbica suave* com coeficientes inteiros e *um ponto racional fixado*.
- Do ponto de vista complexo, sendo suave, o fato de ser cúbica equivale ao fato de ter *gênero* 1 (ou seja, trata-se de um toro).

Equivalência biracional

- Duas curvas são *biracionalmente equivalentes* quando existe uma bijeção entre as duas, formada por quocientes de polinômios, excluindo no máximo um subconjunto finito.

Equivalência biracional

- Duas curvas são *biracionalmente equivalentes* quando existe uma bijeção entre as duas, formada por quocientes de polinômios, excluindo no máximo um subconjunto finito.

- Exemplo: a parametrização $(0, t) \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ é uma equivalência biracional entre a circunferência $x^2 + y^2 - 1 = 0$ e a reta $x = 0$.

Equivalência biracional

- Duas curvas são *biracionalmente equivalentes* quando existe uma bijeção entre as duas, formada por quocientes de polinômios, excluindo no máximo um subconjunto finito.

- Exemplo: a parametrização $(0, t) \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ é uma equivalência biracional entre a circunferência $x^2 + y^2 - 1 = 0$ e a reta $x = 0$.

- *Definição:* uma *curva elíptica* é uma curva *projetiva* biracionalmente equivalente a uma *cúbica* plana *suave* com coeficientes inteiros e *um ponto racional fixado*, de modo que a equivalência racional respeite os pontos racionais.

Equivalência biracional

- Desta maneira, uma quártica da forma

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e$$

com coeficientes inteiros, tal que o polinômio $f(x) = ax^4 + bx^3 + cx^2 + dx + e$ não tem raízes múltiplas, é uma curva elíptica.

Equivalência biracional

- Desta maneira, uma quártica da forma

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e$$

com coeficientes inteiros, tal que o polinômio $f(x) = ax^4 + bx^3 + cx^2 + dx + e$ não tem raízes múltiplas, é uma curva elíptica.

- Exemplo: a quártica $\bar{y}^4 = 1 - \bar{x}^4$ é biracionalmente equivalente à cúbica suave $y^2 = x^3 - \frac{3}{8}x^2 + \frac{1}{16}x - \frac{1}{256}$, através da equivalência $x = -\frac{1}{4}\frac{1}{\bar{x}-1}$ e $y = \frac{1}{16}\frac{\bar{y}}{(\bar{x}-1)^2}$.

Equivalência biracional

- Desta maneira, uma quártica da forma

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e$$

com coeficientes inteiros, tal que o polinômio $f(x) = ax^4 + bx^3 + cx^2 + dx + e$ não tem raízes múltiplas, é uma curva elíptica.

- Exemplo: a quártica $\bar{y}^4 = 1 - \bar{x}^4$ é biracionalmente equivalente à cúbica suave $y^2 = x^3 - \frac{3}{8}x^2 + \frac{1}{16}x - \frac{1}{256}$, através da equivalência $x = -\frac{1}{4}\frac{1}{\bar{x}-1}$ e $y = \frac{1}{16}\frac{\bar{y}}{(\bar{x}-1)^2}$.

- Pergunta: Por que as curvas elípticas têm este nome?

Integrais elípticas

- Resposta: As curva elípticas estão estritamente relacionadas com as *integrais elípticas*.

Integrais elípticas

- Resposta: As curva elípticas estão estritamente relacionadas com as *integrais elípticas*.
- O primeiro exemplo de integral elíptica é a integral que define o perímetro de uma elipse.

Integrais elípticas

- Resposta: As curva elípticas estão estritamente relacionadas com as *integrais elípticas*.
- O primeiro exemplo de integral elíptica é a integral que define o perímetro de uma elipse.
- Dada uma elipse $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, a integral que define o perímetro é:

$$4 \int_0^1 \sqrt{\frac{1 - k^2 x^2}{1 - x^2}}\, dx, \qquad k := \sqrt{\frac{a^2 - b^2}{a^2}} \neq 1.$$

Integrais elípticas

- Resposta: As curva elípticas estão estritamente relacionadas com as *integrais elípticas*.
- O primeiro exemplo de integral elíptica é a integral que define o perímetro de uma elipse.
- Dada uma elipse $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, a integral que define o perímetro é:

$$4\int_0^1 \sqrt{\frac{1-k^2x^2}{1-x^2}}\,dx, \qquad k := \sqrt{\frac{a^2-b^2}{a^2}} \neq 1.$$

- Consideremos a função a ser integrada $y = \sqrt{\frac{1-k^2x^2}{1-x^2}}$.

Integrais elípticas

- Trata-se de uma parte da curva $y^2(1-x^2) = (1-k^2x^2)$.

Integrais elípticas

- Trata-se de uma parte da curva $y^2(1-x^2) = (1-k^2x^2)$.
- Vamos considerar a equivalência biracional:

$$\bar{x} := x \qquad \bar{y} := y(1-x^2).$$

Integrais elípticas

- Trata-se de uma parte da curva $y^2(1-x^2) = (1-k^2x^2)$.
- Vamos considerar a equivalência biracional:

$$\bar{x} := x \qquad \bar{y} := y(1-x^2).$$

- Obtemos $\bar{y}^2 = (1-k^2\bar{x}^2)(1-\bar{x}^2)$.

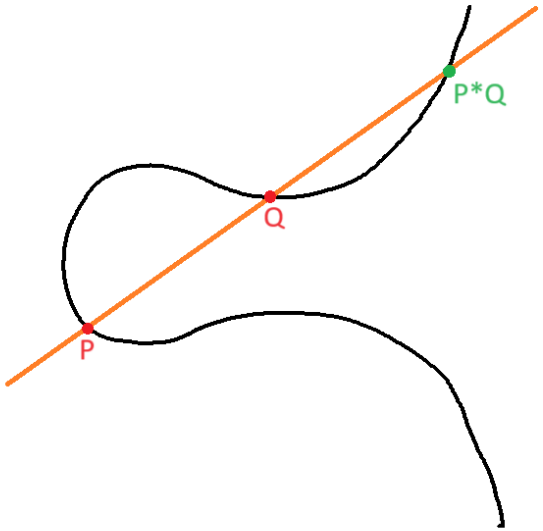
Integrais elípticas

- Trata-se de uma parte da curva $y^2(1-x^2) = (1-k^2x^2)$.
- Vamos considerar a equivalência biracional:

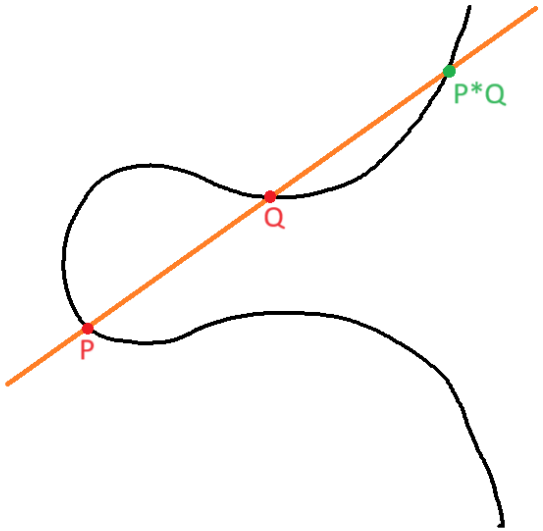
$$\bar{x} := x \qquad \bar{y} := y(1-x^2).$$

- Obtemos $\bar{y}^2 = (1-k^2\bar{x}^2)(1-\bar{x}^2)$.
- O polinômio $f(\bar{x}) = (1-k^2\bar{x}^2)(1-\bar{x}^2)$ não possui raízes múltiplas e, portanto, trata-se de uma curva elíptica.

Estrutura de grupo

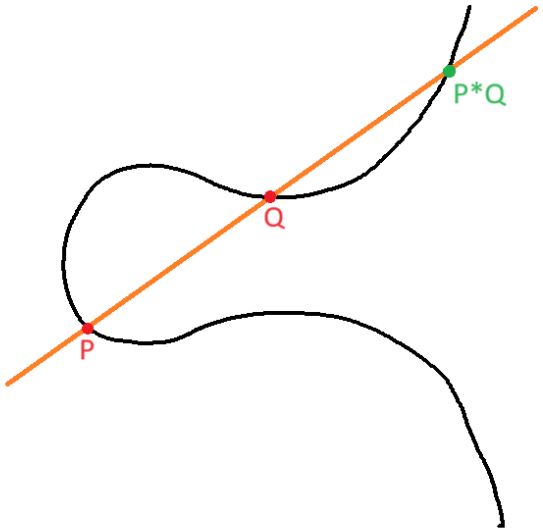


Estrutura de grupo



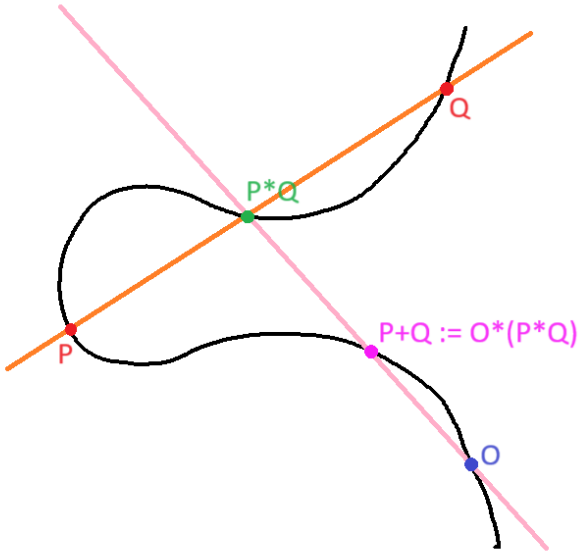
- Precisamos de *dois* pontos para encontrar um terceiro. Portanto, não podemos projetar a curva em uma reta.

Estrutura de grupo

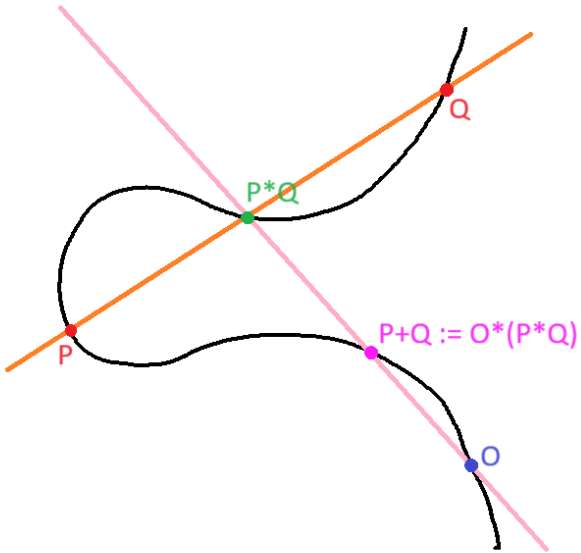


- Precisamos de *dois* pontos para encontrar um terceiro. Portanto, não podemos projetar a curva em uma reta.
- Porém, podemos utilizar esta operação para dotar a curva de uma estrutura algébrica adequada.

Estrutura de grupo

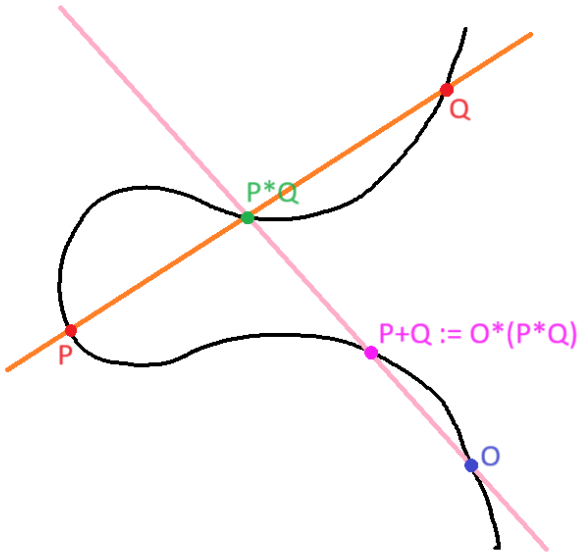


Estrutura de grupo



- Fixamos uma origem O na curva.

Estrutura de grupo



- Fixamos uma origem O na curva.
- Definimos $P + Q := O * (P * Q)$.

Estrutura de grupo

- Obtemos uma estrutura de *grupo abeliano*.

Estrutura de grupo

- Obtemos uma estrutura de *grupo abeliano*.
- Pode-se verificar que a operação '$+$' é associativa.

Estrutura de grupo

- Obtemos uma estrutura de *grupo abeliano*.
- Pode-se verificar que a operação '$+$' é associativa.
- É trivialmente comutativa, pois $P * Q = Q * P$.

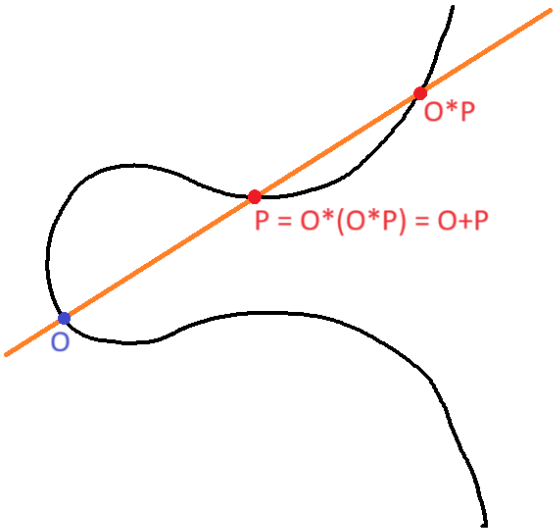
Estrutura de grupo

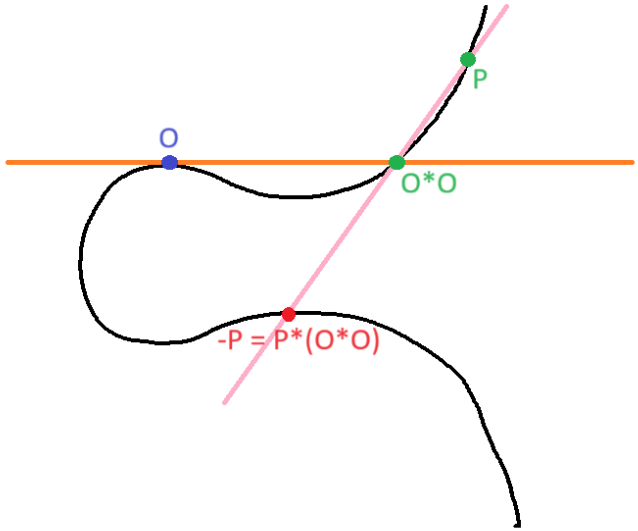
- Obtemos uma estrutura de *grupo abeliano*.
- Pode-se verificar que a operação '$+$' é associativa.
- É trivialmente comutativa, pois $P * Q = Q * P$.
- A origem O é o zero do grupo.

Estrutura de grupo

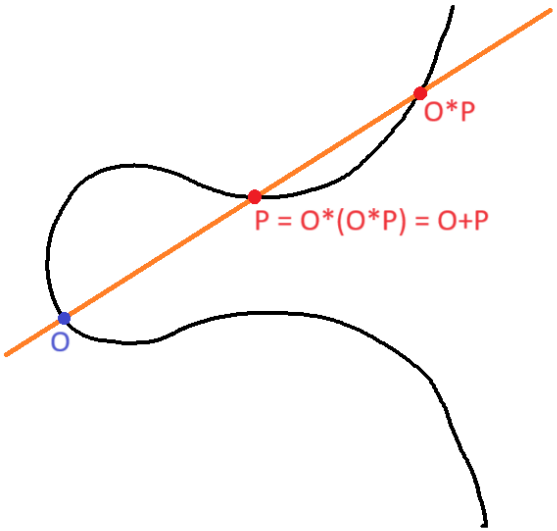
- Obtemos uma estrutura de *grupo abeliano*.
- Pode-se verificar que a operação '$+$' é associativa.
- É trivialmente comutativa, pois $P * Q = Q * P$.
- A origem O é o zero do grupo.
- O oposto de P é o ponto $-P = P * (O * O)$.

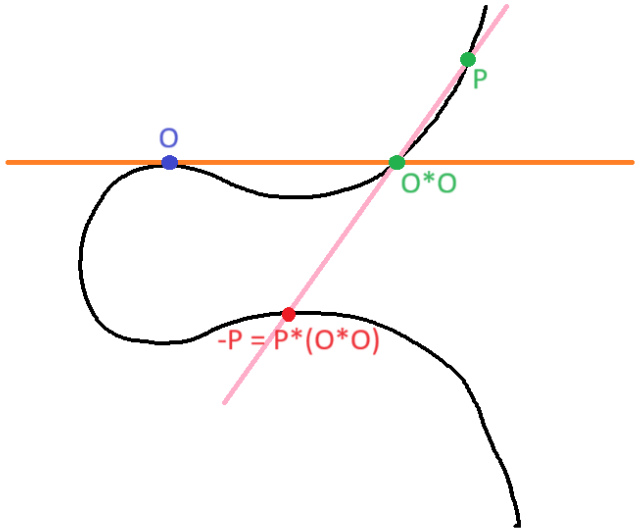
Estrutura de grupo





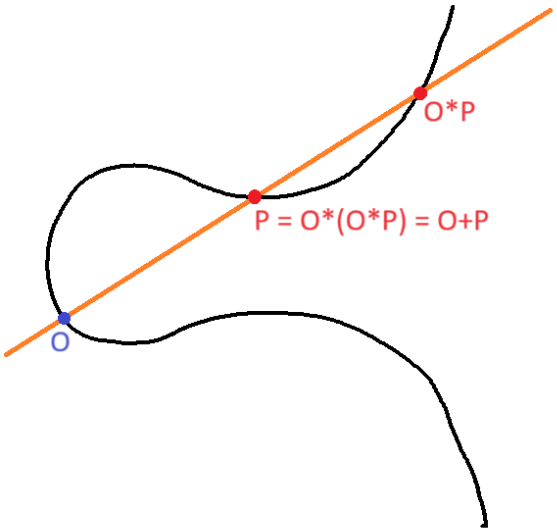
Estrutura de grupo

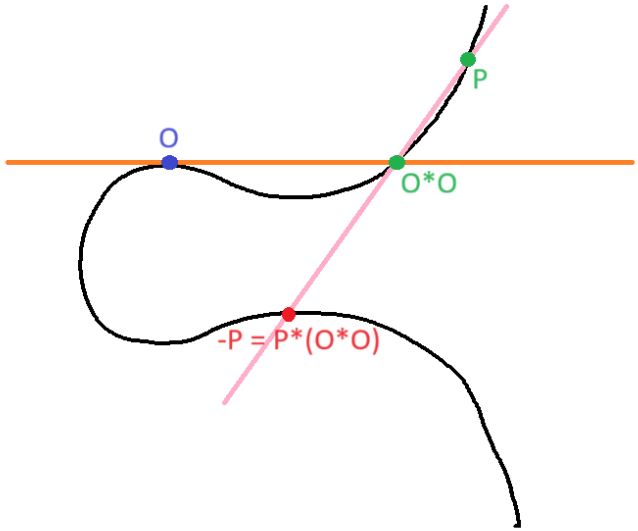




- Segue da construção que $O + P = P$.

Estrutura de grupo





- Segue da construção que $O + P = P$.
- Segue da construção que $P + (-P) = O$.

Teorema de Mordell

- Os pontos racionais, caso existam, formam um subgrupo.

Teorema de Mordell

- Os pontos racionais, caso existam, formam um subgrupo.
- Dada uma curva elíptica C, denotamos por $\hat{C}$ o subgrupo formado pelos pontos racionais.

Teorema de Mordell

- Os pontos racionais, caso existam, formam um subgrupo.
- Dada uma curva elíptica C, denotamos por $\hat{C}$ o subgrupo formado pelos pontos racionais.
- *Teorema de Mordell:* O grupo abeliano $\hat{C}$ é finitamente gerado.

Teorema de Mordell

- Os pontos racionais, caso existam, formam um subgrupo.
- Dada uma curva elíptica C, denotamos por $\hat{C}$ o subgrupo formado pelos pontos racionais.
- *Teorema de Mordell:* O grupo abeliano $\hat{C}$ é finitamente gerado.
- Portanto, $\hat{C} \simeq \mathbb{Z}^r \oplus \operatorname{Tor} \hat{C}$, sendo $\operatorname{Tor} \hat{C} \simeq \mathbb{Z}_{n_1}^{r_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}^{r_k}$ um grupo finito.

Posto Algébrico

- Vimos que $\hat{C} \simeq \mathbb{Z}^r \oplus \operatorname{Tor} \hat{C}$.

Posto Algébrico

- Vimos que $\hat{C} \simeq \mathbb{Z}^r \oplus \operatorname{Tor} \hat{C}$.
- Conhecemos um método para calcular explicitamente o grupo $\operatorname{Tor} \hat{C}$.

Posto Algébrico

- Vimos que $\hat{C} \simeq \mathbb{Z}^r \oplus \operatorname{Tor} \hat{C}$.
- Conhecemos um método para calcular explicitamente o grupo $\operatorname{Tor} \hat{C}$.
- Por definição, o número natural r é o posto do grupo $\hat{C}$. Não sabemos como calculá-lo em geral.

Posto Algébrico

- Vimos que $\hat{C} \simeq \mathbb{Z}^r \oplus \operatorname{Tor} \hat{C}$.
- Conhecemos um método para calcular explicitamente o grupo $\operatorname{Tor} \hat{C}$.
- Por definição, o número natural r é o posto do grupo $\hat{C}$. Não sabemos como calculá-lo em geral.
- *Definição:* O *Posto Algébrico* de uma curva elíptica C é o posto do grupo $\hat{C}$.

Redução módulo p

- Consideremos uma curva elíptica $y^2 = x^3 + ax^2 + bx + c$, sendo $a, b, c \in \mathbb{Z}$.

Redução módulo p

- Consideremos uma curva elíptica $y^2 = x^3 + ax^2 + bx + c$, sendo $a, b, c \in \mathbb{Z}$.
- Para cada p primo, podemos considerar a mesma curva com coeficientes em $\mathbb{Z}_p$, que denotamos por C_p.

Redução módulo p

- Consideremos uma curva elíptica $y^2 = x^3 + ax^2 + bx + c$, sendo $a, b, c \in \mathbb{Z}$.
- Para cada p primo, podemos considerar a mesma curva com coeficientes em $\mathbb{Z}_p$, que denotamos por C_p.
- Fica definido o grupo abeliano C_p como no caso real.

Redução módulo p

- Consideremos uma curva elíptica $y^2 = x^3 + ax^2 + bx + c$, sendo $a, b, c \in \mathbb{Z}$.
- Para cada p primo, podemos considerar a mesma curva com coeficientes em $\mathbb{Z}_p$, que denotamos por C_p.
- Fica definido o grupo abeliano C_p como no caso real.
- Qual é a cardinalidade de C_p?

Redução módulo p

- Seja $\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$, sendo $p > 2$.

Redução módulo p

- Seja $\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$, sendo $p > 2$.
- Metade dos elementos de $\mathbb{Z}_p^*$ são quadrados (isso segue do morfismo $x \mapsto x^2$, cujo kernel é $\{\pm 1\}$).

Redução módulo p

- Seja $\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$, sendo $p > 2$.
- Metade dos elementos de $\mathbb{Z}_p^*$ são quadrados (isso segue do morfismo $x \mapsto x^2$, cujo kernel é $\{\pm 1\}$).
- Portanto, os pontos $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$, que satisfazem $y^2 = x$, são $(0, 0)$ e $(\pm a, a^2)$ para cada a^2, logo, são $1 + \frac{p-1}{2} \cdot 2 = p$.

Redução módulo p

- Seja $\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$, sendo $p > 2$.
- Metade dos elementos de $\mathbb{Z}_p^*$ são quadrados (isso segue do morfismo $x \mapsto x^2$, cujo kernel é $\{\pm 1\}$).
- Portanto, os pontos $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$, que satisfazem $y^2 = x$, são $(0, 0)$ e $(\pm a, a^2)$ para cada a^2, logo, são $1 + \frac{p-1}{2} \cdot 2 = p$.
- Por isso, supondo que a imagem de $f(x) = x^3 + ax^2 + bx + c$ seja uniformemente distribuída entre quadrados e não quadrados, esperamos que haja p pontos na curva $y^2 = f(x)$.

Redução módulo p

- Acrescentando o ponto ao infinito, obtemos $p + 1$ pontos.

Redução módulo p

- Acrescentando o ponto ao infinito, obtemos $p+1$ pontos.
- Seja $|C_p| = p + 1 - \epsilon_p$.

Redução módulo p

- Acrescentando o ponto ao infinito, obtemos $p+1$ pontos.
- Seja $|C_p| = p + 1 - \epsilon_p$.
- Esperamos que ϵ_p seja "pequeno".

Redução módulo p

- Acrescentando o ponto ao infinito, obtemos $p+1$ pontos.
- Seja $|C_p| = p + 1 - \epsilon_p$.
- Esperamos que ϵ_p seja "pequeno".
- *Teorema de Hasse-Weil:* Se a curva C_p for non-singular, então $|\epsilon_p| \leq 2\sqrt{p}$.

Redução módulo p

- Acrescentando o ponto ao infinito, obtemos $p+1$ pontos.
- Seja $|C_p| = p + 1 - \epsilon_p$.
- Esperamos que ϵ_p seja "pequeno".
- *Teorema de Hasse-Weil:* Se a curva C_p for non-singular, então $|\epsilon_p| \leq 2\sqrt{p}$.
- A sequência $\{\epsilon_p\}_{p \text{ primo}}$ é uma informação significativa relativa à curva elíptica C.

Séries de Dirichlet

- Dada uma sequência de números complexos $\{a_n\}_{n\in\mathbb{N}^*}$, a *série de Dirichlet* correspondente é a função analítica $f(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$.

Séries de Dirichlet

- Dada uma sequência de números complexos $\{a_n\}_{n\in\mathbb{N}^*}$, a *série de Dirichlet* correspondente é a função analítica $f(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$.
- Em geral, a série converge em um domínio do plano complexo, mas a soma pode ser estendida analiticamente a um domínio maior.

Séries de Dirichlet

- Dada uma sequência de números complexos $\{a_n\}_{n\in\mathbb{N}^*}$, a *série de Dirichlet* correspondente é a função analítica $f(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$.
- Em geral, a série converge em um domínio do plano complexo, mas a soma pode ser estendida analiticamente a um domínio maior.
- As séries de Dirichlet são particularmente interessantes por terem boas propriedades aditivas e multiplicativas.

Séries de Dirichlet

- Dada uma sequência de números complexos $\{a_n\}_{n\in\mathbb{N}^*}$, a *série de Dirichlet* correspondente é a função analítica $f(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$.
- Em geral, a série converge em um domínio do plano complexo, mas a soma pode ser estendida analiticamente a um domínio maior.
- As séries de Dirichlet são particularmente interessantes por terem boas propriedades aditivas e multiplicativas.
- Exemplo: se $a_n = 1$ para todo n, obtemos $\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \frac{1}{1-p^{-s}}$.

L-Função de uma curva elíptica

- Dada uma curva elíptica C, temos a sequência $\{\epsilon_p\}_{p \text{ primo}}$.

L-Função de uma curva elíptica

- Dada uma curva elíptica C, temos a sequência $\{\epsilon_p\}_{p \text{ primo}}$.
- Definimos:

$$L(C,s) := \prod_{p \text{ primo}} \left(1 - \frac{\epsilon_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

L-Função de uma curva elíptica

- Dada uma curva elíptica C, temos a sequência $\{\epsilon_p\}_{p \text{ primo}}$.
- Definimos:

$$L(C,s) := \prod_{p \text{ primo}} \left(1 - \frac{\epsilon_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

- Por que definimos $L(C,s)$ desta maneira?

L-Função de uma curva elíptica

- Dada uma curva elíptica C, temos a sequência $\{\epsilon_p\}_{p \text{ primo}}$.
- Definimos:

$$L(C,s) := \prod_{p \text{ primo}} \left(1 - \frac{\epsilon_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

- Por que definimos $L(C,s)$ desta maneira?
- Temos que:

$$\left(1-\frac{\epsilon_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1} = \sum_{k=0}^{+\infty} \left(\frac{\epsilon_p}{p^s} - \frac{1}{p^{2s-1}}\right)^k$$
$$= \sum_{k=0}^{+\infty} \sum_{i=0}^{k} \binom{k}{i} \left(\frac{\epsilon_p}{p^s}\right)^i \left(\frac{1}{p^{2s-1}}\right)^{k-i} = \ldots = \sum_{n=1}^{\infty} \frac{\epsilon_n}{n^s}.$$

L-Função de uma curva elíptica

- Dada uma curva elíptica C, temos a sequência $\{\epsilon_p\}_{p \text{ primo}}$.

L-Função de uma curva elíptica

- Dada uma curva elíptica C, temos a sequência $\{\epsilon_p\}_{p \text{ primo}}$.
- Vimos que $L(C,s) = \sum_{n=1}^{\infty} \frac{\epsilon_n}{n^s}$, ou seja, $L(C,s)$ é uma série de Dirichlet.

L-Função de uma curva elíptica

- Dada uma curva elíptica C, temos a sequência $\{\epsilon_p\}_{p \text{ primo}}$.
- Vimos que $L(C,s) = \sum_{n=1}^{\infty} \frac{\epsilon_n}{n^s}$, ou seja, $L(C,s)$ é uma série de Dirichlet.
- Temos que:

L-Função de uma curva elíptica

- Dada uma curva elíptica C, temos a sequência $\{\epsilon_p\}_{p \text{ primo}}$.
- Vimos que $L(C,s) = \sum_{n=1}^{\infty} \frac{\epsilon_n}{n^s}$, ou seja, $L(C,s)$ é uma série de Dirichlet.
- Temos que:
  - ϵ_p coincide com o valor definido anteriormente para todo p primo;

L-Função de uma curva elíptica

- Dada uma curva elíptica C, temos a sequência $\{\epsilon_p\}_{p \text{ primo}}$.
- Vimos que $L(C,s) = \sum_{n=1}^{\infty} \frac{\epsilon_n}{n^s}$, ou seja, $L(C,s)$ é uma série de Dirichlet.
- Temos que:
  - ϵ_p coincide com o valor definido anteriormente para todo p primo;
  - $\epsilon_{p^k} = \cdots$ (veremos isso daqui a pouco);

L-Função de uma curva elíptica

- Dada uma curva elíptica C, temos a sequência $\{\epsilon_p\}_{p \text{ primo}}$.
- Vimos que $L(C,s) = \sum_{n=1}^{\infty} \frac{\epsilon_n}{n^s}$, ou seja, $L(C,s)$ é uma série de Dirichlet.
- Temos que:
  - ϵ_p coincide com o valor definido anteriormente para todo p primo;
  - $\epsilon_{p^k} = \cdots$ (veremos isso daqui a pouco);
  - $\epsilon_{p_1^{k_1} \cdots p_l^{k_l}} = \epsilon_{p_1^{k_1}} \cdots \epsilon_{p_l^{k_l}}$.

L-Função de uma curva elíptica

- Vale a relação recursiva $\epsilon_{p^k} = \epsilon_{p^{k-1}}\epsilon_p - p\epsilon_{p^{k-2}}$.

L-Função de uma curva elíptica

- Vale a relação recursiva $\epsilon_{p^k} = \epsilon_{p^{k-1}}\epsilon_p - p\epsilon_{p^{k-2}}$.
- Exceto pelo termo $p\epsilon_{p^{k-2}}$, trata-se de uma extensão natural a todos os naturais da sequência $\{\epsilon_p\}_{p \text{ primo}}$.

L-Função de uma curva elíptica

- Vale a relação recursiva $\epsilon_{p^k} = \epsilon_{p^{k-1}}\epsilon_p - p\epsilon_{p^{k-2}}$.
- Exceto pelo termo $p\epsilon_{p^{k-2}}$, trata-se de uma extensão natural a todos os naturais da sequência $\{\epsilon_p\}_{p \text{ primo}}$.
- Como $|\epsilon_p| \leq 2\sqrt{p}$, pode-se demonstrar que a série $\sum_{n=1}^{\infty} \frac{\epsilon_n}{n^s}$ converge para $\text{Re}(s) > \frac{3}{2}$.

L-Função de uma curva elíptica

- Vale a relação recursiva $\epsilon_{p^k} = \epsilon_{p^{k-1}}\epsilon_p - p\epsilon_{p^{k-2}}$.
- Exceto pelo termo $p\epsilon_{p^{k-2}}$, trata-se de uma extensão natural a todos os naturais da sequência $\{\epsilon_p\}_{p \text{ primo}}$.
- Como $|\epsilon_p| \leq 2\sqrt{p}$, pode-se demonstrar que a série $\sum_{n=1}^{\infty} \frac{\epsilon_n}{n^s}$ converge para $\text{Re}(s) > \frac{3}{2}$.
- Enfim, $L(C, s)$ pode ser estendida analiticamente a uma função definida em $\mathbb{C}$ todo.

Ordem em um ponto

- Uma função analítica, localmente em $s_0 \in \mathbb{C}$, é uma série de potências $f(s) = \sum_{n=1}^{+\infty} a_n(s - s_0)^n$.

Ordem em um ponto

- Uma função analítica, localmente em $s_0 \in \mathbb{C}$, é uma série de potências $f(s) = \sum_{n=1}^{+\infty} a_n (s - s_0)^n$.
- A *ordem* de f em s_0, que denotamos por $\mathrm{ord}_{s_0} f$, é o mínimo número $n \in \mathbb{N}$ tal que $a_n \neq 0$.

Ordem em um ponto

- Uma função analítica, localmente em $s_0 \in \mathbb{C}$, é uma série de potências $f(s) = \sum_{n=1}^{+\infty} a_n (s - s_0)^n$.
- A *ordem* de f em s_0, que denotamos por $\mathrm{ord}_{s_0} f$, é o mínimo número $n \in \mathbb{N}$ tal que $a_n \neq 0$.
- Logo, $\mathrm{ord}_{s_0} f = k$ se, e somente se, $f(s) = (s - s_0)^k g(s)$, sendo $g(s_0) \neq 0$.

Ordem em um ponto

- Uma função analítica, localmente em $s_0 \in \mathbb{C}$, é uma série de potências $f(s) = \sum_{n=1}^{+\infty} a_n (s - s_0)^n$.
- A *ordem* de f em s_0, que denotamos por $\mathrm{ord}_{s_0} f$, é o mínimo número $n \in \mathbb{N}$ tal que $a_n \neq 0$.
- Logo, $\mathrm{ord}_{s_0} f = k$ se, e somente se, $f(s) = (s - s_0)^k g(s)$, sendo $g(s_0) \neq 0$.
- Claramente, $\mathrm{ord}_{s_0} f = 0$ se, e somente se, $f(s_0) \neq 0$; ademais, se $\mathrm{ord}_{s_0} f > \mathrm{ord}_{s_0} g$, então f tende a 0 mais rapidamente do que g para $s \to s_0$.

L-Função de uma curva elíptica

- Analisemos a função $L(C, s)$ em $s = 1$.

L-Função de uma curva elíptica

- Analisemos a função $L(C, s)$ em $s = 1$.
- Fingindo que a série de Dirichlet convirja em $s = 1$, temos que:

$$\begin{aligned} L(C,1) &= \prod_p \left(1 - \frac{\epsilon_p}{p} + \frac{1}{p}\right)^{-1} \\ &= \prod_p \frac{p}{p+1-\epsilon_p} = \prod_p \frac{p}{p+1-\epsilon_p} \\ &= \prod_p \frac{p}{|C_p|}. \end{aligned}$$

L-Função de uma curva elíptica

- Analisemos a função $L(C, s)$ em $s = 1$.
- Fingindo que a série de Dirichlet convirja em $s = 1$, temos que:

$$\begin{aligned} L(C,1) &= \prod_p \left(1 - \frac{\epsilon_p}{p} + \frac{1}{p}\right)^{-1} \\ &= \prod_p \frac{p}{p+1-\epsilon_p} = \prod_p \frac{p}{p+1-\epsilon_p} \\ &= \prod_p \frac{p}{|C_p|}. \end{aligned}$$

- Portanto, fingimos que a fórmula (errada) $L(C,1) = \frac{p}{|C_p|}$ seja válida.

L-Função de uma curva elíptica

- Numericamente, Birch e SD viram que, quando o posto algébrico de C aumenta, a cardinalidade de C_p se torna mediamente bem maior do que p; logo, o quociente $\frac{p}{|C_p|}$ diminui.

L-Função de uma curva elíptica

- Numericamente, Birch e SD viram que, quando o posto algébrico de C aumenta, a cardinalidade de C_p se torna mediamente bem maior do que p; logo, o quociente $\frac{p}{|C_p|}$ diminui.
- Uma justificação teórica bem imprecisa pode ser a seguinte: quando $\hat{C}$ é muito grande, a curva C contém muitos pontos racionais e, portanto, é mais provável que a redução módulo p contenha mais pontos do que a média prevista $p+1$.

L-Função de uma curva elíptica

- Numericamente, Birch e SD viram que, quando o posto algébrico de C aumenta, a cardinalidade de C_p se torna mediamente bem maior do que p; logo, o quociente $\frac{p}{|C_p|}$ diminui.
- Uma justificação teórica bem imprecisa pode ser a seguinte: quando $\hat{C}$ é muito grande, a curva C contém muitos pontos racionais e, portanto, é mais provável que a redução módulo p contenha mais pontos do que a média prevista $p+1$.
- Em particular, para que o produto $\prod_p \frac{p}{|C_p|}$ seja zero, os termos $\frac{p}{|C_p|}$ têm que ser estavelmente menores do que 1.

L-Função de uma curva elíptica

- Numericamente, Birch e SD viram que, quando o posto algébrico de C aumenta, a cardinalidade de C_p se torna mediamente bem maior do que p; logo, o quociente $\frac{p}{|C_p|}$ diminui.
- Uma justificação teórica bem imprecisa pode ser a seguinte: quando $\hat{C}$ é muito grande, a curva C contém muitos pontos racionais e, portanto, é mais provável que a redução módulo p contenha mais pontos do que a média prevista $p+1$.
- Em particular, para que o produto $\prod_p \frac{p}{|C_p|}$ seja zero, os termos $\frac{p}{|C_p|}$ têm que ser estavelmente menores do que 1.
- Isso parece acontecer se, e somente se, $\hat{C}$ é infinito.

L-Função de uma curva elíptica

- Portanto, este argumento sugere que a ordem de $L(C, s)$ em $s = 1$ é positiva se, e somente se, o posto algébrico de C é positivo.

L-Função de uma curva elíptica

- Portanto, este argumento sugere que a ordem de $L(C, s)$ em $s = 1$ é positiva se, e somente se, o posto algébrico de C é positivo.
- Ademais, se o posto algébrico de C cresce, o quociente $\frac{p}{|C_p|}$ parece diminuir.

L-Função de uma curva elíptica

- Portanto, este argumento sugere que a ordem de $L(C, s)$ em $s = 1$ é positiva se, e somente se, o posto algébrico de C é positivo.
- Ademais, se o posto algébrico de C cresce, o quociente $\frac{p}{|C_p|}$ parece diminuir.
- Logo, o produto $\prod_p \frac{p}{|C_p|}$ tende mais rapidamente a 0 e, portanto, a ordem de $L(C, s)$ em $s = 1$ cresce.

L-Função de uma curva elíptica

- Portanto, este argumento sugere que a ordem de $L(C, s)$ em $s = 1$ é positiva se, e somente se, o posto algébrico de C é positivo.
- Ademais, se o posto algébrico de C cresce, o quociente $\frac{p}{|C_p|}$ parece diminuir.
- Logo, o produto $\prod_p \frac{p}{|C_p|}$ tende mais rapidamente a 0 e, portanto, a ordem de $L(C, s)$ em $s = 1$ cresce.
- Parece haver uma ligação bem forte entre o posto algébrico de C e a ordem de $L(C, s)$ em $s = 1$.

Conjetura de Birch e Swinnerton-Dyer

- Definição (já vista): O *posto algébrico* de uma curva elíptica C, que denotamos por $\mathrm{rk}_{\mathrm{alg}} C$, é o posto do grupo abeliano $\hat{C}$.

Conjetura de Birch e Swinnerton-Dyer

- Definição (já vista): O *posto algébrico* de uma curva elíptica C, que denotamos por $\mathrm{rk}_{\mathrm{alg}} C$, é o posto do grupo abeliano $\hat{C}$.
- Definição: O *Posto Analítico* de uma curva elíptica C, que denotamos por $\mathrm{rk}_{\mathrm{an}} C$, é a ordem da função analítica $L(C, s)$ no ponto $s = 1$.

Conjetura de Birch e Swinnerton-Dyer

- Definição (já vista): O *posto algébrico* de uma curva elíptica C, que denotamos por $\mathrm{rk}_{\mathrm{alg}} C$, é o posto do grupo abeliano $\hat{C}$.
- Definição: O *Posto Analítico* de uma curva elíptica C, que denotamos por $\mathrm{rk}_{\mathrm{an}} C$, é a ordem da função analítica $L(C, s)$ no ponto $s = 1$.
- Conjetura de Birch e Swinnerton-Dyer: $\mathrm{rk}_{\mathrm{alg}} C = \mathrm{rk}_{\mathrm{an}} C$ para toda curva elíptica C.

Conjetura de Birch e Swinnerton-Dyer

- A que ponto está a pesquisa sobre esta conjetura?

Conjetura de Birch e Swinnerton-Dyer

- A que ponto está a pesquisa sobre esta conjetura?
- Foi demonstrado rigorosamente que $\mathrm{rk}_{\mathrm{an}} C = 0 \Rightarrow \mathrm{rk}_{\mathrm{alg}} C = 0$ e $\mathrm{rk}_{\mathrm{an}} C = 1 \Rightarrow \mathrm{rk}_{\mathrm{alg}} C = 1$.

Conjetura de Birch e Swinnerton-Dyer

- A que ponto está a pesquisa sobre esta conjetura?
- Foi demonstrado rigorosamente que $\mathrm{rk}_{\mathrm{an}} C = 0 \Rightarrow \mathrm{rk}_{\mathrm{alg}} C = 0$ e $\mathrm{rk}_{\mathrm{an}} C = 1 \Rightarrow \mathrm{rk}_{\mathrm{alg}} C = 1$.
- Temos resultados parciais na direção inversa, mas com hipóteses complicadas para verificar.

Conjetura de Birch e Swinnerton-Dyer

- A que ponto está a pesquisa sobre esta conjetura?
- Foi demonstrado rigorosamente que $\mathrm{rk}_{\mathrm{an}} C = 0 \Rightarrow \mathrm{rk}_{\mathrm{alg}} C = 0$ e $\mathrm{rk}_{\mathrm{an}} C = 1 \Rightarrow \mathrm{rk}_{\mathrm{alg}} C = 1$.
- Temos resultados parciais na direção inversa, mas com hipóteses complicadas para verificar.
- Foi demonstrado que, a respeito de uma medida adequada, uma porcentagem positiva de curvas elípticas tem posto analítico 0.

Conjetura de Birch e Swinnerton-Dyer

- A que ponto está a pesquisa sobre esta conjetura?
- Foi demonstrado rigorosamente que $\mathrm{rk}_{\mathrm{an}} C = 0 \Rightarrow \mathrm{rk}_{\mathrm{alg}} C = 0$ e $\mathrm{rk}_{\mathrm{an}} C = 1 \Rightarrow \mathrm{rk}_{\mathrm{alg}} C = 1$.
- Temos resultados parciais na direção inversa, mas com hipóteses complicadas para verificar.
- Foi demonstrado que, a respeito de uma medida adequada, uma porcentagem positiva de curvas elípticas tem posto analítico 0.
- Também foi demonstrado que pelo menos o 62.5% das curvas elípticas tem posto algébrico 0 ou 1, mas isso não é suficiente para concluir que satisfazem a conjetura.

Aplicações da conjetura

- Em geral, é bem difícil calcular ambos os postos.

Aplicações da conjetura

- Em geral, é bem difícil calcular ambos os postos.
- Todavia, conhecemos algoritmos computacionais válidos para calcular o posto analítico quando for menor ou igual a 3.

Aplicações da conjetura

- Em geral, é bem difícil calcular ambos os postos.
- Todavia, conhecemos algoritmos computacionais válidos para calcular o posto analítico quando for menor ou igual a 3.
- Se a conjetura é válida, então isso permite calcular o posto algébrico de várias curvas elípticas.

Aplicações da conjetura

- Em geral, é bem difícil calcular ambos os postos.
- Todavia, conhecemos algoritmos computacionais válidos para calcular o posto analítico quando for menor ou igual a 3.
- Se a conjetura é válida, então isso permite calcular o posto algébrico de várias curvas elípticas.
- Calcular o posto algébrico é essencial para descrever o grupo $\hat{C}$, formado pelos pontos racionais da curva.

Aplicações da conjetura

- Um problema relevante na Teoria dos Números é o *Problema dos Números Congruentes*: quais números inteiros coincidem com a área de um triângulo retângulo de lados racionais?

Aplicações da conjetura

- Um problema relevante na Teoria dos Números é o *Problema dos Números Congruentes*: quais números inteiros coincidem com a área de um triângulo retângulo de lados racionais?

- Foi demonstrado que n é congruente se, e somente se, o grupo $\hat{C}$ da curva elíptica $y^2 = x^3 - n^2x$ é infinito.

Aplicações da conjetura

- Um problema relevante na Teoria dos Números é o *Problema dos Números Congruentes*: quais números inteiros coincidem com a área de um triângulo retângulo de lados racionais?
- Foi demonstrado que n é congruente se, e somente se, o grupo $\hat{C}$ da curva elíptica $y^2 = x^3 - n^2x$ é infinito.
- Se a conjetura é válida, então:

Aplicações da conjetura

- Um problema relevante na Teoria dos Números é o *Problema dos Números Congruentes*: quais números inteiros coincidem com a área de um triângulo retângulo de lados racionais?
- Foi demonstrado que n é congruente se, e somente se, o grupo $\hat{C}$ da curva elíptica $y^2 = x^3 - n^2x$ é infinito.
- Se a conjetura é válida, então:
  - todo número n tal que $n \equiv_8 5, 6, 7$ é congruente;

Aplicações da conjetura

- Um problema relevante na Teoria dos Números é o *Problema dos Números Congruentes*: quais números inteiros coincidem com a área de um triângulo retângulo de lados racionais?
- Foi demonstrado que n é congruente se, e somente se, o grupo $\hat{C}$ da curva elíptica $y^2 = x^3 - n^2x$ é infinito.
- Se a conjetura é válida, então:
  - todo número n tal que $n \equiv_8 5, 6, 7$ é congruente;
  - se n for ímpar e sem fatores primos quadrados, podemos estabelecer facilmente se é congruente ou não.

Obrigado a todos!