Cotas para el GCD. (Héctor Pastén, 22/11/18)

Teo: (Bugeaud-Corvaja-Zannier '03) Sean a, b enteros positivos mult. indep. (si después de tomar log). Sea $\varepsilon > 0$. Entonces para todos salvo finitos $n \geq 1$ se tiene

$$\gcd(a^n - 1, b^n - 1) < \exp(\varepsilon \cdot n).$$

Cor: (Conj. de Pisot/Hadamard) Sean A, B enteros positivos. Si existen ∞ n con $A^n - 1 \mid B^n - 1 \Rightarrow B = A^r$ para algún $r \geq 0$.

[obs: $B = A^r$, $B^n - 1 = (A^n - 1)(A^{n(r-1)} + \cdots + A^n + 1)$]

Teo (Subespacio/$\mathbb{Z}$) $S \subseteq M_{\mathbb{Q}}$ con $\infty \in S$, $q = N$, $L_{v,j} \in \mathbb{Q}[x_1, \ldots, x_N]$ con $j = 1, \ldots, N$. $\Rightarrow$ lo de siempre.

Estrategia: $d_n = \dfrac{a^n - 1}{\gcd(a^n - 1, b^n - 1)} \in \mathbb{Z}$. Basta mostrar que si $\exists^\infty n$ con (*) $d_n \leq a^{(1-\varepsilon)\cdot n} \Rightarrow$ contradicción.

Sea $\mathcal{N} = \{ n : (*) \checkmark \}$ y asumiremos $\mathcal{N}$ es infinito.

Fijamos: $k > 2/\varepsilon$, h cumple $a^h > 2 b^{h^2} \cdot a^k$, $N = hk + h + k$

obs: $\varepsilon N > \varepsilon hk > 2h$. $S = \{\infty, p : p \mid ab\}$.

Plan:

(1) Construir $L_{v,j}$'s

(2) Construir $\underline{a}(n) \in \mathbb{Z}^N$, para $n \in \mathcal{N}$.

(3) Asegurarse que para $n \in \mathcal{N}$, $\prod_{v \in S} \prod_{i=1}^{N} |L_{v,j}(\underline{a}(n))|_v$ es chico

T. Sbsp $\Rightarrow$ los $\underline{a}(n)$ están en finitos hiperplanos

(4) deducir una identidad algebraica contradictoria

Lema: Sean j, n enteros positivos. Entonces:

$\star$ $$\left| \underbrace{\frac{b^{jn}-1}{a^n-1} - \sum_{r=1}^{h} \left(\frac{b^j}{a^r}\right)^n + \sum_{s=1}^{h} \frac{1}{a^{jsn}}}_{(\star\star)} \right| < 2\, b^{jn} \cdot a^{-(h+1)n}$$

Dem:
$$\frac{1}{a^n-1} = \frac{1}{a^n} \cdot \sum_{r=0}^{\infty} \frac{1}{a^{rn}} = \sum_{r=1}^{\infty} \frac{1}{a^{rn}}$$
$$= \sum_{r=1}^{h} \frac{1}{a^{rn}} + \frac{1}{a^{(h+1)n}} \cdot \frac{1}{1-\frac{1}{a^n}}$$
$$= \quad " \quad + \frac{1}{a^{(h+1)n}} \underbrace{\frac{a^n}{a^n-1}}_{\leq 2} \Rightarrow \left| \frac{b^{jn}-1}{a^n-1} - \sum_{r=1}^{h} \frac{b^{jn}-1}{a^{rn}} \right| < \frac{2 \cdot b^{jn}}{a^{(h+1)n}}$$ ■

(1) $N = hk+h+k$, $(x_1, \dots, x_N) = (\underline{z}, \underline{y_0}, \dots, \underline{y_k})$
con $\underline{z} = (z_1, \dots, z_k)$, $\underline{y_j} = (y_{j1}, \dots, y_{jk})$ $\quad 0 \leq j \leq k$
$[\, k + (k+1)h = kh+h+k \,]$

Para $r \in S \setminus \{\infty\}$, $L_{rj}(\underline{x}) = x_j$
Para $r = \infty$
$$L_{\infty j}(\underline{x}) = \begin{cases} z_j + (y_{0i} + \dots + y_{0h}) - (y_{j1} + \dots + y_{jh}) & 1 \leq j \leq k \\ x_j \quad \text{si } k < j \leq N \end{cases}$$

(2) Construir $\underline{a}(n)$ $(n \in \mathbb{N})$. Notar: $b^{jn}-1$ es múltiplo de b^n-1
$\Rightarrow d_n \cdot \frac{b^{jn}-1}{a^n-1} \in \mathbb{Z}$, así $\frac{b^{jn}-1}{a^n-1} = \frac{c_{nj}}{d_n}$.

$$\underline{a}(n) := d_n \cdot a^{hn} \cdot \Big(\underbrace{\frac{b^n-1}{a^n-1}, \dots, \frac{b^{kn}-1}{a^n-1}}_{\underline{z}}, \underbrace{a^{-n}, \dots, a^{-hn}}_{\underline{y_0}}, \underbrace{b^n a^{-n}, \dots, b^n a^{-hn}}_{\underline{y_1}}, \dots \Big)$$

Luego $\|\underline{a}(n)\|_{\sup} < A^n$.

→ Suponer $\sum_{i,j\geq 0} \gamma_{ij}(a^n)^i \cdot (b^n)^j = 0$. Notar que $a^i b^j$ son distintos (indep. mult)

$0 = \sum \gamma_{ij}(a^i b^j)^n \underset{\text{dist}}{\Rightarrow}$ hay $a^i b^j$ max. con $\gamma_{ij} \neq 0$ $n \to \infty$ $\to\leftarrow$.

obs 1 : $j > k$, entonces $L_{\nu j} = X_j \Rightarrow L_{\nu j}(\underline{a}(n)) = d_n$ (S-unidad)

$\Rightarrow \prod_{\nu \in S} |L_{\nu j}(\underline{a}(n))|_\nu = \prod_{\nu \in S} |d_n|_\nu \leq |d_n|_\infty = d_n$

obs 2 : Si $\nu = \infty$, $1 \leq j \leq k \Rightarrow |L_{\infty j}(\underline{a}(n))|_\infty = d_n \cdot a^{hn} \cdot |(**)|$.

y así por ★ : $|L_{\infty j}(\underline{a}(n))|_\infty < d_n \cdot a^{hn} \cdot 2 \cdot b^{jn} \cdot a^{-(h+1)n}$

$2 d_n^n \cdot a^{-n} \cdot b^{jn} \leq d_n \cdot b^{kn}$

obs 3 : Si $\nu \neq \infty$ y $j \leq k$ $L_{\infty j}(X) = X_j$

$|L_{\nu j}(\underline{a}(n))|_\nu = \left| d_n \cdot a^{hn} \frac{b^{jn}-1}{a^n-1} \right|_\nu = |c_{nj} \cdot a^{hn}|_\nu \leq |a^{hn}|_\nu$

$\Rightarrow$ ~~multiplicar~~, si $1 \leq j \leq k \Rightarrow \prod_{\infty \neq \nu \in S} |L_{\nu j}(\underline{a}(n))|_\nu \leq \prod_{p \text{ prim}} |a|_p^{hn} = \frac{1}{a^{hn}}$

obs 1-2-3 : $\prod_{\nu \in S} \prod_{j=1}^{N} |L_{\nu j}(\underline{a}(n))|_\nu < d_n^{N-k} \cdot \left(d_n b^{kn} \cdot \frac{1}{a^{hn}} \right)^k$

$\% < d_n^N \cdot b^{k^2 n} \cdot \frac{1}{a^{hnk}} \leq (a^{(1-\varepsilon)n})^N \cdot b^{k^2 n} \cdot a^{-hnk} = \left(a^{N - \varepsilon N - hk} \cdot b^{k^2} \right)^n$

como $n \in \mathbb{N}$

$\Rightarrow \quad \% < \left(a^{h+k-\varepsilon N} \cdot b^{k^2} \right)^n$ y $\varepsilon N > 2h$

$\Rightarrow \quad \% < \left(a^{k-h} \cdot b^{k^2} \right)^n$ y $a^h > 2 b^{k^2} \cdot a^k$

$\to \quad \% < \frac{1}{2^n}$, $n \in \mathbb{N}$

pero $\delta = \log 2 / \log A > 0 \Rightarrow \frac{1}{2^n} = \frac{1}{\|\underline{a}(n)\|_{\sup}^{\delta}}$

$\Rightarrow$ Teo subespacio dice hay un ∞ con muchos de los $\underline{a}(n)$ $(n \in \mathbb{N})$.

$\exists \beta_1, \ldots, \beta_k, \alpha_{ij} \in \mathbb{Q}$ no todos nulos t.q. $\exists^\infty n$ con

$\beta_1 \frac{b^n - 1}{a^n - 1} + \ldots + \beta_k \frac{b^{kn} - 1}{a^n - 1} + \sum \alpha_{ij} \frac{b^{in}}{a^{jn}} = 0$

obs 1 : a, b mult indep $\Rightarrow$ las funciones $n \mapsto a^n$, $n \mapsto b^n$ son alg. indep.

$\Rightarrow \beta_1 \frac{Y-1}{X-1} + \ldots + \beta_k \frac{Y^k - 1}{X-1} + \sum \alpha_{ij} \frac{Y^i}{X^j} = 0 \Rightarrow \frac{f(Y)}{X-1} + \frac{g(X,Y)}{X^h} = 0$

$\Rightarrow X-1 \mid f(Y) \Rightarrow f(Y) = 0 \Rightarrow g(X,Y) = 0 \Rightarrow$ todo cero $\to\leftarrow$ ■