L'ABC de l'Aritmètica

Xavier Xarles

Només hi ha un títol, però en teníem més!

Només hi ha un títol, però en teníem més!

Més enllà de Fermat.

Només hi ha un títol, però en teníem més!

La llibreta perduda de Fermat.

Només hi ha un títol, però en teníem més!

Suma de potències
o la potència de la suma.

Només hi ha un títol, però en teníem més!

La Panacea de la Geometria Aritmètica

L'Últim Teorema de Fermat.

A. Wiles, 1994.
"Formulada" per Pierre de Fermat (1601-1665).

Sigui $n \geq 3$. Si tenim enters x, y i z tals que

$$x^n + y^n = z^n$$

aleshores $xyz = 0$.

La conjectura de Catalan.

P. Mihailescu, 2002.
Formulada per Eugène Charles Catalan el 1844.

Siguin a, b, c i d nombres enters més grans que 1. Si

$$a^b = c^d + 1$$

aleshores $a = 3$, $b = 2$, $c = 2$ i $d = 3$.

Super-Fermat

Super-Fermat

“La conjectura de Beal (1996)” 75.000$

Super-Fermat

“La conjectura de Beal (1996)” 75.000$
“El Problema de Brun (1914)”

Super-Fermat

“La conjectura de Beal (1996)” 75.000$
“El Problema de Brun (1914)”
“La conjectura de Catalan-Fermat”

Super-Fermat

"La conjectura de Beal (1996)" 75.000$
"El Problema de Brun (1914)"
"La conjectura de Catalan-Fermat"

Si n, m i r són enters més grans o iguals que 3, aleshores

$$a^n + b^m = c^r$$

no té cap solució amb a, b i c enters primers entre si i diferents de zero.

Super-Fermat

"La conjectura de Beal (1996)" 75.000$
"El Problema de Brun (1914)"
"La conjectura de Catalan-Fermat"

Si n, m i r són enters més grans o iguals que 3, aleshores

$$a^n + b^m = c^r$$

no té cap solució amb a, b i c enters primers entre si i diferents de zero.

Observació.

La condició de ser primers entre si és necessària.

Observació.

La condició de ser primers entre si és necessària.

Per exemple, suposem que donats a, b, n i m tenim que

$$a^n + b^m = k$$

Observació.

La condició de ser primers entre si és necessària.

Per exemple, suposem que donats a, b, n i m tenim que

$$a^n + b^m = k$$

Multiplicant per k^{nm} tenim per tant que

$$(k^m a)^n + (k^n b)^m = k^{nm+1}$$

Super-Fermat (bis).

Hi ha un nombre finit d'enters n, m i r amb $1/n + 1/m + 1/r < 1$ i potències a^n, b^m i c^r amb a, b i c enters primers entre si amb $abc \neq 0$ i tals que

$$a^n + b^m = c^r .$$

Les úniques solucions són:

- $a^5 + b^2 = c^4$ (Nils Bruin 1999)

$$2^5 + 7^2 = 3^4 \ , \ 3^5 + 11^4 = 122^2$$

Les úniques solucions són:

- $a^5 + b^2 = c^4$ (Nils Bruin 1999)

$$2^5 + 7^2 = 3^4 \ , \ 3^5 + 11^4 = 122^2$$

- $a^8 + b^2 = c^3$ (Nils Bruin 1999)

$$33^8 + 1549034^2 = 15613^3 \ , \ 43^8 + 96222^3 = 30042907^2$$

Les úniques solucions són:

- $a^5 + b^2 = c^4$ (Nils Bruin 1999)

$$2^5 + 7^2 = 3^4 \ , \ 3^5 + 11^4 = 122^2$$

- $a^8 + b^2 = c^3$ (Nils Bruin 1999)

$$33^8 + 1549034^2 = 15613^3 \ , \ 43^8 + 96222^3 = 30042907^2$$

- $a^3 + b^2 = c^9$ (Nils Bruin 2003): $7^3 + 13^2 = 2^9$

Les úniques solucions són:

- $a^5 + b^2 = c^4$ (Nils Bruin 1999)

$$2^5 + 7^2 = 3^4\ ,\ 3^5 + 11^4 = 122^2$$

- $a^8 + b^2 = c^3$ (Nils Bruin 1999)

$$33^8 + 1549034^2 = 15613^3\ ,\ 43^8 + 96222^3 = 30042907^2$$

- $a^3 + b^2 = c^9$ (Nils Bruin 2003): $7^3 + 13^2 = 2^9$
- $a^3 + b^2 = c^7$ (Bjorn Poonen, Ed Schaefer, Michael Stoll “2004”)

$$1414^3 + 2213459^2 = 65^7\ ,\ 9262^3 + 15312283^2 = 113^7$$

$$2^7 + 17^3 = 71^2\ ,\ 17^7 + 76271^3 = 21063928^2$$

Mega-Fermat.

Siguin A, B i C tres nombres enters diferents de zero.

Aleshores hi ha un nombre finit d'enters n, m i r amb $1/n + 1/m + 1/r < 1$ i potències x^n, y^m i z^r amb x, y i z enters primers entre si amb $xyz \neq 0$ i tals que

$$Ax^n + By^m = Cz^r$$

Mega-Fermat.

Siguin A, B i C tres nombres enters diferents de zero.

Aleshores hi ha un nombre finit d'enters n, m i r amb $1/n + 1/m + 1/r < 1$ i potències x^n, y^m i z^r amb x, y i z enters primers entre si amb $xyz \neq 0$ i tals que

$$Ax^n + By^m = Cz^r$$

H. Darmon i A. Granville (1995): Si fixem n, m i r, hi ha un nombre finit de x, y i z complint això.

Mega-Fermat.

Siguin A, B i C tres nombres enters diferents de zero.

Aleshores hi ha un nombre finit d'enters n, m i r amb $1/n + 1/m + 1/r < 1$ i potències x^n, y^m i z^r amb x, y i z enters primers entre si amb $xyz \neq 0$ i tals que

$$Ax^n + By^m = Cz^r$$

H. Darmon i A. Granville (1995): Si fixem n, m i r, hi ha un nombre finit de x, y i z complint això.

És conseqüència del Teorema de Faltings (conjectura de Mordell).

Totes aquestes conjectures tenen en comú que tracten de com es comporten les potències quan se sumen.

Totes aquestes conjectures tenen en comú que tracten de com es comporten les potències quan se sumen.

Per poder entendre què podria estar passant, el que farem és estudiar el cas dels polinomis.

Totes aquestes conjectures tenen en comú que tracten de com es comporten les potències quan se sumen.

Per poder entendre què podria estar passant, el que farem és estudiar el cas dels polinomis.

Aquesta és una idea molt usual en aritmètica: hi ha moltes i molt profundes analogies entre els polinomis (sobre $\mathbb{Q}$, sobre $\mathbb{C}$, sobre un cos finit) i els enters.

Fermat Polinòmic.

(Lioville 1851)

Sigui $n \geq 3$. Aleshores no hi ha polinomis $X(t)$, $Y(t)$ i $Z(t)$ amb coeficients a $\mathbb{C}$, primers entre si, de grau > 0, tals que

$$X^n + Y^n = Z^n. \qquad (1)$$

Demostració

Derivem $X^n + Y^n = Z^n$ (1):

$$nX^{n-1}X' + nY^{n-1}Y' = nZ^{n-1}Z'$$

Demostració

Derivem $X^n + Y^n = Z^n$ (1):

$$nX^{n-1}X' + nY^{n-1}Y' = nZ^{n-1}Z'$$

Dividim per n:

$$X^{n-1}X' + Y^{n-1}Y' = Z^{n-1}Z' \qquad (2)$$

Demostració

Derivem $X^n + Y^n = Z^n$ (1):

$$nX^{n-1}X' + nY^{n-1}Y' = nZ^{n-1}Z'$$

Dividim per n:

$$X^{n-1}X' + Y^{n-1}Y' = Z^{n-1}Z' \qquad (2)$$

Multipliquem (1) per Y', (2) per Y i restem:

$$X^{n-1}(XY' - YX') = Z^{n-1}(ZY' - YZ')$$

Demostració

Derivem $X^n + Y^n = Z^n$ (1):

$$nX^{n-1}X' + nY^{n-1}Y' = nZ^{n-1}Z'$$

Dividim per n:

$$X^{n-1}X' + Y^{n-1}Y' = Z^{n-1}Z' \qquad (2)$$

Multipliquem (1) per Y', (2) per Y i restem:

$$X^{n-1}(XY' - YX') = Z^{n-1}(ZY' - YZ')$$

Com que X i Z són coprimers, tenim que

$$X^{n-1} \text{ divideix } ZY' - YZ'$$

Demostració (cont)

$ZY' - YZ'$ no pot valdre zero, ja que si no tindríem $(Z/Y)' = 0$, i per tant Z i Y serien múltiples un de l'altre.

Demostració (cont)

$ZY' - YZ'$ no pot valdre zero, ja que si no tindríem $(Z/Y)' = 0$, i per tant Z i Y serien múltiples un de l'altre.
Prenem graus i tenim

$$(n-1)\deg(X) \leq \deg(ZY' - YZ') \leq$$

$$\leq \deg(Y) + \deg(Z) - 1$$

Demostració (cont)

$ZY' - YZ'$ no pot valdre zero, ja que si no tindríem $(Z/Y)' = 0$, i per tant Z i Y serien múltiples un de l'altre.
Prenem graus i tenim

$$(n-1)\deg(X) \leq \deg(ZY' - YZ') \leq$$

$$\leq \deg(Y) + \deg(Z) - 1$$

O sigui

$$n\deg(X) < \deg(X) + \deg(Y) + \deg(Z)$$

Demostració (cont)

Podem fer el mateix amb Y i amb Z (l'equació (1) és "simètrica").

Demostració (cont)

Podem fer el mateix amb Y i amb Z (l'equació (1) és "simètrica").
Obtenim 3 equacions que en sumar-les ens dóna:

$$n(\deg(X) + \deg(Y) + \deg(Z)) <$$

$$< 3(\deg(X) + \deg(Y) + \deg(Z))$$

Demostració (cont)

Podem fer el mateix amb Y i amb Z (l'equació (1) és "simètrica").
Obtenim 3 equacions que en sumar-les ens dóna:

$$n(\deg(X) + \deg(Y) + \deg(Z)) <$$

$$< 3(\deg(X) + \deg(Y) + \deg(Z))$$

O sigui

$$n < 3.$$

Demostració (cont)

Podem fer el mateix amb Y i amb Z (l'equació (1) és "simètrica").
Obtenim 3 equacions que en sumar-les ens dóna:

$$n(\deg(X) + \deg(Y) + \deg(Z)) <$$

$$< 3(\deg(X) + \deg(Y) + \deg(Z))$$

O sigui

$$n < 3.$$

Q.E.D.

Demostració (cont)

Podem fer el mateix amb Y i amb Z (l'equació (1) és "simètrica").
Obtenim 3 equacions que en sumar-les ens dóna:

$$n(\deg(X) + \deg(Y) + \deg(Z)) <$$

$$< 3(\deg(X) + \deg(Y) + \deg(Z))$$

O sigui

$$n < 3.$$

Q.E.D.

Què hi ha en el fons d'aquesta demostració?

Proposició

R. C. Mason, 1983.

Si tenim tres polinomis $A(t)$, $B(t)$ i $C(t)$ de $\mathbb{C}[t]$, primers entre si, tals que

$$A + B = C,$$

aleshores

$$\max(\deg(A), \deg(B), \deg(C)) <$$

$$< \sharp\{\alpha \in \mathbb{C} \mid \alpha \text{ arrel de } ABC\}.$$

Demostració

$$\Delta := \begin{vmatrix} A & B \\ A' & B' \end{vmatrix} = \begin{vmatrix} A & C \\ A' & C' \end{vmatrix} = \begin{vmatrix} C & B \\ C' & B' \end{vmatrix}$$

Demostració

$$\Delta := \begin{vmatrix} A & B \\ A' & B' \end{vmatrix} = \begin{vmatrix} A & C \\ A' & C' \end{vmatrix} = \begin{vmatrix} C & B \\ C' & B' \end{vmatrix}$$

Observem que $\Delta \neq 0$, ja que:

$$\Delta = 0 \Rightarrow \exists \lambda \in \mathbb{C} \text{ tal que } A = \lambda B.$$

Demostració

$$\Delta := \begin{vmatrix} A & B \\ A' & B' \end{vmatrix} = \begin{vmatrix} A & C \\ A' & C' \end{vmatrix} = \begin{vmatrix} C & B \\ C' & B' \end{vmatrix}$$

Observem que $\Delta \neq 0$, ja que:

$$\Delta = 0 \Rightarrow \exists \lambda \in \mathbb{C} \text{ tal que } A = \lambda B.$$

Si $\alpha \in \mathbb{C}$ és una arrel de A amb multiplicitat e,

$$(t-\alpha)^e \text{ divideix } A \text{ i } (t-\alpha)^{e-1} \text{ divideix } A',$$

d'on $(t-\alpha)^{e-1}$ divideix Δ.

Demostració

$$\Delta := \begin{vmatrix} A & B \\ A' & B' \end{vmatrix} = \begin{vmatrix} A & C \\ A' & C' \end{vmatrix} = \begin{vmatrix} C & B \\ C' & B' \end{vmatrix}$$

Observem que $\Delta \neq 0$, ja que:

$$\Delta = 0 \Rightarrow \exists \lambda \in \mathbb{C} \text{ tal que } A = \lambda B.$$

Si $\alpha \in \mathbb{C}$ és una arrel de A amb multiplicitat e,

$$(t-\alpha)^e \text{ divideix } A \text{ i } (t-\alpha)^{e-1} \text{ divideix } A',$$

d'on $(t-\alpha)^{e-1}$ divideix Δ.

Així tenim

$$A \text{ divideix a } \Delta \prod_{A(\alpha)=0} (t-\alpha).$$

Demostració (cont)

Fent el mateix amb B i C obtenim finalment que

$$ABC \text{ divideix a } \Delta \prod_{ABC(\alpha)=0} (t-\alpha)$$

Demostració (cont)

Fent el mateix amb B i C obtenim finalment que

$$ABC \text{ divideix a } \Delta \prod_{ABC(\alpha)=0} (t-\alpha)$$

Prenem ara graus. El grau de Δ compleix que

$$\deg(\Delta) \leq \deg(A) + \deg(B) - 1$$

Demostració (cont)

Fent el mateix amb B i C obtenim finalment que

$$ABC \text{ divideix a } \Delta \prod_{ABC(\alpha)=0} (t-\alpha)$$

Prenem ara graus. El grau de Δ compleix que

$$\deg(\Delta) \leq \deg(A) + \deg(B) - 1$$

Per tant tenim que

$$\deg(A) + \deg(B) + \deg(C) \leq$$

$$\leq \deg(A) + \deg(B) - 1 + \sharp\{\alpha \in \mathbb{C} \mid \alpha \text{ arrel de } ABC\}$$

Demostració (cont)

D'on tenim que

$$\deg(C) < \sharp\{\alpha \in \mathbb{C} \mid \alpha \text{ arrel de } ABC\}$$

Demostració (cont)

D'on tenim que

$$\deg(C) < \sharp\{\alpha \in \mathbb{C} \mid \alpha \text{ arrel de } ABC\}$$

Tenim el mateix amb A i amb B utilitzant que

$$\deg(\Delta) \leq \deg(C) + \deg(B) - 1$$

$$\deg(\Delta) \leq \deg(A) + \deg(C) - 1$$

Demostració (cont)

D'on tenim que

$$\deg(C) < \sharp\{\alpha \in \mathbb{C} \mid \alpha \text{ arrel de } ABC\}$$

Tenim el mateix amb A i amb B utilitzant que

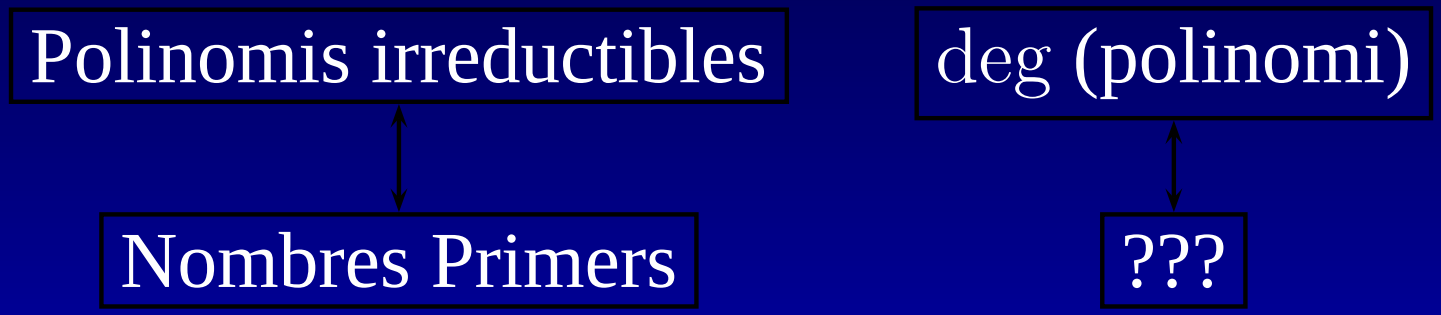
$$\deg(\Delta) \leq \deg(C) + \deg(B) - 1$$

$$\deg(\Delta) \leq \deg(A) + \deg(C) - 1$$

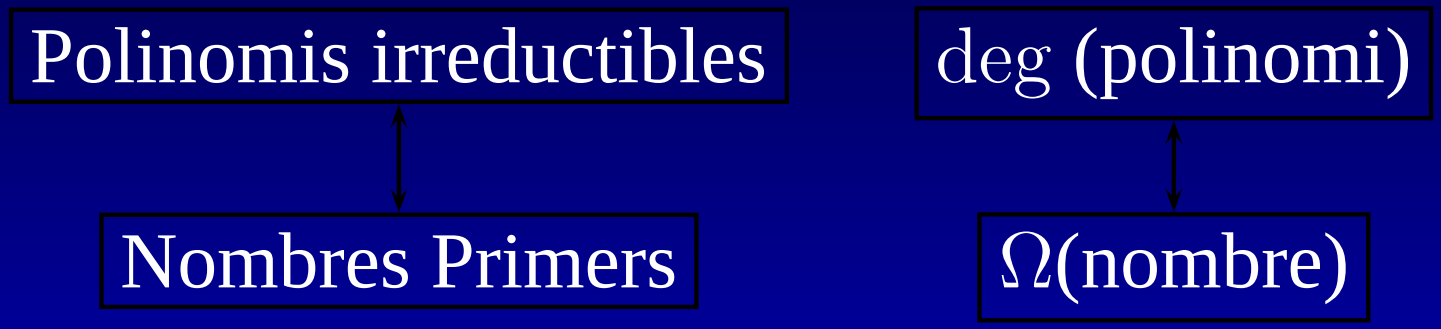
Q.E.D.

Analitzem com podríem “traduir” aquest resultat a una conjectura per als nombres enters.

Analitzem com podríem “traduir” aquest resultat a una conjectura per als nombres enters.



Analitzem com podríem “traduir” aquest resultat a una conjectura per als nombres enters.



on

$$\Omega(n) := \sharp\{p^r \text{ amb } p \text{ primer } \mid p^r \text{ divideix } n\}$$

és el nombre de factors primers de n comptats amb multiplicitat.

Primer intent

Si

$$a + b = c$$

amb a, b i c enters primers entre si, aleshores

$$\Omega(c) < \omega(abc) := \sharp\{p \text{ primer } \mid p \text{ divideix } abc\}.$$

Primer intent

Si

$$a + b = c$$

amb a, b i c enters primers entre si, aleshores

$$\Omega(c) < \omega(abc) := \sharp\{p \text{ primer } \mid p \text{ divideix } abc\}.$$

Però aquest resultat és clarament fals!

Per exemple, per a

$$1 + 3 = 4$$

tindríem que $2 < 2$.

Per exemple, per a

$$1 + 3 = 4$$

tindríem que $2 < 2$.
Per a

$$1 + 7 = 8$$

que $3 < 2$.

Per exemple, per a

$$1 + 3 = 4$$

tindríem que $2 < 2$.
Per a

$$1 + 7 = 8$$

que $3 < 2$.
O, més en general, si $2^p - 1$ és primer (un primer de Mersene), aleshores

$$1 + (2^p - 1) = 2^p$$

i tindríem que $p < 2$!!!

Per exemple, per a

$$1 + 3 = 4$$

tindríem que $2 < 2$.
Per a

$$1 + 7 = 8$$

que $3 < 2$.
O, més en general, si $2^p - 1$ és primer (un primer de Mersene), aleshores

$$1 + (2^p - 1) = 2^p$$

i tindríem que $p < 2$!!!

El problema és que hem fet una mala analogia

ABC polinòmic

Si tenim tres polinomis $A(t)$, $B(t)$ i $C(t)$ de $\mathbb{Q}[t]$, primers entre si, tals que

$$A + B = C,$$

aleshores

$$\max(\deg(A), \deg(B), \deg(C)) < \sum_{P(t) \setminus ABC} \deg(P(t)),$$

on la suma és sobre tots els polinomis *irreductibles* que divideixen ABC.

Així el problema és que els nombres primers no tenen tots “grau” 1.

Així el problema és que els nombres primers no tenen tots “grau” 1.

¿Quin és l’anàleg del grau en els nombres enters?

Així el problema és que els nombres primers no tenen tots “grau” 1.

¿Quin és l’anàleg del grau en els nombres enters?

EL LOGARITME!

Segon intent

Si $a + b = c$ amb a, b i c enters primers entre si, aleshores

$$\max\{\log|a|, \log|b|, \log|c|\} < \sum_{\substack{p \text{ primer} \\ p|abc}} \log(p).$$

Segon intent

Si $a+b=c$ amb a, b i c enters primers entre si, aleshores

$$\max\{\log|a|, \log|b|, \log|c|\} < \sum_{\substack{p \text{ primer} \\ p|abc}} \log(p).$$

Equivalentment,

$$\max\{|a|, |b|, |c|\} < \prod_{\substack{p \text{ primer} \\ p|abc}} p.$$

Ara bé, aquest resultat tampoc és cert, com podem veure de

$$1 + 8 = 9$$

d'on tindríem que $9 < 2 \cdot 3 = 6$

Ara bé, aquest resultat tampoc és cert, com podem veure de

$$1 + 8 = 9$$

d'on tindríem que $9 < 2 \cdot 3 = 6$
O bé

$$1 + 3^2 \cdot 7 = 2^6$$

d'on tindríem que $2^6 = 64 < 2 \cdot 3 \cdot 7 = 42$

Ara bé, aquest resultat tampoc és cert, com podem veure de

$$1 + 8 = 9$$

d'on tindríem que $9 < 2 \cdot 3 = 6$
O bé

$$1 + 3^2 \cdot 7 = 2^6$$

d'on tindríem que $2^6 = 64 < 2 \cdot 3 \cdot 7 = 42$

Potser el problema és que cal multiplicar la part dreta de la desigualtat per una constant?

Segon intent (bis)

Existeix una constant K tal que, si $a + b = c$ amb a, b i c enters primers entre si, aleshores

$$\max\{|a|, |b|, |c|\} \leq K \text{rad}(abc).$$

Notació:

$$\text{rad}(a) := \prod_{\substack{p \text{ primer} \\ p|a}} p.$$

Segon intent (bis)

Existeix una constant K tal que, si $a + b = c$ amb a, b i c enters primers entre si, aleshores

$$\max\{|a|, |b|, |c|\} \leq K\text{rad}(abc).$$

Notació:

$$\text{rad}(a) := \prod_{\substack{p \text{ primer} \\ p|a}} p.$$

Però això tampoc és cert!

Contraexemple

Petit Teorema de Fermat (de fet, Fermat-Euler) $\Rightarrow$

Contraexemple

Petit Teorema de Fermat (de fet, Fermat-Euler) $\Rightarrow$
Si p nombre primer i $r \geq 1$ tenim que

$$2^{p^{r-1}(p-1)} \equiv 1 \pmod{p^r}$$

Contraexemple

Petit Teorema de Fermat (de fet, Fermat-Euler) $\Rightarrow$
Si p nombre primer i $r \geq 1$ tenim que

$$2^{p^{r-1}(p-1)} \equiv 1 \pmod{p^r}$$

Posem

$$a = 2^{p^{r-1}(p-1)}\,,\ b = -1 \text{ i } c = 2^{p^{r-1}(p-1)} - 1$$

$\Rightarrow$ p^r divideix c.

Contraexemple

Petit Teorema de Fermat (de fet, Fermat-Euler) $\Rightarrow$
Si p nombre primer i $r \geq 1$ tenim que

$$2^{p^{r-1}(p-1)} \equiv 1 \pmod{p^r}$$

Posem

$$a = 2^{p^{r-1}(p-1)}\,,\ b = -1 \text{ i } c = 2^{p^{r-1}(p-1)} - 1$$

$\Rightarrow p^r$ divideix c.
Així

$$c \leq K \cdot \text{rad}(abc) \leq K \cdot 2c/p^{r-1},$$

d'on tindríem que $\forall p > 2$ i $\forall r > 1$

$$K \geq p^{r-1}/2.$$

La conjectura ABC

Masser i Oesterlé, 1985.

Per a tot $\epsilon > 0$, existeix una constant K_ϵ tal que, si $a + b = c$ amb a, b i c enters primers entre si, aleshores

$$\max\{|a|, |b|, |c|\} \leq K_\epsilon \text{rad}(abc)^{1+\epsilon}.$$

La conjectura ABC (bis)

Hi ha també versions més explícites:

La conjectura ABC (bis)

Hi ha també versions més explícites:
Si $\epsilon = 1$, *aleshores podem prendre* $K_1 = 1$. *Així tindríem*

$$\max\{|a|, |b|, |c|\} \leq \mathrm{rad}(abc)^2.$$

La conjectura ABC (bis)

Hi ha també versions més explícites:
Si $\epsilon = 1$, *aleshores podem prendre* $K_1 = 1$. *Així tindríem*

$$\max\{|a|, |b|, |c|\} \leq \text{rad}(abc)^2.$$

Existeixen constants absolutes K *i* L *tals que*

$$\max\{|a|, |b|, |c|\} \leq K\,\text{rad}(abc)\,L^{\omega(\text{rad}(abc))}$$

(on $\omega(N)$ *és el nombre de primers que divideixen* N*).*

Teorema

C. L. Steward i Kunrui Yu, 1996.

Existeix una constant C efectivament calculable tal que, si $a + b = c$ amb a, b i c enters primers entre si, aleshores

$$\max\{|a|, |b|, |c|\} \leq \exp\left(C \cdot \mathrm{rad}(abc)^{1/3} \log(\mathrm{rad}(abc))^3\right)$$

$$\leq \exp\left(C_\epsilon \mathrm{rad}(abc)^{1/3+\epsilon}\right)$$

Conseqüència:

Si

$$S := \text{ conjunt finit de primers}$$

aleshores el conjunt

$$ABC_S := \{a + b = c \mid (a, b, c) = 1 \text{ i } p | abc \Rightarrow p \in S\}$$

és finit.

Conseqüència:

Si

$$S := \text{ conjunt finit de primers}$$

aleshores el conjunt

$$ABC_S := \{a + b = c \mid (a, b, c) = 1 \text{ i } p|abc \Rightarrow p \in S\}$$

és finit.

Per exemple, quan $S = \{2, 3\}$, aleshores tenim

$$ABC_S := \{1 + 2 = 3,\ 1 + 3 = 2^2,\ 1 + 2^3 = 3^2\}$$

(Levi ben Gerson $(1288 - 1344)$)

Exercici

- Trobeu aquest conjunt ABC_S, utilitzant la versió amb $\epsilon = 1$ de la conjectura, en el cas $S = \{2, 3, 5\}$.

Exercici

- Trobeu aquest conjunt ABC_S, utilitzant la versió amb $\epsilon = 1$ de la conjectura, en el cas $S = \{2, 3, 5\}$.
- (***)Demostreu ara que efectivament aquestes són totes les solucions (sense utilitzar cap conjectura!).

Exercici

- Trobeu aquest conjunt ABC_S, utilitzant la versió amb $\epsilon = 1$ de la conjectura, en el cas $S = \{2, 3, 5\}$.
- (***)Demostreu ara que efectivament aquestes són totes les solucions (sense utilitzar cap conjectura!).
- Exemples:

$$2 + 3 = 5 \ , \ 1 + 2^4 \cdot 5 = 3^4 \ , \ 3 + 5^3 = 2^7 \ , \ \ldots$$

Exercici

- Trobeu aquest conjunt ABC_S, utilitzant la versió amb $\epsilon = 1$ de la conjectura, en el cas $S = \{2, 3, 5\}$.
- (***)Demostreu ara que efectivament aquestes són totes les solucions (sense utilitzar cap conjectura!).
- Exemples:

$$2 + 3 = 5 \ , \ 1 + 2^4 \cdot 5 = 3^4 \ , \ 3 + 5^3 = 2^7 \ , \ \ldots$$

- (Indicació: N'hi ha 16).

ABC $\Rightarrow$ “Catalan”

Suposem que tenim a, b, c i d enters més grans o iguals que 2 tals que

$$a^b + 1 = c^d.$$

ABC $\Rightarrow$ "Catalan"

Suposem que tenim a, b, c i d enters més grans o iguals que 2 tals que

$$a^b + 1 = c^d.$$

La conjectura abc implica que

$$c^d \leq K_\epsilon \text{rad}(ac)^{1+\epsilon} \leq K_\epsilon (ac)^{1+\epsilon}$$

ABC $\Rightarrow$ "Catalan"

Suposem que tenim a, b, c i d enters més grans o iguals que 2 tals que

$$a^b + 1 = c^d.$$

La conjectura abc implica que

$$c^d \leq K_\epsilon \text{rad}(ac)^{1+\epsilon} \leq K_\epsilon (ac)^{1+\epsilon}$$

Igualment tenim que

$$a^b < c^d \leq K_\epsilon (ac)^{1+\epsilon}$$

ABC $\Rightarrow$ "Catalan"

Suposem que tenim a, b, c i d enters més grans o iguals que 2 tals que

$$a^b + 1 = c^d.$$

La conjectura abc implica que

$$c^d \leq K_\epsilon \text{rad}(ac)^{1+\epsilon} \leq K_\epsilon (ac)^{1+\epsilon}$$

Igualment tenim que

$$a^b < c^d \leq K_\epsilon (ac)^{1+\epsilon}$$

Així tenim que

$$a^{b-2-2\epsilon} c^{d-2-2\epsilon} < K_\epsilon^2$$

ABC $\Rightarrow$ "Catalan"

Prenen logaritmes en base 2, i utilitzant que a i $c \geq 2$ tenim que

$$b + d < 4 + 4\epsilon + 2\log_2(K_\epsilon)$$

ABC $\Rightarrow$ "Catalan"

Prenen logaritmes en base 2, i utilitzant que a i $c \geq 2$ tenim que

$$b + d < 4 + 4\epsilon + 2\log_2(K_\epsilon)$$

Per tant b i d estan acotats.

ABC $\Rightarrow$ "Catalan"

Prenen logaritmes en base 2, i utilitzant que a i $c \geq 2$ tenim que

$$b + d < 4 + 4\epsilon + 2\log_2(K_\epsilon)$$

Per tant b i d estan acotats.

A més: Podem també acotar a i c en funció de K_ϵ per a b i d no massa petits.

ABC $\Rightarrow$ "Catalan"

Prenen logaritmes en base 2, i utilitzant que a i $c \geq 2$ tenim que

$$b + d < 4 + 4\epsilon + 2\log_2(K_\epsilon)$$

Per tant b i d estan acotats.

A més: Podem també acotar a i c en funció de K_ϵ per a b i d no massa petits.
(No ens diu res, per exemple, si $b = d = 2$).

ABC $\Rightarrow$ “Catalan”

Treballant amb la versió explícita que ens diu que $K_1 = 1$, tindríem que

$$b + d < 8$$

i, de fet, si $c > a$, aleshores $d = 2$ o 3, i si $c < a$, aleshores $b = 2$ o 3.

ABC $\Rightarrow$ "Catalan"

Treballant amb la versió explícita que ens diu que $K_1 = 1$, tindríem que

$$b + d < 8$$

i, de fet, si $c > a$, aleshores $d = 2$ o 3, i si $c < a$, aleshores $b = 2$ o 3.
En resum, només ens caldria considerar a part els casos

$$2 \leq d \leq 3 \text{ i } 2 \leq b \leq 5$$

$$2 \leq b \leq 3 \text{ i } 4 \leq d \leq 5$$

(que són coneguts i "fàcils").

ABC $\Rightarrow$ “Fermat”

ABC $\Rightarrow$ “Fermat”

Exercici!

ABC $\Rightarrow$ "Fermat"

Exercici!

Indicació: Preneu $\epsilon = 1/8$, i proveu que les "solucions" estan acotades en funció de $K_{1/8}$

ABC $\Rightarrow$ "Fermat"

Exercici!

Indicació: Preneu $\epsilon = 1/8$, i proveu que les "solucions" estan acotades en funció de $K_{1/8}$

O bé preneu la versió amb $K_1 = 1$ i proveu que $n \leq 5$

Problema General

Calcular les solucions $(x, y) \in \mathbb{Q}^2$ d'una equació

$$f(x, y) = 0$$

on $f(x, y) \in \mathbb{Q}[x, y]$.

Problema General

Calcular les solucions $(x, y) \in \mathbb{Q}^2$ d'una equació

$$f(x, y) = 0$$

on $f(x, y) \in \mathbb{Q}[x, y]$.

Desingularització

Problema General

Calcular les solucions $(x, y) \in \mathbb{Q}^2$ d'una equació

$$f(x, y) = 0$$

on $f(x, y) \in \mathbb{Q}[x, y]$.

Desingularització

$\Downarrow$

Problema General

Calcular les solucions $(x, y) \in \mathbb{Q}^2$ d'una equació

$$f(x, y) = 0$$

on $f(x, y) \in \mathbb{Q}[x, y]$.

Desingularització

$\Downarrow$

Ens podem reduir al cas que $f(x, y)$ és no singular (també en l'"infinit")

Teorema de Faltings

G. Faltings, 1984.

(abans anomenada Conjectura de Mordell)

Teorema de Faltings

G. Faltings, 1984.

(abans anomenada Conjectura de Mordell)

Si $f(x,y) \in \mathbb{Q}[x,y]$ és no singular a tot arreu (també al ∞) i el seu grau és > 3, aleshores té un nombre finit de solucions a $\mathbb{Q}$.

Teorema de Faltings

G. Faltings, 1984.

(abans anomenada Conjectura de Mordell)

Si $f(x,y) \in \mathbb{Q}[x,y]$ és no singular a tot arreu (també al ∞) i el seu grau és > 3, aleshores té un nombre finit de solucions a $\mathbb{Q}$.

Tota corba no singular i projectiva de gènere ≥ 2 sobre $\mathbb{Q}$ té un nombre finit de solucions racionals.

Teorema de Faltings

G. Faltings, 1984.

(abans anomenada Conjectura de Mordell)

Si $f(x,y) \in \mathbb{Q}[x,y]$ és no singular a tot arreu (també al ∞) i el seu grau és > 3, aleshores té un nombre finit de solucions a $\mathbb{Q}$.

Tota corba no singular i projectiva de gènere ≥ 2 sobre $\mathbb{Q}$ té un nombre finit de solucions racionals.

El mateix és cert a les extensions finites de $\mathbb{Q}$ (cossos de nombres), per exemple per a $\mathbb{Q}(\sqrt{2})$.

Exemples d'aplicació.

Les següents equacions tenen un nombre finit de solucions racionals:

- $y^2 = (x^2 + 1)(x^2 + 2)(x^2 + 2x + 2)$.

Exemples d'aplicació.

Les següents equacions tenen un nombre finit de solucions racionals:

- $y^2 = (x^2 + 1)(x^2 + 2)(x^2 + 2x + 2)$.
- $y^2 = \frac{1}{5}x^5 + \frac{1}{2}x^4 + \frac{1}{3}x^3 - \frac{1}{30}x$.

Exemples d'aplicació.

Les següents equacions tenen un nombre finit de solucions racionals:

- $y^2 = (x^2+1)(x^2+2)(x^2+2x+2)$.
- $y^2 = \frac{1}{5}x^5 + \frac{1}{2}x^4 + \frac{1}{3}x^3 - \frac{1}{30}x$.
- Si $p(x) \in \mathbb{Q}[x]$ no té arrels múltiples, i $\deg(p(x)) \geq 5$:

$$y^2 = p(x).$$

Exemples d'aplicació.

Les següents equacions tenen un nombre finit de solucions racionals:

- $y^2 = (x^2+1)(x^2+2)(x^2+2x+2)$.
- $y^2 = \frac{1}{5}x^5 + \frac{1}{2}x^4 + \frac{1}{3}x^3 - \frac{1}{30}x$.
- Si $p(x) \in \mathbb{Q}[x]$ no té arrels múltiples, i $\deg(p(x)) \geq 5$:

$$y^2 = p(x).$$

- $x^4 + y^4 = 17$.

Exemples d'aplicació.

Les següents equacions tenen un nombre finit de solucions racionals:

- $y^2 = (x^2+1)(x^2+2)(x^2+2x+2)$.
- $y^2 = \frac{1}{5}x^5 + \frac{1}{2}x^4 + \frac{1}{3}x^3 - \frac{1}{30}x$.
- Si $p(x) \in \mathbb{Q}[x]$ no té arrels múltiples, i $\deg(p(x)) \geq 5$:

$$y^2 = p(x).$$

- $x^4 + y^4 = 17$.
- Si $F(x,y)$ polinomi homogeni irreductible, i $k \in \mathbb{Q}$:

$$F(x,y) = k.$$

Problema: “Mordell Efectiu”

Trobar un mètode per calcular totes les solucions.

Problema: “Mordell Efectiu”

Trobar un mètode per calcular totes les solucions.
Per exemple:

Problema: “Mordell Efectiu”

Trobar un mètode per calcular totes les solucions.
Per exemple:

- $y^2 = (x^2+1)(x^2+2)(x^2+2x+2)$ aleshores $x = 0, 1/2$ (Flynn 1997).

Problema: “Mordell Efectiu”

Trobar un mètode per calcular totes les solucions. Per exemple:

- $y^2 = (x^2+1)(x^2+2)(x^2+2x+2)$ aleshores $x = 0, 1/2$ (Flynn 1997).
- $y^2 = \frac{1}{5}x^5 + \frac{1}{2}x^4 + \frac{1}{3}x^3 - \frac{1}{30}x$, aleshores

$$x \in \{-\frac{5}{4}, -\frac{6}{5}, -1, -\frac{1}{2}, -\frac{1}{9}, 0, \frac{1}{2}, 1\}$$

(Bruin i Flynn, 2003)

Problema: “Mordell Efectiu”

Trobar un mètode per calcular totes les solucions. Per exemple:

- $y^2 = (x^2+1)(x^2+2)(x^2+2x+2)$ aleshores $x = 0, 1/2$ (Flynn 1997).
- $y^2 = \frac{1}{5}x^5 + \frac{1}{2}x^4 + \frac{1}{3}x^3 - \frac{1}{30}x$, aleshores

$$x \in \{-\frac{5}{4}, -\frac{6}{5}, -1, -\frac{1}{2}, -\frac{1}{9}, 0, \frac{1}{2}, 1\}$$

  (Bruin i Flynn, 2003)
- $x^4 + y^4 = 17$, aleshores $x = \pm 1, \pm 2$ (Flynn i Wetherell, 2001).

ABC $\Rightarrow$ Mordell efectiu

N. Elkies, 1991.

Si la conjectura ABC és certa, i $\forall \epsilon > 0$ sabem calcular explícitament K_ϵ, aleshores:

ABC $\Rightarrow$ Mordell efectiu

N. Elkies, 1991.

Si la conjectura ABC és certa, i $\forall \epsilon > 0$ sabem calcular explícitament K_ϵ, aleshores:

Hi ha un mètode efectiu per trobar totes les solucions de qualsevol corba no singular i projectiva de gènere ≥ 2 sobre $\mathbb{Q}$.

Mordell efectiu $\Rightarrow$ ABC

L. Moret-Bailly, 1999.

Si podem trobar fites *bones* per a la "mida" de les coordenades dels punts racionals d'una equació com les d'abans, però en qualsevol cos de nombres, aleshores la conjectura ABC és certa.

Altres conseqüències

Se sap que la conjectura ABC implica també:

Altres conseqüències

Se sap que la conjectura ABC implica també:

- Una millora del teorema de Siegel.

Altres conseqüències

Se sap que la conjectura ABC implica també:

- Una millora del teorema de Siegel.
- Una millora del teorema de Baker.

Altres conseqüències

Se sap que la conjectura ABC implica també:

- Una millora del teorema de Siegel.
- Una millora del teorema de Baker.
- Una millora del teorema de Roth.

Altres conseqüències

Se sap que la conjectura ABC implica també:

- Una millora del teorema de Siegel.
- Una millora del teorema de Baker.
- Una millora del teorema de Roth.
- Que no hi ha zeros de Siegel (conseqüència de la hipòtesi de Riemann Generalitzada).

Altres conseqüències

Se sap que la conjectura ABC implica també:

- Una millora del teorema de Siegel.
- Una millora del teorema de Baker.
- Una millora del teorema de Roth.
- Que no hi ha zeros de Siegel (conseqüència de la hipòtesi de Riemann Generalitzada).
- La conjectura de Szpiro i de l'altura sobre corbes el·líptiques.

Altres conseqüències

Se sap que la conjectura ABC implica també:

- Una millora del teorema de Siegel.
- Una millora del teorema de Baker.
- Una millora del teorema de Roth.
- Que no hi ha zeros de Siegel (conseqüència de la hipòtesi de Riemann Generalitzada).
- La conjectura de Szpiro i de l'altura sobre corbes el·líptiques.
- I fins a 23 conjectures diferents més.

Altres conseqüències (2)

La conjectura ABC ve implicada també per:

- Una millora del teorema de Siegel.
- Una millora del teorema de Baker.
- Una millora del teorema de Roth.
- La conjectura de l'altura sobre corbes el·líptiques.