Dos Números Congruentes às Curvas Elípticas

Wodson Mendson

UFMG

Outubro - 2015

Orientador: Israel Vainsencher

Pontos Racionais

Dada uma curva X irredutível descrita por um polinômio não constante $p(x, y) \in \mathbb{Z}[x, y]$ um problema interessante consiste em estudar a existencia de pontos $\mathbb{Q}$ - racionais em X. Algumas perguntas interessantes:

Pontos Racionais

Dada uma curva X irredutível descrita por um polinômio não constante $p(x, y) \in \mathbb{Z}[x, y]$ um problema interessante consiste em estudar a existencia de pontos $\mathbb{Q}$ - racionais em X. Algumas perguntas interessantes:

- Existe um ponto $(x, y) \in \mathbb{Q}^2$ em X?

Pontos Racionais

Dada uma curva X irredutível descrita por um polinômio não constante $p(x, y) \in \mathbb{Z}[x, y]$ um problema interessante consiste em estudar a existencia de pontos $\mathbb{Q}$ - racionais em X. Algumas perguntas interessantes:

- Existe um ponto $(x, y) \in \mathbb{Q}^2$ em X?
- Se existir, existem mais?

Pontos Racionais

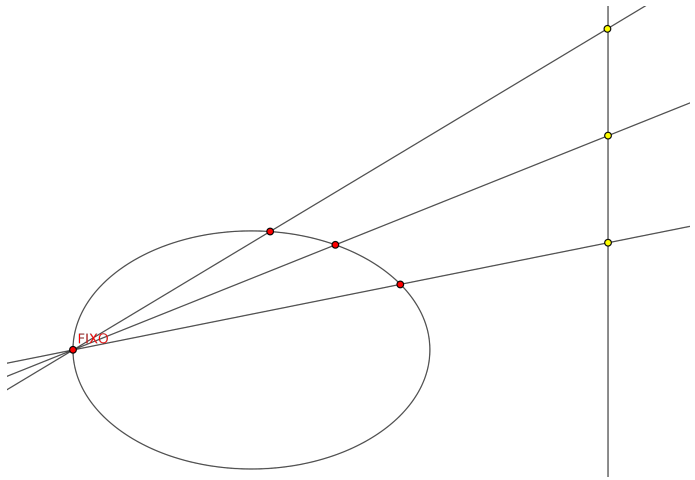
Dada uma curva X irredutível descrita por um polinômio não constante $p(x, y) \in \mathbb{Z}[x, y]$ um problema interessante consiste em estudar a existencia de pontos $\mathbb{Q}$ - racionais em X. Algumas perguntas interessantes:

- Existe um ponto $(x, y) \in \mathbb{Q}^2$ em X?
- Se existir, existem mais?
- Podemos construir todos os pontos $(x, y) \in \mathbb{Q}^2$ de X?

Pontos Racionais

Dada uma curva X irredutível descrita por um polinômio não constante $p(x, y) \in \mathbb{Z}[x, y]$ um problema interessante consiste em estudar a existencia de pontos $\mathbb{Q}$ - racionais em X. Algumas perguntas interessantes:

- Existe um ponto $(x, y) \in \mathbb{Q}^2$ em X?
- Se existir, existem mais?
- Podemos construir todos os pontos $(x, y) \in \mathbb{Q}^2$ de X?



Casos

- (grau 1): problema trivial!.

Casos

- (grau 1): problema trivial!.
- (grau 2): Mais interessante. A resposta para a primeira pergunta nem sempre é positiva. Mas, se existir ponto $\mathbb{Q}$- racional podemos construir todos os outros, exceto possivelmente um número finito de pontos. Alguns exemplos: $C_1 : x^2 + y^2 = 3$ e $C_2 : x^2 - 2y^2 = 1$.

Casos

- (grau 1): problema trivial!.
- (grau 2): Mais interessante. A resposta para a primeira pergunta nem sempre é positiva. Mas, se existir ponto $\mathbb{Q}$- racional podemos construir todos os outros, exceto possivelmente um número finito de pontos. Alguns exemplos: $C_1 : x^2 + y^2 = 3$ e $C_2 : x^2 - 2y^2 = 1$.
- (grau 3): Mais elegante. No caso não singular, mostra-se que existe um conjunto S finito de pontos $\mathbb{Q}$-racionais da cúbica tal que todo ponto racional pode ser obtido de S via um operação bem definida na cúbica.

Números congruentes

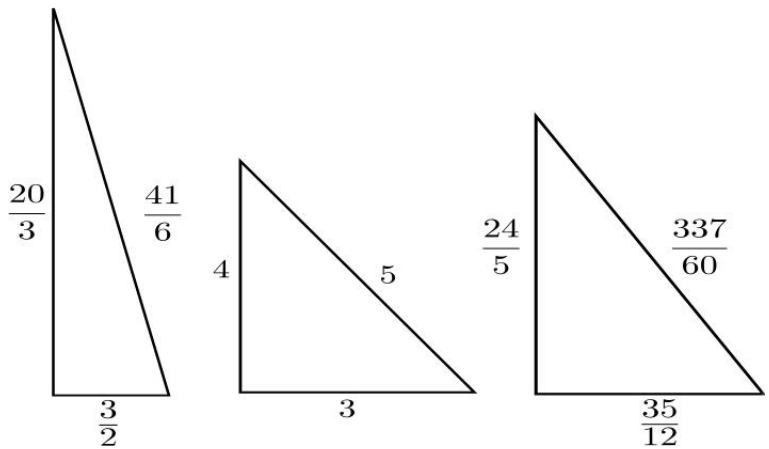
Seja $n \in \mathbb{Z} > 0$. Dizemos que n é congruente se n ocorre como área de algum triangulo retangulo racional (x, y, z). Aqui, consideramos x, y catetos e z hipotenusa.

Números congruentes

Seja $n \in \mathbb{Z} > 0$. Dizemos que n é congruente se n ocorre como área de algum triangulo retangulo racional (x, y, z). Aqui, consideramos x, y catetos e z hipotenusa.

Exemplo

$n = 5, 6, 7$ são congruentes. Já, $n = 1, 2$ e $n = 3$ não são inteiros congruentes, resultado devido à Fermat.



Números congruentes

Podemos determinar uma infinidade de inteiros congruentes.

Números congruentes

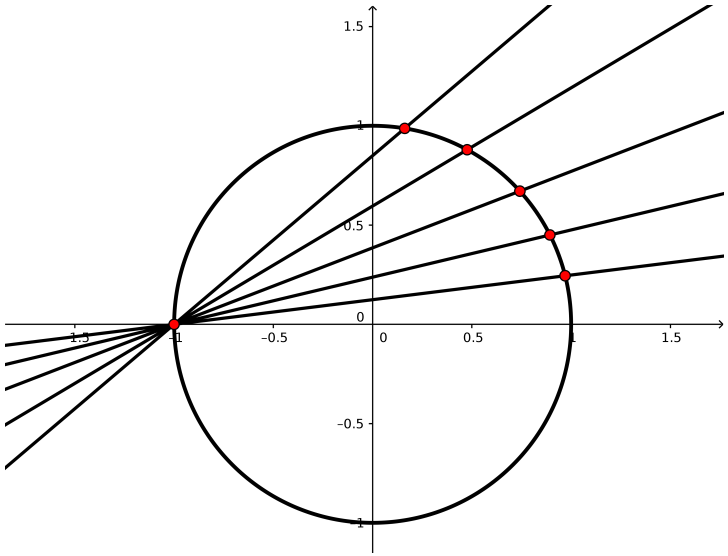
Podemos determinar uma infinidade de inteiros congruentes. De fato, de $x^2 + y^2 = z^2$ obtemos $u = \frac{x}{z}$ e $v = \frac{y}{z}$ um ponto no circulo unitário $u^2 + v^2 = 1$.

Números congruentes

Podemos determinar uma infinidade de inteiros congruentes. De fato, de $x^2 + y^2 = z^2$ obtemos $u = \frac{x}{z}$ e $v = \frac{y}{z}$ um ponto no circulo unitário $u^2 + v^2 = 1$. A parametrização racional do circulo $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ permite escrever $x = a^2 - b^2$, $y = 2ab$ e $z = a^2 + b^2$, com $a > b$ inteiros.

Números congruentes

Podemos determinar uma infinidade de inteiros congruentes. De fato, de $x^2 + y^2 = z^2$ obtemos $u = \frac{x}{z}$ e $v = \frac{y}{z}$ um ponto no circulo unitário $u^2 + v^2 = 1$. A parametrização racional do circulo $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ permite escrever $x = a^2 - b^2$, $y = 2ab$ e $z = a^2 + b^2$, com $a > b$ inteiros.



Formas equivalentes

O problema mais dificil consiste em determinar se um dado inteiro $n \in \mathbb{Z}$ é congruente. O seguinte resultado permite caracterizar um inteiro (livre de quadrados) de diferentes formas:

Formas equivalentes

O problema mais dificil consiste em determinar se um dado inteiro $n \in \mathbb{Z}$ é congruente. O seguinte resultado permite caracterizar um inteiro (livre de quadrados) de diferentes formas:

Teorema

Seja $n \in \mathbb{Z} > 0$ livre de quadrados. Os seguintes são equivalentes:

- *(a) n é congruente;*

Formas equivalentes

O problema mais dificil consiste em determinar se um dado inteiro $n \in \mathbb{Z}$ é congruente. O seguinte resultado permite caracterizar um inteiro (livre de quadrados) de diferentes formas:

Teorema

Seja $n \in \mathbb{Z} > 0$ livre de quadrados. Os seguintes são equivalentes:

- *(a)* *n é congruente;*
- *(b)* *$\exists x$ quadrado em $\mathbb{Q}$, tal que $x - n, x, x + n$ são quadrados;*

Formas equivalentes

O problema mais dificil consiste em determinar se um dado inteiro $n \in \mathbb{Z}$ é congruente. O seguinte resultado permite caracterizar um inteiro (livre de quadrados) de diferentes formas:

Teorema

Seja $n \in \mathbb{Z} > 0$ livre de quadrados. Os seguintes são equivalentes:

- *(a)* n *é congruente;*
- *(b)* $\exists x$ *quadrado em* $\mathbb{Q}$*, tal que* $x - n, x, x + n$ *são quadrados;*
- *(c)* $\exists$ *ponto* (x, y) $\mathbb{Q}$*-racional na cúbica* $C_n : y^2 = x^3 - n^2 x$ *com* $y \neq 0$*;*

Formas equivalentes

O problema mais dificil consiste em determinar se um dado inteiro $n \in \mathbb{Z}$ é congruente. O seguinte resultado permite caracterizar um inteiro (livre de quadrados) de diferentes formas:

Teorema

Seja $n \in \mathbb{Z} > 0$ livre de quadrados. Os seguintes são equivalentes:

- *(a)* n *é congruente;*
- *(b)* $\exists x$ *quadrado em* $\mathbb{Q}$*, tal que* $x - n, x, x + n$ *são quadrados;*
- *(c)* $\exists$ *ponto* (x, y) $\mathbb{Q}$*-racional na cúbica* $C_n : y^2 = x^3 - n^2x$ *com* $y \neq 0$*;*

Assumindo o item 3 (e de alguns resultados) podemos concluir que existe infinidade de pontos $\mathbb{Q}$-racionais na cúbica. Assim, estudar o problema do número congruente equivale a estudar quando uma determinada curva de grau 3 admite uma infinidade de pontos $\mathbb{Q}$-racionais.

Demonstração

$(a) \Longrightarrow (b)$. Seja n inteiro congruente.Então, $\exists (a, b, c)$ triangulo racional tal que $a^2 + b^2 = c^2$ e $n = \frac{ab}{2}$. Defina $x = (\frac{c}{2})^2$. Nesse caso, $x - n = (\frac{a-b}{2})^2$ e $x + n = (\frac{a+b}{2})^2$ satisfaz (b).

Demonstração

$(a) \Longrightarrow (b)$. Seja n inteiro congruente.Então, $\exists (a, b, c)$ triangulo racional tal que $a^2 + b^2 = c^2$ e $n = \frac{ab}{2}$. Defina $x = (\frac{c}{2})^2$. Nesse caso, $x - n = (\frac{a-b}{2})^2$ e $x + n = (\frac{a+b}{2})^2$ satisfaz (b).

$(b) \Longrightarrow (a)$ Sejam $x - n, x, x + n$ quadrados em $\mathbb{Q}$. Definamos (a, b, c) pondo

$$a = (x + n)^{\frac{1}{2}} - (x - n)^{\frac{1}{2}}$$

$$b = (x + n)^{\frac{1}{2}} + (x - n)^{\frac{1}{2}}$$

$$c = 2x^{\frac{1}{2}}$$

Demonstração

$(b) \Longrightarrow (c)$ Suponhamos $x-n, x, x+n$ quadrados. Nesse caso, temos $(x-n)x(x+n)$ quadrado em $\mathbb{Q}$ e assim, obtemos $(x, y) \in C_n$ com $y \neq 0$.

Demonstração

$(b) \Longrightarrow (c)$ Suponhamos $x-n, x, x+n$ quadrados. Nesse caso, temos $(x-n)x(x+n)$ quadrado em $\mathbb{Q}$ e assim, obtemos $(x, y) \in C_n$ com $y \neq 0$.

A demonstração de $(c) \Longrightarrow b$ é mais interessante. De fato, seguirá de um critério para divisibilidade, em um certo sentido, na cúbica C_n. Antes de mostrar a implicação $(c) \Longrightarrow b$ precisamos estudar curvas que ocorrem no problema acima.

Plano $\mathbb{P}^2_{\mathbb{K}}$

Seja $\mathbb{K}$ um corpo. O plano projetivo $\mathbb{P}^2$ associado a $\mathbb{K}^3$ consiste no seguinte conjunto

$$\mathbb{P}^2_{\mathbb{K}} := \{v \in \mathbb{K}^3; \quad v \neq 0\}/\equiv$$

onde $v \equiv w \iff \exists \alpha \in \mathbb{K}^*$ tal que $v = \alpha w$.

Um elemento de $\mathbb{P}^2_{\mathbb{K}}$ é identificado, em $\mathbb{K}^3$, como um subespaço de dimensão 1 (reta pela origem).

Plano $\mathbb{P}^2_{\mathbb{K}}$

Seja $\mathbb{K}$ um corpo. O plano projetivo $\mathbb{P}^2$ associado a $\mathbb{K}^3$ consiste no seguinte conjunto

$$\mathbb{P}^2_{\mathbb{K}} := \{v \in \mathbb{K}^3; \quad v \neq 0\}/\equiv$$

onde $v \equiv w \iff \exists \alpha \in \mathbb{K}^*$ tal que $v = \alpha w$.

Um elemento de $\mathbb{P}^2_{\mathbb{K}}$ é identificado, em $\mathbb{K}^3$, como um subespaço de dimensão 1 (reta pela origem).Dado um ponto $(x, y, z) \in \mathbb{K}^3$ denotamos sua classe em $\mathbb{P}^2$ por $[x : y : z]$.

Plano $\mathbb{P}^2_{\mathbb{K}}$

Seja $\mathbb{K}$ um corpo. O plano projetivo $\mathbb{P}^2$ associado a $\mathbb{K}^3$ consiste no seguinte conjunto

$$\mathbb{P}^2_{\mathbb{K}} := \{v \in \mathbb{K}^3; \quad v \neq 0\}/\equiv$$

onde $v \equiv w \iff \exists \alpha \in \mathbb{K}^*$ tal que $v = \alpha w$.

Um elemento de $\mathbb{P}^2_{\mathbb{K}}$ é identificado, em $\mathbb{K}^3$, como um subespaço de dimensão 1 (reta pela origem).Dado um ponto $(x, y, z) \in \mathbb{K}^3$ denotamos sua classe em $\mathbb{P}^2$ por $[x : y : z]$.

Curvas projetivas X em $\mathbb{P}^2$ são curvas descritas por polinômios homogêneos. Os pontos da forma $[x : y : 0]$ são chamados de pontos no infinito.

As curvas que ocorrem no problema do número congruente são casos particulares das chamadas curvas elipticas. Mais geralmente, fixemos $\mathbb{K}$ corpo, com $char(\mathbb{K}) \neq 2, 3$. Curvas elipticas são curvas cúbicas projetivas não singulares descritas por equações do tipo:

$$\bar{C} : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \qquad a_i \in \mathbb{K}$$

As curvas que ocorrem no problema do número congruente são casos particulares das chamadas curvas elipticas. Mais geralmente, fixemos $\mathbb{K}$ corpo, com $char(\mathbb{K}) \neq 2, 3$. Curvas elipticas são curvas cúbicas projetivas não singulares descritas por equações do tipo:

$$\bar{C} : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \qquad a_i \in \mathbb{K}$$

Por meio de uma mudança de variáveis podemos reduzir curvas do tipo $\bar{C}$ a curvas do tipo:

$$C : y^2z = x^3 + Axz^2 + Bz^3 \qquad 4A^3 + 27B^2 \neq 0 \quad A, B \in \mathbb{K}$$

As curvas que ocorrem no problema do número congruente são casos particulares das chamadas curvas elipticas. Mais geralmente, fixemos $\mathbb{K}$ corpo, com $char(\mathbb{K}) \neq 2, 3$. Curvas elipticas são curvas cúbicas projetivas não singulares descritas por equações do tipo:

$$\bar{C} : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \qquad a_i \in \mathbb{K}$$

Por meio de uma mudança de variáveis podemos reduzir curvas do tipo $\bar{C}$ a curvas do tipo:

$$C : y^2z = x^3 + Axz^2 + Bz^3 \qquad 4A^3 + 27B^2 \neq 0 \quad A, B \in \mathbb{K}$$

Notemos que $[0 : 1 : 0]$ é o único ponto no infinito da cúbica.

As curvas que ocorrem no problema do número congruente são casos particulares das chamadas curvas elipticas. Mais geralmente, fixemos $\mathbb{K}$ corpo, com $char(\mathbb{K}) \neq 2, 3$. Curvas elipticas são curvas cúbicas projetivas não singulares descritas por equações do tipo:

$$\bar{C} : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \qquad a_i \in \mathbb{K}$$

Por meio de uma mudança de variáveis podemos reduzir curvas do tipo $\bar{C}$ a curvas do tipo:

$$C : y^2z = x^3 + Axz^2 + Bz^3 \qquad 4A^3 + 27B^2 \neq 0 \quad A, B \in \mathbb{K}$$

Notemos que $[0 : 1 : 0]$ é o único ponto no infinito da cúbica. Assim, podemos identificar o conjunto dos pontos $\mathbb{K}$ - racionais da cúbica projetiva com o conjunto:

$$C(\mathbb{K}) := \{(x, y) \in \mathbb{K}^2; \quad y^2 = x^3 + Ax + B, 4A^3 + 27B^2 \neq 0\} \cup \{O\}$$

Exemplos

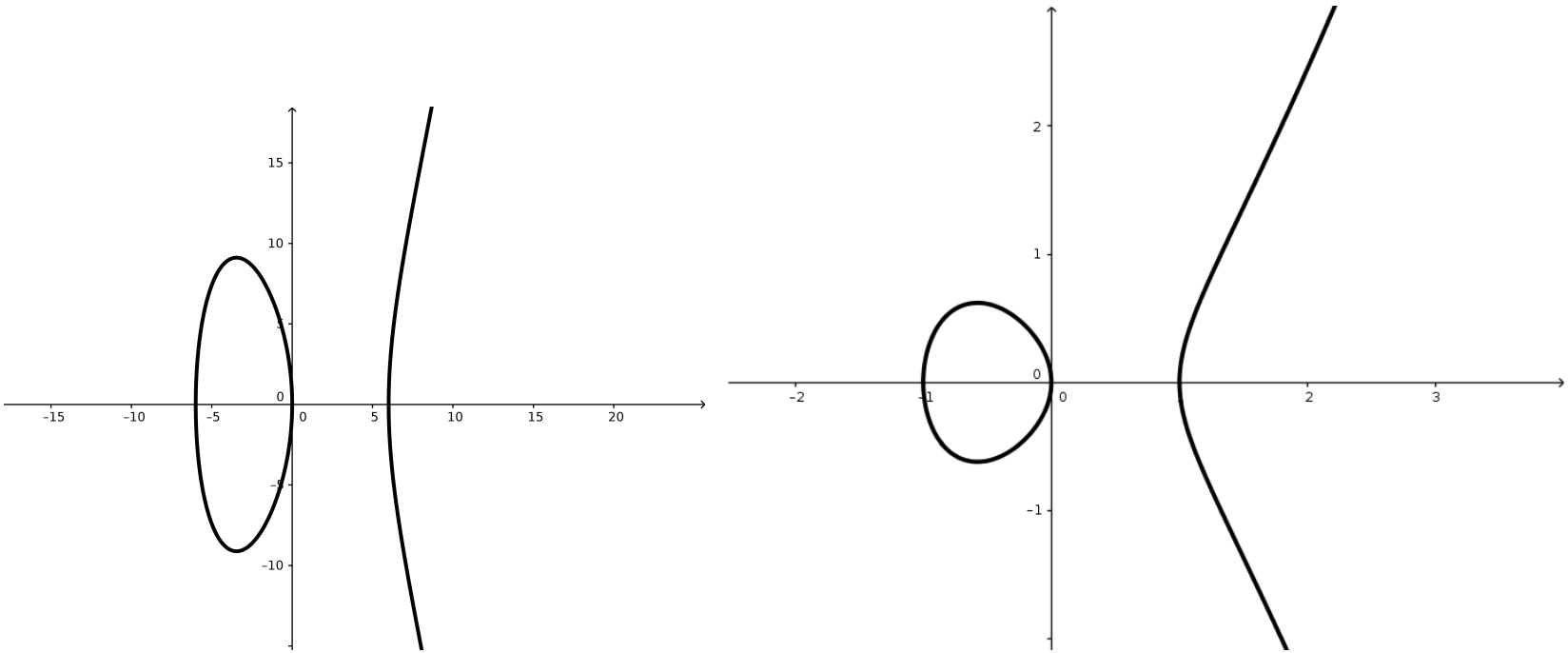
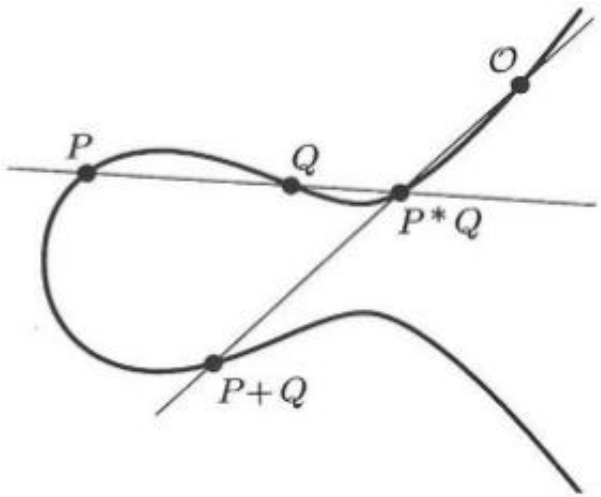


Figure: $C_1 : y^2 = x^3 - 36x$ e $C_2 : y^2 = x^3 - x$

Mais adiante, veremos que $\#C_1(\mathbb{Q})$ é infinito e $\#C_2(\mathbb{Q}) = 4$.

Lei de Grupo



Seja O um ponto fixo de $C(\mathbb{K})$ e P, Q pontos $\mathbb{K}$ - racionais. Definamos um operação $*$ que associa P, Q ao ponto $P * Q =$ terceiro ponto de interseção da reta PQ com a cúbica.
Usando O fixo, definamos outra operação pondo $P \oplus Q := O * (P * Q)$.

Lei de Grupo

Teorema

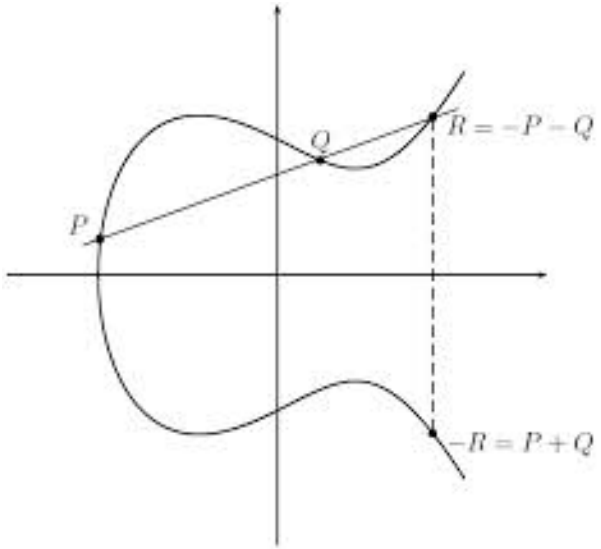
Seja C curva eliptica definida sobre $\mathbb{K}$ e considere o conjunto $C(\mathbb{K})$ munido da operação $\oplus$ definida acima. Então $(C(\mathbb{K}), \oplus)$ é um grupo abeliano, com o ponto O desempenhando o elemento neutro. Dado $P \in C(\mathbb{K})$ temos $-P = (O * O) * P$.

Mostra-se que a lei de grupo independe da escolha para o elemento neutro.

No que segue estaremos interessados no caso em que $\mathbb{K} = \mathbb{Q}$. Sendo $char(\mathbb{Q}) = 0$ podemos nesse caso trabalhar com a forma mais simples $y^2 = x^3 + Ax + B$ com $A, B \in \mathbb{Z}$ e $\triangle = 4A^3 + 27B^2 \neq 0$.

Curvas elipticas sobre $\mathbb{Q}$

Aqui tomaremos O o ponto no infinito da cúbica $C : y^2 = x^3 + Ax + B$ para desempenhar o elemento neutro. Nesse caso, fórmulas para a soma são simplificadas. O inverso de $P = (x, y)$, por exemplo, é $-P = (x, -y)$.



Denotamos o subgrupo dos pontos de ordem dividindo n por $C[n]$.

Curvas elipticas sobre $\mathbb{Q}$

Teorema (Mordell, 1922)

$C(\mathbb{Q})$ é finitamente gerado.

Curvas elipticas sobre $\mathbb{Q}$

Teorema (Mordell, 1922)

$C(\mathbb{Q})$ é finitamente gerado.

Assim, pelo teorema da estrutura para grupos abelianos finitamente gerados, temos

$$C(\mathbb{Q}) \simeq \mathbb{Z}^r \times C(\mathbb{Q})_{tor}$$

Curvas elipticas sobre $\mathbb{Q}$

Teorema (Mordell, 1922)

$C(\mathbb{Q})$ é finitamente gerado.

Assim, pelo teorema da estrutura para grupos abelianos finitamente gerados, temos

$$C(\mathbb{Q}) \simeq \mathbb{Z}^r \times C(\mathbb{Q})_{tor}$$

O teorema garante que $\exists\{P_1, ..., P_r\}$ pontos de ordem infinita, independentes, e $\{Q_1, ..., Q_k\}$ pontos de ordem finita, tais que $\forall P \in C(\mathbb{Q})$ se escreve como:

$$P = n_1 P_1 + ... + n_r P_r + m_1 Q_1 + ... + m_k Q_k$$

com inteiros n_i, m_j

Curvas elipticas sobre $\mathbb{Q}$

O inteiro r é chamado o posto de $C(\mathbb{Q})$ e determiná-lo é um problema dificil. Não se sabe o quanto pode ser grande. Em 2006, Elkies exibiu uma curva eliptica com $r \geq 28$ e esse é o maior exemplo conhecido.

Curvas elipticas sobre $\mathbb{Q}$

O inteiro r é chamado o posto de $C(\mathbb{Q})$ e determiná-lo é um problema dificil. Não se sabe o quanto pode ser grande. Em 2006, Elkies exibiu uma curva eliptica com $r \geq 28$ e esse é o maior exemplo conhecido.

Por outro lado, a parte de torção é bem conhecida e de fato computável:

Curvas elipticas sobre $\mathbb{Q}$

O inteiro r é chamado o posto de $C(\mathbb{Q})$ e determiná-lo é um problema dificil. Não se sabe o quanto pode ser grande. Em 2006, Elkies exibiu uma curva eliptica com $r \geq 28$ e esse é o maior exemplo conhecido.

Por outro lado, a parte de torção é bem conhecida e de fato computável:

Teorema (Nagell-Lutz)

Seja $C : y^2 = x^3 + Ax + B$ *curva eliptica e* $\triangle = 4A^3 + 27B^2$

(I) Se $P = (x, y) \in C(\mathbb{Q})_{tor} \Longrightarrow x, y \in \mathbb{Z}$ *e* $y = 0$ *ou* $y^2 | \triangle$;

Curvas elipticas sobre $\mathbb{Q}$

O inteiro r é chamado o posto de $C(\mathbb{Q})$ e determiná-lo é um problema dificil. Não se sabe o quanto pode ser grande. Em 2006, Elkies exibiu uma curva eliptica com $r \geq 28$ e esse é o maior exemplo conhecido.

Por outro lado, a parte de torção é bem conhecida e de fato computável:

Teorema (Nagell-Lutz)

Seja $C : y^2 = x^3 + Ax + B$ *curva eliptica e* $\triangle = 4A^3 + 27B^2$

(I) Se $P = (x, y) \in C(\mathbb{Q})_{tor} \Longrightarrow x, y \in \mathbb{Z}$ *e* $y = 0$ *ou* $y^2 | \triangle$;

(II) Se $p \in \mathbb{Z} > 2$ *é um primo tal que* $p \nmid \triangle$ *então o mapa:*

$$C(\mathbb{Q})_{tor} \xrightarrow{\pi} C(\mathbb{F}_p)$$

que associa $(x, y) \longmapsto (\bar{x}, \bar{y})$ *e* $O \longmapsto \bar{O}$ *é homomorfismo injetivo;*

Aplicação

Dada $C_n : y^2 = x^3 - n^2x$ mostraremos que $C_n(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Mas antes precisamos do seguinte

Aplicação

Dada $C_n : y^2 = x^3 - n^2x$ mostraremos que $C_n(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Mas antes precisamos do seguinte

Lema

Seja $C : y^2 = x^3 + bx$, *com* b *inteiro e* $\triangle = 4b^3$. *Então,*
$\#C(\mathbb{F}_p) = p + 1 \quad \forall p \equiv 3 < 4 >, \quad p \nmid \triangle$, p *primo.*

Aplicação

Dada $C_n : y^2 = x^3 - n^2x$ mostraremos que $C_n(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Mas antes precisamos do seguinte

Lema

Seja $C : y^2 = x^3 + bx$, *com* b *inteiro e* $\triangle = 4b^3$. *Então,*
$\#C(\mathbb{F}_p) = p + 1 \quad \forall p \equiv 3 < 4 >, \quad p \nmid \triangle$, p *primo.*

Prova

Ora, fixemos $p \equiv 3 < 4 >$. *Nesse caso* $-1 \notin \mathbb{F}_p^{*^2}$ *e dado* $x \in \mathbb{F}_p^*$ *temos* $x \in \mathbb{F}_p^{*^2} \iff -x \notin \mathbb{F}_p^{*^2}$.

Aplicação

Dada $C_n : y^2 = x^3 - n^2x$ mostraremos que $C_n(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Mas antes precisamos do seguinte

Lema

Seja $C : y^2 = x^3 + bx$, com b inteiro e $\triangle = 4b^3$. Então,
$\#C(\mathbb{F}_p) = p + 1 \quad \forall p \equiv 3 < 4 >, \quad p \nmid \triangle$, *$p$ primo.*

Prova

Ora, fixemos $p \equiv 3 < 4 >$. Nesse caso $-1 \notin \mathbb{F}_p^{*^2}$ e dado $x \in \mathbb{F}_p^*$ temos $x \in \mathbb{F}_p^{*^2} \iff -x \notin \mathbb{F}_p^{*^2}$.Além disso, a função $f(x) = x^3 + bx$ é impar e assim, também temos $f(x) \in \mathbb{F}_p^{*^2} \iff -f(x) = f(-x) \notin \mathbb{F}_p^{*^2}$.

Aplicação

Dada $C_n : y^2 = x^3 - n^2x$ mostraremos que $C_n(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Mas antes precisamos do seguinte

Lema

Seja $C : y^2 = x^3 + bx$, com b inteiro e $\triangle = 4b^3$. Então,
$\#C(\mathbb{F}_p) = p + 1 \quad \forall p \equiv 3 < 4 >, \quad p \nmid \triangle$, *$p$ primo.*

Prova

Ora, fixemos $p \equiv 3 < 4 >$. Nesse caso $-1 \notin \mathbb{F}_p^{*^2}$ e dado $x \in \mathbb{F}_p^*$ temos $x \in \mathbb{F}_p^{*^2} \iff -x \notin \mathbb{F}_p^{*^2}$.Além disso, a função $f(x) = x^3 + bx$ é impar e assim, também temos $f(x) \in \mathbb{F}_p^{*^2} \iff -f(x) = f(-x) \notin \mathbb{F}_p^{*^2}$.

Percorrendo o grupo $\mathbb{F}_p^*$ obtemos $\frac{p-1}{2}$ possibilidades para coordenadas x (valores para os quais $f(x)$ é quadrado). Mas para cada contribuição de x obtemos 2 valores para y.

Aplicação

Dada $C_n : y^2 = x^3 - n^2x$ mostraremos que $C_n(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Mas antes precisamos do seguinte

Lema

Seja $C : y^2 = x^3 + bx$, com b inteiro e $\triangle = 4b^3$. Então,
$\#C(\mathbb{F}_p) = p + 1 \quad \forall p \equiv 3 < 4 >, \quad p \nmid \triangle$, *$p$ primo.*

Prova

Ora, fixemos $p \equiv 3 < 4 >$. Nesse caso $-1 \notin \mathbb{F}_p^{*^2}$ e dado $x \in \mathbb{F}_p^*$ temos $x \in \mathbb{F}_p^{*^2} \iff -x \notin \mathbb{F}_p^{*^2}$.Além disso, a função $f(x) = x^3 + bx$ é impar e assim, também temos $f(x) \in \mathbb{F}_p^{*^2} \iff -f(x) = f(-x) \notin \mathbb{F}_p^{*^2}$.

Percorrendo o grupo $\mathbb{F}_p^*$ obtemos $\frac{p-1}{2}$ possibilidades para coordenadas x (valores para os quais $f(x)$ é quadrado). Mas para cada contribuição de x obtemos 2 valores para y.Daí, temos $p-1$ pontos. Considerando $(0,0)$ e O obtemos $p+1$ pontos no grupo $C(\mathbb{F}_p)$.

Aplicação

Proposição

Seja $C_n : y^2 = x^3 - n^2x$ *a cúbica associada ao problema do inteiro congruente. Então* $C_n(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Aplicação

Proposição

Seja $C_n : y^2 = x^3 - n^2x$ a cúbica associada ao problema do inteiro congruente. Então $C_n(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Prova

Como $C[2] = \{O, (0,0), (n,0), (-n,0)\} \subset C(\mathbb{Q})_{tor}$ é suficiente mostrarmos que $\#C(\mathbb{Q})_{tor} | 4$.

Aplicação

Proposição

Seja $C_n : y^2 = x^3 - n^2x$ a cúbica associada ao problema do inteiro congruente. Então $C_n(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Prova

Como $C[2] = \{O, (0,0), (n,0), (-n,0)\} \subset C(\mathbb{Q})_{tor}$ é suficiente mostrarmos que $\#C(\mathbb{Q})_{tor}|4$.Para esse fim, vamos usar o teorema de primos em progressão de Dirichlet: $\exists$ infinidade de primos da forma $p \equiv a < b >$ com a e b coprimos.

Aplicação

Proposição

Seja $C_n : y^2 = x^3 - n^2x$ a cúbica associada ao problema do inteiro congruente. Então $C_n(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Prova

Como $C[2] = \{O, (0,0), (n,0), (-n,0)\} \subset C(\mathbb{Q})_{tor}$ é suficiente mostrarmos que $\#C(\mathbb{Q})_{tor}|4$.Para esse fim, vamos usar o teorema de primos em progressão de Dirichlet: $\exists$ infinidade de primos da forma $p \equiv a < b >$ com a e b coprimos.Mostremos os seguintes fatos:

- *(i) $8 \nmid \#C(\mathbb{Q})_{tor}$;*
- *(ii) $3 \nmid \#C(\mathbb{Q})_{tor}$;*
- *(iii) $q \nmid \#C(\mathbb{Q})_{tor} \quad \forall q > 3$ primo;*

(i) Se $8 \mid \#C(\mathbb{Q})_{tor}$, podemos encontrar $p \equiv 3 < 8 >$ e $p \nmid \triangle$ tal que $8 \mid \#C(\mathbb{F}_p) = p + 1$. Mas daí, $p + 1 \equiv 0 < 8 > \Longrightarrow p \equiv 7 < 8 >$, contradição.

(i) Se $8 \mid \#C(\mathbb{Q})_{tor}$, podemos encontrar $p \equiv 3 < 8 >$ e $p \nmid \triangle$ tal que $8 \mid \#C(\mathbb{F}_p) = p + 1$. Mas daí, $p + 1 \equiv 0 < 8 > \Longrightarrow p \equiv 7 < 8 >$, contradição.

(ii) Se $3 \mid \#C(\mathbb{Q})_{tor}$ temos $3 \mid p + 1$ por algum $p \equiv 7 < 12 >$ e $p \nmid \triangle$. Daí, $p + 1 \equiv 0 < 3 > \Longrightarrow p \equiv -1 < 3 >$ uma contradição, já que a escolha de p implica $p \equiv 1 < 3 >$.

(i) Se $8 \mid \#C(\mathbb{Q})_{tor}$, podemos encontrar $p \equiv 3 < 8 >$ e $p \nmid \triangle$ tal que $8 \mid \#C(\mathbb{F}_p) = p + 1$. Mas daí, $p + 1 \equiv 0 < 8 > \Longrightarrow p \equiv 7 < 8 >$, contradição.

(ii) Se $3 \mid \#C(\mathbb{Q})_{tor}$ temos $3 \mid p + 1$ por algum $p \equiv 7 < 12 >$ e $p \nmid \triangle$. Daí, $p + 1 \equiv 0 < 3 > \Longrightarrow p \equiv -1 < 3 >$ uma contradição, já que a escolha de p implica $p \equiv 1 < 3 >$.

(iii)Se $q > 3$ é tal que $q \mid \#C(\mathbb{Q})_{tor}$ tomemos p primo com $p \equiv 3 < 4q >$ e $p \nmid \triangle$. Temos $q \mid \#C(\mathbb{Q})_{tor} \Longrightarrow q \mid \#C(\mathbb{F}_p) = p + 1 \Longrightarrow p \equiv -1 < q >$, o que contradiz a escoha de p já que $p \equiv 3 < 4q > \Longrightarrow p \equiv 3 < q >$.

Dos possíveis divisores de $\#C(\mathbb{Q})_{tor}$ temos $C[2] = C(\mathbb{Q})_{tor}$.

(i) Se $8 \mid \#C(\mathbb{Q})_{tor}$, podemos encontrar $p \equiv 3 < 8 >$ e $p \nmid \triangle$ tal que $8 \mid \#C(\mathbb{F}_p) = p + 1$. Mas daí, $p + 1 \equiv 0 < 8 > \Longrightarrow p \equiv 7 < 8 >$, contradição.

(ii) Se $3 \mid \#C(\mathbb{Q})_{tor}$ temos $3 \mid p + 1$ por algum $p \equiv 7 < 12 >$ e $p \nmid \triangle$. Daí, $p + 1 \equiv 0 < 3 > \Longrightarrow p \equiv -1 < 3 >$ uma contradição, já que a escolha de p implica $p \equiv 1 < 3 >$.

(iii)Se $q > 3$ é tal que $q \mid \#C(\mathbb{Q})_{tor}$ tomemos p primo com $p \equiv 3 < 4q >$ e $p \nmid \triangle$. Temos $q \mid \#C(\mathbb{Q})_{tor} \Longrightarrow q \mid \#C(\mathbb{F}_p) = p + 1 \Longrightarrow p \equiv -1 < q >$, o que contradiz a escoha de p já que $p \equiv 3 < 4q > \Longrightarrow p \equiv 3 < q >$.

Dos possíveis divisores de $\#C(\mathbb{Q})_{tor}$ temos $C[2] = C(\mathbb{Q})_{tor}$.

Corolário

$rank(C_n(\mathbb{Q})) = 0 \Longleftrightarrow$ n não é congruente.

Teorema de Mordell

Seguirá de dois resultados:

- $C(\mathbb{Q})/2C(\mathbb{Q})$ é finito;
- O grupo $C(\mathbb{Q})$ é normado

Teorema de Mordell

Seguirá de dois resultados:

- $C(\mathbb{Q})/2C(\mathbb{Q})$ é finito;
- O grupo $C(\mathbb{Q})$ é normado, no seguinte sentido:

$\exists$ uma função $\hat{h} : C(\mathbb{Q}) \longrightarrow \mathbb{R} \geq 0$ satisfazendo as seguintes propriedades:

- $\hat{h}(2P) = 4\hat{h}(P) \quad \forall P \in C(\mathbb{Q})$;

Teorema de Mordell

Seguirá de dois resultados:

- $C(\mathbb{Q})/2C(\mathbb{Q})$ é finito;
- O grupo $C(\mathbb{Q})$ é normado, no seguinte sentido:

$\exists$ uma função $\hat{h} : C(\mathbb{Q}) \longrightarrow \mathbb{R} \geq 0$ satisfazendo as seguintes propriedades:

- $\hat{h}(2P) = 4\hat{h}(P) \quad \forall P \in C(\mathbb{Q})$;
- $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q) \quad \forall P, Q \in C(\mathbb{Q})$ (Lei do paralelogramo)

Teorema de Mordell

Seguirá de dois resultados:

- $C(\mathbb{Q})/2C(\mathbb{Q})$ é finito;
- O grupo $C(\mathbb{Q})$ é normado, no seguinte sentido:

$\exists$ uma função $\hat{h} : C(\mathbb{Q}) \longrightarrow \mathbb{R} \geq 0$ satisfazendo as seguintes propriedades:

- $\hat{h}(2P) = 4\hat{h}(P) \quad \forall P \in C(\mathbb{Q})$;
- $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q) \quad \forall P, Q \in C(\mathbb{Q})$ (Lei do paralelogramo)
- Dado $c \in \mathbb{R} \geq 0$ conjunto $S_c := \{P \in C(\mathbb{Q}); \quad \hat{h}(P) \leq c\}$ é finito;

Teorema de Mordell

Assumindo os resultados acima, o seguinte teorema garante a finitude:

Teorema

Seja G um grupo abeliano tal que G/mG é finito por algum $m \in \mathbb{Z}$ e seja $\hat{h} : G \longrightarrow \mathbb{R} \geq 0$ uma função satisfazendo as propriedades acima. Então G é finitamente gerado.

Teorema de Mordell

Assumindo os resultados acima, o seguinte teorema garante a finitude:

Teorema

Seja G um grupo abeliano tal que G/mG é finito por algum $m \in \mathbb{Z}$ e seja $\hat{h} : G \longrightarrow \mathbb{R} \geq 0$ uma função satisfazendo as propriedades acima. Então G é finitamente gerado.

No caso $G = C(\mathbb{Q})$, a finitude do índice seguirá de um critério para divisibilidade por 2 no grupo $C(\mathbb{Q})$. Aqui, assumimos $C : y^2 = (x - \alpha)(x - \beta)(x - \gamma)$ com α, β e $\gamma \in \mathbb{Z}$.

$[C(\mathbb{Q}) : 2C(\mathbb{Q})] < \infty$

Teorema

Seja C curva eliptica acima e (x_1, y_1) um ponto $\mathbb{Q}$-racional. Existe $(x_2, y_2) \in C(\mathbb{Q})$ tal que $2(x_2, y_2) = (x_1, y_1) \iff x_1 - \alpha$, $x_1 - \beta$, $x_1 - \gamma$ são quadrados em $\mathbb{Q}$.

$[C(\mathbb{Q}) : 2C(\mathbb{Q})] < \infty$

Teorema

Seja C curva eliptica acima e (x_1, y_1) um ponto $\mathbb{Q}$-racional. Existe $(x_2, y_2) \in C(\mathbb{Q})$ tal que $2(x_2, y_2) = (x_1, y_1) \iff x_1 - \alpha$, $x_1 - \beta$, $x_1 - \gamma$ são quadrados em $\mathbb{Q}$.

O teorema acima pode ser usado para completar as formulações equivalentes de um inteiro congruente.

$[C(\mathbb{Q}) : 2C(\mathbb{Q})] < \infty$

Teorema

Seja C curva eliptica acima e (x_1, y_1) um ponto $\mathbb{Q}$-racional. Existe $(x_2, y_2) \in C(\mathbb{Q})$ tal que $2(x_2, y_2) = (x_1, y_1) \iff x_1 - \alpha$, $x_1 - \beta$, $x_1 - \gamma$ são quadrados em $\mathbb{Q}$.

O teorema acima pode ser usado para completar as formulações equivalentes de um inteiro congruente. De fato, suponhamos (x, y) ponto da cúbica $y^2 = x^3 - n^2x$ com $y \neq 0$. Como os pontos de ordem 2 são $\{O, (n, 0), (-n, 0), (0, 0)\}$ segue que $P = (x, y)$ não possui ordem 2.

$[C(\mathbb{Q}) : 2C(\mathbb{Q})] < \infty$

Teorema

Seja C curva eliptica acima e (x_1, y_1) um ponto $\mathbb{Q}$-racional. Existe $(x_2, y_2) \in C(\mathbb{Q})$ tal que $2(x_2, y_2) = (x_1, y_1) \iff x_1 - \alpha$, $x_1 - \beta$, $x_1 - \gamma$ são quadrados em $\mathbb{Q}$.

O teorema acima pode ser usado para completar as formulações equivalentes de um inteiro congruente. De fato, suponhamos (x, y) ponto da cúbica $y^2 = x^3 - n^2x$ com $y \neq 0$. Como os pontos de ordem 2 são $\{O, (n, 0), (-n, 0), (0, 0)\}$ segue que $P = (x, y)$ não possui ordem 2. Assim, duplicando P, obtemos outro ponto (x_1, y_1). Pelo critério acima, vemos que $x_1 - n$, x_1, $x_1 - n$ são quadrados e daí, segue a implicação $(c) \Longrightarrow (b)$.

Usando o critério de divisibilidade, pode-se mostrar que a seguinte sequência

$$0 \longrightarrow 2C(\mathbb{Q}) \xrightarrow{i} C(\mathbb{Q}) \xrightarrow{\Phi_\alpha \times \Phi_\beta} (\mathbb{Q}^*/\mathbb{Q}^{*2})^2$$

é exata

Usando o critério de divisibilidade, pode-se mostrar que a seguinte sequência

$$0 \longrightarrow 2C(\mathbb{Q}) \xrightarrow{i} C(\mathbb{Q}) \xrightarrow{\Phi_\alpha \times \Phi_\beta} (\mathbb{Q}^*/\mathbb{Q}^{*^2})^2$$

é exata , onde
$\Phi_\alpha : C(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*^2}$ é definido por:

$$\Phi_\alpha(x,y) = \begin{cases} (x-\alpha)\mathbb{Q}^{*^2} & \text{se} \quad P \notin \{(\alpha,0), O\}; \\ (\alpha-\beta)(\alpha-\gamma)\mathbb{Q}^{*^2} & \text{se} \quad P = (\alpha,0); \\ 1.\mathbb{Q}^{*^2} & \text{se} \quad P = O; \end{cases}$$

Φ_β é definido de maneira similar.

Usando o critério de divisibilidade, pode-se mostrar que a seguinte sequência

$$0 \longrightarrow 2C(\mathbb{Q}) \xrightarrow{i} C(\mathbb{Q}) \xrightarrow{\Phi_\alpha \times \Phi_\beta} (\mathbb{Q}^*/\mathbb{Q}^{*^2})^2$$

é exata , onde
$\Phi_\alpha : C(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*^2}$ é definido por:

$$\Phi_\alpha(x,y) = \begin{cases} (x-\alpha)\mathbb{Q}^{*^2} & \text{se} \quad P \notin \{(\alpha,0), O\}; \\ (\alpha-\beta)(\alpha-\gamma)\mathbb{Q}^{*^2} & \text{se} \quad P = (\alpha,0); \\ 1.\mathbb{Q}^{*^2} & \text{se} \quad P = O; \end{cases}$$

Φ_β é definido de maneira similar. E
$Im(\Phi_\alpha \times \Phi_\beta) \subset \{((-1)^{\alpha_0} p_1^{\alpha_1} ... p_k^{\alpha_k}, (-1)^{\beta_0} p_1^{\beta_1} ... p_k^{\beta_k}); \quad p_j \mid \triangle \text{ e } \alpha_i, \beta_j \in \{0,1\}\}$

O problema do Posto

O seguinte resultado permite determinar uma cota superior para o posto de curvas elipticas da forma: $C : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$, com $\alpha, \beta, \gamma \in \mathbb{Z}$ e $\triangle = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$.

Proposição

$r \leq 2\#\{p \text{ primo}; \quad p \mid \triangle\}$

A cota acima pode ser refinada. Um primo p se diz **mau** se p divide exatamente um dos fatores $(\alpha-\beta), (\alpha-\gamma), (\beta-\gamma)$ de $\triangle$. Se diz, **muito mau** se p divide todos os fatores.

O problema do Posto

O seguinte resultado permite determinar uma cota superior para o posto de curvas elipticas da forma: $C : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$, com $\alpha, \beta, \gamma \in \mathbb{Z}$ e $\triangle = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$.

Proposição

$r \leq 2\#\{p \text{ primo}; \quad p \mid \triangle\}$

A cota acima pode ser refinada. Um primo p se diz **mau** se p divide exatamente um dos fatores $(\alpha-\beta), (\alpha-\gamma), (\beta-\gamma)$ de $\triangle$. Se diz, **muito mau** se p divide todos os fatores.

Proposição

$r \leq t_1 + 2t_2 - 1$ *onde* $t_1 = \{p \text{ primo}; \quad p \mid \triangle$ *é mau*$\}$ *e* $t_2 = \{p$ *primo*; $\quad p \mid \triangle$ *é muito mau*$\}$

Exemplos

- $C_1 : y^2 = x^3 - x = (x-1)x(x+1)$ tem posto 0. Aqui $\triangle = (1-0)^2(-1-0)^2(1+1)^2 = 4$. Assim, $t_1 = 1$ e $t_2 = 0$. Pela cota do posto acima, temos $r \leq t_1 + 2t_2 - 1 = 0$;

Exemplos

- $C_1 : y^2 = x^3 - x = (x-1)x(x+1)$ tem posto 0. Aqui $\triangle = (1-0)^2(-1-0)^2(1+1)^2 = 4$. Assim, $t_1 = 1$ e $t_2 = 0$. Pela cota do posto acima, temos $r \leq t_1 + 2t_2 - 1 = 0$;

- Vimos anteriormente que $5, 6$ e 7 são congruentes. Assim, as curvas $y^2 = x^3 - 25x$, $y^2 = x^3 - 36x$ e $y^2 = x^3 - 49x$ admitem infinidade de pontos $\mathbb{Q}$-racionais;

Exemplos

- $C_1 : y^2 = x^3 - x = (x-1)x(x+1)$ tem posto 0. Aqui $\triangle = (1-0)^2(-1-0)^2(1+1)^2 = 4$. Assim, $t_1 = 1$ e $t_2 = 0$. Pela cota do posto acima, temos $r \leq t_1 + 2t_2 - 1 = 0$;

- Vimos anteriormente que $5, 6$ e 7 são congruentes. Assim, as curvas $y^2 = x^3 - 25x$, $y^2 = x^3 - 36x$ e $y^2 = x^3 - 49x$ admitem infinidade de pontos $\mathbb{Q}$-racionais;

- Considere $y^2 = x^3 + 8$, com $\triangle = 27.8^2$. Aplicando redução mod p para $p = 5, 13$ obtemos: $\#C(\mathbb{F}_5) = 6$ e $\#C(\mathbb{F}_{13}) = 16$. Do teorema de Nagell-Lutz, temos $\#C(\mathbb{Q})_{tor} \mid 2.3, 2^4 \Longrightarrow \#C(\mathbb{Q})_{tor} = 1, 2$. Como $\{O, (-2, 0)\} \subset C(\mathbb{Q})_{tor}$ temos que $C(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z}$. Note que $(1, \pm 3) \in C(\mathbb{Q}) \Longrightarrow rank(C) \geq 1$.

Mordell Geral

O caso geral, i.é, para cúbicas do tipo $y^2 = p(x)$ com $p(x) \in \mathbb{Z}[x]$ de grau 3 seguirá de algumas considerações sobre números algébricos. O problema consiste em mostrar que $[C(\mathbb{K}) : 2C(\mathbb{K})]$ é finito, onde $\mathbb{K}$ é o corpo de decomposição do polinômio $p(x)$.

Mordell Geral

O caso geral, i.é, para cúbicas do tipo $y^2 = p(x)$ com $p(x) \in \mathbb{Z}[x]$ de grau 3 seguirá de algumas considerações sobre números algébricos. O problema consiste em mostrar que $[C(\mathbb{K}) : 2C(\mathbb{K})]$ é finito, onde $\mathbb{K}$ é o corpo de decomposição do polinômio $p(x)$.

- $[C(\mathbb{K}) : 2C(\mathbb{K})]$ finito mostra o teorema de Mordell para cúbicas sobre $\mathbb{K}$, e precisamos de informações sobre $\mathbb{Q}$.

Mordell Geral

O caso geral, i.é, para cúbicas do tipo $y^2 = p(x)$ com $p(x) \in \mathbb{Z}[x]$ de grau 3 seguirá de algumas considerações sobre números algébricos. O problema consiste em mostrar que $[C(\mathbb{K}) : 2C(\mathbb{K})]$ é finito, onde $\mathbb{K}$ é o corpo de decomposição do polinômio $p(x)$.

- $[C(\mathbb{K}) : 2C(\mathbb{K})]$ finito mostra o teorema de Mordell para cúbicas sobre $\mathbb{K}$, e precisamos de informações sobre $\mathbb{Q}$.
- A demonstração do caso sobre $\mathbb{Q}$ está relacionada algumas propriedades do anel de inteiros de $\mathbb{Q}$ tais como como fatoração única e a finitude do grupo de unidades.

Fatoração única não vale em geral para o anel de inteiros de uma extensão finita $\mathbb{K}/\mathbb{Q}$. Tome, por exemplo, $(1 - \sqrt{-5})(1 + \sqrt{-5}) = 2.3$ em $\mathbb{Z}[\sqrt{-5}]$.

Referências

[1] Silverman, Joseph H., and John Tate. Rational Points on Elliptic Curves. Springer Science Business Media, 1992;

[2] Knapp, Anthony W. Elliptic curves. Vol. 40. Princeton University Press, 1992;

[3] Husemöller, Dale. "Elliptic curves, volume 111 of Graduate Texts in Mathematics." (2004);

[4] Conrad, Keith. "The congruent number problem." The Harvard College Mathematics Review 2 (2008): 58-74;

Obrigado!!!