Computing continued fractions on real quadratic fields

Xevi Guitart[1] Marc Masdeu[2]

[1]Universitat Politècnica de Catalunya

[2]Columbia University

Cuartas Jornadas de Teoría de Números

Índex

Fracciones contínuas: caso clásico

Dados $q_1, q_2, q_3 \ldots, q_n \in \mathbb{Z}$, su fracción contínua (finita) es:

$$[q_1, q_2, \ldots, q_n] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}} \in \mathbb{Q}$$

Fracciones contínuas: caso clásico

Dados $q_1, q_2, q_3 \ldots, q_n \in \mathbb{Z}$, su fracción contínua (finita) es:

$$[q_1, q_2, \ldots, q_n] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}} \in \mathbb{Q}$$

Teorema (Clásico)

Todo $x \in \mathbb{Q}$ es una fracción contínua finita.

Fracciones contínuas: caso clásico

Dados $q_1, q_2, q_3 \ldots, q_n \in \mathbb{Z}$, su fracción contínua (finita) es:

$$[q_1, q_2, \ldots, q_n] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}} \in \mathbb{Q}$$

Teorema (Clásico)

Todo $x \in \mathbb{Q}$ es una fracción contínua finita.

Se puede calcular eficientemente: si $x = a/b$

$$\begin{aligned} a &= q_1 b + r_1, \quad \text{con } |r_1| < |b| \\ b &= q_2 r_1 + r_2, \quad \text{con } |r_2| < |r_1| \\ r_2 &= q_3 r_1 + r_3, \quad \text{con } |r_3| < |r_2| \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} \end{aligned}$$

y entonces $x = [q_1, q_2, \ldots, q_n]$.

Fracciones contínuas en cuerpos de números

Sea F un cuerpo de números con anillo de enteros $\mathcal{O}_F$.
Dados $q_1, q_2, \ldots, q_n \in \mathcal{O}_F$ definimos la fracción contínua

$$[q_1, q_2, \ldots, q_n] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}} \in F$$

Fracciones contínuas en cuerpos de números

Sea F un cuerpo de números con anillo de enteros $\mathcal{O}_F$.
Dados $q_1, q_2, \ldots, q_n \in \mathcal{O}_F$ definimos la fracción contínua

$$[q_1, q_2, \ldots, q_n] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}} \in F$$

- Es cierto que todo $x \in F$ es una fracción continua?

Fracciones contínuas en cuerpos de números

Sea F un cuerpo de números con anillo de enteros $\mathcal{O}_F$.
Dados $q_1, q_2, \ldots, q_n \in \mathcal{O}_F$ definimos la fracción contínua

$$[q_1, q_2, \ldots, q_n] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}} \in F$$

- Es cierto que todo $x \in F$ es una fracción continua?

Teorema (Cooke-Vaserštein)

Si F no es cuadrático imaginario, entonces todo $x \in F$ es una fracción contínua con coeficientes en $\mathcal{O}_F$ si y sólo si $h(F) = 1$.

Fracciones contínuas en cuerpos de números

Sea F un cuerpo de números con anillo de enteros $\mathcal{O}_F$.
Dados $q_1, q_2, \ldots, q_n \in \mathcal{O}_F$ definimos la fracción contínua

$$[q_1, q_2, \ldots, q_n] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}} \in F$$

- Es cierto que todo $x \in F$ es una fracción continua?

Teorema (Cooke-Vaserštein)

Si F no es cuadrático imaginario, entonces todo $x \in F$ es una fracción contínua con coeficientes en $\mathcal{O}_F$ si y sólo si $h(F) = 1$.

- El algoritmo clásico funciona, sólo si F es euclídeo.

Fracciones contínuas en cuerpos de números

Sea F un cuerpo de números con anillo de enteros $\mathcal{O}_F$.
Dados $q_1, q_2, \ldots, q_n \in \mathcal{O}_F$ definimos la fracción contínua

$$[q_1, q_2, \ldots, q_n] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}} \in F$$

- Es cierto que todo $x \in F$ es una fracción continua?

Teorema (Cooke-Vaserštein)

Si F no es cuadrático imaginario, entonces todo $x \in F$ es una fracción contínua con coeficientes en $\mathcal{O}_F$ si y sólo si $h(F) = 1$.

- El algoritmo clásico funciona, sólo si F es euclídeo.
- Los únicos cuerpos cuadráticos reales euclídeos son $\mathbb{Q}(\sqrt{m})$, con

$$m \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$$

(Oppenheim, Erdos, Brauer, Davenport, Swinnerton-Dyer,...)

Fracciones contínuas en cuerpos de números

Sea F un cuerpo de números con anillo de enteros $\mathcal{O}_F$.
Dados $q_1, q_2, \ldots, q_n \in \mathcal{O}_F$ definimos la fracción contínua

$$[q_1, q_2, \ldots, q_n] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}} \in F$$

- Es cierto que todo $x \in F$ es una fracción continua?

Teorema (Cooke-Vaserštein)

Si F no es cuadrático imaginario, entonces todo $x \in F$ es una fracción contínua con coeficientes en $\mathcal{O}_F$ si y sólo si $h(F) = 1$.

- El algoritmo clásico funciona, sólo si F es euclídeo.
- Los únicos cuerpos cuadráticos reales euclídeos son $\mathbb{Q}(\sqrt{m})$, con

$$m \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$$

(Oppenheim, Erdos, Brauer, Davenport, Swinnerton-Dyer,...)

Objetivo

F cuadrático real, $h(F) = 1$: algoritmo para calcular f.c. de $x \in F$

Algunas aplicaciones: formas modulares

- Fracciones contínuas en $\mathbb{Q}$:
  - Se utilizan en el llamado Truco de Manin, para el cálculo de símbolos modulares.

Algunas aplicaciones: formas modulares

- Fracciones contínuas en $\mathbb{Q}$:
  - Se utilizan en el llamado Truco de Manin, para el cálculo de símbolos modulares.
- Fracciones contínuas en F:
  - Análogamente, aparecen en el algoritmo de símbolos modulares para formas modulares de Hilbert sobre F.

Algunas aplicaciones: formas modulares

- Fracciones contínuas en $\mathbb{Q}$:
  - Se utilizan en el llamado Truco de Manin, para el cálculo de símbolos modulares.
- Fracciones contínuas en F:
  - Análogamente, aparecen en el algoritmo de símbolos modulares para formas modulares de Hilbert sobre F.
  - Cálculo efectivo de puntos ATR en curvas elípticas.
    Sea E/F es una curva elíptica sobre un cuerpo totalmente real F i K/F es una extension ATR (Almost Totally Real). Los puntos ATR son unos puntos de Stark-Heegner definidos por Darmon mediante integrales adecuadas de la forma modular de Hilbert asociada a E, conjeturalmente definidos sobre K.

Índex

Cuerpos euclídeos y cuerpos E_2

- F cuerpo de números, $\mathcal{O}_F$ anillo de enteros, $\mathrm{Nm} = \mathrm{Nm}_{F/\mathbb{Q}}$.

Cuerpos euclídeos y cuerpos E_2

- F cuerpo de números, $\mathcal{O}_F$ anillo de enteros, $\mathrm{Nm} = \mathrm{Nm}_{F/\mathbb{Q}}$.

Definición

F es euclídeo si para todo $\alpha, \beta \in \mathcal{O}_F$, $\beta \neq 0$ existen $q, r \in \mathcal{O}_F$ tales que

$$\alpha = q\beta + r,$$

con $|\mathrm{Nm}(r)| < |\mathrm{Nm}(\beta)|$

Cuerpos euclídeos y cuerpos E_2

- F cuerpo de números, $\mathcal{O}_F$ anillo de enteros, $\mathrm{Nm} = \mathrm{Nm}_{F/\mathbb{Q}}$.

Definición

F es euclídeo si para todo $\alpha, \beta \in \mathcal{O}_F$, $\beta \neq 0$ existen $q, r \in \mathcal{O}_F$ tales que

$$\alpha = q\beta + r,$$

con $|\mathrm{Nm}(r)| < |\mathrm{Nm}(\beta)|$

Definición (G. E. Cooke, 1973)

F es 2-stage euclidean (o E_2) si para todo $\alpha, \beta \in \mathcal{O}_F$, $\beta \neq 0$, existen q_1, q_2, r_1, r_2:

$$\begin{aligned} \alpha &= q_1\beta + r_1 \\ \beta &= q_2 r_1 + r_2. \end{aligned}$$

con $|\mathrm{Nm}(r_2)| < |\mathrm{Nm}(\beta)|$.

Cuerpos E_k

- Más en general:

Definición (G. E. Cooke, 1973)

F es k-stage euclidean (o E_k) si para todo $\alpha, \beta \in \mathcal{O}_F$ existen q_i, r_i:

$$\begin{aligned} \alpha &= q_1\beta + r_1 \\ \beta &= q_2 r_1 + r_2. \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k, \end{aligned}$$

con $|\mathrm{Nm}(r_k)| < |\mathrm{Nm}(\beta)|$

Cuerpos E_k y fracciones contínuas

Si F es E_k para algun k, entonces para todo $\alpha, \beta \in \mathcal{O}_F$ podemos encontrar una cadena de división

$$\begin{aligned} \alpha &= q_1 b + r_1, \\ \beta &= q_2 r_1 + r_2, \\ r_2 &= q_3 r_1 + r_3, \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} \end{aligned}$$

y entonces $\alpha/\beta = [q_1, q_2, \ldots, q_n]$.

Conclusión

Si F es E_k y sabemos encontrar de forma efectiva cadenas de división para cualquier par $\alpha, \beta \in \mathcal{O}_F$, sabemos calcular fracciones contínuas para todo $x \in F$.

Resultados sobre cuerpos E_k

Teorema (Cooke-Vaserštein)

Si $F \neq$ cuadratico imaginario: F es E_k para algún k si y sólo si $h(F) = 1$.

Resultados sobre cuerpos E_k

Teorema (Cooke-Vaserštein)

Si $F \neq$ cuadratico imaginario: F es E_k para algún k si y sólo si $h(F) = 1$.

Teorema (Cohn)

F cuadrático imaginario es k-stage euclidean si y solo si es euclideano.

Resultados sobre cuerpos E_k

Teorema (Cooke-Vaserštein)

Si $F \neq$ cuadratico imaginario: F es E_k para algún k si y sólo si $h(F) = 1$.

Teorema (Cohn)

F cuadrático imaginario es k-stage euclidean si y solo si es euclideano.

Se sabe que los cuerpos $\mathbb{Q}(\sqrt{m})$ con $m \in \{14, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 77, 89, 93, 97, 101, 109, 113, 129, 133, 137, 149, 157, 161, 173, 177, 181, 193, 197, 201, 213, 253\}$
son 2-stage euclidean (y no son euclídeos).

Resultados sobre cuerpos E_k

Teorema (Cooke-Vaserštein)

Si $F \neq$ cuadratico imaginario: F es E_k para algún k si y sólo si $h(F) = 1$.

Teorema (Cohn)

F cuadrático imaginario es k-stage euclidean si y solo si es euclideano.

Se sabe que los cuerpos $\mathbb{Q}(\sqrt{m})$ con $m \in \{14, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 77, 89, 93, 97, 101, 109, 113, 129, 133, 137, 149, 157, 161, 173, 177, 181, 193, 197, 201, 213, 253\}$
son 2-stage euclidean (y no son euclídeos).

Teorema (Cooke-Weinberger)

Assumiendo GRH:

- Si F no es cuadrático imaginario y $h(F) = 1$, entonces F es E_4.
- Si F es cuadrático real y $h(F) = 1$, entonces F es E_2.

Resultados sobre cuerpos E_k

Teorema (Cooke-Vaserštein)

Si $F \neq$ cuadratico imaginario: F es E_k para algún k si y sólo si $h(F) = 1$.

Teorema (Cohn)

F cuadrático imaginario es k-stage euclidean si y solo si es euclideano.

Se sabe que los cuerpos $\mathbb{Q}(\sqrt{m})$ con $m \in \{14, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 77, 89, 93, 97, 101, 109, 113, 129, 133, 137, 149, 157, 161, 173, 177, 181, 193, 197, 201, 213, 253\}$
son 2-stage euclidean (y no son euclídeos).

Teorema (Cooke-Weinberger)

Assumiendo GRH:

- Si F no es cuadrático imaginario y $h(F) = 1$, entonces F es E_4.
- Si F es cuadrático real y $h(F) = 1$, entonces F es E_2.

- Conjeturalmente todos los cuadráticos reales con $h(F) = 1$ son E_2.

Resultado principal

Algoritmo

1. Input: F cuadrático real con $h(F) = 1$. Si F es E_2 el algoritmo termina y demuestra que es E_2.
2. Una vez terminado el paso 1, dado $x \in F$ calcula la fracción contínua de x con coeficientes en $\mathcal{O}_F$.

Resultado principal

Algoritmo

1. Input: F cuadrático real con $h(F) = 1$. Si F es E_2 el algoritmo termina y demuestra que es E_2.
2. Una vez terminado el paso 1, dado $x \in F$ calcula la fracción contínua de x con coeficientes en $\mathcal{O}_F$.

- Hemos implementado el algoritmo y está disponible como patch de Sage.
- Como aplicacion tenemos

Resultado principal

Algoritmo

1. Input: F cuadrático real con $h(F) = 1$. Si F es E_2 el algoritmo termina y demuestra que es E_2.
2. Una vez terminado el paso 1, dado $x \in F$ calcula la fracción contínua de x con coeficientes en $\mathcal{O}_F$.

- Hemos implementado el algoritmo y está disponible como patch de Sage.
- Como aplicacion tenemos

Teorema

Todos los cuerpos cuadráticos reales con número de clases 1 y discriminante menor que 8000 son E_2.

Índex

Propiedad

Sean $\alpha, \beta \in \mathcal{O}_F$, $\beta \neq 0$. La cadena de división

$$\begin{aligned} \alpha &= q_1\beta + r_1 \\ \beta &= q_2 r_1 + r_2. \end{aligned}$$

cumple que $|\mathrm{Nm}(r_2)| < |\mathrm{Nm}(\beta)|$ si y sólo si

$$\left|\mathrm{Nm}\left(\frac{\alpha}{\beta} - [q_1, q_2]\right)\right| < \frac{1}{|\mathrm{Nm}(q_2)|}$$

Propiedad

Sean $\alpha, \beta \in \mathcal{O}_F$, $\beta \neq 0$. La cadena de división

$$\begin{aligned} \alpha &= q_1\beta + r_1 \\ \beta &= q_2 r_1 + r_2. \end{aligned}$$

cumple que $|\mathrm{Nm}(r_2)| < |\mathrm{Nm}(\beta)|$ si y sólo si

$$\left|\mathrm{Nm}\left(\frac{\alpha}{\beta} - [q_1, q_2]\right)\right| < \frac{1}{|\mathrm{Nm}(q_2)|}$$

Si consideramos el embedding $\iota\colon F = \mathbb{Q}(\sqrt{m}) \hookrightarrow \mathbb{R}^2$ dado por $\sqrt{m} \mapsto (\sqrt{m}, -\sqrt{m})$, la norma se extiende como $\mathrm{Nm}(x_0, x_1) = x_0 x_1$. Entonces, dado $q = [q_1, q_2]$ definimos

$$V(q) = \{x \in \mathbb{R}^2 \colon |\mathrm{Nm}(x - q)| < \frac{1}{|\mathrm{Nm}(q_2)|}\}.$$

Propiedad

Sean $\alpha, \beta \in \mathcal{O}_F$, $\beta \neq 0$. La cadena de división

$$\begin{aligned} \alpha &= q_1\beta + r_1 \\ \beta &= q_2 r_1 + r_2. \end{aligned}$$

cumple que $|\mathrm{Nm}(r_2)| < |\mathrm{Nm}(\beta)|$ si y sólo si

$$\left|\mathrm{Nm}\left(\frac{\alpha}{\beta} - [q_1, q_2]\right)\right| < \frac{1}{|\mathrm{Nm}(q_2)|}$$

Si consideramos el embedding $\iota\colon F = \mathbb{Q}(\sqrt{m}) \hookrightarrow \mathbb{R}^2$ dado por $\sqrt{m} \mapsto (\sqrt{m}, -\sqrt{m})$, la norma se extiende como $\mathrm{Nm}(x_0, x_1) = x_0 x_1$. Entonces, dado $q = [q_1, q_2]$ definimos

$$V(q) = \{x \in \mathbb{R}^2 \colon |\mathrm{Nm}(x - q)| < \frac{1}{|\mathrm{Nm}(q_2)|}\}.$$

Com $\iota(F)$ es denso en $\mathbb{R}^2$, tenemos que F es E_2 si y sólo si todo $x \in \mathbb{R}^2$ pertenece a $V(q)$, para algun $q = [q_1, q_2] = q_1 + \frac{1}{q_2}$.

Podemos restringirnos a un dominio fundamental, módulo translaciones de $\mathcal{O}_F$:

$$D = \{a\iota(1) + b\iota(\omega) \colon a, b \in [0, 1)\},$$

donde $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\omega$

Proposición

F es E_2 si y sólo si D está contenido en la unión de un número finito de regiones de la forma $V(q)$ con $q = [q_1, q_2]$.

Podemos restringirnos a un dominio fundamental, módulo translaciones de $\mathcal{O}_F$:

$$D = \{a\iota(1) + b\iota(\omega) \colon a, b \in [0, 1)\},$$

donde $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\omega$

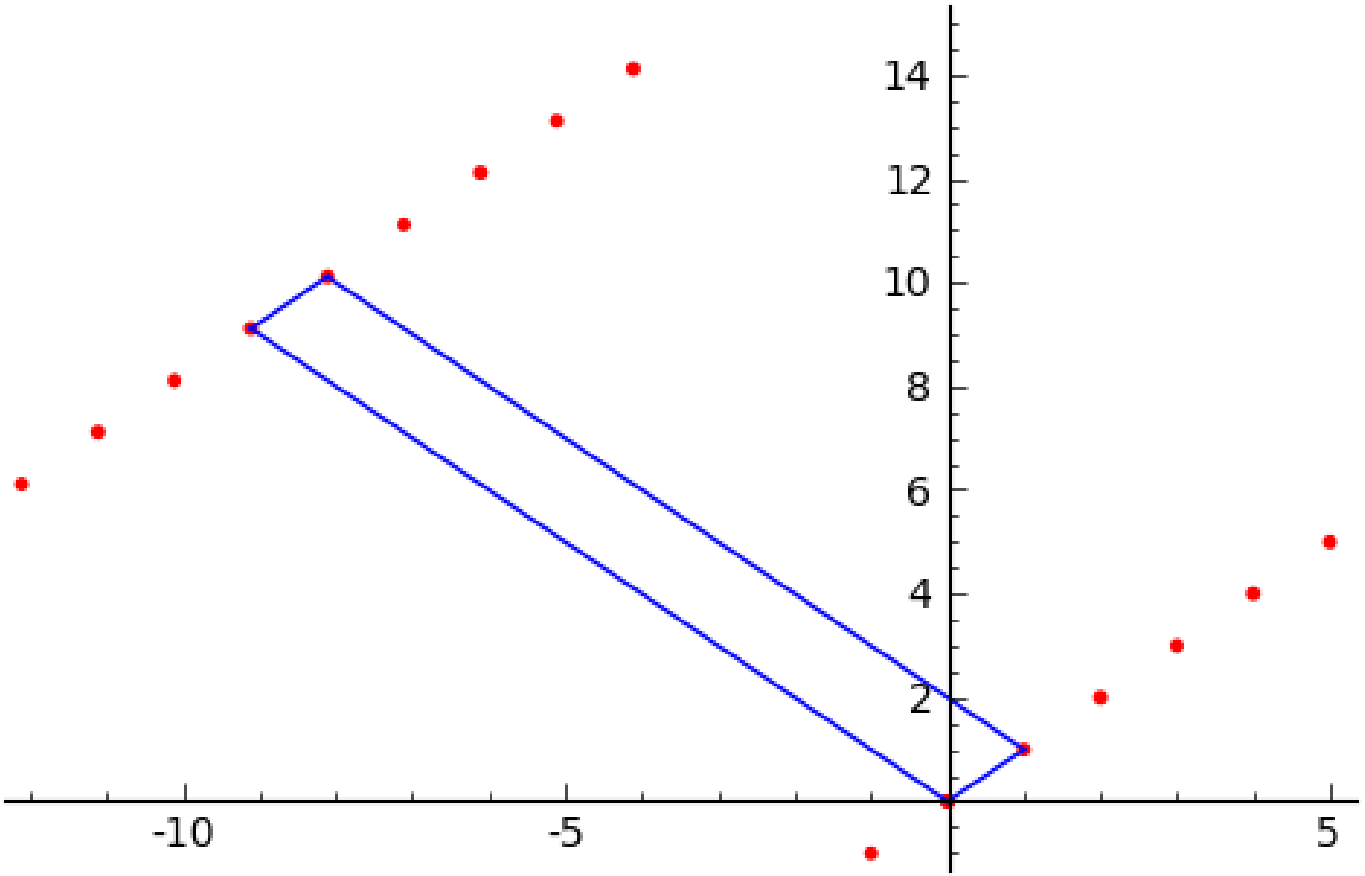
Proposición

F es E_2 si y sólo si D está contenido en la unión de un número finito de regiones de la forma $V(q)$ con $q = [q_1, q_2]$.

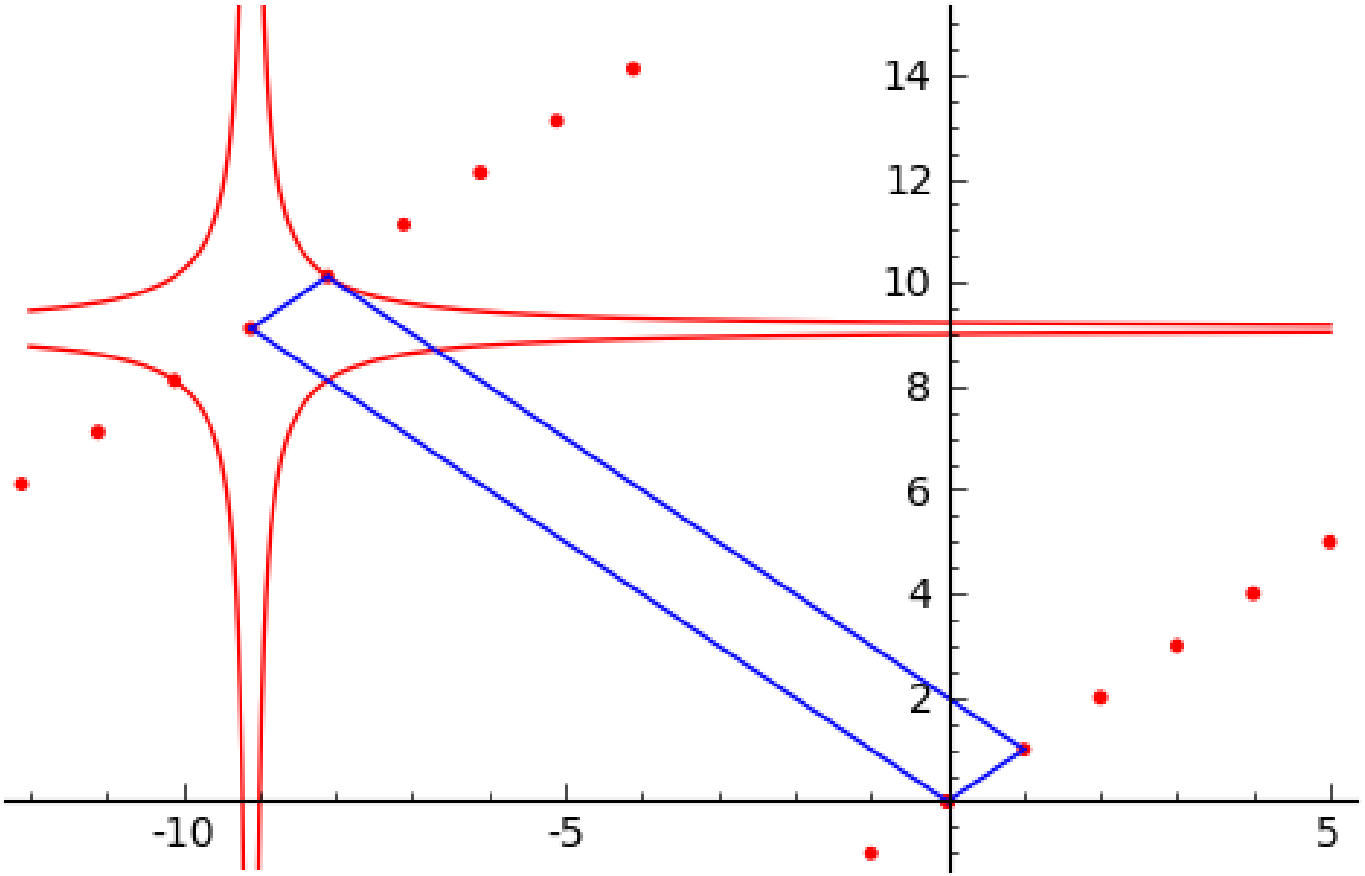
Idea naíf del algoritmo

1. Generar en orden las fracciones de longitud 2 de la forma $[q_1, q_2] = q_1 + \frac{1}{q_2}$
2. En cada paso comprovar si las regiones $V(q)$ generadas cubren D.

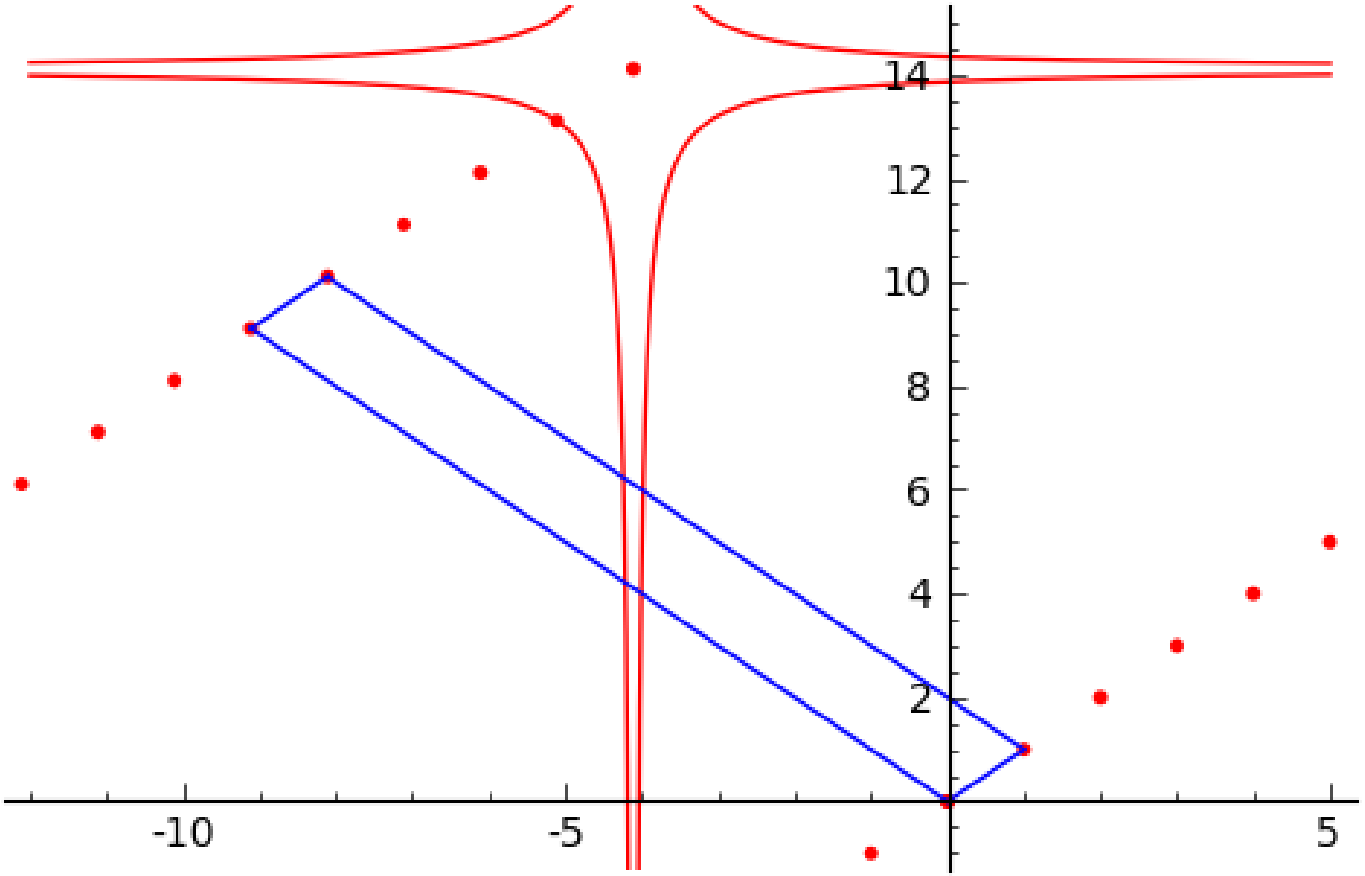
Ejemplo: $F = \mathbb{Q}(\sqrt{83})$



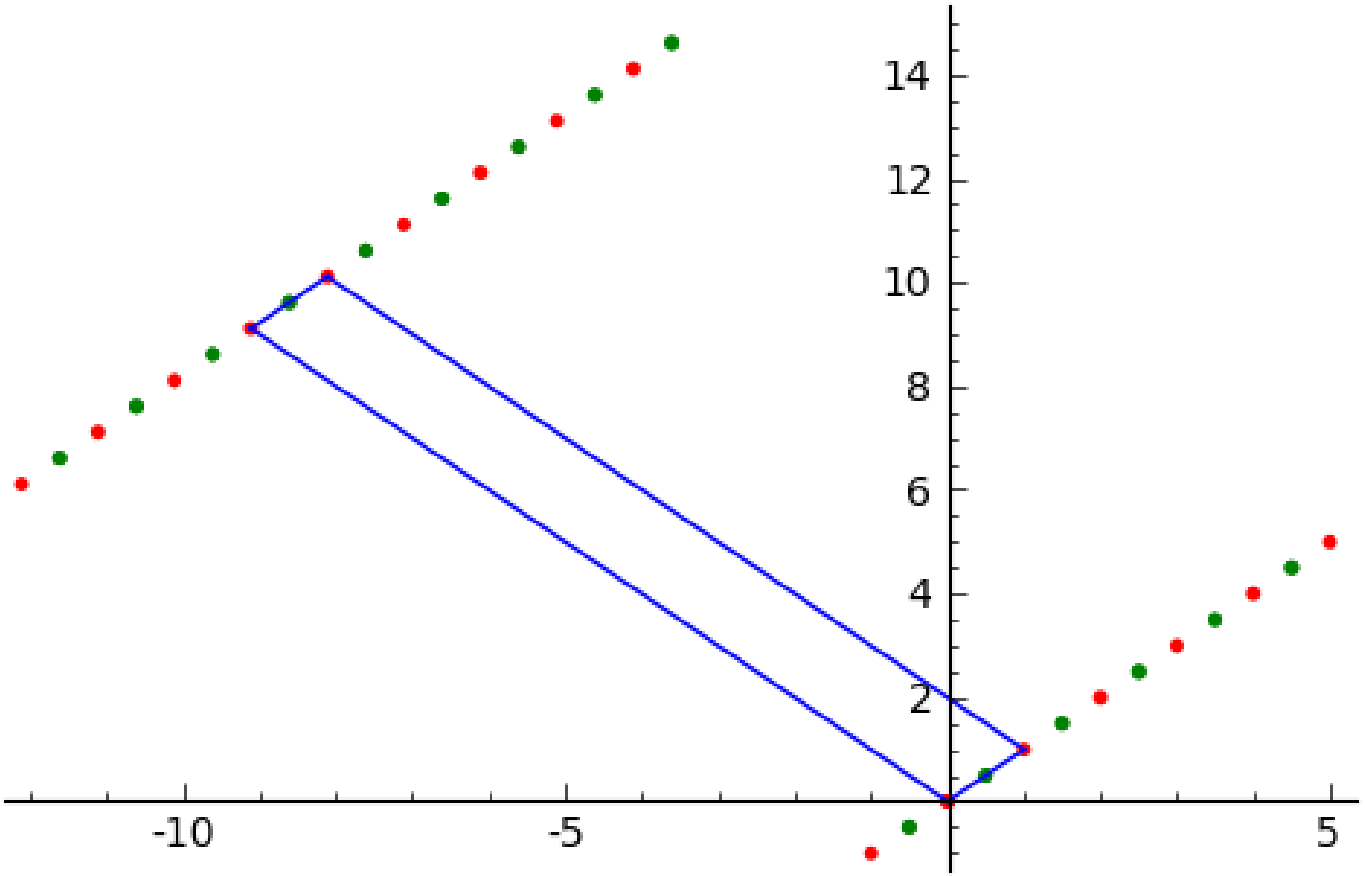
Ejemplo: $F = \mathbb{Q}(\sqrt{83})$



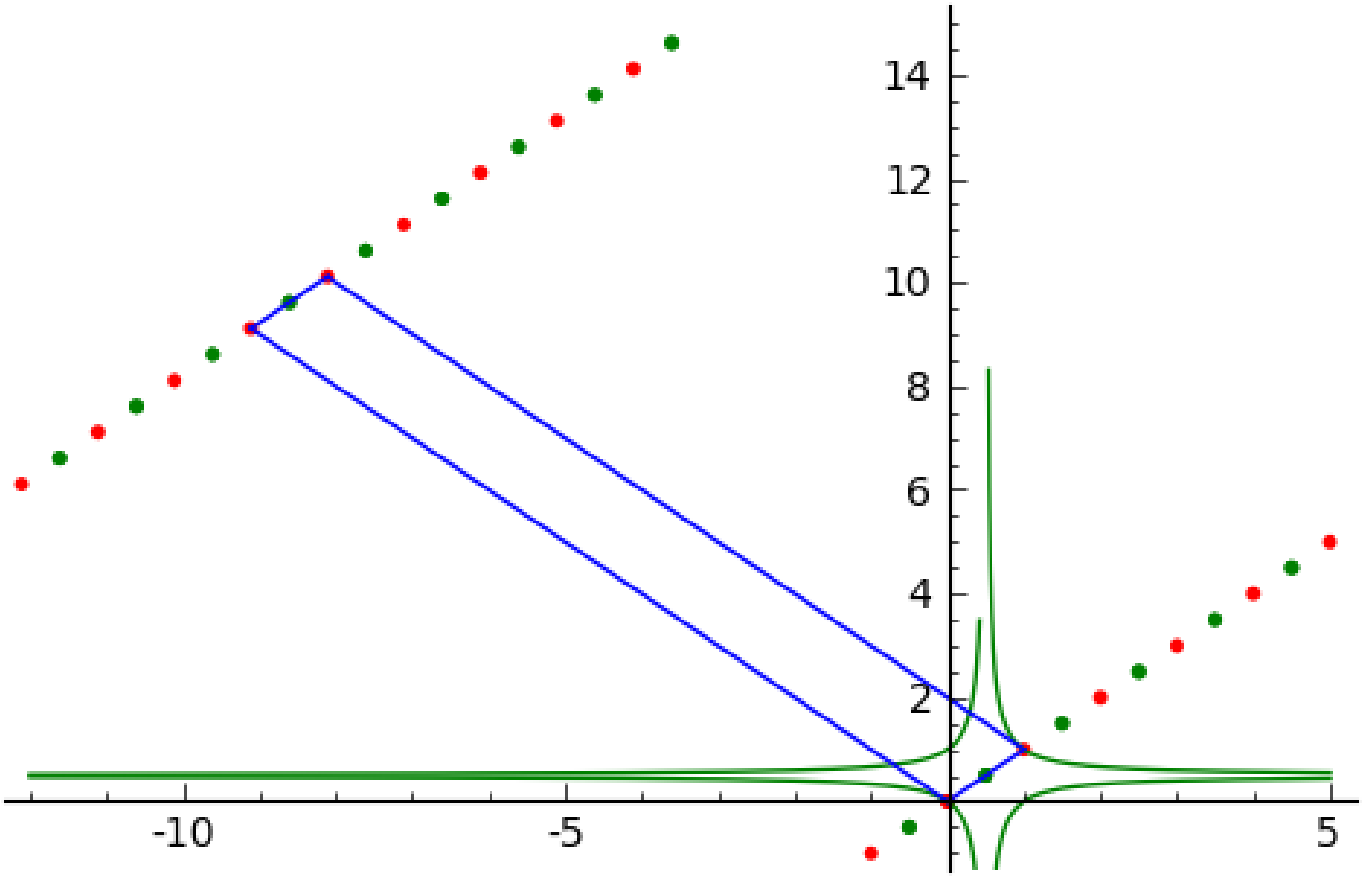
Ejemplo: $F = \mathbb{Q}(\sqrt{83})$



Ejemplo: $F = \mathbb{Q}(\sqrt{83})$: $q_1 + \frac{1}{2}$



Ejemplo: $F = \mathbb{Q}(\sqrt{83})$: $q_1 + \frac{1}{2}$



Índex

Ejecución del algoritmo implementado

Teorema

Todos los cuerpos cuadráticos reales con número de clases 1 y discriminante menor que 8000 son E_2.

Ejecución del algoritmo implementado

Teorema

Todos los cuerpos cuadráticos reales con número de clases 1 y discriminante menor que 8000 son E_2.

- F es E_2 si D se puede cubrir con regiones $V(q)$, con $q = q_1 + \frac{1}{q_2}$.

Ejecución del algoritmo implementado

Teorema

Todos los cuerpos cuadráticos reales con número de clases 1 y discriminante menor que 8000 son E_2.

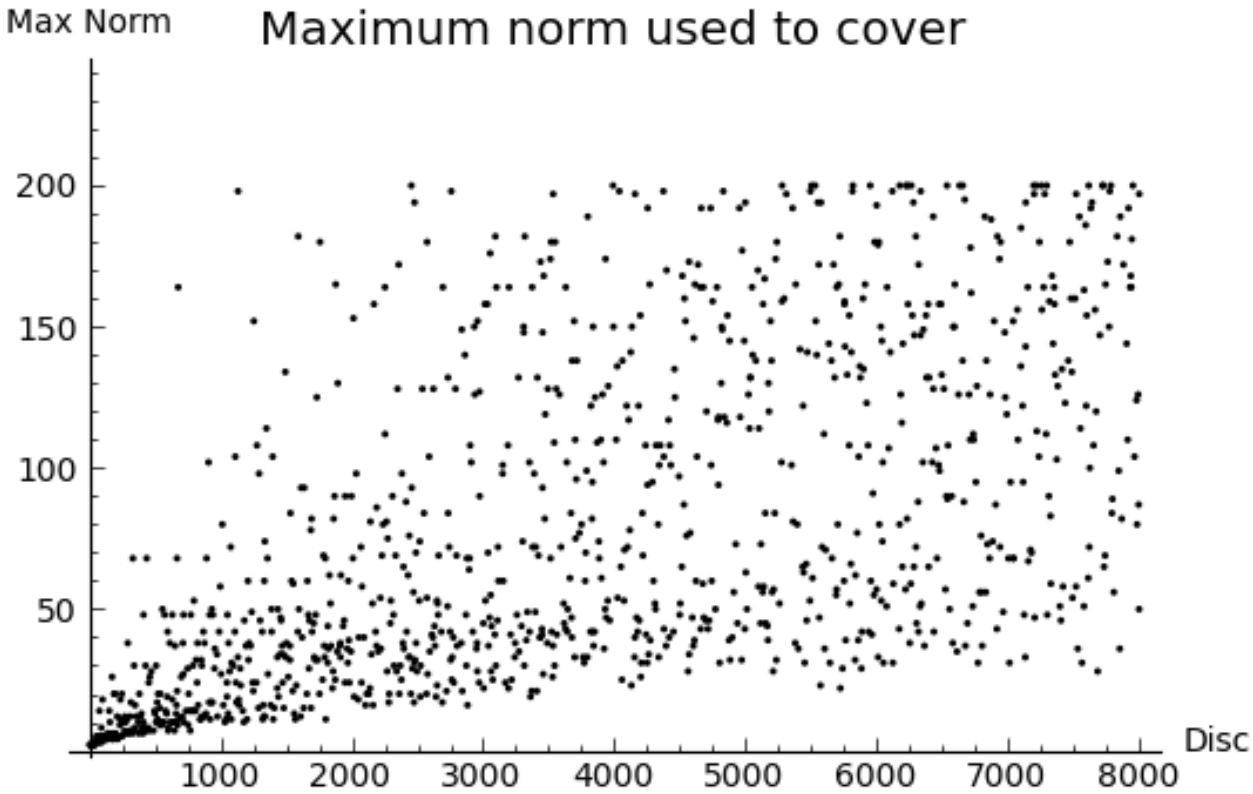
- F es E_2 si D se puede cubrir con regiones $V(q)$, con $q = q_1 + \frac{1}{q_2}$.
- F es euclídeo si D se puede cubrir con regiones $V(q)$, con $q = q_1$.

Ejecución del algoritmo implementado

Teorema

Todos los cuerpos cuadráticos reales con número de clases 1 y discriminante menor que 8000 son E_2.

- F es E_2 si D se puede cubrir con regiones $V(q)$, con $q = q_1 + \frac{1}{q_2}$.
- F es euclídeo si D se puede cubrir con regiones $V(q)$, con $q = q_1$.
- La norma máxima de los q_2 necesarios para cubrir D se puden interpretar una medida de euclideanidad.


Max Norm
Maximum norm used to cover
200
150
100
50
1000
2000
3000
4000
5000
6000
7000
8000
Disc

Teorema

Para cada n, existen un número finito de cuadraticos reales tales que el dominio fundamental se puede cubrir con $V(q)$'s, con $q = q_1 + \frac{1}{q_2}$ y $\mathrm{Nm}(q_2) \leq n$.

- Para $n = 2$, experimentalmente son los $\mathbb{Q}(\sqrt{m})$ con

$$m \in \{14, 22, 31, 89, 97, 113, 129, 137, 161, 193, 209\}.$$

Computing continued fractions on real quadratic fields

Xevi Guitart[1] Marc Masdeu[2]

[1]Universitat Politècnica de Catalunya

[2]Columbia University

Cuartas Jornadas de Teoría de Números