Quadrats en progressió aritmètica

Xavier Xarles

Seminari de Teoria de Nombres

2 de Febrer de 2006

Problema

Quants quadrats (enters) hi ha en progressió aritmètica?

Problema

Quants quadrats (enters) hi ha en progressió aritmètica?

Exemple: $1, 25, 49$.

Problema

Quants quadrats (enters) hi ha en progressió aritmètica?

Exemple: $1, 25, 49$.

Teorema (Fermat)

No hi ha 4 quadrats en progressió aritmètica.

Demostració

x_1^2, x_2^2 i x_3^2 estan en progressió aritmètica si

Demostració

x_1^2, x_2^2 i x_3^2 estan en progressió aritmètica si

$$x_1^2 - x_2^2 = x_2^2 - x_3^2$$

Demostració

x_1^2, x_2^2 i x_3^2 estan en progressió aritmètica si

$$x_1^2 - x_2^2 = x_2^2 - x_3^2$$

$$x_1^2 + x_3^2 = 2x_2^2$$

Una cònica.

Demostració

x_1^2, x_2^2 i x_3^2 estan en progressió aritmètica si

$$x_1^2 - x_2^2 = x_2^2 - x_3^2$$

$$x_1^2 + x_3^2 = 2x_2^2$$

Una cònica.

Té per tant infinites solucions (primitives)

Demostració (cont)

x_1^2, x_2^2, x_3^2 i x_3^2 estan en progressió aritmètica si

Demostració (cont)

x_1^2, x_2^2, x_3^2 i x_3^2 estan en progressió aritmètica si

$$x_1^2 + x_3^2 = 2x_2^2$$

$$x_2^2 + x_4^2 = 2x_3^2$$

Demostració (cont)

x_1^2, x_2^2, x_3^2 i x_3^2 estan en progressió aritmètica si

$$x_1^2 + x_3^2 = 2x_2^2$$

$$x_2^2 + x_4^2 = 2x_3^2$$

Intersecció de dues quàdriques.

Demostració (cont)

x_1^2, x_2^2, x_3^2 i x_3^2 estan en progressió aritmètica si

$$x_1^2 + x_3^2 = 2x_2^2$$
$$x_2^2 + x_4^2 = 2x_3^2$$

Intersecció de dues quàdriques.

Una corba de gènere 1. I com que té punts racionals (e.g. $[1:1:1:1]$), és una corba el·líptica!

Demostració (cont)

x_1^2, x_2^2, x_3^2 i x_3^2 estan en progressió aritmètica si

$$x_1^2 + x_3^2 = 2x_2^2$$
$$x_2^2 + x_4^2 = 2x_3^2$$

Intersecció de dues quàdriques.

Una corba de gènere 1. I com que té punts racionals (e.g. $[1:1:1:1]$), és una corba el·líptica!

$$E : Y^2 = (X+4)(X-12)(X-8).$$

Demostració (cont)

$E : Y^2 = (X + 4)(X - 12)(X - 8)$ té rang zero

Demostració (cont)

$E : Y^2 = (X + 4)(X - 12)(X - 8)$ té rang zero

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

Demostració (cont)

$E : Y^2 = (X + 4)(X - 12)(X - 8)$ té rang zero

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

Els punts racionals corresponent a

$$x_1 = 1, x_2 = \pm 1, x_3 = \pm 1, x_4 = \pm 1$$

Demostració (cont)

$E : Y^2 = (X + 4)(X - 12)(X - 8)$ té rang zero

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

Els punts racionals corresponent a

$$x_1 = 1, x_2 = \pm 1, x_3 = \pm 1, x_4 = \pm 1$$

I.e. la successió

$$1, 1, 1, 1$$

Problema

Que passa si permetem que siguin de $\mathbb{Z}[\sqrt{D}]$ per un cert $D \in \mathbb{Z}$?

Problema

Que passa si permetem que siguin de $\mathbb{Z}[\sqrt{D}]$ per un cert $D \in \mathbb{Z}$?

Exemple

$$1,\ 5^2 = 25,\ 7^2 = 49,\ 73$$

A $\mathbb{Z}[\sqrt{73}]$ hi ha quatre quadrats en progressió aritmètica.

Problema

Que passa si permetem que siguin de $\mathbb{Z}[\sqrt{D}]$ per un cert $D \in \mathbb{Z}$?

Exemple

$$1,\ 5^2 = 25,\ 7^2 = 49,\ 73$$

A $\mathbb{Z}[\sqrt{73}]$ hi ha quatre quadrats en progressió aritmètica.

Exemple

$$7^2 = 49, 13^2 = 169, 17^2 = 289, 409, 23^2 = 529$$

Problema

Que passa si permetem que siguin de $\mathbb{Z}[\sqrt{D}]$ per un cert $D \in \mathbb{Z}$?

Exemple

$$1,\ 5^2 = 25,\ 7^2 = 49,\ 73$$

A $\mathbb{Z}[\sqrt{73}]$ hi ha quatre quadrats en progressió aritmètica.

Exemple

$$7^2 = 49, 13^2 = 169, 17^2 = 289, 409, 23^2 = 529$$

A $\mathbb{Z}[\sqrt{409}]$ hi ha cinc quadrats en progressió aritmètica.

Problema General

Quants quadrats hi ha com màxim en un cos de nombres K en progressió aritmètica?

(Excloent és clar el cas de la progressió aritmètica constant)

Teorema

Per a tot $d \geq 1$, existeix una constant $F(d)$, depenent només de d tal que,

Teorema

Per a tot $d \geq 1$, existeix una constant $F(d)$, depenent només de d tal que,

Si $K/\mathbb{Q}$ és un cos de nombres amb $[K : \mathbb{Q}] = d$

Teorema

Per a tot $d \geq 1$, existeix una constant $F(d)$, depenent només de d tal que,

Si $K/\mathbb{Q}$ és un cos de nombres amb $[K : \mathbb{Q}] = d$

I $a_n := a \cdot n + b$ és una progressió aritmètica amb a i $b \in K$,

Teorema

Per a tot $d \geq 1$, existeix una constant $F(d)$, depenent només de d tal que,

Si $K/\mathbb{Q}$ és un cos de nombres amb $[K : \mathbb{Q}] = d$

I $a_n := a \cdot n + b$ és una progressió aritmètica amb a i $b \in K$,

I a_i és un quadrat a K per
$i = j, j + 1, j + 2, \cdots, j + F(d)$,

Teorema

Per a tot $d \geq 1$, existeix una constant $F(d)$, depenent només de d tal que,

Si $K/\mathbb{Q}$ és un cos de nombres amb $[K : \mathbb{Q}] = d$

I $a_n := a \cdot n + b$ és una progressió aritmètica amb a i $b \in K$,

I a_i és un quadrat a K per
$i = j, j + 1, j + 2, \cdots, j + F(d)$,

Aleshores $a = 0$ (i.e. $\{a_n\}$ és la successió constant).

Traducció del problema

Una successió aritmètica amb n quadrats no nuls consecutius:

$$x_1^2,\ x_2^2,\ x_3^2,\ \ldots,\ x_n^2$$

ens determina 2^{n-1} punts de la corba de $\mathbb{P}^{n-1}$:

Traducció del problema

Una successió aritmètica amb n quadrats no nuls consecutius:

$$x_1^2,\ x_2^2,\ x_3^2,\ \ldots,\ x_n^2$$

ens determina 2^{n-1} punts de la corba de $\mathbb{P}^{n-1}$:

$$C_n : \begin{cases} x_1^2 + x_3^2 = 2x_2^2 \\ x_2^2 + x_4^2 = 2x_3^2 \\ \ldots \quad \ldots \\ x_{n-2}^2 + x_n^2 = 2x_{n-1}^2 \end{cases}$$

Traducció del problema

Una successió aritmètica amb n quadrats no nuls consecutius:

$$x_1^2,\ x_2^2,\ x_3^2,\ \ldots,\ x_n^2$$

ens determina 2^{n-1} punts de la corba de $\mathbb{P}^{n-1}$:

$$C_n : \begin{cases} x_1^2 + x_3^2 = 2x_2^2 \\ x_2^2 + x_4^2 = 2x_3^2 \\ \cdots \quad \cdots \\ x_{n-2}^2 + x_n^2 = 2x_{n-1}^2 \end{cases}$$

Cada successió ens dona els 2^{n-1} punts

$$[x_1 : \pm x_2 : \pm x_3 : \cdots : \pm x_n].$$

La corba C_n

La corba C_n té gènere

$$g = (n-2)2^{n-1} + 1$$

La corba C_n

La corba C_n té gènere

$$g = (n-2)2^{n-1} + 1$$

(Demostració: usar el recobriment de grau 2 $C_n \to C_{n-1}$, ramificat als punts "$x_n = 0$", fórmula de Hurwitz, inducció.)

La corba C_n

La corba C_n té gènere

$$g = (n-2)2^{n-1} + 1$$

(Demostració: usar el recobriment de grau 2 $C_n \to C_{n-1}$, ramificat als punts "$x_n = 0$", fórmula de Hurwitz, inducció.)

Té sempre 2^{n-1} punts "trivials" corresponents a la successió constant (igual a 1).

La corba C_n

La corba C_n té gènere

$$g = (n-2)2^{n-1} + 1$$

(Demostració: usar el recobriment de grau 2 $C_n \to C_{n-1}$, ramificat als punts "$x_n = 0$", fórmula de Hurwitz, inducció.)

Té sempre 2^{n-1} punts "trivials" corresponents a la successió constant (igual a 1).

És no singular en característica 0 o si char$(K) > n$. (Criteri Jacobià)

Idea

Volem demostrar que si $[K : \mathbb{Q}] = d$, i n és prou gran, aleshores

$$C_n(K) = \{[1 : \pm 1 : \pm 1 : \cdots : \pm 1]\}.$$

Idea

Volem demostrar que si $[K : \mathbb{Q}] = d$, i n és prou gran, aleshores

$$C_n(K) = \{[1 : \pm 1 : \pm 1 : \cdots : \pm 1]\}.$$

Prenem

$$C_n^{(d)} := C_n^d / S_n$$

el producte simètric.

Idea

Volem demostrar que si $[K : \mathbb{Q}] = d$, i n és prou gran, aleshores

$$C_n(K) = \{[1 : \pm 1 : \pm 1 : \cdots : \pm 1]\}.$$

Prenem

$$C_n^{(d)} := C_n^d / S_n$$

el producte simètric.

Volem veure que si $n >> d$ aleshores

$$C_n^{(d)}(\mathbb{Q}) = \{\text{“punts trivials”}\}$$

.

Primer pas.

Sols cal veure que $C_n^{(d)}(\mathbb{Q})$ sols té un nombre finit de punts per $n >> d$.

Primer pas.

Sols cal veure que $C_n^{(d)}(\mathbb{Q})$ sols té un nombre finit de punts per $n >> d$.

Demostració: Suposem $P^{(d)} \in C_n^{(d)}(\mathbb{Q})$ no trivial. Aleshores $P \in C_n(K)$ no trivial per $K/\mathbb{Q}$ de grau d

Primer pas.

Sols cal veure que $C_n^{(d)}(\mathbb{Q})$ sols té un nombre finit de punts per $n >> d$.

Demostració: Suposem $P^{(d)} \in C_n^{(d)}(\mathbb{Q})$ no trivial. Aleshores $P \in C_n(K)$ no trivial per $K/\mathbb{Q}$ de grau d

Tenim per tant $\{a_i\}$ de K amb n quadrats consecutius.

Primer pas (cont)

Exercici: Una successió no constant en un cos de nombres no pot tenir infinits quadrats consecutius.

Primer pas (cont)

Exercici: Una successió no constant en un cos de nombres no pot tenir infinits quadrats consecutius.

Sigui n_P el nombres de quadrats consecutius de $\{a_i\}$.

Primer pas (cont)

Exercici: Una successió no constant en un cos de nombres no pot tenir infinits quadrats consecutius.

Sigui n_P el nombres de quadrats consecutius de $\{a_i\}$.

Fem el mateix per a cada punt no trivial.

Primer pas (cont)

Exercici: Una successió no constant en un cos de nombres no pot tenir infinits quadrats consecutius.

Sigui n_P el nombres de quadrats consecutius de $\{a_i\}$.

Fem el mateix per a cada punt no trivial.

Prenem $n > n_P$ per a tot $P^{(d)} \in C_n^{(d)}(\mathbb{Q})$

Primer pas (cont)

Exercici: Una successió no constant en un cos de nombres no pot tenir infinits quadrats consecutius.

Sigui n_P el nombres de quadrats consecutius de $\{a_i\}$.

Fem el mateix per a cada punt no trivial.

Prenem $n > n_P$ per a tot $P^{(d)} \in C_n^{(d)}(\mathbb{Q})$

Q.E.D.

Segon Pas

Criteri(Faltings,Frey,...):
Si una corba C té gonalitat $q_{\mathbb{Q}}(C)$ més gran que $2d$, aleshores $C^{(d)}$ té un nombre finit de punts sobre $\mathbb{Q}$.

Segon Pas

Criteri(Faltings,Frey,...):
Si una corba C té gonalitat $q_{\mathbb{Q}}(C)$ més gran que $2d$, aleshores $C^{(d)}$ té un nombre finit de punts sobre $\mathbb{Q}$.

Gonalitat sobre K: el mínim q tal que existeix un morfisme de grau q $C \to \mathbb{P}^1$ definit sobre K.

Segon Pas

Criteri(Faltings,Frey,...):
Si una corba C té gonalitat $q_{\mathbb{Q}}(C)$ més gran que $2d$, aleshores $C^{(d)}$ té un nombre finit de punts sobre $\mathbb{Q}$.

Gonalitat sobre K: el mínim q tal que existeix un morfisme de grau q $C \to \mathbb{P}^1$ definit sobre K.

Exemples:
Gonalitat 2 és equivalent a hiperel·líptica.
Gonalitat 3 a trigonal.

Tercer Pas

Com calcular la gonalitat?

Tercer Pas

Com calcular la gonalitat?

Sigui un primer p de bona reducció de C, $\widetilde{C}$ la reducció.

Tercer Pas

Com calcular la gonalitat?

Sigui un primer p de bona reducció de C, $\widetilde{C}$ la reducció.

Aleshores $q_{\mathbb{Q}}(C) \geq q_{\mathbb{F}_p}(\widetilde{C})$.

Tercer Pas

Com calcular la gonalitat?

Sigui un primer p de bona reducció de C, $\widetilde{C}$ la reducció.

Aleshores $q_{\mathbb{Q}}(C) \geq q_{\mathbb{F}_p}(\widetilde{C})$.

Però la gonalitat sobre $\mathbb{F}_p$ té relació amb el nombre de punts racionals.

Tercer Pas (cont)

Sigui C una corba sobre $\mathbb{F}_p$ amb r punts racionals. Aleshores $q \geq r/(p+1)$

Tercer Pas (cont)

Sigui C una corba sobre $\mathbb{F}_p$ amb r punts racionals. Aleshores $q \geq r/(p+1)$

Demostració: Prenem $\phi : C \to P^1$ de grau q. Aleshores

$$\sharp C(\mathbb{F}_p) \leq q \sharp \mathbb{P}^1(\mathbb{F}_p)$$

Quart Pas

Prenem $p > n$. Aleshores C_n té bona reducció a p. Sigui $C_{n,p}$ la reducció.

Quart Pas

Prenem $p > n$. Aleshores C_n té bona reducció a p. Sigui $C_{n,p}$ la reducció.

Fet:

$$\sharp C_{n,p}(\mathbb{F}_{p^2}) \geq 2^{n-1} + p2^{n-2}$$

Quart Pas

Prenem $p > n$. Aleshores C_n té bona reducció a p. Sigui $C_{n,p}$ la reducció.

Fet:

$$\sharp C_{n,p}(\mathbb{F}_{p^2}) \geq 2^{n-1} + p2^{n-2}$$

Conseqüència:

$$q_{\mathbb{F}_{p^2}}(C_{n,p}) \geq 2^{n-2}\frac{p+2}{p^2+1} > 2^{n-2}/n$$

Quart Pas

Prenem $p > n$. Aleshores C_n té bona reducció a p. Sigui $C_{n,p}$ la reducció.

Fet:

$$\sharp C_{n,p}(\mathbb{F}_{p^2}) \geq 2^{n-1} + p2^{n-2}$$

Conseqüència:

$$q_{\mathbb{F}_{p^2}}(C_{n,p}) \geq 2^{n-2}\frac{p+2}{p^2+1} > 2^{n-2}/n$$

Conseqüència:

$$2^{n-3} \geq q_{\mathbb{Q}}(C_n) \geq q_{\mathbb{F}_p}(\widetilde{C_{n,p}}) \geq q_{\mathbb{F}_{p^2}}(\widetilde{C_{n,p}}) > 2^{n-2}/n$$

Cinquè Pas

$$\sharp C_{n,p}(\mathbb{F}_{p^2}) \geq 2^{n-1} + p2^{n-2}$$

Cinquè Pas

$$\sharp C_{n,p}(\mathbb{F}_{p^2}) \geq 2^{n-1} + p2^{n-2}$$

Prenem una successió aritmètica a $\mathbb{F}_p$ qualsevol, no zero. N'hi ha $p+1$ de diferents, mòdul equivalència. (les de la forma $a_i = i + b$ variant b entre 0 i $p-1$, i la constant.)

Cinquè Pas

$$\sharp C_{n,p}(\mathbb{F}_{p^2}) \geq 2^{n-1} + p2^{n-2}$$

Prenem una successió aritmètica a $\mathbb{F}_p$ qualsevol, no zero. N'hi ha $p+1$ de diferents, mòdul equivalència. (les de la forma $a_i = i + b$ variant b entre 0 i $p-1$, i la constant.)

A $\mathbb{F}_{p^2}$ cadascuna té tots els membres quadrats.

Cinquè Pas

$$\sharp C_{n,p}(\mathbb{F}_{p^2}) \geq 2^{n-1} + p2^{n-2}$$

Prenem una successió aritmètica a $\mathbb{F}_p$ qualsevol, no zero. N'hi ha $p+1$ de diferents, mòdul equivalència. (les de la forma $a_i = i + b$ variant b entre 0 i $p-1$, i la constant.)

A $\mathbb{F}_{p^2}$ cadascuna té tots els membres quadrats.

La successió constant ens dóna 2^{n-1} punts.
Les altres successions ens determinen 2^{n-2} punts o més (compte amb els $a_i = 0$, que només n'hi ha un com a molt doncs $p > n$.)

Cinquè Pas

$$\sharp C_{n,p}(\mathbb{F}_{p^2}) \geq 2^{n-1} + p2^{n-2}$$

Prenem una successió aritmètica a $\mathbb{F}_p$ qualsevol, no zero. N'hi ha $p+1$ de diferents, mòdul equivalència. (les de la forma $a_i = i + b$ variant b entre 0 i $p-1$, i la constant.)

A $\mathbb{F}_{p^2}$ cadascuna té tots els membres quadrats.

La successió constant ens dóna 2^{n-1} punts.
Les altres successions ens determinen 2^{n-2} punts o més (compte amb els $a_i = 0$, que només n'hi ha un com a molt doncs $p > n$.)

Tenim per tant $2^{n-1} + p2^{n-2}$ punts diferents a $C(\mathbb{F}_{p^2})$.

Resum

Volem que per n prou gran

$$q_{\mathbb{Q}}(C_n) \stackrel{?}{\geq} 2d$$

i sabem

$$q_{\mathbb{Q}}(C_n) > 2^{n-2}/n.$$

Resum

Volem que per n prou gran

$$q_{\mathbb{Q}}(C_n) \stackrel{?}{\geq} 2d$$

i sabem

$$q_{\mathbb{Q}}(C_n) > 2^{n-2}/n.$$

Prenem n tal que

$$2^{n-2}/n > 2d$$

Aleshores $C_n^{(d)}$ té un nombre finit de punts sobre $\mathbb{Q}$.

Resum (cont)

Per tant per n prou gran en funció de d, $C_n^{(d)}$ només té els punts trivials sobre $\mathbb{Q}$

Resum (cont)

Per tant per n prou gran en funció de d, $C_n^{(d)}$ només té els punts trivials sobre $\mathbb{Q}$

Per tant si n és prou gran en funció de d no hi ha n quadrats consecutius en successió aritmètica no constant

Resum (cont)

Per tant per n prou gran en funció de d, $C_n^{(d)}$ només té els punts trivials sobre $\mathbb{Q}$

Per tant si n és prou gran en funció de d no hi ha n quadrats consecutius en successió aritmètica no constant

Q.E.D.

Problemes per resoldre

- Hi ha 6 quadrats consecutius en un cos quadràtic?

Problemes per resoldre

- Hi ha 6 quadrats consecutius en un cos quadràtic?
- Podem determinar una cota inferior efectiva per $F(d)$?

Problemes per resoldre

- Hi ha 6 quadrats consecutius en un cos quadràtic?
- Podem determinar una cota inferior efectiva per $F(d)$?
- Podem determinar una cota superior efectiva per $F(d)$?

Generalitzacions

I si enlloc de successió aritmètica posem “valors consecutius de un polinomi de grau dos”?

Generalitzacions

I si enlloc de successió aritmètica posem “valors consecutius de un polinomi de grau dos”?

El problema es tradueix a estudiar punts racionals de certes superfícies.

Generalitzacions

I si enlloc de successió aritmètica posem “valors consecutius de un polinomi de grau dos”?

El problema es tradueix a estudiar punts racionals de certes superfícies.

La conjectura de Lang permetria demostrar que: existeix una C tal que si un polinomi de grau dos té més de C valors quadrats consecutius, aleshores és un polinomi al quadrat.

L'àlgebra dels dits:
mentre passa la tarda
cargolo el destí.