Ecuaciones de Thue

Paloma Bengoechea

ETH Zurich

December 8, 2020

Thue, 1918: Sea $F(x, y) \in \mathbb{Z}[x, y]$ irreducible sobre $\mathbb{Q}$, $\mathrm{gr}(F) \geq 3$. Sea $m \in \mathbb{N}$. Las ecuaciones e inecuaciones de Thue

$$|F(x, y)| = m, \qquad |F(x, y)| \leq m$$

tienen un número finito de soluciones.

$$n = \mathrm{gr}(F) \geq 3$$

$$s = \#\text{coeficientes no nulos de } F$$

Mahler, 1933: Las ecuaciones de Thue tienen $< c_1(F)^{1+w(m)}$ soluciones, $w(m) = \#$ divisores primos de m.

Mahler, 1933: Las inecuaciones de Thue tienen $< c_2(F)m^{2/n}$ soluciones.

Evertse, 1984: Las ecuaciones de Thue tienen $< c_3^{n(1+w(m))}$ soluciones primitivas $((x, y) = 1)$.

Bombieri-Schmidt, 1987: Las ecuaciones de Thue tienen $< c_4 n^{1+w(m)}$ soluciones primitivas.
Si $m = 1$, esta cota es la mejor posible salvo por el valor de la constante c_4.
Si $m \gg 0$, podemos elegir $c_4 = 215$.

Stewart, 1991: podemos elegir $c_4 = 2800$.

Conjetura (Siegel, 1929)

Sea s el número de coeficientes no nulos de F. Las ecuaciones de Thue tienen $< c(s)$ soluciones.

La conjetura es falsa: se conocen ejemplos de ecuaciones de Thue cúbicas cuyo número de soluciones depende de m (Chowla, Mahler, Silverman).

Conjetura Modificada de Siegel: Las ecuaciones de Thue tienen $< c(s, m)$ soluciones.

Mueller, 1987: ecuaciones binomiales ($s = 2$)

Mueller-Schmidt, 1987; Thomas, 2000: ecuaciones trinomiales ($s = 3$)

Cuando $n \gg s$, F se llama *sparse form* o *fewnomial*.

Teorema (Schmidt, 1987)

Las inecuaciones de Thue tienen

$$\ll \sqrt{ns} m^{\frac{2}{n}} (1 + \log m^{\frac{1}{n}})$$

soluciones.

Thunder suprimió el factor $\log m^{\frac{1}{n}}$ para 'muchos' valores de m.

Teorema (Mueller-Schmidt, 1988)

Las inecuaciones de Thue tienen

$$\ll s^2 m^{\frac{2}{n}} (1 + \log m^{\frac{1}{n}})$$

soluciones.

Mueller-Schmidt suprimió el factor $\log m^{\frac{1}{n}}$ cuando $n \geq 4s$.

Conjeturas (Mueller-Schmidt)

1. s^2 *debería ser* s
2. *El factor* $\log m^{\frac{1}{n}}$ *debería poderse suprimir para* $n \geq 3$.
3. *Hay una cota superior* $c(s)$ *cuando* $m < H(F)^{1-\frac{s}{n}}$.

Teorema 1 (B, 2020)

Supongamos $|D(F)| \geq D_0(n)$. *Las inecuaciones de Thue tienen*

$$\ll sm^{\frac{2}{n}}$$

soluciones.

$D_0(n) = (n(n-1))^{8n(n-1)}$.

Hay un número finito de clases de $\mathrm{SL}(2,\mathbb{Z})$ equivalencia de formas con grado fijado y discriminante acotado, por tanto el teorema incluye casi todas las formas de grado fjado.

Teorema 2 (B-Akthari, 2020)

Supongamos $|D(F)| \geq D_1(n)$ *y* $m < \dfrac{|D(F)|^{\frac{1}{8(n-1)}}}{(3n^{800\log^2 n})^{\frac{n}{2}}(ns)^{2s+n}}$. *Las inecuaciones de Thue tienen*

$$\ll s$$

soluciones primitivas si $n \geq s^2$,

$$\ll s \log s$$

soluciones primitivas si $n < s^2$.

$D_1(n) = (10n)^{8n(n-1)}$.

Ideas en las demostraciones

Separar las soluciones por 'tamaño':

Ej (T1, T'87): (x, y) es *pequeña* si $|y| \leq Y$ y *grande* si $|y| > Y$.

Ej (T2, T'88): (x, y) es *pequeña* si $\min(|x|, |y|) \leq Y_0$, *media* si $\min > Y_0$ y $\max \leq Y_1$, y *grande* si $\max > Y_1$.

Soluciones medias y grandes:
Si (x, y) es una solución con $y > 0$,

$$\left|\alpha - \frac{x}{y}\right| \leq \frac{C(F, m)}{y^n}$$

donde α es una raíz de $F(x, 1)$,

$$C(F, m) = 2^{n-1} n^{(n-1)/2} M(F)^{n-2} |F(x, y)||D(F)|^{-1/2}$$

(Lewis-Mahler, Bombieri-Schmidt, Stewart).

$$\frac{1}{yy'} \leq \left|\frac{x}{y} - \frac{x'}{y'}\right| \leq \frac{2C(F, m)}{y^n} \qquad \Longrightarrow y' \geq \frac{y^{n-1}}{2C(F, m)}$$

Soluciones pequeñas: más difícil!

T'87: Cambiar F por transformadas $F_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}$ más sencillas con $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL(2,\mathbb{Z})$.

Usar la transformada con medida de Mahler minimal entre las $\mathrm{GL}(2,\mathbb{Z})$ equivalentes.
Usar que $F(x,1)$ y su derivada $F_x(x,1)$ tienen $\ll s$ ceros reales.
$\rightarrow \ll \sqrt{ns}\, m^{\frac{2}{n}}(1+\log m^{\frac{1}{n}})$ soluciones pequeñas

T'88: Usar la hipótesis: F tiene s coeficientes no nulos (más fuerte).
Estudiar la distribución de las raíces de $F(x,1)$ y $F(1,y)$ con el polígono de Newton
$\rightarrow \ll s^2 m^{2/n}(1+\log m^{\frac{1}{n}})$ soluciones pequeñas

T1: Combinamos las dos hipótesis: medida de Mahler minimal y s coeficientes no nulos asumiendo $D(F) \geq D_0(n)$.
$\rightarrow \ll sm^{2/n}$ soluciones pequeñas

T2: Cuando m está acotado en términos de $D(F)$, más fácil contar soluciones pequeñas (x, y), $|y| \leq Y = Y(m)$.

Conjetura folclórica: Si fijamos m y el grado n, el 100% de ecuaciones de Thue son insolubles.

Teorema (Akhtari-Bhargava, 2019)

Sea $m \in \mathbb{N}$, $n \geq 3$. Una proporción positiva de ecuaciones de Thue

$$|F(x, y)| = m,$$

con F primitiva, maximal, de grado n, no tienen solución en $\mathbb{Z}$ pero tienen solución en $\mathbb{Z}_p$, para todo primo p, cuando se ordenan por $H(F)$.

Una forma se llama *maximal* si no se puede escribir como $G(ax + by, cx + dy)$, donde $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ es una matriz entera con $|\det(\gamma)| > 1$ y G es una forma binaria.

Teorema (B, 2020)

Sea $m \in \mathbb{N}$, $n \geq 3$. Una proporción positiva de formas primitivas maximales de grado n representan cada entero positivo $\leq m$ en $\mathbb{Z}_p$ para todo primo p pero no en $\mathbb{Z}$.

Observación

Ambos teoremas también funcionan para formas cúbicas ordenadas por discriminante en lugar de altura, y para formas cuárticas ordenadas por los dos generadores I, J de sus anillos de invariantes.

Ideas en las demostraciones

$F \xrightarrow{\text{transformaciones lineales}}$ muchas formas G_j

- Localmente: Imponemos ciertas condiciones sobre F tales que cada G_j representará a cada $h \leq m$ en $\mathbb{Z}_p$ para todo p.

- Globalmente: Muchas formas G_j no representarán a ningún $h \leq m$ en $\mathbb{Z}$.

Sea $g = \dfrac{(n-1)(n-2)}{2}$.
Sea M un entero tal que

$$M > \max(m, (2g+1)^2).$$

Sean $p_1, \ldots, p_k$ todos los primos inferiores a M.

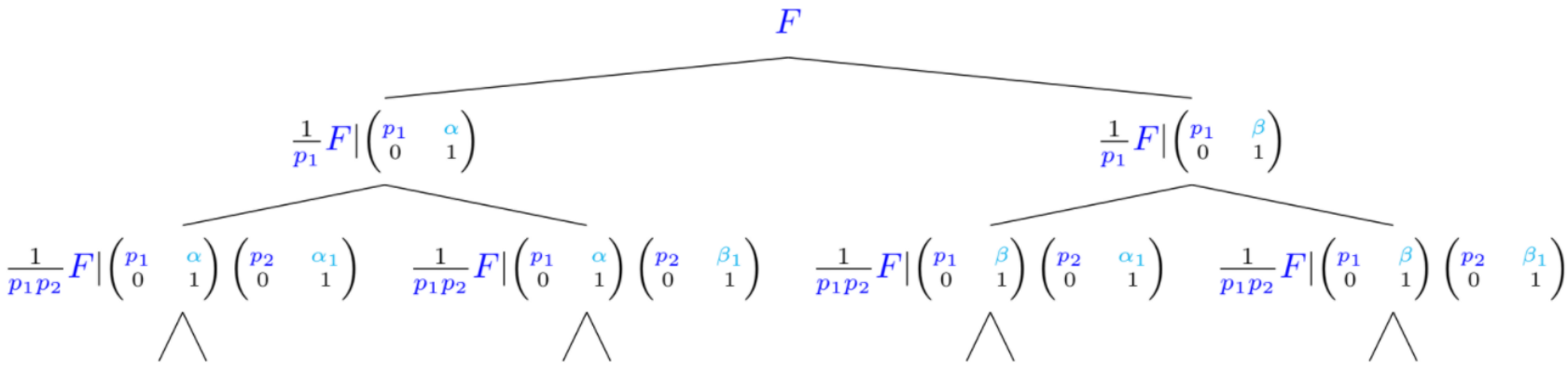
Condiciones sobre F

(i) F es primitiva

(ii) F tiene grupo de Galois S_n (luego F es irreducible y maximal)

(iii) $F(x,1)$ tiene dos raíces simples α_i, β_i en $\mathbb{F}_{p_i}$ para todo $i = 1, \ldots, k$.

(iv) Cuando $p > M$, $F \not\equiv cM(x,y)^r \pmod{p}$, donde $r > 1$, $M(x,y)$ es una forma binaria arbitraria y $c > 0$ una constante arbitraria.
($\Rightarrow$ G_j es irreducible sobre $\mathbb{F}_p$)



Último paso: obtenemos 2^k formas G_j, $j = 1, \ldots, 2^k$.

Cada forma del árbol es primitiva, irreducible sobre $\mathbb{Q}$ y maximal.

En cada nivel, las formas son inequivalentes entre ellas.

$$H(G_j) \leq \left(\prod_{i=1}^{k} p_i\right)^{n-1} \frac{2^{(n+1)k}}{(n+1)^{k/2}} H(F)$$

Localmente

Cada G_j representa cada entero $h \leq m$ en $\mathbb{Z}_p$ para todo p.

- $p \leq M$: Por construcción de G_j

- $p > M$:

$$C : hz^n = G_j(x, y) \qquad \text{sobre } \mathbb{F}_p$$

con género $g = (n-1)(n-2)/2$.

G_j es irreducible sobre $\mathbb{F}_p \Rightarrow C$ es lisa.

Cota de Hasse-Weil: sea $N = \#\{(x, y) \in C\}$,
$N \geq p + 1 - 2g\sqrt{p} > 0$ pues $p > M \geq (2g+1)^2$.

$\Rightarrow$ existe un punto no singular $(x_0, y_0, z_0) \in C$ con $z_0 \neq 0$

$\Rightarrow (x_0 z_0^{-1}, y_0 z_0^{-1})$ es solución de $G_j(x, y) = h$ modulo p.

El lema de Hensel la levanta a una solución sobre $\mathbb{Z}_p$.

Globalmente

$$\#\left\{(x,y)\in\mathbb{Z}^2:\ G_j(x,y)\leq m,\ j\in\{1,\ldots,2^k\}\right\}$$

$$\hookrightarrow \#\left\{(x,y)\in\mathbb{Z}^2:\ F(x,y)\leq m\prod_{i=1}^{k}p_i\right\}\leq cnm$$

$\Rightarrow$ al menos $2^k - cnm$ formas G_j no representan a ningún entero $\leq m$ en $\mathbb{Z}$.

Densidad positiva

$N_m(X)$= # formas primitivas maximales de grado n, altura $< X$ representan a todo entero $\leq m$ en $\mathbb{Z}_p$ para todo p y a ninguno en $\mathbb{Z}$.

$$\liminf_{X\to\infty} \frac{N_m(X)}{X^{n+1}} > 0?$$

$N(\tilde{X})$= # formas F con $H(F) < \tilde{X}$

$$N_m(X) \geq (2^k - cnm)N(\tilde{X})$$

$$N(\tilde{X}) \sim (2\tilde{X})^{n+1} \prod_p \mu_p \gg X^{n+1}$$

donde μ_p es la densidad p-ádica del conjunto de formas con ciertas congruencias en el espacio de formas enteras binarias de grado n.

Gracias!