Jornada Teoria de Nombres (Cargols)

Diferencias de potencias perfectas y potencias de primos

Pedro-José Cazorla García

Universidad Pontificia Comillas

26 de octubre de 2024

Conjetura de Catalan

Conjetura (Catalan, 1844)

La única solución a la ecuación diofántica

$$y^n - z^m = 1$$

en enteros y, z, n, m con $y, z > 0$ y $n, m > 1$ viene dada por la tupla

$$(y, z, n, m) = (3, 2, 2, 3).$$

Conjetura de Catalan

Conjetura (Catalan, 1844)

La única solución a la ecuación diofántica

$$y^n - z^m = 1$$

en enteros y, z, n, m con $y, z > 0$ y $n, m > 1$ viene dada por la tupla

$$(y, z, n, m) = (3, 2, 2, 3).$$

Problema abierto durante muchos años, y finalmente demostrado por **Mihăilescu** en 2002

Una generalización natural del problema

Pregunta:

¿Podemos resolver la ecuación diofántica

$$y^n - z^m = D$$

para un valor $D > 0$ arbitrario?

Una generalización natural del problema

Pregunta:

¿Podemos resolver la ecuación diofántica

$$y^n - z^m = D$$

para un valor $D > 0$ arbitrario?

Respuesta:

¡¡Ni siquiera sabemos si tiene un número **finito** de soluciones!!

Lo que sí podemos resolver

Pregunta:

¿Podemos resolver la ecuación diofántica

$$y^n - q^\alpha = C_1 x^2,$$

donde q es un primo fijo y C_1 es un entero libre de cuadrados fijo?

Lo que sí podemos resolver

Pregunta:

¿Podemos resolver la ecuación diofántica

$$y^n - q^\alpha = C_1 x^2,$$

donde q es un primo fijo y C_1 es un entero libre de cuadrados fijo?

Respuesta:

¡Sí!

Lo que sí podemos resolver

Pregunta:

¿Podemos resolver la ecuación diofántica

$$y^n - q^\alpha = C_1 x^2,$$

donde q es un primo fijo y C_1 es un entero libre de cuadrados fijo?

Respuesta:

¡Sí! La ecuación

$$C_1 x^2 + q^\alpha = y^n$$

es una variación de la **ecuación generalizada de Lebesgue–Nagell**, que ha sido ampliamente estudiada (recientemente por Bennett y Siksek en 2022).

Estrategia

Nuestra ecuación

$$C_1 x^2 + q^\alpha = y^n$$

Estrategia

Nuestra ecuación

$$C_1 x^2 + q^\alpha = y^n$$

Durante el resto de la charla, asumiremos que y es par.

Estrategia

Nuestra ecuación

$$C_1 x^2 + q^\alpha = y^n$$

Durante el resto de la charla, asumiremos que y es par.

1. Acotar n, de forma que $n < N_0(C_1, q)$.
2. Resolver la ecuación para cada valor restante de n.

Estrategia: acotar n

Nuestra ecuación

$$C_1 x^2 + q^\alpha = y^n$$

1. Acotar n, de forma que $n < N_0(C_1, q)$. Dos técnicas:

Estrategia: acotar n

Nuestra ecuación

$$C_1 x^2 + q^\alpha = y^n$$

1. Acotar n, de forma que $n < N_0(C_1, q)$. Dos técnicas:
   - Formas lineales en logaritmos ($q-$ádicos y complejos): siempre funcionan, pero la cota obtenida es mala.

Estrategia: acotar n

Nuestra ecuación

$$C_1 x^2 + q^\alpha = y^n$$

1. Acotar n, de forma que $n < N_0(C_1, q)$. Dos técnicas:
   - Formas lineales en logaritmos ($q-$ádicos y complejos): siempre funcionan, pero la cota obtenida es mala.
   - Método modular: no siempre funciona pero la cota es excelente.

Estrategia: resolver para n fijo

Nuestra ecuación

$$C_1 x^2 + q^\alpha = y^n$$

2. Resolver la ecuación para cada valor restante de n. De nuevo, dos técnicas:

Estrategia: resolver para n fijo

Nuestra ecuación

$$C_1 x^2 + q^\alpha = y^n$$

2. Resolver la ecuación para cada valor restante de n. De nuevo, dos técnicas:

    - Ecuaciones de Thue–Mahler (estudiadas recientemente por Gherga–Siksek, 2022): muy útiles en teoría, impracticable para exponentes grandes ($n > 11$).

Estrategia: resolver para n fijo

Nuestra ecuación

$$C_1 x^2 + q^\alpha = y^n$$

2. Resolver la ecuación para cada valor restante de n. De nuevo, dos técnicas:

   - Ecuaciones de Thue–Mahler (estudiadas recientemente por Gherga–Siksek, 2022): muy útiles en teoría, impracticable para exponentes grandes ($n > 11$).
   - Método modular: puede aplicarse a todos los exponentes $n > 5$, pero **siempre falla si la ecuación tiene soluciones**.

El método modular en pocas palabras

$$C_1 x^2 + q^\alpha = y^n$$

El método modular en pocas palabras

$$C_1 x^2 + q^\alpha = y^n$$

Siguiendo las recetas de Bennett y Skinner (2004), definimos F mediante la siguiente ecuación:

$$F : Y^2 + XY = X^3 + \frac{C_1 x - 1}{4} X^2 + \frac{C_1 y^n}{64} X.$$

Esta ecuación define una **curva elíptica**, que llamaremos la **curva de Frey**.

Continuación del método modular

$$F : Y^2 + XY = X^3 + \frac{C_1 x - 1}{4} X^2 + \frac{C_1 y^n}{64} X.$$

Esta ecuación define una **curva elíptica**, que llamaremos la **curva de Frey**.

Continuación del método modular

$$F : Y^2 + XY = X^3 + \frac{C_1 x - 1}{4} X^2 + \frac{C_1 y^n}{64} X.$$

Esta ecuación define una **curva elíptica**, que llamaremos la **curva de Frey**.

Por el teorema de la modularidad (Wiles, Conrad, Diamond, Taylor, Breuil, 2001), junto con el teorema de bajada de nivel de Ribet (1986), puede demostrarse que

$$\overline{\rho}_n(F) \cong \overline{\rho}_n(f)$$

para cierta $f \in S_2^{new}(\Gamma_0(N))$.

Continuación del método modular

$$F : Y^2 + XY = X^3 + \frac{C_1 x - 1}{4} X^2 + \frac{C_1 y^n}{64} X.$$

Esta ecuación define una **curva elíptica**, que llamaremos la **curva de Frey**.

Por el teorema de la modularidad (Wiles, Conrad, Diamond, Taylor, Breuil, 2001), junto con el teorema de bajada de nivel de Ribet (1986), puede demostrarse que

$$\overline{\rho}_n(F) \cong \overline{\rho}_n(f)$$

para cierta $f \in S_2^{new}(\Gamma_0(N))$.

Objetivo: Demostrar que, para todas las formas f, existe un primo ℓ para el que

$$\overline{\rho}_n(F)(Frob_\ell) \neq \overline{\rho}_n(f)(Frob_\ell).$$

Un lema fundamental

Lemma

Sea $\ell = 2kn + 1$ un primo (+ condiciones técnicas). Entonces, se tiene que $\overline{\rho}_n(F)(Frob_\ell)$ depende únicamente de:

- *La clase de $q \pmod{\ell}$.*
- *La clase de $\alpha \pmod{2n}$, que denotaremos por β.*
- *Cierto $\omega \in \{0, 1, \ldots, \ell - 1\}$ que satisface la siguiente ecuación de congruencia:*

$$(C_1\omega^2 + q^\beta)^{2k} \equiv 1 \pmod{\ell}.$$

Un lema fundamental

Lemma

Sea $\ell = 2kn + 1$ un primo (+ condiciones técnicas). Entonces, se tiene que $\overline{\rho}_n(F)(Frob_\ell)$ depende únicamente de:

- *La clase de q (mod ℓ).*
- *La clase de α (mod $2n$), que denotaremos por β.*
- *Cierto $\omega \in \{0, 1, \ldots, \ell - 1\}$ que satisface la siguiente ecuación de congruencia:*

$$(C_1\omega^2 + q^\beta)^{2k} \equiv 1 \pmod{\ell}.$$

Empleando este lema, calcular todas las posibilidades de $\overline{\rho}_n(F)(Frob_\ell)$ es un cálculo finito, con lo que podemos encontrar un ℓ que demuestre que

$$\overline{\rho}_n(F)(Frob_\ell) \neq \overline{\rho}_n(f)(Frob_\ell).$$

Conclusiones

Con todas las herramientas mencionadas, podemos demostrar que

Teorema (C-G, 2023)

Podemos encontrar todas las soluciones

$$C_1 x^2 + q^\alpha = y^n,$$

donde $1 \leq C_1 \leq 20$ es un entero libre de cuadrados fijo y $2 \leq q < 25$ es un primo fijo.

Conclusiones

Con todas las herramientas mencionadas, podemos demostrar que

Teorema (C-G, 2023)

Podemos encontrar todas las soluciones

$$C_1 x^2 + q^\alpha = y^n,$$

donde $1 \leq C_1 \leq 20$ es un entero libre de cuadrados fijo y $2 \leq q < 25$ es un primo fijo.

Los rangos son "máximos" porque:

$$21 \cdot 79^2 + 11^1 = 2^{17}$$

$$3 \cdot 209^2 + 29^1 = 2^{17}.$$

Conjetura de Catalan

¿Alguna pregunta?