$\mathbb{Q}$-curvas y algunas ecuaciones diofánticas

Lucas Villagra Torcomian
Universidad Nacional de Córdoba

20 de Agosto de 2020 – Seminario LATeN

El método de modularidad

Teorema (Fermat-Wiles)
Si $n \geq 3$, la ecuación $x^n + y^n = z^n$ no tiene solución entera tal que $xyz \neq 0$.

Teorema (Fermat-Wiles)
Si $n \geq 3$, la ecuación $x^n + y^n = z^n$ no tiene solución entera tal que $xyz \neq 0$.

Observación
Basta probarlo para $n = p \geq 3$ primo.

Teorema (Fermat-Wiles)
Si $n \geq 3$, la ecuación $x^n + y^n = z^n$ no tiene solución entera tal que $xyz \neq 0$.

Observación
Basta probarlo para $n = p \geq 3$ primo.

Demostración (idea).

(1) A una solución (A, B, C) le asociamos la curva elíptica $E_{(A,B)} : y^2 = X(X - A^p)(X + B^p)$ (curva de Frey) que satisface $\Delta = \frac{1}{2^8} A^{2p} B^{2p} (\underbrace{A^p + B^p}_{=C^p})^2 = \frac{1}{2^8} (ABC)^{2p}$.

(2) $E = E_{(A,B)}$ es modular (Wiles, Taylor-Wiles). Consideramos la representación de Galois $\rho_{E,p}$ que se obtiene al mirar la acción de $\mathrm{Gal}_{\mathbb{Q}}$ en $E[p]$. Sabemos que $\rho_{E,p}$ es irreducible (por el teorema de clasificación de Mazur).

El método de modularidad

Por modularidad, existe $g \in S_k(N, \varepsilon)$ tal que $\rho_{E,p} \equiv \rho_{g,p}$ (mód p), donde $\varepsilon = 1$, $k = 2$ y $N = N_E$ es el producto de los primos $\ell \neq p$ en donde la curva E tiene mala reducción (i.e. $v_\ell(\Delta) \neq 0$).

El método de modularidad

Por modularidad, existe $g \in S_k(N, \varepsilon)$ tal que $\rho_{E,p} \equiv \rho_{g,p}$ (mód p), donde $\varepsilon = 1$, $k = 2$ y $N = N_E$ es el producto de los primos $\ell \neq p$ en donde la curva E tiene mala reducción (i.e. $v_\ell(\Delta) \neq 0$).

(3) Entamos en condiciones de hacer bajada de nivel.

Teorema (Bajada de nivel de Ribet)
Supongamos que $\rho_{E,p}$ es absolutamente irreducible. Si $\ell \neq p$ es un primo de reducción multiplicativa y $p | v_\ell(\Delta)$ entonces podemos quitar a ℓ del producto anterior. Más aún, si $\rho_{E,p}$ es "finita" en p, también podemos sacar p.

Es decir que existe $f \in S_2(2)$ tal que $\rho_{E,p} \equiv \rho_{f,p}$ (mód p).

El método de modularidad

Por modularidad, existe $g \in S_k(N, \varepsilon)$ tal que $\rho_{E,p} \equiv \rho_{g,p}$ (mód p), donde $\varepsilon = 1$, $k = 2$ y $N = N_E$ es el producto de los primos $\ell \neq p$ en donde la curva E tiene mala reducción (i.e. $v_\ell(\Delta) \neq 0$).

(3) Entamos en condiciones de hacer bajada de nivel.

Teorema (Bajada de nivel de Ribet)
Supongamos que $\rho_{E,p}$ es absolutamente irreducible. Si $\ell \neq p$ es un primo de reducción multiplicativa y $p | v_\ell(\Delta)$ entonces podemos quitar a ℓ del producto anterior. Más aún, si $\rho_{E,p}$ es "finita" en p, también podemos sacar p.

Es decir que existe $f \in S_2(2)$ tal que $\rho_{E,p} \equiv \rho_{f,p}$ (mód p).

(4) Como $S_2(2) = 0$, absurdo. □

Por modularidad, existe $g \in S_k(N, \varepsilon)$ tal que $\rho_{E,p} \equiv \rho_{g,p}$ (mód p), donde $\varepsilon = 1$, $k = 2$ y $N = N_E$ es el producto de los primos $\ell \neq p$ en donde la curva E tiene mala reducción (i.e. $v_\ell(\Delta) \neq 0$).

(3) Entamos en condiciones de hacer bajada de nivel.

Teorema (Bajada de nivel de Ribet)
Supongamos que $\rho_{E,p}$ es absolutamente irreducible. Si $\ell \neq p$ es un primo de reducción multiplicativa y $p | v_\ell(\Delta)$ entonces podemos quitar a ℓ del producto anterior. Más aún, si $\rho_{E,p}$ es "finita" en p, también podemos sacar p.

Es decir que existe $f \in S_2(2)$ tal que $\rho_{E,p} \equiv \rho_{f,p}$ (mód p).

(4) Como $S_2(2) = 0$, absurdo. □

Observación
Cuándo usamos qué $ABC \neq 0$!!!???

(1) **Construcción de una curva** (a partir de una supuesta solución) de manera que $\Delta = c \cdot D^p$, donde c dependa de la ecuación que queremos resolver pero no de la solución y D sí dependa de la solución.
Además, queremos que los primos que dividan a D sean primos de reducción multiplicativa para la curva.

El método de modularidad

(1) **Construcción de una curva** (a partir de una supuesta solución) de manera que $\Delta = c \cdot D^p$, donde c dependa de la ecuación que queremos resolver pero no de la solución y D sí dependa de la solución.
Además, queremos que los primos que dividan a D sean primos de reducción multiplicativa para la curva.

(2) **Modularidad de la curva:** la curva es modular porque...

El método de modularidad

(1) **Construcción de una curva** (a partir de una supuesta solución) de manera que $\Delta = c \cdot D^p$, donde c dependa de la ecuación que queremos resolver pero no de la solución y D sí dependa de la solución.
Además, queremos que los primos que dividan a D sean primos de reducción multiplicativa para la curva.

(2) **Modularidad de la curva:** la curva es modular porque...

(3) **Bajada de nivel** para determinar una forma nueva de tipo (N, k, ε) que *casi* no dependa de la solución.

El método de modularidad

(1) **Construcción de una curva** (a partir de una supuesta solución) de manera que $\Delta = c \cdot D^p$, donde c dependa de la ecuación que queremos resolver pero no de la solución y D sí dependa de la solución.
Además, queremos que los primos que dividan a D sean primos de reducción multiplicativa para la curva.

(2) **Modularidad de la curva:** la curva es modular porque...

(3) **Bajada de nivel** para determinar una forma nueva de tipo (N, k, ε) que *casi* no dependa de la solución.

(4) **Eliminación de las posibles formas**.

Ecuación de Fermat generalizada

Teorema (Darmon y Granville, 1995)
Sean $a, b, c \in \mathbb{Z}$ fijos. Si (p, q, r) es una tripla de primos tal que $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ entonces la ecuación

$$ax^p + by^q = cz^r$$

tiene finitas soluciones **primitivas**.

Ejemplos

Ejemplos

Algunos ejemplos de ecuaciones resultas con este método son:

- $x^n + y^n = z^2$, $x^n + y^n = z^3$ (Darmon-Merel 1997, Poonen 1998)
- $x^4 + y^2 = z^p$ (Ellemberg 2004)
- $x^4 + dy^2 = z^p$ para $d = 2, 3$ (Dieulefait, Jiménez-Urroz 2009)
- $x^2 + y^6 = z^n$ (Bennet-Chen 2012)

$$x^4 + dy^2 = z^p$$

$x^4 + 6y^2 = z^p$, construcción de la curva

Veamos que la ecuación $x^4 + 6y^2 = z^p$ no tiene solución primitiva no trivial si $p > 19$.

$x^4 + 6y^2 = z^p$, construcción de la curva

Veamos que la ecuación $x^4 + 6y^2 = z^p$ no tiene solución primitiva no trivial si $p > 19$.

Observación (advertencia)
Para p más chico esto no es necesariamente cierto (notar que $11^4 + 6 \cdot 19^2 = 7^5$*).*

$x^4 + 6y^2 = z^p$, construcción de la curva

Veamos que la ecuación $x^4 + 6y^2 = z^p$ no tiene solución primitiva no trivial si $p > 19$.

Observación (advertencia)
Para p más chico esto no es necesariamente cierto (notar que $11^4 + 6 \cdot 19^2 = 7^5$*).*

(1) **Construcción de una curva:** Dada (A, B, C) una solución primitiva, consideremos la curva $E = E_{(A,B)} : y^2 = x^3 + 4Ax^2 + 2(A^2 + \sqrt{-6}B)x$, definida sobre $K = \mathbb{Q}(\sqrt{-6})$ y cuyo discriminante está dado por

$$\Delta = 2^9(A^2 + \sqrt{-6}B)^2(A^2 - \sqrt{-6}B) = 2^9(A^2 + \sqrt{-6}B)C^p.$$

$x^4 + 6y^2 = z^p$, construcción de la curva

Veamos que la ecuación $x^4 + 6y^2 = z^p$ no tiene solución primitiva no trivial si $p > 19$.

Observación (advertencia)
Para p más chico esto no es necesariamente cierto (notar que $11^4 + 6 \cdot 19^2 = 7^5$*).*

(1) **Construcción de una curva:** Dada (A, B, C) una solución primitiva, consideremos la curva $E = E_{(A,B)} : y^2 = x^3 + 4Ax^2 + 2(A^2 + \sqrt{-6}B)x$, definida sobre $K = \mathbb{Q}(\sqrt{-6})$ y cuyo discriminante está dado por

$$\Delta = 2^9(A^2 + \sqrt{-6}B)^2(A^2 - \sqrt{-6}B) = 2^9(A^2 + \sqrt{-6}B)C^p.$$

(2) **Modularidad de la curva:** E es modular porque...

$x^4 + 6y^2 = z^p$, construcción de la curva

Veamos que la ecuación $x^4 + 6y^2 = z^p$ no tiene solución primitiva no trivial si $p > 19$.

Observación (advertencia)
Para p más chico esto no es necesariamente cierto (notar que $11^4 + 6 \cdot 19^2 = 7^5$*).*

(1) **Construcción de una curva:** Dada (A, B, C) una solución primitiva, consideremos la curva $E = E_{(A,B)} : y^2 = x^3 + 4Ax^2 + 2(A^2 + \sqrt{-6}B)x$, definida sobre $K = \mathbb{Q}(\sqrt{-6})$ y cuyo discriminante está dado por

$$\Delta = 2^9(A^2 + \sqrt{-6}B)^2(A^2 - \sqrt{-6}B) = 2^9(A^2 + \sqrt{-6}B)C^p.$$

(2) **Modularidad de la curva:** E es modular porque... ¿Por qué es modular?

$x^4 + 6y^2 = z^p$, construcción de la curva

Veamos que la ecuación $x^4 + 6y^2 = z^p$ no tiene solución primitiva no trivial si $p > 19$.

Observación (advertencia)
Para p más chico esto no es necesariamente cierto (notar que $11^4 + 6 \cdot 19^2 = 7^5$*).*

(1) **Construcción de una curva:** Dada (A, B, C) una solución primitiva, consideremos la curva $E = E_{(A,B)} : y^2 = x^3 + 4Ax^2 + 2(A^2 + \sqrt{-6}B)x$, definida sobre $K = \mathbb{Q}(\sqrt{-6})$ y cuyo discriminante está dado por

$$\Delta = 2^9(A^2 + \sqrt{-6}B)^2(A^2 - \sqrt{-6}B) = 2^9(A^2 + \sqrt{-6}B)C^p.$$

(2) **Modularidad de la curva:** E es modular porque... ¿Por qué es modular?
No hay ningún resultado que garantice con genereralidad la modularidad de curvas sobre cuerpos cuadráticos imaginarios.

Sea $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ no trivial. Notemos que $E^\sigma : y^2 = x^3 + 4Ax^2 + 2(A^2 - \sqrt{-6}B)x$.

$$\to -2y^2 = x^3 + 4Ax^2 + 2(A^2 - \sqrt{-6}B)x$$

$$\to -\frac{1}{8}y^2 = -\frac{1}{8}x^3 + Ax^2 - (A^2 - \sqrt{-6}B)x$$

$$\to y^2 = x^3 - 8Ax^2 + 8(A^2 - \sqrt{-6}B)x,$$

el cociente de E por $(0,0)$. Luego, E y E^σ son isógenas. Por lo tanto, E es una $\mathbb{Q}$-curva definida sobre $\mathbb{Q}(\sqrt{-6}, \sqrt{-2})$.

Sea $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ no trivial. Notemos que $E^\sigma : y^2 = x^3 + 4Ax^2 + 2(A^2 - \sqrt{-6}B)x$.

$$\to -2y^2 = x^3 + 4Ax^2 + 2(A^2 - \sqrt{-6}B)x$$

$$\to -\frac{1}{8}y^2 = -\frac{1}{8}x^3 + Ax^2 - (A^2 - \sqrt{-6}B)x$$

$$\to y^2 = x^3 - 8Ax^2 + 8(A^2 - \sqrt{-6}B)x,$$

el cociente de E por $(0,0)$. Luego, E y E^σ son isógenas. Por lo tanto, E es una $\mathbb{Q}$-curva definida sobre $\mathbb{Q}(\sqrt{-6}, \sqrt{-2})$.

Teorema (Ribet)
Para toda $\mathbb{Q}$-curva existe un twist tal que la representación asociada desciende a $\mathbb{Q}$.

Sea ε el caracter correspondiente a la extensión $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ y sea ψ_{-2} el caracter correspondiente a la extensión $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$

Sea ε el caracter correspondiente a la extensión $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ y sea ψ_{-2} el caracter correspondiente a la extensión $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$

Teorema (Pacetti - V.T.)
Existe un caracter de Hecke $\chi : \mathrm{Gal}_K \to \overline{\mathbb{Q}}$ *tal que:*

1. $\chi^2 = \varepsilon$ *como caracteres de* Gal_K,
2. χ *sólo ramifica en el primo arriba de* 2,
3. ${}^{\tau}\chi = \chi \cdot \psi_{-2}$ *como caracteres de* Gal_K.

Sea ε el caracter correspondiente a la extensión $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ y sea ψ_{-2} el caracter correspondiente a la extensión $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$

Teorema (Pacetti - V.T.)
Existe un caracter de Hecke $\chi : \mathrm{Gal}_K \to \overline{\mathbb{Q}}$ *tal que:*

1. $\chi^2 = \varepsilon$ *como caracteres de* Gal_K,
2. χ *sólo ramifica en el primo arriba de* 2,
3. ${}^{\tau}\chi = \chi \cdot \psi_{-2}$ *como caracteres de* Gal_K.

Teorema (Pacetti - V.T.)
La representación $\rho_{E,p} \otimes \chi$ *desciende a una representación (de dimensión* 2*) de* $\mathrm{Gal}_{\mathbb{Q}}$*, adjunta a una forma nueva de tipo* (N, k, ε) *con* $k = 2$, ε *como antes y* $N = 2^e \cdot 3 \cdot \prod_q q^{v_q(N_E)}$, $e = 8, 9$.

Sea ε el caracter correspondiente a la extensión $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ y sea ψ_{-2} el caracter correspondiente a la extensión $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$

Teorema (Pacetti - V.T.)
Existe un caracter de Hecke $\chi : \mathrm{Gal}_K \to \overline{\mathbb{Q}}$ *tal que:*

1. $\chi^2 = \varepsilon$ *como caracteres de* Gal_K,
2. χ *sólo ramifica en el primo arriba de* 2,
3. ${}^{\tau}\chi = \chi \cdot \psi_{-2}$ *como caracteres de* Gal_K.

Teorema (Pacetti - V.T.)
La representación $\rho_{E,p} \otimes \chi$ *desciende a una representación (de dimensión* 2*) de* $\mathrm{Gal}_{\mathbb{Q}}$*, adjunta a una forma nueva de tipo* (N, k, ε) *con* $k = 2$, ε *como antes y* $N = 2^e \cdot 3 \cdot \prod_q q^{v_q(N_E)}$, $e = 8, 9$.

(3) **Bajada de nivel:**

Teorema (Ellemberg)
Si K *es cuadrático imaginario y* E *es una* $\mathbb{Q}$*-curva sin CM, entonces existe* N_K *tal que si* $p > N_K$ *la representacion* $\rho_{E,p}$ *es suryectiva.*

$x^4 + 6y^2 = z^p$, bajada de nivel

Como existe $q \nmid 6$ tal que E tiene reducción multiplicativa en q, tenemos bajada de nivel e imagen grande.

Luego, por el teorema de baja de nivel, existe $f \in S_2(n, \varepsilon)$, donde $n = 2^e \cdot 3$, tal que

$$\rho_{E,p} \equiv \rho_{f,K,p} \otimes \chi^{-1} \quad (\text{mód } p).$$

$x^4 + 6y^2 = z^p$, bajada de nivel

Como existe $q \nmid 6$ tal que E tiene reducción multiplicativa en q, tenemos bajada de nivel e imagen grande.

Luego, por el teorema de baja de nivel, existe $f \in S_2(n, \varepsilon)$, donde $n = 2^e \cdot 3$, tal que

$$\rho_{E,p} \equiv \rho_{f,K,p} \otimes \chi^{-1} \quad (\text{mód } p).$$

Como existe $q \nmid 6$ tal que E tiene reducción multiplicativa en q, tenemos bajada de nivel e imagen grande.

Luego, por el teorema de baja de nivel, existe $f \in S_2(n, \varepsilon)$, donde $n = 2^e \cdot 3$, tal que

$$\rho_{E,p} \equiv \rho_{f,K,p} \otimes \chi^{-1} \pmod{p}.$$

Teorema (truco de Mazur)
Sea $f \in S(n, \varepsilon)$ tal que $\rho_{E,p} \equiv \rho_{f,K,p} \otimes \chi^{-1}$ (mód p). Sea $q \neq p$ primo tal que $q \nmid n$. Sea

$$B(q,f) = \begin{cases} N(a_q(E)\chi(q) - a_q(f)) & \text{si } A^4 + 6B^2 \not\equiv 0 \pmod{q} \text{ y } \left(\frac{-6}{q}\right) = 1, \\ N(a_q(f)^2 - a_q(E)\chi(q) - 2q\varepsilon(q)) & \text{si } A^4 + 6B^2 \not\equiv 0 \pmod{q} \text{ y } \left(\frac{-6}{q}\right) = -1, \\ N(\varepsilon^{-1}(q)(q+1)^2 - a_q(g)^2) & \text{si } A^4 + 6B^2 \equiv 0 \pmod{q}. \end{cases}$$

Entonces $p \mid B(q,f)$.

(4) **Eliminación de las posibles formas:**

(4) **Eliminación de las posibles formas:**
Calculando

$$C(q,g) = \prod_{\substack{(A,B)\in\mathbb{F}_q^2 \\ (A,B)\neq(0,0)}} B(q,g)$$

vamos a poder dar una cota para p (si tenemos suerte).

(4) **Eliminación de las posibles formas:**

Calculando

$$C(q, g) = \prod_{\substack{(A,B)\in\mathbb{F}_q^2 \\ (A,B)\neq(0,0)}} B(q, g)$$

vamos a poder dar una cota para p (si tenemos suerte).

- El espacio $S_2(2^8 \cdot 3)$ tiene 10 formas (clases de conjugación). Seis de ellas tienen CM. Computando $C(5, f)$ puedo descartar a todas (las que no tienen CM) para $p > 7$.

(4) **Eliminación de las posibles formas:**
Calculando

$$C(q,g) = \prod_{\substack{(A,B)\in\mathbb{F}_q^2 \\ (A,B)\neq(0,0)}} B(q,g)$$

vamos a poder dar una cota para p (si tenemos suerte).

- El espacio $S_2(2^8 \cdot 3)$ tiene 10 formas (clases de conjugación). Seis de ellas tienen CM. Computando $C(5,f)$ puedo descartar a todas (las que no tienen CM) para $p > 7$.
- El espacio $S_2(2^9 \cdot 3)$ tiene 13 formas (clases de conjugación) de las cuales 3 tienen CM. Nuevamente, calculando $C(q,f)$ para $q = 23, 29, 31$ podemos eliminar todas las formas para $p > 19$.

(4) **Eliminación de las posibles formas:**
Calculando

$$C(q,g) = \prod_{\substack{(A,B)\in\mathbb{F}_q^2 \\ (A,B)\neq(0,0)}} B(q,g)$$

vamos a poder dar una cota para p (si tenemos suerte).

- El espacio $S_2(2^8 \cdot 3)$ tiene 10 formas (clases de conjugación). Seis de ellas tienen CM. Computando $C(5,f)$ puedo descartar a todas (las que no tienen CM) para $p > 7$.
- El espacio $S_2(2^9 \cdot 3)$ tiene 13 formas (clases de conjugación) de las cuales 3 tienen CM. Nuevamente, calculando $C(q,f)$ para $q = 23, 29, 31$ podemos eliminar todas las formas para $p > 19$.

Teorema (Pacetti - V.T.)
Sea $p > 19$ un número primo. Entonces no existe solución primitiva no trivial de la ecuación

$$x^4 + 6y^2 = z^p.$$

(4) **Eliminación de las posibles formas:**
Calculando

$$C(q,g) = \prod_{\substack{(A,B)\in\mathbb{F}_q^2 \\ (A,B)\neq(0,0)}} B(q,g)$$

vamos a poder dar una cota para p (si tenemos suerte).

- El espacio $S_2(2^8 \cdot 3)$ tiene 10 formas (clases de conjugación). Seis de ellas tienen CM. Computando $C(5,f)$ puedo descartar a todas (las que no tienen CM) para $p > 7$.
- El espacio $S_2(2^9 \cdot 3)$ tiene 13 formas (clases de conjugación) de las cuales 3 tienen CM. Nuevamente, calculando $C(q,f)$ para $q = 23, 29, 31$ podemos eliminar todas las formas para $p > 19$.

Teorema (Pacetti - V.T.)
Sea $p > 19$ un número primo. Entonces no existe solución primitiva no trivial de la ecuación

$$x^4 + 6y^2 = z^p.$$

Observación
Cuándo usamos qué $ABC \neq 0$!!!???

Teorema
Sea $1 \leq d \leq 7$. *Entonces existe* N_d *tal que si* $p > N_d$ *entonces no existe solucion primitva no trivial de la ecuación*

$$x^4 + dy^2 = z^p$$

Teorema
Sea $1 \leq d \leq 7$. Entonces existe N_d tal que si $p > N_d$ entonces no existe solucion primitva no trivial de la ecuación

$$x^4 + dy^2 = z^p$$

Demostración.

- $d = 1$: Ellemberg.
- $d = 2, 3$: Dieulefait, Jiménez-Urroz. Además, dieron la curva elíptica que hay que tomar para un d genérico (libre de cuadrados).
- $d = 5, 6, 7$: Pacetti, V.T. □

Si consideramos la ecuación $x^2 + 5y^2 = z^p$, ya no podemos usar el resultado de Ellemberg.

Si consideramos la ecuación $x^2 + 5y^2 = z^p$, ya no podemos usar el resultado de Ellemberg.

Teorema (Pacetti-V.T)
Si (A, B, C) *es una solución tal que* C *es soportado en* 2 *y* 3 *entonces existe* M_K *tal que la representación* $\rho_{E_{A,B},p}$ *es absolutamente irreducible para todo* $p > M_K$.

Luego, nuevamente tenemos garantizada la bajada de nivel.

Si consideramos la ecuación $x^2 + 5y^2 = z^p$, ya no podemos usar el resultado de Ellemberg.

Teorema (Pacetti-V.T)
Si (A, B, C) *es una solución tal que* C *es soportado en* 2 *y* 3 *entonces existe* M_K *tal que la representación* $\rho_{E_{A,B},p}$ *es absolutamente irreducible para todo* $p > M_K$.

Luego, nuevamente tenemos garantizada la bajada de nivel.

¿Cómo eliminamos las formas con CM?

Recordemos que en el 2012 Bennet y Chen resolvieron la ecuación $x^2 + y^6 = z^n$. En el 2020, Koutsianas demostró que la única solución (no trivial) de $x^2 + 3y^6 = z^n$ para $n \geq 3$ es $(A, B, C, n) = (\pm 47, \pm 2, \pm 7, 4)$.

Recordemos que en el 2012 Bennet y Chen resolvieron la ecuación $x^2 + y^6 = z^n$. En el 2020, Koutsianas demostró que la única solución (no trivial) de $x^2 + 3y^6 = z^n$ para $n \geq 3$ es $(A, B, C, n) = (\pm 47, \pm 2, \pm 7, 4)$.

Dada una solución de la ecuación $x^2 + dy^6 = z^p$ podemos considerar la curva

$$E_{(A,B)} : y^2 + 6B\sqrt{-d}xy - 4d(A + B^3\sqrt{-d})y = x^3$$

con discriminante $\Delta = -2^8 3^3 d^4 C^p (A + B^3\sqrt{-d})^2$ y razonar de manera análoga.

Recordemos que en el 2012 Bennet y Chen resolvieron la ecuación $x^2 + y^6 = z^n$. En el 2020, Koutsianas demostró que la única solución (no trivial) de $x^2 + 3y^6 = z^n$ para $n \geq 3$ es $(A, B, C, n) = (\pm 47, \pm 2, \pm 7, 4)$.

Dada una solución de la ecuación $x^2 + dy^6 = z^p$ podemos considerar la curva

$$E_{(A,B)} : y^2 + 6B\sqrt{-d}xy - 4d(A + B^3\sqrt{-d})y = x^3$$

con discriminante $\Delta = -2^8 3^3 d^4 C^p (A + B^3\sqrt{-d})^2$ y razonar de manera análoga.

Observación
El hecho de que tengamos todas las herramientas para seguir los cuatro pasos dados no nos garantiza el éxito. A saber, pudimos probar la no existencia de soluciones para $d = 2, 3, 6$ pero no para $d = 5, 7$.

¡Muchas gracias!