Universidad Autónoma de Zacatecas
Unidad de Matemáticas

Del Número de Soluciones de la Ecuación de Thue

Tesis en opción al título de

Maestría en Matemáticas

presenta:

Arilín Susana Haro Palma.

bajo la dirección de:

Dr. Santos Hernández Hernández

Zacatecas, Zac. Octubre de 2016

Del Número de Soluciones de la Ecuación de Thue

Arilín Susana Haro Palma.
Unidad de Matemáticas
Universidad Autónoma de Zacatecas

Título: Del Número de Soluciones de la Ecuación de Thue.
Autor: Arilín Susana Haro Palma.
Figuras: Arilín Haro.
Compilador: LaTeX (Editor adecuado para textos científicos.).
Edición en LaTeX Arilín Susana Haro Palma.
Número de páginas: 60.
Lugar: Zacatecas, Zac., México.

Mientras se sienta que se ríe el alma,
sin que los labios rían,
mientras se llore, sin que el llanto acuda
a nublar la pupila,
mientras el corazón y la cabeza
batallando prosigan,
mientras haya esperanzas y recuerdos,
¡habrá poesía!

Gustavo Adolfo Bécquer

A mi madre por por enseñarme a volar,
A mi esposo por volar conmigo.

Es para ustedes mi trabajo.

Agradecimientos

Se retrocede con seguridad
pero se avanza a tientas
uno adelanta manos como un ciego
y distingue el relámpago la lluvia
los rostros insepultos la ceniza
la sonrisa del necio las afrentas
un barrunto de pena en el espejo
la baranda oxidada con sus pájaros
la opaca incertidumbre de los otros
enfrentada a la propia incertidumbre
se avanza a tientas...

Mario Benedetti

Quiero agradecer a CONACYT por financiar estos dos años de la maestría, también a la Universidad Autónoma de Zacatecas, en particular a la Unidad de Matemáticas por ser tan amables conmigo y hacerme sentir bienvenida, también gracias a mis profesores por compartirme algo de sus conocimientos, deben saber que disfrute todos mis cursos y que de todos aprendí; agradezco a René Schoof, Martin Kalzar y Umberto Zannier por responder mis correos y con ellos aclarar mis dudas.

También quiero agradecer a mis compañeros y amigos por hacer mis clases y fines de semanas más alegres; agradezco a mi familia, en especial a mi mamá por alentar y respetar mis decisiones, y por supuesto, gracias a mi amado esposo Luis Jorge por siempre ayudarme a avanzar.

Índice general

Introducción.

Una ecuación diofántica es una ecuación de la forma $f(X_1, \ldots, X_n) = 0$ donde f es una función, usualmente un polinomio de coeficientes enteros, y se buscan soluciones enteras; es natural hacernos ciertas preguntas sobre estas ecuaciones, por ejemplo:
1) ¿La ecuación tiene solución?
2) ¿Cuántas soluciones tiene?
3) ¿Es posible encontrar todas las soluciones?

El ejemplo más sencillo de una ecuación diofántica es $p(X) = 0$ donde $p(X) = a_n X^n + \cdots + a_0$ es un polinomio en una variable, para este caso sabemos que hay a lo más n soluciones enteras (o racionales), más aún, hay un criterio para saber qué números racionales pueden ser solución de la ecuación cuando los coeficientes del polinomio son enteros.

Teorema 0.1. *Sea* $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$, *con* $a_0, a_n \neq 0$ *y si* $x = \frac{p}{q}$ *con* $(p, q) = 1$ *es raíz de* $f(X)$ *entonces* $p | a_0$ *y* $q | a_n$.

Así, para encontrar los enteros qué satisfacen la ecuación sólo hace falta probar con los divisores del término independiente, por lo tanto, tratándose de esta ecuación tenemos respuesta a las tres preguntas.
Otro ejemplo sencillo es la ecuación $aX + bY = c$ es decir una ecuación linear en dos variables con coeficientes enteros, para esta ecuación sabemos que si $c = 0$ las parejas $(nb, -na)$ satisfacen la ecuación. Por otro lado, si $c \neq 0$ tenemos el siguiente resultado

Teorema 0.2. *La ecuación $aX + bY = c$ tiene solución entera si y sólo si $(a, b)|c$, donde (a, b) es el máximo común divisor de a y b. Además si (x_0, y_0) es una solución entonces las parejas $(x_0 + \frac{b}{(a,b)}t, y_0 - \frac{a}{(a,b)}t)$ con $t \in \mathbb{Z}$ son todas las soluciones enteras de la ecuación.*

Gracias a este teorema sabemos cuándo esta ecuación tiene soluciones enteras y además resulta fácil encontrar todas las soluciones, para ver más sobre esta ecuación consultar [NZM91].

Luego tenemos el polinomio general de grado dos, $f(X, Y) = aX^2 + bXY^2 + cY^2 + dX + eY + f$, para este se sabe si la ecuación $f(X, Y) = 0$ tiene una infinidad de soluciones o sólo un número finito de las mismas dependiendo de su discriminante $\Delta = b^2 - 4ac$:
• si $\Delta < 0$ entonces la ecuación tiene sólo un número finito de soluciones,
• si $\Delta = 0$, en caso de que exista una solución entonces existe una infinidad de éstas, por último,
• si $\Delta > 0$ distinguimos dos casos, dependiendo de si Δ es un número cuadrado o no, si sí lo es la ecuación tendrá soló un número finito de soluciones, en cambio, si δ no es un número cuadrado se tiene que existe una solución si y sólo si existe una infinidad de soluciones, pero para analizar este último caso nos vemos en la necesidad de fijarnos en la ecuación de Pell $X^2 - \Delta Y^2 = 1$, para la cual tenemos el siguiente resultado:

Teorema 0.3. *La ecuación de Pell $X^2 - dY^2 = 1$ tiene una infinidad de soluciones enteras (x, y) cuando $d \in \mathbb{Z}_{>0}$ no es un cuadrado.*

En este caso, sabemos que si tenemos una solución no trivial (diferente de $x = 1$ y $y = 0$) entonces esta solución genera una infinidad de soluciones, pero a diferencia del caso lineal aquí no es tan fácil encontrar una solución que genere a todas las demás, (para leer más acerca de la ecuación de Pell se puede consultar [Ivo], o bien, [Zan09]) como herramienta para demostrar este teorema utilizamos aproximaciones diofánticas, en particular el teorema de Dirichlet.

Teorema 0.4 (Dirichlet)**.** *Sean $\alpha \in \mathbb{R}$ y $Q > 0$ un entero positivo. Entonces existen enteros p y q primos relativos tales que*

$$0 < q < Q \quad y \quad |\alpha - \frac{p}{q}| \leq \frac{1}{q(Q+1)}.$$

Una vez analizadas las ecuaciones con polinomios de primer y segundo grado lo natural es preguntarnos qué pasa con las de grado mayor o igual a tres, y sucede que nos encontramos con la necesidad de mejorar la aproximación diofántica que nos brinda el teorema de Dirichlet; es así que llegamos al

teorema de aproximación de Thue, el cuál nos permite saber qué pasa en el caso en que $f(X, Y)$ es un polinomio homogéneo de grado mayor o igual que tres.

En el primer capítulo consideramos el teorema de Thue [1.1], el cual analiza la ecuación $f(X, Y) = c$, donde f es un polinomio homogéneo en dos variables con coeficientes enteros, sin factores lineales o cuadráticos y donde c es un entero no cero; para la demostración de este teorema será necesario ver algunos resultados de aproximaciones diofánticas, como lo es el teorema de Liouville [1.3], mismo en el que Axel Thue trabajó hasta obtener el teorema de aproximación de Thue que podemos ver en [Thu09], y de éste se desprende el llamado teorema de Thue.

En el capítulo dos se analizan las soluciones enteras de la ecuación de Thue $|f(X, Y)| = 1$; con el objetivo de dar una cota para el número de soluciones a dicha ecuación, primero se cuentan las soluciones grandes (que resultan ser pocas) con ayuda del principio fuerte entre las distancias (2.20), que nos dice lo rápido que van creciendo las magnitudes de las soluciones de la ecuación $|f(X, Y)| = 1$, luego de contar las soluciones grandes se procede a contar el número de soluciones pequeñas y finalmente se da una cota para el número de soluciones de la ecuación estudiada. Esto lo hacemos basados en el artículo [BS87].

Zacatecas, Zac., México, Octubre del 2016

1
Teorema de Thue

En este capítulo veremos el teorema de Thue, empezaremos por enunciarlo, seguiremos con algunos teoremas de aproximación diofántica de números racionales a números algebraicos tales como el Teorema de Aproximación de Thue; siguiendo la linea de Umberto Zannier en [Zan09], será necesario utilizar una sección entera para la demostración de dicho teorema, y al final del capítulo demostraremos el Teorema de Thue utilizando el Teorema de Aproximación de Thue, también veremos una forma más general del Teorema de Thue (Teorema 1.11), y concluiremos con algunas aplicaciones de este último, en este capitulo tratamos de llenar lo huecos de algunas demostraciones intentado así que sea un trabajo autocontenido.

Teorema 1.1 (Thue, 1909)**.** *Sea $f \in \mathbb{Z}[X,Y]$ homogéneo, irreducible (sobre $\mathbb{Q}$) de grado mayor o igual que 3 y sea $c \in \mathbb{Z}$ no cero. Entonces la ecuación $f(X,Y) = c$ tiene sólo un número finito de soluciones enteras.*

Notemos que la condición sobre el grado de f no puede ser eliminada pues sabemos de algunos polinomios homogéneos lineales y cuadráticos para los cuales la ecuación $f(X,Y) = c$ tiene una infinidad de soluciones enteras, por ejemplo $f(X,Y) = aX + bY$ y $f(X,Y) = X^2 - dY^2$ en ambos casos existe una infinidad de soluciones enteras para la ecuación $f(X,Y) = c$.

1.1. Aproximaciones Diofánticas

Supongamos que $f \in \mathbb{Z}[X,Y]$ es un polinomio homogéneo irreducible de grado $d \geq 3$. A la ecuación $f(X,Y) = c$ la llamaremos ecuación de Thue. Entonces

$$\begin{aligned} f(X,Y) =& a_0X^d + a_1X^{d-1}Y + \cdots + a_{d-1}XY^{d-1} + a_dY^d \\ =& Y^d\left(a_0\frac{X^d}{Y^d} + a_1\frac{X^{d-1}}{Y^{d-1}} + \cdots + a_{d-1}\frac{X}{Y} + a_d\right) \\ =& Y^d a_0 \prod_{i=1}^{d}(\frac{X}{Y} - \alpha_i) \\ =& a_0 \prod_{i=1}^{d}(X - \alpha_i Y) \end{aligned}$$

con $a_0 \neq 0$ y los α_i raíces de $f(X,1)$, definimos $\eta = \text{mín}_{i\neq j}\,|\alpha_i - \alpha_j|$, notemos que $\eta > 0$ pues $f(X,1)$ es irreducible.

Proposición 1.2. *Si $f(x,y) = c$ para $x, y \in \mathbb{Z}/\{0\}$, entonces existe una raíz α de $f(X,1)$ tal que $|\alpha - \frac{x}{y}| \leq \frac{B}{|y|^d}$ donde $B = |c|(\frac{2}{\eta})^{d-1}$*

Demostración. Supongamos que $f(x,y) = c$, entonces $a_0\prod_{i=1}^{d}(x - \alpha_i y) = c$, sea $\alpha \in \{\alpha_1, \ldots, \alpha_d\}$ tal que $\mu = |x - \alpha y| \leq |x - \alpha_i y|$ para $i = 1, \ldots, d$ entonces

$$\mu^d = |x - \alpha y|^d \leq \prod_{i=1}^{d}|x - \alpha_i y| = \frac{|f(x,y)|}{|a_0|} = \frac{|c|}{|a_0|} \leq |c|.$$

Ahora distinguimos dos casos $|y| \leq \frac{2\mu}{\eta}$ y $|y| > \frac{2\mu}{\eta}$

Caso 1 Supongamos que $|y| \leq \frac{2\mu}{\eta}$ entonces

$$\mu|y|^{d-1} \leq \mu\left(\frac{2\mu}{\eta}\right)^{d-1} = \mu^d\left(\frac{2}{\eta}\right)^{d-1} \leq |c|\left(\frac{2}{\eta}\right)^{d-1}$$

por lo tanto

$$|\frac{x}{y} - \alpha| = \frac{|x - \alpha y|}{|y|} = \frac{\mu}{|y|} \leq \frac{|c|\left(\frac{2}{\eta}\right)^{d-1}}{|y|^d} = \frac{B}{|y|^d}.$$

Caso 2 Supongamos que $|y| > \frac{2\mu}{\eta}$ entonces $\frac{|y|\eta}{2} > \mu$, notemos que si $\alpha_j \neq \alpha$ tenemos

$$\begin{aligned}|x-\alpha_j y| =& |x-\alpha y+\alpha y-\alpha_j y| = |(\alpha-\alpha_j)y + x - \alpha y| \\ \geq& ||(\alpha-\alpha_j)y| - |x-\alpha y|| \geq |(\alpha-\alpha_j)y| - |x-\alpha y| \\ =& |\alpha-\alpha_j||y| - |x-\alpha y| = |\alpha-\alpha_j||y| - \mu \geq \eta|y| - \mu \\ \geq& \eta|y| - \frac{|y|\eta}{2} = \frac{\eta|y|}{2}\end{aligned}$$

lo que implica

$$|c| = |a_0|\prod_{i=1}^{d}|x-\alpha_i y| = |a_0||x-\alpha y|\prod_{\alpha_i\neq\alpha}|x-\alpha_i y| \geq |a_0||x-\alpha y|\left(\frac{\eta|y|}{2}\right)^{d-1}$$

entonces $|x-\alpha y| \leq \frac{|c|}{|a_0|\left(\frac{\eta|y|}{2}\right)^{d-1}} \leq \frac{|c|}{\left(\frac{\eta|y|}{2}\right)^{d-1}} = \frac{|c|}{\left(\frac{\eta}{2}\right)^{d-1}|y|^{d-1}}$ por lo tanto $|\frac{x}{y} - \alpha| \leq \frac{|c|}{\left(\frac{\eta}{2}\right)^{d-1}|y|^d} = \frac{B}{|y|^d}$.

Así la proposición ha quedado demostrada para ambos casos.

□

Teorema 1.3 (Liouville 1844)**.** *Sea $\alpha \in \mathbb{R}$ algebraico de grado d. Entonces existe un número $c > 0$ tal que, para cualesquiera $p, q \in \mathbb{Z}$ con $q > 0$ y $\frac{p}{q} \neq \alpha$ se cumple $|\alpha - \frac{p}{q}| \geq \frac{c}{q^d}$.*

Demostración. Sea $f(X) = a_0X^d + \cdots + a_d \in \mathbb{Z}$ el polinomio mínimo de α con $a_0 > 0$. Ahora, si $f(\frac{p}{q}) \neq 0$ tenemos

$$|f\left(\frac{p}{q}\right)| = |a_0\left(\frac{p}{q}\right)^d + \cdots + a_d| = \frac{|a_0p^d + \cdots + a_dq^d|}{q^d} \geq \frac{1}{q^d} \tag{1.1}$$

de el teorema del valor medio tenemos que $f(\alpha) - f(\frac{p}{q}) = (\alpha - \frac{p}{q})f'(\beta)$ con β entre α y $\frac{p}{q}$, por lo tanto $|f(\frac{p}{q})| = |f(\alpha) - f(\frac{p}{q})| = |\alpha - \frac{p}{q}||f'(\beta)|$, ahora distinguimos dos casos, $|\alpha - \frac{p}{q}| > 1$ y $|\alpha - \frac{p}{q}| \leq 1$,

- $|\alpha - \frac{p}{q}| > 1$ implica $|\alpha - \frac{p}{q}| > \frac{1}{q^d}$ y el teorema se cumple con $c = 1$;
- $|\alpha - \frac{p}{q}| \leq 1$ implica que $\beta \in [\alpha - 1, \alpha + 1] = I$ (pues β esta entre α y $\frac{p}{q}$) y $|f'(\beta)| \leq \max_{t\in I}|f'(t)| = M$, así tenemos que $|\alpha - \frac{p}{q}| = \frac{|f(\frac{p}{q})|}{|f'(\beta)|} \geq \frac{1}{|f'(\beta)|q^d} \geq \frac{1}{Mq^d}$ por lo tanto el teorema se cumple con $c = \frac{1}{M}$.

En ambos casos tenemos que el teorema se cumple para $c := \min(1, \frac{1}{M})$ □

Ahora veremos el teorema de aproximación de Thue

Teorema 1.4 (Thue 1909)**.** *Sea α un número algebraico de grado $d \geq 3$. Para todo $\epsilon > 0$ existe $\nu > 0$ tal que para cualesquiera $p, q \in \mathbb{Z}$ con $q > 0$ se cumple que*

$$|\alpha - \frac{p}{q}| > \frac{\nu}{q^{1+\frac{d}{2}+\epsilon}}. \tag{1.2}$$

Notemos que si $\alpha \notin \mathbb{R}$ entonces el teorema se sigue de forma trivial, pues tendríamos $\alpha = u + iv$ con $v \neq 0$, entonces

$$|\alpha - \frac{p}{q}| = \sqrt{(u - \frac{p}{q})^2 + v^2} \geq \sqrt{v^2} = |v| \geq \frac{|v|}{q^{1+\frac{d}{2}+\epsilon}}$$

por lo tanto $\nu = \frac{|v|}{2}$ cumple el teorema.

Teorema 1.5. *Sea $\alpha \in \mathbb{R}$ algebraico de grado $d \geq 3$. Para todo $\epsilon > 0$ hay sólo un número finito de racionales $\frac{p}{q}$ con $q > 0$ tales que*

$$|\alpha - \frac{p}{q}| < \frac{1}{q^{1+\frac{d}{2}+\epsilon}}. \tag{1.3}$$

Pedir que la desigualdad 1.3 se cumpla es equivalente a pedir que

$$|\alpha q - p| < \frac{1}{q^{\frac{d}{2}+\epsilon}},$$

ahora notemos que si α es un número real y consideramos $q > 0$ arbitrario pero fijo entonces hay sólo un número finito de enteros p tales que 1.3 se cumple, pues en el intervalo $(q\alpha - \frac{1}{q^{\frac{d}{2}+\epsilon}}, q\alpha\frac{1}{q^{\frac{d}{2}+\epsilon}})$ hay sólo un número finito de enteros.

Lema 1.6. *Los teoremas 1.4 y 1.5 son equivalentes.*

Demostración. Veamos que el Teorema 1.5 implica el Teorema 1.4.
Sea $\alpha \in \mathbb{R}$ algebraico de grado $d \geq 3$, sea $\epsilon > 0$, y supongamos que el Teorema 1.5 se cumple, sean $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$ los racionales que cumplen 1.3, para $i = 1, \ldots, n$ sea $\mu_i = |\alpha - \frac{p_i}{q_i}|q^{1+\frac{d}{2}+\epsilon}$ así $\mu_i < 1$ y sea $\mu = \text{mín}_{1\leq i\leq n}\, \mu_i$ y $\nu = \frac{\mu}{2}$ entonces $|\alpha - \frac{p_i}{q_i}|q^{1+\frac{d}{2}+\epsilon} > \nu$ para $i = 1, \ldots, n$ entonces $|\alpha - \frac{p_i}{q_i}| > \frac{\nu}{q^{1+\frac{d}{2}+\epsilon}}$ para $i = 1, \ldots, n$, ahora, si $\frac{p}{q} \neq \frac{p_i}{q_i}$ con $1 \leq i \leq n$ entonces, $|\alpha - \frac{p}{q}| \geq \frac{1}{q^{1+\frac{d}{2}+\epsilon}} > \frac{\nu}{q^{1+\frac{d}{2}+\epsilon}}$ por lo tanto $|\alpha - \frac{p}{q}| > \frac{\nu}{q^{1+\frac{d}{2}+\epsilon}}$ para cualquier racional $\frac{p}{q}$ con $q > 0$.
Ahora veamos que el Teorema 1.4 implica el Teorema 1.5.
Sea $\alpha \in \mathbb{R}$ algebraico de grado $d \geq 3$, sea $\epsilon > 0$, y supongamos que el Teorema

1.4 se cumple, entonces existe $\nu > 0$ tal que para cualesquiera $p, q \in \mathbb{Z}$ con $q > 0$ la desigualdad 1.2 se cumple. Notemos que $\frac{\nu}{q^{1+\frac{d}{2}+\frac{\epsilon}{2}}} = \frac{1}{q^{1+\frac{d}{2}+\epsilon}}(\nu q^{\frac{\epsilon}{2}})$, luego, si $q > \frac{1}{\nu^{\frac{2}{\epsilon}}}$ entonces $\frac{1}{q^{1+\frac{d}{2}+\epsilon}}(\nu q^{\frac{\epsilon}{2}}) > \frac{1}{q^{1+\frac{d}{2}+\epsilon}}$, por lo tanto para todo q mayor que $\frac{1}{\nu^{\frac{2}{\epsilon}}}$ se tiene que $|\alpha - \frac{p}{q}| > \frac{1}{q^{1+\frac{d}{2}+\epsilon}}$ y esto implica que sólo existe un número finito de números racionales $\frac{p}{q}$ con $q > 0$ tales que $|\alpha - \frac{p}{q}| < \frac{1}{q^{1+\frac{d}{2}+\epsilon}}$. □

Con el objetivo de probar el teorema de aproximación de Thue [1.4] demostraremos el Teorema 1.5.

Mejoras al Teorema de aproximación de Thue se pueden ver en [Dys47] donde el exponente es menor igual que $\sqrt{2d}$, luego en 1955 Roth [Rot97] mejoró aún más el exponente dejando sólo en $2 + \epsilon$.

1.2. Prueba de el Teorema de Aproximación de Thue

Sean $\alpha \in \mathbb{R}$ algebraico de grado $d \geq 3$ y $\epsilon > 0$; diremos que $\frac{p}{q}$ con $p, q \in \mathbb{Z}$ y $q > 0$ es una aproximación excelente de α respecto a ϵ si $(p, q) = 1$ y $|\alpha - \frac{p}{q}| \leq \frac{1}{q^{1+\frac{d}{2}+\epsilon}}$.

Observación 1.7. *Sea $\frac{p}{q}$ una aproximación excelente de α respecto a ϵ, entonces existe sólo un número finito de parejas $s, t \in \mathbb{Z}$ con $t > 0$ tales que $\frac{p}{q} = \frac{s}{t}$ y $|\alpha - \frac{s}{t}| \leq \frac{1}{t^{1+\frac{d}{2}+\epsilon}}$.*

Demostración. Sean $s, t \in \mathbb{Z}$ con $t > 0$ tales que $\frac{p}{q} = \frac{s}{t}$, entonces $s = mp$ y $t = mq$ para algún $m \in \mathbb{Z}_{>0}$ y $|\alpha - \frac{s}{t}| = |\alpha - \frac{p}{q}|$, pero $\frac{1}{(mq)^{1+\frac{d}{2}+\epsilon}}$ tiende a cero cuando m va a infinito, por lo tanto existe un $N > 0$ tal que $|\alpha - \frac{p}{q}| > \frac{1}{(mq)^{1+\frac{d}{2}+\epsilon}}$ para todo $m > N$, es decir, sólo existe un número finito de enteros $m > 0$ tales que $|\alpha - \frac{mp}{mq}| < \frac{1}{(mq)^{1+\frac{d}{2}+\epsilon}}$, esto prueba la observación.

□

Así que para cada aproximación excelente hay sólo un número finito de aproximaciones que cumplen el Teorema 1.5; siendo así, para probar el Teorema de Thue (1.5) basta ver que existe sólo un número finito de aproximaciones excelentes.

Empezaremos por definir al operador $D_j = \frac{1}{j!}\frac{\partial^j}{\partial X^j}$ notemos que si

$f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ tenemos

$$\begin{aligned} D_k f =& \frac{1}{k!} \sum_{i=k}^{n} i \cdots (i-k+1) a_i X^{i-k} \\ =& \sum_{i=k}^{n} \frac{i \cdots (i-k+1)}{k!} a_i X^{i-k} \\ =& \sum_{i=k}^{n} \frac{i!}{k!(i-k)!} a_i X^{i-k} \\ =& \sum_{i=k}^{n} \binom{i}{k} a_i X^{i-k} \end{aligned}$$

por lo tanto el operador D_k manda a $\mathbb{Z}[X]$ en $\mathbb{Z}[X]$. Ahora definiremos la norma de f como $||f|| = \text{máx}_{0 \leq i \leq n}\{|a_i|\}$,

Proposición 1.8. *Sean* $f(X) = \sum_{i=1}^{n} a_i X^i$ *y* $g(X) = \sum_{i=0}^{m} b_j X^j$ *entonces*

a) $||f + g|| \leq ||f|| + ||g||$

b) $||fg|| \leq (n+1)||f||||g||$

c) $||D_k f|| \leq \binom{n}{k} ||f|| \leq 2^n ||f||$

Demostración. a) Sin pérdida de generalidad podemos asumir $m \leq n$, entonces

$$||f + g|| = \max_{0 \leq i \leq n}\{|a_i + b_i|\} \leq \max_{0 \leq i \leq n}\{|a_i|\} + \max_{0 \leq i \leq n}\{|b_i|\} = ||f|| + ||g||.$$

b) Tenemos que $fg = \sum_{k=0}^{n+m} (\sum_{i+j=k} a_i b_j) x^k$, luego

$$|\sum_{i+j=k} a_i b_j| \leq \sum_{i+j=k} |a_i b_j| = \sum_{i+j=k} |a_i||b_j|$$

pero en cada término de la sumatoria aparece un a_i diferente, por lo tanto hay a lo mas $n+1$ sumandos y como $|a_i| \leq ||f||$ y $|b_i| \leq ||g||$ entonces

$$||fg|| = \max_{0 \leq k \leq n+m}\{|\sum_{i+j=k} a_i b_j|\} \leq (n+1)||f||||g||.$$

c) Tenemos que $D_k f = \sum_{i=k}^{n} \binom{i}{k} a_i X^{i-k}$ entonces

$$||D_k f|| = \max_{k \leq i \leq n}\{\binom{i}{k}|a_i|\} \leq \max_{k \leq i \leq n}\{\binom{i}{k}\}||f||,$$

y del teorema del binomio tenemos que $\binom{n}{k} \leq 2^n$, por lo tanto

$$||D_k f|| \leq \binom{n}{k}||f|| \leq 2^n||f||.$$

□

Para $\epsilon > 0$ fijo definimos $\mu = 1 + \frac{d}{2} + \epsilon$ y elegimos $\lambda < \frac{1}{2}$ racional tal que $\delta = (1 + \frac{2\epsilon}{d})(1 - \lambda) > 0$ (podemos hacer esto pues $\lambda < 1$ implica $\delta > 0$). Como α es algebraico de grado d, $\{1, \alpha, \ldots, \alpha^{d-1}\}$ es una base de $\mathbb{Q}(\alpha)$ por lo tanto cada potencia r se puede escribir de la siguiente manera

$$\alpha^r = c_{r,0} + c_{r,1}\alpha + \cdots + c_{r,d-1}\alpha^{d-1} \text{ con } c_{r,s} \in \mathbb{Q}. \tag{1.4}$$

Proposición 1.9. *Existe un entero $b > 0$ que depende sólo de α tal que $b^r c_{r,s} \in \mathbb{Z}$ para cuales quiera $r, s \geq 0$. Más aun $|c_{r,s}| \leq B_1^r$ donde $B_1 = 1 + \text{máx}_{r \leq d}\{|c_{r,s}|\}$.*

Demostración. Sea $b > 0$ un común denominador de los $c_{d,s}$. Si $r \leq d$ la desigualdad es consecuencia de la definición de B_1, ahora, si $r > d$ tenemos

$$\begin{aligned}
\alpha^{r+1} =& \alpha^r \alpha \\
=& c_{r,0}\alpha + c_{r,1}\alpha^2 + \cdots + c_{r,d-2}\alpha^{d-1} + c_{r,d-1}(c_{d,0} + \cdots + c_{d,d-1}\alpha^{d-1}) \\
=& c_{r,d-1}c_{d,0} + (c_{r,d-1}c_{d,1} + c_{r,0})\alpha + \cdots + (c_{r,d-1}c_{d,d-1} + c_{r,d-2})\alpha^{d-1}
\end{aligned}$$

Haciendo esto inductivamente tenemos que $\text{máx}\,|c_{r,s}| \leq B_1^r$ y también que b^r es un común denominador para los $c_{r,s}$, tal como queríamos. □

Los pasos que seguiremos para demostrar el teorema de aproximación de Thue serán los siguientes:

- Supondremos que hay una infinidad de aproximaciones excelentes de α, y tomaremos u, v dos de éstas, con denominadores suficientemente grandes y el denominador de v suficientemente mayor que el de u (vease la ecuación 1.5).
- Dependiendo de u y v construiremos polinomios $F_n(X, Y)$ con coeficientes enteros no muy grandes y tal que $D_j F_n(\alpha, \alpha) = 0$ para muchas j (veanse la ecuaciones 1.6 y 1.8).
- Encontraremos una cota superior para $|D_j F_n(u, v)|$ (vease la ecuación 1.10).
- Encontraremos una cota inferior para $|D_j F_n(u, v)|$, cuando $D_j F_n(u, v) \neq 0$ (vease 1.11).

- Veremos que $D_j F_n(u, v) \neq 0$ para i suficientemente pequeño y obtendremos una contradicción (vease 1.16).

Sean $u = \frac{p}{q}$ y $v = \frac{r}{s}$ con $p, q, r, s \in \mathbb{Z}$, $(p, q) = 1$ y $(r, s) = 1$ aproximaciones excelentes de α con $0 < q < s$, entonces

$$|\alpha - \frac{p}{q}| \leq \frac{1}{q^\mu} \qquad |\alpha - \frac{r}{s}| \leq \frac{1}{s^\mu} \qquad 0 < q < s. \tag{1.5}$$

1.2.1. Construcción de polinomios F_n

Para el primer paso construiremos una sucesión de polinomios F_n, y el F buscado será un F_r para algún r que dependerá de u y v.

Los F_n que construiremos serán de la forma

$$F_n(X, Y) = P_n(X) + Y Q_n(X) \in \mathbb{Z}[X, Y], \tag{1.6}$$

con $deg_x F_n = \text{máx}(deg(Q_n), deg(P_n)) \leq n$, tales que $D_j F_n(\alpha, \alpha) = 0$ para $0 \leq j \leq m$ (pronto diremos quién es esta m). Disponemos de $2n + 2$ coeficientes (de P_n y Q_n) que veremos como variables. Cada condición $D_j F_n(\alpha, \alpha) = 0$ corresponde a una condición lineal de las variables. Sin embargo esta condición está definida sobre $\mathbb{Q}(\alpha)$ y nosotros la queremos en $\mathbb{Q}$. Para obtener ecuaciones definidas sobre $\mathbb{Q}$ usaremos la base $\{1, \alpha, \ldots, \alpha^{d-1}\}$ de $\mathbb{Q}(\alpha)/\mathbb{Q}$; esta base transforma cada ecuación original en d nuevas ecuaciones lineales, esta vez sobre $\mathbb{Q}$. Como tenemos m condiciones $D_j F_n(\alpha, \alpha) = 0$ tenemos un total de md formas lineales en $2n + 2$ variables. Así la condición $md < 2n + 2$ asegura una solución no trivial para los coeficientes de P_n y Q_n. Para tener buenas cotas para las soluciones enteras escogemos m poco menor que $\frac{2n+2}{d}$. Veamos ahora que sistema de ecuaciones obtenemos. Escribimos a P_n y Q_n de la siguiente manera:

$$P_n(X) = x_0 + \cdots + x_n X^n \qquad Q_n(X) = y_0 + \cdots + y_n X^n$$

$$\begin{aligned}
D_jF_n(\alpha,\alpha) = D_jP_n(\alpha) + \alpha D_jQ_n(\alpha) &= \sum_{s=j}^{n} x_s \binom{s}{j} \alpha^{s-j} + \sum_{s=j}^{n} y_s \binom{s}{j} \alpha^{s-j+1} \\
&= \sum_{s=j}^{n} x_s \binom{s}{j} \sum_{i=0}^{d-1} c_{s-j,i}\alpha^i + \sum_{s=j}^{n} y_s \binom{s}{j} \sum_{i=0}^{d-1} c_{s-j+1,i}\alpha^i \\
&= \sum_{s=j}^{n} \sum_{i=0}^{d-1} \alpha^i \left(x_s \binom{s}{j} c_{s-j,i} + y_s \binom{s}{j} c_{s-j+1,i} \right) \\
&= \sum_{i=0}^{d-1} \alpha^i \sum_{s=j}^{n} \left(x_s \binom{s}{j} c_{s-j,i} + y_s \binom{s}{j} c_{s-j+1,i} \right) \\
&= L_{n,0}^{(j)}(\underline{x}) + \alpha L_{n,1}^{(j)}(\underline{x}) + \cdots + \alpha^{d-1} L_{n,d-1}^{(j)}(\underline{x})
\end{aligned}$$

donde

$$L_{n,i}^{(j)} = \sum_{s=j}^{n} \left(x_s \binom{s}{j} c_{s-j,i} + y_s \binom{s}{j} c_{s-j+1,i} \right)$$

son formas lineales y $\underline{x} = (x_0, \ldots, x_n, y_0, \ldots, y_n)$. De la proposición 1.9 tenemos $b^{n+1}L_{n,i}^{(j)}$ tiene coeficientes enteros y también que los coeficientes de $L_{n,i}^{(j)}$ están acotados por $2^n B_1^{n+1}$, así que los coeficientes de $b^{n+1}L_{n,i}^{(j)}$ están acotados por $b^{n+1}2^n B_1^{n+1} \leq B_2^n$ con $B_2 = (2bB_1)^2$.

Por otro lado $D_jF_n(\alpha,\alpha) = 0$ implica que $L_{n,i}^{(j)} = 0$ para $0 \leq j \leq m-1$ y $0 \leq i \leq d-1$, y es así como obtenemos un sistema de md ecuaciones.

Lema 1.10 (Siegel)**.** *Para $i = 1, \ldots, N$, $j = 1, \ldots, M$ donde $N > M$ sean a_{ij} enteros con valor absoluto a lo más $A \geq 1$. Entonces existen enteros $t_1, \ldots, t_N$ no todos cero tales que $|t_i| \leq (NA)^{\frac{M}{N-M}}$ y $\sum_{i=1}^{N} a_{ij}t_i = 0$*

Demostración. Sea

$$T = \left[(NA)^{\frac{M}{N-M}} \right] \geq 1, \qquad I_T = \{0, 1, \ldots, T\}$$

y consideremos los vectores $\underline{x} = (x_1, \ldots, x_N) \in I_T^N \subset \mathbb{Z}^N$, entonces hay $(T+1)^N$ de estos vectores. Consideremos

$$L : \mathbb{Z}^N \to \mathbb{Z}^N \ \text{ definida por } \ L(\underline{x}) = (\sum_{i=1}^{N} a_{ij}x_i)_{j=1}^{M}.$$

Sea $S_+^j = \sum_{i=1}^{N} \text{máx}\{0, a_{ij}\}$ y $S_-^j = \sum_{i=1}^{N} \text{mín}\{0, a_{ij}\}$, entonces

$$S_+^j - S_-^j = \sum_{i=1}^{N} |a_{ij}| \leq NA \quad \text{y} \quad S_-^j T \leq \sum_{i=1}^{N} a_{ij}x_i \leq S_+^j T$$

para $\underline{x} \in I_T^N$. El intervalo $[S_-^j, S_+^j]$ contiene $S_+^j - S_-^j \leq NAT + 1$ enteros, entonces $L(I_T^N)$ tiene a lo más $(NAT+1)^M$ puntos. Por definición de T tenemos $T + 1 > (NA)^{\frac{M}{N-M}}$, así que $(T + 1)^{N-M} > (NA)^M$ y

$$\#(I_T^N) = (T + 1)^N > (T + 1)^M \geq (NAT + 1)^M \geq \#(L(I_T^N))$$

entonces existen $\underline{x'}, \underline{x''} \in I_T^N$ tales que $L(\underline{x'}) = L(\underline{x''})$; sea $\underline{t} = (t_1, \ldots, t_N) = \underline{x'} - \underline{x''} \neq 0$, entonces $L(\underline{t}) = ((\sum_{i=1}^N a_{ij}t_i)_j)_{j=1}^M = 0$, con $|t_i| \leq T = (NA)^{\frac{M}{N-M}}$ para $1 \leq i \leq N$ como queríamos. □

Ahora apliquemos el lema a las md formas lineales $b^{n+1}L_{n,i}^{(j)}$ para $0 \leq j \leq m - 1$ y $0 \leq i \leq d - 1$ en las $2n + 2$ variables x_k, y_k,$0 \leq k \leq n$.

Consideremos sólo los valores n tales que $(2n + 2)(1 - \lambda)$ es un entero múltiplo de d (estos existen por que λ es racional), para estos valores de n definimos

$$m = \frac{(2n + 2)(1 - \lambda)}{d} \tag{1.7}$$

y apliquemos el lema con $N = 2n + 2$, $M = md = (2n + 2)(1 - \lambda) < N$ y $A = B_2^n \leq 1$. Notemos que $N - M = \lambda N$ entonces $\frac{M}{N-M} = \frac{1-\lambda}{\lambda}$, así el lema nos da un vector $(\underline{x}, \underline{y})$ no cero tal que

$$|x_k|, |y_k| \leq (NA)^{\frac{M}{N-M}} = ((2n + 2)B_2^n)^{\frac{1-\lambda}{\lambda}} \leq (4B_2)^{\frac{n}{\lambda}} \leq B_3^n$$

con $B_3 = (4B_2)^{\frac{1}{\lambda}}$, y esta cota implica que los polinomios P_n, Q_n cumplen que

$$||P_n||, ||Q_n|| \leq B_3^n \tag{1.8}$$

por lo tanto hemos construido polinomios $F_n(X) = P_n(X) + YQ_n(X) \neq 0$ como los necesitábamos.

1.2.2. Una cota superior para $|D_jF_n(u, v)|$

Tenemos $F_n(X, Y) = P_n(X) + YQ_n(X) \in \mathbb{Z}[X, Y]$. Recordemos que F_n tiene un cero de orden $\geq m$ en $X = \alpha$, así que podemos escribir $F_n(X, \alpha) = (X - \alpha)^m R_n(X)$ para algún polinomio R_n. Por lo tanto

$$F_n(X, Y) = F_n(X, \alpha) + (Y - \alpha)Q_n(X) = (X - \alpha)^m R_n(X) + (Y - \alpha)Q_n(X).$$

Entonces, para $j = 0, 1, ..., m - 1$,

$$D_jF_n(X, Y) = (X - \alpha)^{m-j} R_{n,j}(X) + (Y - \alpha)D_jQ_n(X), \tag{1.9}$$

para algún polinomio $R_{j,n}(X)$.

Ahora queremos acotar $\|R_{j,n}\|$ y $\|D_jQ_n\|$. Pero por propiedad c) de la norma y por 1.8 inmediatamente tenemos que

$$\|D_jQ_n\| \leq (2B_3)^n$$

y de 1.9 tenemos que

$$D_jF_n(X,\alpha) = (x-\alpha)^{m-j}R_{n,j}(X).$$

Entonces, pensando en que $\mathbb{C}(X) \subset \mathbb{C}[[X]]$ y escribiendo la serie formal

$$\begin{aligned}\frac{1}{(\alpha - X)^s} =& \frac{\alpha^{-s}}{(1-X/\alpha)^s} \\ =& \sum_{r\geq 0}\binom{-s}{r}\alpha^{-r-s}X^r \\ =& \sum_{r\geq 0}(-1)^r\binom{s+r-1}{r}\alpha^{-r-s}X^r\end{aligned}$$

obtenemos $R_{n,j}(X) \in \mathbb{C}[X] \subset \mathbb{C}[[X]]$ como el producto formal de $D_jF_n(X,\alpha)$ y $\frac{1}{(X-\alpha)^{m-j}}$. Como $R_{n,j}$ tiene grado a lo mas $n-m$, necesitamos solamente considerar las primeras $n-m$ potencias de X provenientes del producto. Los coeficientes de la serie formal, para $s = m-j$ y $r \leq n-m$, pueden ser inmediatamente acotadas por $2^n \max(1, |1/\alpha|)^n$. También, los coeficientes de $D_jF_n(X,\alpha) = D_jP_n(X) + \alpha D_jQ_n(X)$ están acotados por $\|D_jP_n\| + |\alpha|\|D_jQ - n\| \leq 2^n(1+|\alpha|)B_3^n$.

Todo esto implica que $\|R_{n,j}\| \leq (n+1)2^{2n}\max(1, 1/|\alpha|)^n(1+|\alpha|)B_3^n$.

Entonces tenemos que

$$\|R_{j,n}\|, \|D_jQ_n\| \leq B_4^n, \quad j = 0,\ 1, ...,\ m-1,$$

donde $B_4 = 16\max(1, 1/|\alpha|)(1+|\alpha|)B_3$.

Ahora daremos una cota superior para $|D_jF_n(u,v)|$ con $u,\ v$ excelentes aproximaciones como en 1.5; el que sean como en 1.5 implica que $|u|,\ |v| \leq 1+|\alpha|$, por lo tanto tenemos:

$$\begin{aligned}|D_jF_n(u,v)| &= |(u-\alpha)|^{m-j}R_{n,j}(u) + (v-\alpha)D_jQ_n(u) \\ &\leq |u-\alpha|^{m-j}(n+1)\|R_{n,j}\|(1+|\xi|)^n + |v-\alpha|(n+1)\|D_jQ_n\|(1+|\alpha|)^n \\ &\leq (|u-\alpha|^{m-j} + |v-\alpha|)(n+1)(1+|\alpha|)^nB_4^n \\ &\leq (q^{-\mu(m-j)} + s^{-\mu})B_5^n\end{aligned}$$

donde podemos escoger $B_5 = 2(1+|\alpha|)B_4$.

Así

$$|D_jF_n(u,v)| \leq (q^{-\mu(m-j)} + s^{-\mu})B_5^n. \tag{1.10}$$

1.2.3. Una cota inferior para $|D_j F_n(u,v)|$

Sabemos que $D_j F_n(X,Y)$ tiene coeficientes enteros y grado $\leq n-j$ en X y grado ≤ 1 en Y. Entonces $D_j F_n(u,v) = \frac{w}{t}$ con $w, t \in \mathbb{Z}$ y $t|q^{n-j}s$ (esto porque $u = \frac{p}{q}$ y $v = \frac{r}{s}$) así que $t \leq q^{n-j}s$. Entonces $D_j F_n(u,v) = 0$ ó

$$|D_j F_n(u,v)| = \frac{|w|}{|t|} \geq \frac{1}{t} \geq \frac{1}{q^{n-j}s}. \tag{1.11}$$

1.2.4. Una cota superior para la multiplicidad de (u,v)

Ahora queremos encontrar el valor más pequeño de j tal que $D_j F_n(u,v) \neq 0$. Sea h este valor (posiblemente 0 o ∞) así que tenemos $D_h F_n(u,v) \neq 0$ y $D_j F_n(u,v) = 0$ para todo $j = 0,\ 1, ...,\ h-1$, entonces

$$P_n^{(j)}(u) + vQ_n^{(j)}(u) = 0, \quad j = 0,\ 1, ...,\ h-1.$$

Eliminando v de cualquier par de estas ecuaciones obtenemos

$$(P_n^{(j)}Q_n^{(i)} - Q_n^{(j)}P_n^{(i)})(u) = 0, \quad i,j = 0,1,...,h-1. \tag{1.12}$$

Para $i = 0,\ j = 1$ tenemos que $W = W_{P_n,\ Q_n} := P_nQ_n' - P_n'Q_n \in \mathbb{Z}[X]$ se anula en $X = u$. Mas generalmente, la regla del producto $D^j(AB) = \Sigma_{i=0}^{j}\binom{j}{i}A^{(j-i)}B^{(i)}$ nos dice que

$$W^{(j)}(u) = (P_nQ_n' - Q_nP_n')^{(j)}(u) \quad = \sum_{i=0}^{j}\binom{j}{i}(P_n^{(j-i)}Q_n^{(i+1)} - Q_n^{(j-i)}P_n^{(i+1)}).$$

Así que 1.12 en efecto implica que

$$W^{(j)}(u) = 0, \quad j = 0,\ 1, ...,\ h-2. \tag{1.13}$$

Notemos ahora que nuestros polinomios $P_n,\ Q_n$ son linealmente independientes. Para esto supongamos lo contrario; si son linealmente dependientes entonces $P_n = cQ_n$ y

$$F_n(X,\alpha) = P_n(X) + \alpha Q_n(X) = (c+\alpha)Q_n$$

sería un múltiplo escalar de P_n o Q_n. Por otra parte $F_n(X,\alpha)$ es no cero (porque $\alpha \notin \mathbb{Q}$ y $P_n,\ Q_n$ son no ambos cero) y por construcción F_n tiene un cero de multiplicidad al menos m en $X = \alpha$. Pero como estamos suponiendo que $P_n,\ Q_n$ son linealmente dependientes, esto sería cierto también para P_n y Q_n y entonces ellos tendrían un cero de multiplicidad $\geq m$ en cada uno de los

d (recordemos que d es el grado de α) conjugados de α sobre $\mathbb{Q}$. Pero por 1.7 tenemos que

$$md = (2n+2)(1-\lambda)$$

y como hemos escogido $\lambda < 1/2$ tenemos que

$$md > n+1,$$

forzando a $P_n,\ Q_n$ a ser cero, (ya que ambos tienen grado $\leq n$). Pero esto es una contradicción,por lo tanto $P_n,\ Q_n$ son linealmente independientes, es decir, $0 \neq \begin{vmatrix} P_n & Q_n \\ P_n' & Q_n' \end{vmatrix} = W$.

Por otro lado tenemos que 1.13 implica que $(X-u)^{h-i} = \frac{1}{q^{h-1}}(qX-p)^{h-1}$ divide a $W(X)$. Ahora, $W(X)$ tiene coeficientes enteros y $\frac{1}{q^{h-1}}(qX-p)^{h-1}$ es un polinomio primitivo (porque $p,\ q$ son coprimos); entonces por el Lema de Gauss $\frac{1}{q^{h-1}}(qX-p)^{h-1}$ divide a $W(X)$ en $\mathbb{Q}[X]$ y por tanto en $\mathbb{Z}[X]$. Esto implica que q^{h-1} divide al coeficiente líder de W así que en particular $\|W\| \geq q^{h-1}$ (pues W no es identicamente cero). Por otro lado, de 1.8 y de las propiedades de la norma se sigue que

$$\|W\| \leq \|P_nQ_n'\| + \|Q_nP_n'\| \leq 2^n(n+1)B_3^{2n} \leq B_6^n,$$

donde podemos escoger $B_6 = 16B_3^2$. De aquí $q^{h-1} \leq B_6^n$ y aplicando logaritmos obtenemos

$$h \leq 1 + \frac{n log\ B_6}{log\ q}. \tag{1.14}$$

1.2.5. Conclusiones

Recordemos que m fue restringido a estar en cierta sucesión aritmética dependiendo solamente de λ y d (vease la ecuación 1.7). Sea τ la diferencia de tal sucesión aritmética y definimos m como el entero más grande en tal sucesión tal que $q^m \leq s$. Entonces, m cumplirá

$$\frac{log\ s}{log\ q} - \tau \leq m \leq \frac{log\ s}{log\ q} \tag{1.15}$$

Ahora determinaremos n de la ecuación 1.7; notemos que n es un entero ya que m pertenece a dicha sucesión. Ahora, recordemos que $D_hF_n(u,v) \neq 0$. Entonces, por 1.10,

$$|D_hF_n(u,v)| \leq (q^{-\mu(m-h)} + s^{-\mu})B_5^n \leq 2q^{-\mu(m-h)}B_5^n.$$

Por otra parte, comparando con 1.11 obtenemos $(q^{n-h}s)^{-1} \leq 2q^{-\mu(m-h)}B_5^n$, tomando logaritmos obtenemos,

$$\begin{aligned}\mu m - \mu h + h - n &\leq \frac{log\ s}{log\ q} + \frac{log\ 2 + nlog\ B_5}{log\ q} \\ &\leq m + \tau + \frac{log\ 2 + nlog\ B_5}{log\ q}\end{aligned}$$

donde la última desigualdad se sigue de 1.15. sustituyendo 1.14 para h obtenemos

$$\begin{aligned}(\mu - 1)m - n &\leq (\mu - 1)h + \tau + \frac{log\ 2 + nlog\ B_5}{log\ q} \\ &\leq \mu\left(1 + \frac{nlog\ B_6}{log\ q}\right) + \tau + \frac{log\ 2 + nlog\ B_5}{log\ q}.\end{aligned}$$

Ahora tenemos $\mu = 1 + (d/2) + \varepsilon$ mientras que m es dado por 1.7, así que $m > 2n(1 - \lambda)/d$. Por lo tanto,

$$\left(\left(1 + \frac{2\varepsilon}{d}\right)(1 - \lambda) - 1\right)n \leq \mu\left(1 + \frac{nlog\ B_6}{log\ q}\right) + \tau + \frac{log\ 2 + nlog\ B_5}{log\ q},$$

de donde, recordando que $\delta := ((1 + \frac{2\varepsilon}{d})(1 - \lambda) - 1)$,

$$\delta n \leq \mu\left(1 + \frac{nlog\ B_6}{log\ q}\right) + \tau + \frac{log\ 2 + nlog\ B_5}{log\ q}.$$

Recordemos que habíamos escogido λ suficientemente pequeño para que $\delta > 0$. Supongamos ahora que

$$log\ q > \mu\frac{4log\ (2B_5B_6)}{\delta}.$$

Notemos que esto es posible si hay una cantidad infinita de aproximaciones excelentes, ya que $B_5,\ B_6,\ \delta$ dependen solamente de $\alpha,\ \varepsilon,\ \lambda$ (así que finalmente en $\alpha,\ \varepsilon$). Entonces nuestra última ecuación nos lleva a

$$\delta n \leq \mu + \frac{\delta}{4}n + \tau + \frac{\delta}{4}n \leq \mu + \tau + \frac{\delta}{2}n,$$

de donde

$$n \leq \frac{2(\mu + \tau)}{\delta}.$$

De cualquier forma comparando con 1.15 obtenemos

$$\frac{log\ s}{log\ q} \leq \tau + \mu + \leq \tau + n \leq \tau + \frac{2(\mu + \tau)}{\delta}.$$

Y esto nos da una cota para $\log s$ y por lo tanto también una cota para s

$$\log s > log\ q\left(\tau + \frac{2(\mu+\tau)}{\delta}\right) \tag{1.16}$$

de aquí obtenemos una contradicción pues si hubiera una infinidad de aproximaciones excelentes entonces podríamos tomar s tan grande como queramos. En particular esta contradicción demuestra la finitud del conjunto de aproximaciones excelentes para α.

1.3. El Teorema de Thue

Empezaremos esta sección demostrando el Teorema de Thue [1.1] que fue enunciado al inicio de este capítulo, para esto utilizaremos el Teorema de Thue para aproximaciones diofánticas que se demostró en la sección anterior. Posteriormente veremos una generalización del Teorema de Thue y algunos corolarios.

Demostración del Teorema de Thue. Sea $f \in \mathbb{Z}[X,Y]$ homogéneo irreducible de grado $d \geq 3$. Si $f(x,y) = c$ con x, y enteros no cero, de la Proposición 1.2 sabemos que existe una raíz α de $f(X,1)$ tal que $|\alpha - \frac{x}{y}| \leq B|y|^{-d}$, aplicando el Teorema 1.4 con $\epsilon = \frac{1}{4}$ existe $\nu_\alpha > 0$ tal que $|\alpha - \frac{x}{y}| > \frac{\nu_\alpha}{y^{1+\frac{d}{2}+\frac{1}{4}}}$ entonces $\frac{\nu_\alpha}{y^{1+\frac{d}{2}+\frac{1}{4}}} < B|y|^{-d}$ lo que implica $\nu_\alpha |y|^{\frac{d}{2}-\frac{5}{4}} = \frac{\nu_\alpha}{y^{1+\frac{d}{2}+\frac{1}{4}}}|y|^d < B$; sea $s = \max_{f(\alpha,1)=0} \nu_\alpha > 0$, entonces $s|y|^{\frac{d}{2}-\frac{5}{4}} < B$ usando esto y que $d \geq 3$ tenemos $|y|^{\frac{1}{4}} \leq |y|^{\frac{d}{2}-\frac{5}{4}} < \frac{B}{s}$, es decir, $|y| < (\frac{B}{s})^4$, por lo tanto hemos acotado a y, pero a cada y le corresponde sólo un número finito de x; y esto implica que hay sólo un número finito de enteros $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ tales que $f(x,y) = c$. □

A continuación veremos una forma más general del teorema de Thue.

Teorema 1.11. *Sea $f \in \mathbb{Z}[X,Y]$ homogéneo, de grado mayor o igual que 3, sin factores lineales o cuadráticos y sea $c \in \mathbb{Z}$ no cero. Entonces la ecuación $f(X,Y) = c$ tiene sólo un número finito de soluciones enteras.*

Demostración. Sea f como en el teorema, entonces $f = f_1 \cdots f_r$ donde cada $f_i \in \mathbb{Q}[X,Y]$ es irreducible sobre $\mathbb{Q}$, por otro lado como f es homogéneo, entonces cada f_i es homogéneo y como f no tiene factores lineales ni cuadráticos cada f_i es de grado ≥ 3; para cada f_i consideremos a_i como el mínimo común múltiplo de los denominadores de los coeficientes de f_i, entonces $a_i f_i \in \mathbb{Z}[X,Y]$ y consideremos $a = \prod_{i=1}^r a_i$; sabemos que las soluciones de la ecuación $f(X,Y) = c$ son las mismas de la ecuación $af(X,Y) = ac$, veamos

pues que la ecuación $af(X,Y) = ac$ tiene un número finito de soluciones enteras.
Para esto primero notemos que si $af(x,y) = ac$ entonces $\prod a_i f_i = ac$; y si (x,y) es una solución entera de la ecuación, entonces $a_i f_i(x,y)$ es un entero que divide a ac, y esto nos da un número finito de sistemas ecuaciones $a_i f_i = c_i$ donde cada c_i es un divisor de c y $c_1 \cdots c_r = c$, pero por el teorema de Thue 1.1 para cada una de estas ecuaciones hay sólo un número finito de soluciones enteras, y por lo tanto hay sólo un número finito de soluciones enteras a cada sistema de ecuaciones, de aquí que la ecuación $af(X,Y) = ac$ tiene sólo un número finito de soluciones enteras.

□

Corolario 1.12. *Sea $f(X,Y) \in \mathbb{Z}[X,Y]$ un polinomio homogéneo irreducible de grado d y sea $g(X,Y) \in \mathbb{Z}[X,Y]$ un polinomio de grado $m < \frac{d}{2} - 1$. Entonces la ecuación $f(X,Y) = g(X,Y)$ tiene sólo un número finito de soluciones $(x,y) \in \mathbb{Z}^2$*

Demostración. Escribamos $g(X,Y) = \sum_{i+j \leq m} a_{i,j} X^i Y^j$. Entonces cuando $x, y \in \mathbb{Z}$ tenemos $g(x,y) = c \in \mathbb{Z}$ con $|c| \leq k \max\{|x|,|y|\}^m$, donde $k = \frac{(m+1)(m+2)}{2} \max\{|a_{i,j}|\}$ depende sólo de el polinomio $g(X,Y)$. También podemos escribir $m = \frac{d}{2} - 1 - \delta$ con $\delta \geq \frac{1}{2}$.

Ahora sea $(x,y) \in \mathbb{Z}^2$ una solución de la ecuación $f(X,Y) = g(X,Y)$, y supongamos que $|y| = \max\{|x|,|y|\}$ así $|c| \leq k|y|^m$ (el caso en que $|x| \geq |y|$ se haría de la misma manera), entonces por la Proposición 1.2 existe α raíz de $f(X,1)$ tal que

$$|\alpha - \frac{x}{y}| \leq \frac{R|c|}{|y|^d}$$

donde $R = (\frac{2}{\eta})^{d-1}$ depende sólo de el polinomio $f(X,Y)$, por lo tanto

$$|\alpha - \frac{x}{y}| \leq \frac{Rk|y|^m}{|y|^d} = \frac{Rk}{|y|^{d-m}} = \frac{Rk}{|y|^{d-\frac{d}{2}+1+\delta}} = \frac{Rk}{|y|^{\frac{d}{2}+1+\delta}},$$

por otro lado como $f(X,Y)$ es irreducible, $f(X,1)$ también lo es, por lo tanto $deg(\alpha) = d$, ahora apliquemos el teorema de aproximación de Thue a α, entonces existe $\gamma > 0$ tal que

$$\frac{\gamma}{|y|^{1+\frac{d}{2}+\frac{1}{4}}} < |\alpha - \frac{x}{y}|,$$

juntando estas dos últimas desigualdades tenemos que

$$\frac{\gamma}{|y|^{1+\frac{d}{2}+\frac{1}{4}}} < \frac{Rk}{|y|^{\frac{d}{2}+1+\delta}}$$

despejando nos queda

$$|y|^{\delta-\frac{1}{4}} < \frac{Rk}{\gamma}$$

entonces

$$|y|^{\frac{1}{4}} < \frac{Rk}{\gamma}$$

y esto implica que sólo hay un número finito de soluciones (x, y) enteras para la ecuación $f(X, Y) = g(X, Y)$. □

Teorema 1.13. *Sea k un campo, y $n \geq 2$ entero, sea $a \in k$, $a \neq 0$. Si para todo primo $p \in \mathbb{Z}$ tal que $p|n$ se tiene que $a \notin k^p$ y si $4|n$ entonces $a \notin -4k^4$. Entonces el polinomio $x^n - a$ es irreducible en $k[X]$.*

La prueba de este teorema se puede ver en la página 297 del libro Algebra de Lang [Lan02].

Corolario 1.14. *Sean $n \geq 3$ entero, $c \in \mathbb{Z}$ no cero y $b \in \mathbb{Z}$ tal que si p es un primo que divide a n entonces b no es una potencia p-ésima y si $4|n$ entonces $b \neq -4m^4$ para toda $m \in \mathbb{N}$. Entonces la ecuación*

$$X^n - bY^n = c$$

tiene sólo un número finito de soluciones (x, y) enteras.

Demostración. Consideremos el polinomio $f(X, Y) = X^n - bY^n$, $k = \mathbb{Q}(Y)$ y $a = bY^n \in k$, entonces por el teorema 1.13 $f(X, Y)$ es irreducible en $\mathbb{Q}(Y)[X]$, en particular es irreducible sobre $\mathbb{Q}[X, Y]$, en estas condiciones podemos aplicar el teorema de Thue a la ecuación $f(X, Y) = c$ y esto prueba el corolario. □

Para ver más acerca del método Thue aplicado a la ecuación $X^2 - dY^2 = c$ se puede consultar [Mat02]. En [TdW89] se puede ver un análisis de las soluciones de la ecuación de Thue usando formas logarítmicas, ahí mismo también se puede ver como aplican el método a ciertas ecuaciones.

2

Soluciones de la ecuación de Thue: $|F(X,Y)| = 1$

En este capítulo analizaremos el caso particular de la ecuación de Thue $|F(X,Y)| = 1$, para esto seguiremos la linea de Bombieri y Schmidt en [BS87], empezaremos con una sección de preliminares para luego analizar la cantidad de soluciones grandes y posteriormente la cantidad de soluciones pequeñas.

2.1. Preliminares

Sea $F(X,Y) \in \mathbb{Z}[X,Y]$ irreducible sobre los racionales, homogéneo de grado $n \geq 3$, y sean $f(X) = F(X,1)$ y $\alpha_1, \alpha_2, \ldots, \alpha_n$ las raíces de $f(X)$.

Definición 2.1. *Definimos el discriminante de $F(X,Y)$ como*

$$D(F) = a_0^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

donde a_0 es el coeficiente líder de $f(X)$.

Observación 2.2. *Notemos que $D(F)$ es el mismo si consideramos el polinomio $F(x,1)$ o $F(1,y)$.*

Demostración. Queremos ver que $a_0^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 = a_n^{2n-2} \prod_{i<j} (\frac{1}{\alpha_i} - \frac{1}{\alpha_j})^2$. ¡Hagamos las cuentas! Empecemos por ver que

$$\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)=\prod_{k=1}^{n}\alpha_k^{n-1}\prod_{1\leq i<j\leq n}(\frac{1}{\alpha_j}-\frac{1}{\alpha_i}) \tag{2.1}$$

probemoslo por inducción sobre n empecemos con $n=2$

$$\begin{aligned}\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)&=(\alpha_1-\alpha_2)\\&=\alpha_1\alpha_2(\frac{1}{\alpha_2}-\frac{1}{\alpha_1})\\&=\prod_{k=1}^{2}\alpha_k^{2-1}\prod_{1\leq i<j\leq 2}(\frac{1}{\alpha_j}-\frac{1}{\alpha_i})\end{aligned}$$

por lo tanto si se cumple para $n=2$.
Ahora veamos la hipótesis de inducción. Supongamos que se cumple para $n-1$ y veamos que se cumple para n, entonces tenemos

$$\prod_{1\leq i<j\leq n-1}(\alpha_i-\alpha_j)=\prod_{k=1}^{n-1}\alpha_k^{n-2}\prod_{1\leq i<j\leq n-1}(\frac{1}{\alpha_j}-\frac{1}{\alpha_i}),$$

y multipliquemos la ecuación por

$$\prod_{i=1}^{n-1}(\alpha_i-\alpha_n)=a_n^{n-1}\prod_{k=1}^{n-1}\alpha_k^{n-1}\prod_{i=1}^{n-1}(\frac{1}{\alpha_n}-\frac{1}{\alpha_i})$$

para obtener

$$\prod_{i=1}^{n-1}(\alpha_i-\alpha_n)\prod_{1\leq i<j\leq n-1}(\alpha_i-\alpha_j)=a_n^{n-1}\prod_{k=1}^{n-1}\alpha_k^{n-1}\prod_{i=1}^{n-1}(\frac{1}{\alpha_n}-\frac{1}{\alpha_i})\prod_{k=1}^{n-1}\alpha_k^{n-2}\prod_{1\leq i<j\leq n-1}(\frac{1}{\alpha_j}-\frac{1}{\alpha_i}),$$

y así

$$\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)=\prod_{k=1}^{n}\alpha_k^{n-1}\prod_{1\leq i<j\leq n}(\frac{1}{\alpha_j}-\frac{1}{\alpha_i})$$

tal como queríamos.
Ahora, elevemos la ecuación 2.1 al cuadrado y multipliquemosla por a_0^{2n-2} para obtener

$$a_0^{2n-2}\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2=a_0^{2n-2}\prod_{k=1}^{n}(\alpha_k^{2n-2})\prod_{1\leq i<j\leq n}(\frac{1}{\alpha_j}-\frac{1}{\alpha_i})^2$$

y así queda demostrada la observación pues como $a_n^2=F(0,1)^2=a_0^2(\prod_{i=1}^{n}\alpha_i)^2$, se tiene que $a_n^{2n-2}=a_0^{2n-2}\prod_{k=1}^{n}\alpha_k^{2n-2}$.

□

Definición 2.3. *Sea* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z})$ *una matriz con* $det(A) = 1$. *Definimos el polinomio* $F_A(X, Y)$ *como a continuación:*

$$F_A(X, Y) = F(aX + bY, cX + dY).$$

Observación 2.4. *Hay una correspondencia entre las raíces* α_i *de* $F(X, 1)$ *y las raíces* ξ_i *de* $F_A(X, 1)$.

Demostración. Notemos que si $cx + d = 0$ entonces $x = -\frac{d}{c}$ y

$$\begin{aligned} F_A(x, 1) =& F(ax + b, cx + d) \\ =& F(-a\frac{d}{c} + b, 0) \\ =& a_0(-a\frac{d}{c} + b)^n \end{aligned}$$

por lo tanto $F_A(X, 1) \neq 0$ cuando $cX+d = 0$, pues si esto ocurriera tendríamos que $a_0 = 0$ ó $-a\frac{d}{c} + b = 0$ y ninguna de éstas es posible pues $a_0 \neq 0$ por definición de coeficiente líder y $-a\frac{d}{c} + b \neq 0$ por que $det(A) \neq 0$. Sea ξ_i una raíz de $F_A(X, 1)$, entonces $c\xi_i + d \neq 0$ y

$$\begin{aligned} 0 =& F_A(\xi_i, 1) = F(a\xi_i + b, c\xi_i + d) \\ &= (c\xi_i + d)^n F(\frac{a\xi_i + b}{c\xi_i + d}, 1) \end{aligned}$$

por lo tanto $F(\frac{a\xi_i+b}{c\xi_i+d}, 1) = 0$, lo que implica que $\frac{a\xi_i+b}{c\xi_i+d}$ es una raíz de $F(X, 1)$, digamos α_i, así $\frac{a\xi_i+b}{c\xi_i+d} = \alpha_i$

De manera semejante a cada raíz α_i de $F(X, 1)$ le corresponde una raíz $\xi_i = \frac{b-\alpha_i d}{c\alpha_i - a}$ de $F_A(X, 1)$.

□

Observación 2.5. *El coeficiente líder de* $F_A(X, 1)$ *es* $a_0 \prod_{i=1}^{n}(a - \alpha_i c)$.

Demostración. Sabemos que si $G(X, Y)$ es un polinomio homogéneo entonces el coeficiente líder del polinomio $G(X, 1)$ es $G(1, 0)$, por lo tanto el coeficiente

líder de $F_A(X,1)$ es

$$\begin{aligned} F_A(1,0) = F(a,c) &= c^n a_0 F(\frac{a}{c}, 1) \\ &= c^n a_0 \prod_{i=1}^{n} (\frac{a}{c} - \alpha_i) \\ &= a_0 \prod_{i=1}^{n} (a - \alpha_i c). \end{aligned}$$

□

Proposición 2.6. *Sean $F(X,Y)$ y $F_A(X,Y)$ como antes. Entonces*

$$D(F_A) = det(A)^{n(n-1)} D(F).$$

Demostración. Empecemos por desarrollar el lado izquierdo de la ecuación

$$\begin{aligned} D(F_A) &= (a_0 \prod_{i=1}^{n} (a - \alpha_i c))^{2n-2} \prod_{i<j} (x_i - x_j)^2 \\ &= a_0^{2n-2} \prod_{i=1}^{n} (a - \alpha_i c)^{2n-2} \prod_{i<j} (\frac{b - \alpha_i d}{c\alpha_i - a} - \frac{b - \alpha_j d}{c\alpha_j - a})^2 \\ &= a_0^{2n-2} \prod_{i=1}^{n} (a - \alpha_i c)^{2n-2} \prod_{i<j} (\frac{(b - \alpha_i d)(c\alpha_j - a) - (c\alpha_i - a)(b - \alpha_j d)}{(c\alpha_i - a)(c\alpha_j - a)})^2 \\ &= a_0^{2n-2} \prod_{i=1}^{n} (a - \alpha_i c)^{2n-2} \prod_{i<j} (\frac{(ad - bc)(\alpha_i - \alpha_j)}{(c\alpha_i - a)(c\alpha_j - a)})^2 \\ &= a_0^{2n-2} \prod_{i=1}^{n} (a - \alpha_i c)^{2n-2} \prod_{i<j} \frac{(ad - bc)^2 (\alpha_i - \alpha_j)^2}{(c\alpha_i - a)^2 (c\alpha_j - a)^2} \\ &= a_0^{2n-2} (ad - bc)^{n(n-1)} \prod_{i=1}^{n} (a - \alpha_i c)^{2n-2} \prod_{i<j} \frac{(\alpha_i - \alpha_j)^2}{(c\alpha_i - a)^2 (c\alpha_j - a)^2} \\ &= a_0^{2n-2} (ad - bc)^{n(n-1)} \prod_{i=1}^{n} (a - \alpha_i c)^{2n-2} \prod_{i<j} \frac{1}{(c\alpha_i - a)^2 (c\alpha_j - a)^2} \prod_{i<j} (\alpha_i - \alpha_j)^2 \end{aligned}$$

Para continuar notemos que

$$\begin{aligned}
\prod_{i<j}\frac{1}{(c\alpha_i-a)^2(c\alpha_j-a)^2} &= \prod_{i<j}[(c\alpha_i-a)(c\alpha_j-a)]^{-2}\\
&=[(c\alpha_1-a)(c\alpha_2-a)]^{-2}[(c\alpha_1-a)(c\alpha_3-a)]^{-2}\cdots[(c\alpha_1-a)(c\alpha_n-a)]^{-2}\\
&\quad\cdot[(c\alpha_2-a)(c\alpha_3-a)]^{-2}[(c\alpha_2-a)(c\alpha_4-a)]^{-2}\cdots[(c\alpha_2-a)(c\alpha_n-a)]^{-2}\\
&\quad\cdots[(c\alpha_{n-1}-a)(c\alpha_n-a)]^{-2}\\
&=[(c\alpha_1-a)^{n-1}(c\alpha_2-a)(c\alpha_3-a)\cdots(c\alpha_n-a)]^{-2}\\
&\quad\cdot[(c\alpha_2-a)^{n-2}(c\alpha_3-a)(c\alpha_4-a)\cdots(c\alpha_n-a)]^{-2}\\
&\quad\cdots[(c\alpha_{n-1}-a)^{1}(c\alpha_n-a)]^{-2}\\
&=[(c\alpha_1-a)^{n-1}(c\alpha_2-a)^{n-1}\cdots(c\alpha_n-a)^{n-1}]^{-2}\\
&=\prod_{i=1}^{n}[(c\alpha_i-a)^{n-1}]^{-2}\\
&=\prod_{i=1}^{n}\frac{1}{(c\alpha_i-a)^{2n-2}},
\end{aligned}$$

Entonces

$$\begin{aligned}
D(F_A) &= a_0^{2n-2}(ad-bc)^{n(n-1)}\prod_{i=1}^{n}(a-\alpha_i c)^{2n-2}\prod_{i<j}\frac{1}{(c\alpha_i-a)^2(c\alpha_j-a)^2}\prod_{i<j}(\alpha_i-\alpha_j)^2\\
&= a_0^{2n-2}(ad-bc)^{n(n-1)}\prod_{i=1}^{n}(a-\alpha_i c)^{2n-2}\prod_{i=1}^{n}\frac{1}{(c\alpha_i-a)^{2n-2}}\prod_{i<j}(\alpha_i-\alpha_j)^2\\
&= a_0^{2n-2}(ad-bc)^{n(n-1)}\prod_{i<j}(\alpha_i-\alpha_j)^2\\
&= (ad-bc)^{n(n-1)}a_0^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2\\
&= det(A)^{n(n-1)}D(F)
\end{aligned}$$

□

Proposición 2.7. *Sea $p\in\mathbb{Z}$ un número primo. Entonces*

$$\mathbb{Z}^2=\cup_{1=0}^{p}A_i(\mathbb{Z}^2)$$

donde $A_0=\begin{pmatrix}p&0\\0&1\end{pmatrix}$ *y* $A_j=\begin{pmatrix}0&-1\\p&j\end{pmatrix}$ *para* $j=1,\ldots,p$.

Demostración. Notemos que la inclusión $\mathbb{Z}^2 \supseteq \cup_{1=0}^{p} A_i(\mathbb{Z}^2)$ se da por que $A_i(\mathbb{Z}^2) \subset \mathbb{Z}^2$ para cada i.

Ahora sea $(x, y) \in \mathbb{Z}^2$, para ver que $(x, y) \in \cup_{1=0}^{p} A_i(\mathbb{Z}^2)$, consideraremos dos casos: $x \equiv 0 \bmod p$ y $x \not\equiv 0 \bmod p$.

- Caso $x \equiv 0 \bmod p$. Si $x \equiv 0 \bmod p$ entonces existe $n \in \mathbb{Z}$ tal que $x = np$, y por tanto $(x, y) = n(p, 0) + y(0, 1)$, por lo tanto $(x, y) \in A_0(\mathbb{Z}^2) \subseteq \cup_{1=0}^{p} A_i(\mathbb{Z}^2)$.

- Caso $x \not\equiv 0 \bmod p$. Supongamos que $x \not\equiv 0 \bmod p$, para ver que $(x, y) \in A_i(\mathbb{Z}^2)$ para algún $i = 1, \ldots, p$ basta encontrar $s, t \in \mathbb{Z}$ tales que $(x, y) = s(0, p) + t(-1, j)$, pero $s(0, p) + t(-1, j) = (-t, sp + jt)$, consideremos pues $t = -x$, y notemos que:
  Si $y \equiv 0 \bmod p$ entonces $p|y$ y por tanto $p|y - it$ para $i = p$, ahora consideremos $s = \frac{y-pt}{p}$, entonces $(x, y) = (-t, sp + pt) = s(0, p) + t(-1, p) \in A_p(\mathbb{Z}^2)$.
  Ahora, si $y \neq 0 \bmod p$ escogemos j tal que $y - jt \equiv 0 \bmod p$, tal j existe por que $\mathbb{Z}_p$ es campo y $x, y \neq 0$ en $\mathbb{Z}_p$ y $s = \frac{y-jt}{p}$ para obtener $(x, y) = (-t, sp + jt) = s(0, p) + t(-1, j) \in A_j(\mathbb{Z}^2)$.

□

Notemos que como $det(A_i) = p$, de la proposición 2.6 se tiene que

$$|D(F_A)| = p^{n(n-1)}|D(F)| \geq p^{n(n-1)}.$$

Ahora, sean N_n el máximo número de soluciones de $|F(X, Y)| = 1$, n_i el número de soluciones de $|F_{A_i}(X, Y)| = 1$ y $N_n(p)$ el máximo número de soluciones de $|F(X, Y)| = 1$ con $|D(F)| \geq p^{n(n-1)}$. Entonces por de la proposición 2.7 tenemos que

$$N_n \leq n_0 + n_1 + \cdots + n_p \leq (p + 1)N_n(p) \tag{2.2}$$

Definición 2.8. *Se define la altura de Mahler de F como*

$$M(F) = |a_0| \prod_{i=1}^{n} \text{máx}\{1, |\alpha_i|\} = |a_0| \prod_{i=1}^{n} z_i$$

donde $z_i = \text{máx}\{1, |\alpha_i|\}$

Observación 2.9. *La altura de Mahler del polinomio F está bien definida, es decir, no depende de la variable que consideremos.*

Demostración. Recordemos que $F(X,Y) = a_0 \prod_{i=1}^{n}(X - \alpha_i Y)$, donde α_i es raíz de $F(X,1)$, ahora notemos que

$$F(1,Y) = a_0 \prod_{i=1}^{n}(1 - \alpha_i Y) = a_0 \prod_{i=1}^{n} \alpha_i \prod_{i=1}^{n}(\frac{1}{\alpha_i} - Y),$$

lo que implica que $\frac{1}{\alpha_i}$ es raíz de $F(1,Y)$, también notemos que a_n el coeficiente líder de $F(1,Y)$ es $F(1,0) = a_0 \prod_{i=1}^{n} \alpha_i$, así obtenemos que

$$\begin{aligned} a_n \prod_{i=1}^{n} \text{máx}\{1, \frac{1}{|\alpha_i|}\} &= a_0(\prod_{i=1}^{n} \alpha_i)(\prod_{i=1}^{n} \text{máx}\{1, \frac{1}{|\alpha_i|}\}) \\ &= a_0(\prod_{i=1}^{n} |\alpha_i|)(\prod_{|\alpha_i|<1} |\alpha_i|) \\ &= a_0 \prod_{\alpha_i>1} |\alpha_i| \\ &= |a_0| \prod_{i=1}^{n} \text{máx}\{1, |\alpha_i|\} \end{aligned}$$

□

Proposición 2.10. *(Desigualdad de Hadamard) Sea* $A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$

con $a_{i,j} \in \mathbb{C}$ *entonces*

$$(det(A))^2 \leq \prod_{i=1}^{n} \left(\sum_{i=1}^{n} |a_{i,j}|^2 \right)$$

Observación 2.11. *Con* $F(X,Y)$ *como antes, se tiene*

$$|D(F)| \leq n^n M(F)^{2n-2}.$$

Demostración. Empecemos por aplicar la desigualdad de Hadamard a la matriz de Vandermonde $V = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix}$

para obtener

$$\begin{aligned}(det(V))^2 =&(\prod_{i<j}(\alpha_i - \alpha_j))^2\\ =&\prod_{i<j}(\alpha_i - \alpha_j)^2\\ \leq&\prod_{i=1}^{n}(\sum_{i=1}^{n}|\alpha_i^{j-1}|^2).\end{aligned}$$

Ahora notemos que

$$\begin{aligned}|D(F)| &= |a_0|^{2n-2}\prod_{i<j}(\alpha_i - \alpha_j)^2\\ &\leq |a_0|^{2n-2}\prod_{i=1}^{n}(\sum_{i=1}^{n}|\alpha_i^{j-1}|^2)\\ &= |a_0|^{2n-2}\prod_{i=1}^{n}(1^2 + |\alpha_i|^2 + |\alpha_i^2|^2 + \cdots + |\alpha_i^{n-1}|^2)\\ &\leq |a_0|^{2n-2}\prod_{i=1}^{n}(1^2 + (z_i)^2 + (z_i^2)^2 + \cdots + (z_i^{n-1})^2)\\ &= |a_0|^{2n-2}\prod_{i=1}^{n}(1^2 + z_i^2 + z_i^4 + \cdots + z_i^{2n-2})\\ &\leq |a_0|^{2n-2}\prod_{i=1}^{n}nz_i^{2n-2}\\ &= n^n|a_0|^{2n-2}\prod_{i=1}^{n}z_i^{2n-2}\\ &= n^n(|a_0|\prod_{i=1}^{n}z_i)^{2n-2}\\ &= n^nM(F)^{2n-2}\end{aligned}$$

lo cual prueba la observación □

Luego cuando $|D(F)| \geq p^{n(n-1)}$, de la observación 2.11 se tiene que

$$M(F) \geq \frac{|D(F)|^{\frac{1}{2n-2}}}{n^{\frac{n}{2n-2}}} \geq \frac{p^{\frac{n(n-1)}{2n-2}}}{n^{\frac{n}{2n-2}}} = \frac{p^{\frac{n}{2}}}{n^{\frac{n}{2n-2}}} \tag{2.3}$$

Definición 2.12. *La resultante de dos polinomios mónicos P y Q se define como:*

$$Res(P,Q) = \prod_{P(\xi)=0} \prod_{Q(\beta)=0} (\beta - \xi)$$

Observación 2.13. *Sea $F(X,Y)$ como antes, así $a_0 Disc(f) = \pm Res(f,f')$. Entonces $a_0 | Res(f,f')$ implica $D(F) \in \mathbb{Z}$.*

Demostración. Notemos que si $a_0 | Res(f,f')$ entonces $Res(f,f') = a_0 m$ para algún $m \in \mathbb{Z}$, ahora notemos que $Res(f,f') \neq 0$ pues como f es irreducible no tiene raíces múltiples, así de $a_0 Disc(f) = \pm Res(f,f')$ obtenemos que $D(F) = m \in \mathbb{Z} \setminus \{0\}$. □

Sea $f(X)$ como antes y α una raíz fija. Definimos el polinomio

$$g(X) = \frac{1}{X-\alpha} f(X).$$

Escribimos

$$D(F) = f'(\alpha)^2 Disc(g), \tag{2.4}$$

esto lo podemos hacer por que

$$f'(X) = [(X-\alpha)g(X)]' = (X-\alpha)g'(X) + g(X)$$

y así $f'(\alpha) = g(\alpha) = a_0 \prod_{i=1}^{n-1} (\alpha - \alpha_i)$.

Definimos

$$G(X,Y) = \frac{F(X,Y)}{X - \alpha Y}$$

Observación 2.14. *Sean $F(X,Y)$ y $f(X)$ como antes. Entonces*

$$|f'(\alpha)| \geq \frac{|D(F)|^{\frac{1}{2}}}{n^{\frac{n-1}{2}} M(F)^{n-2}} \geq \frac{1}{n^{\frac{n-1}{2}} M(F)^{n-2}}$$

Demostración. Despejando en la ecuación 2.4 obtenemos

$$|f'(\alpha)| = \frac{D(F)^{\frac{1}{2}}}{Disc(g)^{\frac{1}{2}}}$$

luego,

$$\begin{aligned} |D(G)| &\leq (n-1)^{n-1} M(G)^{2(n-2)} \\ &\leq n^{n-1} M(G)^{2(n-2)} \\ &\leq n^{n-1} M(F)^{2(n-2)} \end{aligned}$$

donde la primer desigualdad es por la observación 2.11. Así, obtenemos que

$$\frac{1}{D(G)^{\frac{1}{2}}} \geq \frac{1}{n^{\frac{n-1}{2}} M(F)^{n-2}}$$

y por lo tanto

$$|f'(\alpha)| \geq \frac{D(F)^{\frac{1}{2}}}{n^{\frac{n-1}{2}} M(F)^{n-2}} \geq \frac{1}{n^{\frac{n-1}{2}} M(F)^{n-2}} \tag{2.5}$$

como queríamos. □

Sean $x, y \in \mathbb{Z}$ coprimos, se define $\delta = \text{mín}_{1 \leq i \leq n}\{|\frac{x}{y} - \alpha_i|\}$, notemos que sin pérdida de generalidad podemos suponer que $\delta = |\frac{x}{y} - \alpha_n|$.

Observación 2.15. *Notemos que*

$$|F(x,y)| \geq 2^{-n+1}|y|^n |f'(\alpha_n)||\frac{x}{y} - \alpha_n|.$$

Demostración. Recordemos que

$$|F(X,Y|) = |a_0||y|^n \prod_{i=1}^{n} |\frac{X}{Y} - \alpha_i|$$

y que

$$|f'(\alpha_n)| = \prod_{i=1}^{n-1} |\alpha_i - \alpha_n|,$$

entonces para probar la observación basta ver que

$$|a_0| \prod_{i=1}^{n-1} |\frac{X}{Y} - \alpha_i| \geq \frac{1}{2^{n-1}} \prod_{i=1}^{n-1} |\alpha_n - \alpha_i|$$

Para esto, reacomodemos las raíces de $f(X)$ de manera que

$$|\alpha_n - \alpha_i| \leq 2\delta \text{ si } i = 1, \ldots, N$$

y

$$|\alpha_n - \alpha_i| > 2\delta \text{ si } i = N+1, \ldots, n$$

para algún N entre 0 y $n-1$, así

$$\prod_{i=1}^{N} |\frac{x}{y} - \alpha_i| \geq \delta^N \geq \frac{1}{2^N} \prod_{i=1}^{N} |\alpha_n - \alpha_i|, \tag{2.6}$$

por otro lado, si $i = N+1, \ldots, n-1$, entonces

$$\begin{aligned} |\frac{x}{y} - \alpha_i| &= |(\frac{x}{y} - \alpha_n) + (\alpha_n - \alpha_i)| \\ &\geq |\alpha_n - \alpha_i| - |\frac{x}{y} - \alpha_n| \\ &\geq |\alpha_n - \alpha_i| - \frac{1}{2}|\alpha_n - \alpha_i| \\ &= \frac{1}{2}|\alpha_n - \alpha_i| \end{aligned}$$

y por tanto

$$\prod_{i=N+1}^{n-1} |\frac{x}{y} - \alpha_i| \geq \prod_{i=N+1}^{n-1} \frac{1}{2}|\alpha_n - \alpha_i| = \frac{1}{2^{(n-1)-(N+1)}} \prod_{i=N+1}^{n-1} |\alpha_n - \alpha_i|, \qquad (2.7)$$

luego de 2.6 y 2.7 obtenemos que

$$\prod_{i=1}^{n-1} |\frac{x}{y} - \alpha_i| \geq \frac{1}{2^{n-1}} \prod_{i=1}^{n-1} |\alpha_n - \alpha_i|$$

y en particular

$$|a_0| \prod_{i=1}^{n-1} |\frac{x}{y} - \alpha_i| \geq \frac{1}{2^{n-1}} \prod_{i=1}^{n-1} |\alpha_n - \alpha_i|$$

lo que prueba la observación. □

2.2. Soluciones grandes

En esta parte seguiremos pensando en $F(X,Y)$ y $f(X)$ como en la sección anterior, es decir, $F(X,Y)$ será un polinomio irreducible de grado $n \geq 3$ con coeficientes enteros y $f(X)$ será $F(X,1)$. Recordemos también que α_i son las raíces de $f(X)$.

En esta sección nos fijaremos en las soluciones enteras de $F(X,Y)$ que son suficientemente grandes y concluiremos que de éstas has muy pocas, en este caso, a lo más 3 soluciones para cada α_i.

Definición 2.16. *La altura de (x,y) se define como $H(x,y) = \text{máx}\{|x|, |y|\}$.*

Consideremos dos casos: $H(x,y) = |y|$ y $H(x,y) = |x|$.

Para el caso $H(x,y) = |y|$, tenemos que

$$\min_{1\leq i\leq n}\{|\frac{x}{y} - \alpha_i|\} \leq \frac{(2n^{\frac{1}{2}})^{n-1}|F(x,y)|M(F)^{n-2}}{H(x,y)^n}. \tag{2.8}$$

Hagamos las cuentas

$$\begin{aligned}
\min_{1\leq i\leq n}\{|\frac{x}{y} - \alpha_i|\} &= |\frac{x}{y} - \alpha_n| \\
&\leq \frac{2^{n-1}|F(x,y)|}{|y|^n|f'(\alpha_n)|} \\
&\leq \frac{2^{n-1}|F(x,y)|n^{\frac{n-1}{2}}M(F)^{n-2}}{|y|^n} \\
&= \frac{(2n^{\frac{1}{2}})^{n-1}|F(x,y)|M(F)^{n-2}}{|y|^n} \\
&\leq \frac{(2n^{\frac{1}{2}}M(F))^n|F(x,y)|}{|y|^n} \\
&= \frac{(2n^{\frac{1}{2}}M(F))^n|F(x,y)|}{H(x,y)^n}
\end{aligned}$$

la primer desigualdad es consecuencia de la observación 2.15 y la segunda de la 2.14

Para el caso $H(x,y) = |x|$ de consideremos el polinomio $f_1(Y) = F(1,Y)$ y sus raíces $\beta_1, \ldots, \beta_n$ ordenadas de manera que $\min_{1\leq i\leq n}\{|\frac{y}{x} - \beta_i|\} = |\frac{x}{y} - \beta_n|$, de las observaciones 2.15 y 2.14 obtenemos

$$\begin{aligned}
\min_{1\leq i\leq n}\{|\frac{y}{x} - \beta_i|\} &= |\frac{x}{y} - \beta_n| \\
&\leq \frac{2^{n-1}|F(x,y)|}{|x|^n|f'(\beta_n)|} \\
&\leq \frac{2^{n-1}|F(x,y)|n^{\frac{n-1}{2}}M(F)^{n-2}}{|x|^n} \\
&\leq \frac{(2n^{\frac{1}{2}}M(F))^n|F(x,y)|}{|x|^n} \\
&= \frac{(2n^{\frac{1}{2}}M(F))^n|F(x,y)|}{H(x,y)^n}
\end{aligned} \tag{2.9}$$

de la segunda desigualdad obtenemos que

$$\min_{1\leq i\leq n}\{|\frac{y}{x}-\beta_i|\}\leq\frac{(2n^{\frac{1}{2}})^{n-1}|F(x,y)|M(F)^{n-2}}{H(x,y)^n} \tag{2.10}$$

Observación 2.17. *Sea* $\sigma=\max\{1,\alpha_1,\ldots,\alpha_n\}$*, entonces de la ecuación 2.10 obtenemos*

$$\frac{(2n^{\frac{1}{2}})^{n-1}M(F)^{n-2}|F(x,y)|}{H(x,y)^n}\geq\frac{1}{2\sigma^2}\min_{1\leq i\leq n}(1,|\frac{x}{y}-\alpha_i|).$$

Veamos esto por casos dependiendo de $|\frac{y}{x}-\frac{1}{\alpha_i}|$.

- $|\frac{y}{x}-\frac{1}{\alpha_i}|>\frac{1}{2\sigma}$ para todo i, de la desigualdad 2.10 obtenemos

  $$|F(x,y)|\geq\frac{\min\{|\frac{y}{x}-\frac{1}{\alpha_n}|\}H(x,y)^n}{(2n^{\frac{1}{2}})^{n-1}M(F)^{n-2}}\geq\frac{H(x,y)^n}{2\sigma(2n^{\frac{1}{2}})^{n-1}M(F)^{n-2}}\geq\frac{\min\{1,|\frac{x}{y}-\alpha_i|\}H(x,y)^n}{2\sigma(2n^{\frac{1}{2}})^{n-1}M(F)^{n-2}}$$

  y así

  $$\frac{(2n^{\frac{1}{2}})^{n-1}M(F)^{n-2}|F(x,y)|}{H(x,y)^n}\geq\frac{1}{2\sigma}\min_{1\leq i\leq n}(1,|\frac{x}{y}-\alpha_i|).$$

  Y como $\sigma\geq 1$ se tiene que

  $$\frac{(2n^{\frac{1}{2}})^{n-1}M(F)^{n-2}|F(x,y)|}{H(x,y)^n}\geq\frac{1}{2\sigma^2}\min_{1\leq i\leq n}(1,|\frac{x}{y}-\alpha_i|).$$

- $|\frac{y}{x}-\frac{1}{\alpha_n}|=\min_{1\leq i\leq n}\{|\frac{y}{x}-\frac{1}{\alpha_i}|\}\leq\frac{1}{2\sigma}$, recordemos que $\sigma\geq\alpha_n$, y por lo tanto $\frac{1}{\sigma}\leq|\frac{1}{\alpha_n}|$, así obtenemos
  $|\frac{y}{x}|=|\frac{1}{\alpha_n}+(\frac{y}{x}-\frac{1}{\alpha_n})|\geq|\frac{1}{\alpha_n}|-|\frac{y}{x}-\frac{1}{\alpha_n}|\geq\frac{1}{\sigma}-\frac{1}{2\sigma}=\frac{1}{2\sigma}$,
  luego
  $|\frac{y}{x}-\frac{1}{\alpha_n}|=|\frac{y}{x}\frac{1}{\alpha_n}(\alpha_n-\frac{x}{y})|=|\frac{y}{x}||\frac{1}{\alpha_n}||\alpha_n-\frac{x}{y}|\geq\frac{1}{2\sigma}\frac{1}{\sigma}|\alpha_n-\frac{x}{y}|=\frac{1}{2\sigma^2}|\alpha_n-\frac{x}{y}|$
  así, de la desigualdad 2.10 obtenemos

  $$|F(x,y)|\geq\frac{|\frac{y}{x}-\frac{1}{\alpha_n}|H(x,y)^n}{(2n^{\frac{1}{2}})^{n-1}M(F)^{n-2}}\geq\frac{|\frac{x}{y}-\alpha_n|H(x,y)^n}{2\sigma^2(2n^{\frac{1}{2}})^{n-1}M(F)^{n-2}}$$

Lema 2.18. *Para cualquier pareja de enteros* (x,y) *con* $y\neq 0$ *se cumple*

$$\min_{1\leq i\leq n}\{1,|\alpha_i-\frac{x}{y}|\}\leq\frac{(2r^{\frac{1}{2}}M(F))^n|F(x,y)|}{H(x,y)^n}$$

Demostración. Hasta ahora tenemos que

$$\frac{(2n^{\frac{1}{2}})^{n-1}M(F)^{n-2}|F(x,y)|}{H(x,y)^n} \geq \frac{1}{2\sigma^2} \min_{1\leq i\leq n}(1, |\frac{x}{y} - \alpha_i|),$$

esto por la desigualdad 2.8 para el caso $H(x,y) = y$ y por la observación 2.17 para el caso $H(x,y) = x$, luego, por la definición de $M(F)$ y σ tenemos que $1 \leq \sigma \leq M(F)$; multiplicando la desigualdad por $M(F)^2$ obtenemos

$$\frac{\sigma^2}{2\sigma^2} \min_{1\leq i\leq n}(1, |\alpha_i - \frac{x}{y}|) \leq \frac{M(F)^2}{2\sigma^2} \min_{1\leq i\leq n}(1, |\alpha_i - \frac{x}{y}|) \leq \frac{(2n^{\frac{1}{2}})^{n-1}M(F)^n|F(x,y)|}{H(x,y)^n}$$

y finalmente al multiplicar la desigualdad por 2 concluimos lo deseado

$$\min_{1\leq i\leq n}(1, |\alpha_i - \frac{x}{y}|) \leq \frac{(2n^{\frac{1}{2}})^n M(F)^n|F(x,y)|}{H(x,y)^n}.$$

□

Sea α_0 una raíz fija de $F(x,1)$, decimos que $\frac{x}{y}$ y $\frac{x'}{y'}$ son equivalentes si $|\alpha_0 - \frac{x}{y}| = \min_{1\leq i\leq n}\{|\alpha_i - \frac{x}{y}|\}$ y $|\alpha_0 - \frac{x'}{y'}| = \min_{1\leq i\leq n}\{|\alpha_i - \frac{x'}{y'}|\}$, notemos que está relación es de equivalencia con n clases.

Consideremos ahora cualquier clase, digamos la de α_0, y ordenemos las parejas $(x_1, y_1), (x_2, y_2), \ldots$ con $y_i > 0$ que son soluciones de

$$F(x_i, y_i) = 1$$

de manera que $H(x_i, y_i) \leq H(x_{i+1}, y_{i+1})$ para todo i. Notemos que para estas parejas la diferencia $|\frac{x_i}{y_i} - \alpha_0|$ es menor o igual que 1.

Observación 2.19. *Sean (x_i, y_i) las soluciones de la ecuación $F(X,Y) = 1$ pertenecientes a una misma clase. Entonces*

$$\frac{1}{y_i y_{i+1}} \leq |\frac{x_i}{y_i} - \frac{x_{i+1}}{y_{i+1}}| \leq \frac{2C}{H(x_i, y_i)^n}$$

donde

$$C = (2n^{\frac{1}{2}}M(F))^n. \tag{2.11}$$

Demostración. Empezaremos con la desigualdad del lado izquierdo.

$$|\frac{x_i}{y_i} - \frac{x_{i+1}}{y_{i+1}}| = \frac{|x_i y_{i+1} - x_{i+1} y_i|}{y_i y_{i+1}} \geq \frac{1}{y_i y_{i+1}}.$$

Ahora veamos la desigualdad derecha

$$\begin{aligned}|\frac{x_i}{y_i} - \frac{x_{i+1}}{y_{i+1}}| =& |(\frac{x_i}{y_i} - \alpha_0) - (\frac{x_{i+1}}{y_{i+1}} - \alpha_0)| && (2.12)\\ \leq& |\frac{x_i}{y_i} - \alpha| + |\frac{x_{i+1}}{y_{i+1}} - \alpha| && (2.13)\\ \leq& \frac{C}{H(x_i, y_i)^n} + \frac{C}{H(x_{i+1}, y_{i+1})^n} && (2.14)\\ \leq& \frac{2C}{H(x_i, y_i)^n} && (2.15)\end{aligned}$$

La tercer desigualdad se cumple por 2.18 □

Lema 2.20 (Principio fuerte entre las distancias)**.** *Sean (x_i, y_i) soluciones de una misma clase, entonces para $H(x_1, y_1) \geq C^{\frac{1}{r}}$ se tiene*

$$H(x_k, y_k) \geq ((2C)^{-\frac{1}{n-2}} H(x_1, y_1))^{(n-1)^{k-1}}$$

Demostración. Veamoslo por inducción.
$k = 1$
$H(x_1, y_1) \geq ((2C)^{-\frac{1}{n-2}} H(x_1, y_1))^{(n-1)^{1-1}}$, esto se cumple pues $(2C)^{-\frac{1}{n-2}} < 1$.
Ahora vamos con el paso de inducción. Supongamos que

$$H(x_k, y_k) \geq ((2C)^{-\frac{1}{n-2}} H(x_1, y_1))^{(n-1)^{k-1}}$$

□

Sean t y τ números mayores que cero tales que $t < \sqrt{\frac{2}{n}}$ y $\sqrt{2 - nt^2} < \tau < t$ y consideremos

$$\lambda = \frac{2}{t - \tau} \quad \text{y} \quad A_1 = \frac{t^2}{2 - nt^2}(\log M(F) + \frac{n}{2}). \tag{2.16}$$

Diremos que un número racional $\frac{x}{y}$ es una muy buena aproximación a α si

$$|\alpha - \frac{x}{y}| < (4e^{A_1} H(x, y))^{-\lambda} \tag{2.17}$$

se tiene

Lema 2.21 (Principio Thue-Siegel)**.** *Si α es un número de grado n y $\frac{x}{y}$ y $\frac{x'}{y'}$ son dos muy buenas aproximaciones a α entonces*

$$\log(4e^{A_1}) + \log H(x', y') \leq \delta^{-1}\{\log(4e^{A_1}) + \log H(x, y)\}$$

donde $\delta = \frac{nt^2 + \tau^2 - 2}{n-1}$.

Ahora buscaremos un número Y_0 suficientemente grande tal que al tener $Y_0 \leq H(x_1, y_1)$ se tenga que $\frac{x_1}{y_1}, \frac{x_2}{y_2}, \ldots$ son muy buenas aproximaciones a α.

Del lema 2.18 tenemos que

$$|\alpha - \frac{x_i}{y_i}| \leq \frac{C}{H(x_i, y_i)^n},$$

ahora bastaría ver que

$$\frac{C}{H(x_i, y_i)^n} \leq \frac{1}{(4e^{A_1} H(x_i, y_i))^{-\lambda}}$$

para asegurarnos que cada pareja (x_i, y_i) forma una muy buena aproximación a α, despejando $H(x_i, y_i)$ de la desigualdad obtenemos que esto se cumple para

$$Y_0 \geq C^{\frac{1}{r-\lambda}} (4e^{A_1})^{\frac{\lambda}{r-\lambda}}.$$

Utilicemos logaritmos en la desigualdad del principio fuerte entre las distancias para obtener

$$\log H(x_k, y_k) \geq (n-1)^{k-1} \{\log(2C)^{-\frac{1}{n-2}} + \log H(x_1, y_1)\}$$

por otro lado, aplicando el principio de Thue-Siegel a (x_n, y_n) y (x_1, y_1) obtenemos

$$\log(4e^{A_1}) + \log H(x_k, y_k) \leq \delta^{-1} \{\log(4e^{A_1}) + \log H(x_1, y_1)\}$$

y combinando ambas desigualdades tenemos que

$$\log(4e^{A_1}) + (n-1)^{k-1} \{(-\frac{1}{n-2}) \log(2C) + \log H(x_1, y_1)\}$$

$$\leq \delta^{-1} \{\log(4e^{A_1}) + \log H(x_1, y_1)\}$$

lo que nos deja con

$$(n-1)^{k-1} \leq \delta^{-1} \frac{\log Y_0 + \log(4e^{A_1})}{\log Y_0 - (n-2)^{-1} \log(2C)}$$

cuando como en nuestra caso $\log Y_0 > (n-2)^{-1} \log(2C)$.

Consideremos ahora

$$Y_0 = (2C)^{\frac{1}{n-\lambda}} (4e^{A_1})^{\frac{\lambda}{n-\lambda}} \tag{2.18}$$

y obtenemos

$$\begin{aligned}(n-1)^{k-1} \leq & \delta^{-1}\frac{(n-\lambda)^{-1}\log(2C)+n(n-\lambda)^{-1}\log(4e^{A_1})}{(\lambda-2)(n-2)^{-1}(n-\lambda)^{-1}\log(2C)+\lambda(n-\lambda)^{-1}\log(4e^{A_1})}\\ = & \delta^{-1}\frac{\log(2C)+n\log(4e^{A_1})}{(\lambda-2)(n-2)^{-1}\log(2C)+\lambda\log(4e^{A_1})}\\ = & (\delta^{-1}\frac{n-2}{\lambda-2})\frac{\log(2C)+n\log(4e^{A_1})}{\log(2C)+\lambda\log(4e^{A_1})}\\ \leq & \delta^{-1}\frac{n-2}{\lambda-2}\\ \leq & \delta^{-1}\frac{n-1}{\lambda-2}\end{aligned}$$

de aquí $(n-1)^{k-2} \leq \delta^{-1}(\lambda-2)^{-1}$, aplicando logaritmo a la desigualdad y despejando k obtenemos

$$k \leq 2 + \frac{\log(\delta^{-1}(\lambda-2)^{-1})}{\log(n-1)}.$$

Luego considerando las soluciones (x,y) y $(-x,-y)$ de $|F(x,y)|=1$ como una sola habremos probado el siguiente lema.

Lema 2.22. *El número de soluciones enteras (x,y) de la ecuación $|F(x,y)| = 1$ con $H(x,y) \geq Y_0$ es a lo más*

$$n[2 + \frac{\log(\delta^{-1}(\lambda-2)^{-1})}{\log(n-1)}].$$

Consideremos

$$t = \sqrt{\frac{2}{n-a^2}} \quad \text{y} \quad \tau = bt \tag{2.19}$$

con $0 < a < b < 1$ entonces

$$\lambda = \frac{2}{t-\tau} = \frac{2}{(1-b)t} = \frac{2}{(1-b)\sqrt{\frac{2}{n-a^2}}} = \frac{\sqrt{2}\sqrt{n+a^2}}{1-b} > \frac{\sqrt{2n}}{1-b}$$

y

$$\begin{aligned}
\delta^{-1} =& \frac{n-1}{nt^2+\tau^2-2} \\
=& \frac{n-1}{n(\frac{2}{n+a^2})+b^2(\frac{2}{n+a^2})-2} \\
=& \frac{n-1}{2(\frac{n+b^2}{n+a^2}-1)} \\
=& \frac{n-1}{2(\frac{n+b^2-(n+a^2)}{n+a^2})} \\
=& \frac{n-1}{2(\frac{b^2-a^2}{n+a^2})} \\
=& \frac{(n-1)(n+a^2)}{2(b^2-a^2)} \\
<& \frac{(n-1)(n+1)}{2(b^2-a^2)} \\
=& \frac{n^2-1}{2(b^2-a^2)} \\
<& \frac{n^2}{2(b^2-a^2)}
\end{aligned}$$

Luego

$$\frac{\log(\delta^{-1}(\lambda-2)^{-1})}{\log(n-1)} < \frac{\log(\frac{n^2}{2(b^2-a^2)}(\frac{\sqrt{2n}}{1-b}-2)^{-1})}{\log(n-1)},$$

sean

$$s(n) = \log(\frac{n^2}{2(b^2-a^2)}(\frac{\sqrt{2n}}{1-b}-2)^{-1}) \quad \text{y} \quad h(n) = \log(n-1)$$

entonces

$$\begin{aligned}
\lim_{n\to\infty} \frac{\log(\delta^{-1}(\lambda-2)^{-1})}{\log(n-1)} <& \lim_{n\to\infty} \frac{s(n)}{h(n)} \\
=& \frac{s'(n)}{h'(n)} \\
=& \frac{3}{2} < 2
\end{aligned}$$

de aquí que el número de soluciones enteras (x, y) de la ecuación $|F(x, y)| = 1$ con $H(x, y) \geq Y_0$ es a lo más $3n$ cuando n es suficientemente grande.

2.3. Soluciones pequeñas

En esta sección daremos una cota para el número de soluciones pequeñas de la ecuación $F(X, Y) = 1$, es decir las que cumplen $H(x, y) < Y_0$.

Consideremos $\mathbf{x} = (x, y)$ y escribamos

$$F(\mathbf{x}) = F(x, y) = \prod_{i=1}^{n}(x - \alpha_i y)$$

ahora, consideramos

$$L_i(\mathbf{x}) = x - \alpha_i y \quad \text{para} \quad i = 1, \ldots, n.$$

Dado $\mathbf{x}_0 = (x_0, y_0)$ definimos

$$D(\mathbf{x}, \mathbf{x}_0) = xy_0 - x_0 y.$$

Definición 2.23. *Diremos que dos polinomios $F(X, Y)$ y $G(x, y)$ son equivalentes si las ecuaciones $|F(x, y)| = 1$ y $|G(x, y)| = 1$ tienen el mismo número de soluciones.*

Proposición 2.24. *Los polinomios $F(X, Y)$ y $F_A(U, V)$ son equivalentes.*

Demostración. Sea S el conjunto de soluciones enteras de la ecuación $|F(X, Y)| = 1$, y sea S_A el conjunto de las soluciones enteras de $|F_A(U, V)| = 1$ y consideremos la función $s : S_A \to S$ definida por

$$s(u, v) = (au + bv, cu + dv),$$

y veamos que es biyectiva.
Empecemos por comprobar inyectividad, supongamos que $s(u, v) = s(u', v')$, entonces $(au + bv, cu + dv) = (au' + bv', cu' + dv')$, lo que nos lleva a $c(u - u') = d(v' - v)$ y $a(u - u') = b(v' - v)$ y posteriormente a $cb = da$, pero esto no es posible pues $det(A) = 0$, por lo tanto la función $s(u, v)$ es inyectiva.
Para probar suprayectividad consideremos $(x, y) \in S$ y el sistema de ecuaciones

$$\begin{aligned} au + bv &= x \\ cu + bv &= y, \end{aligned}$$

dado que es un sistema de dos ecuaciones y dos incógnitas tiene una única solución (u, v), además como $det(A) = 1$ se tiene que $u, v \in \mathbb{Z}$, por lo tanto $(x, y) = s(u, v)$, lo que implica que la función s es suprayectiva y por lo tanto biyectiva. Lo que prueba que $|F(X,Y)| = 1$ y $|F_A(U,V)| = 1$ tienen el mismo número de soluciones enteras. □

Lema 2.25. *Sean* $\mathbf{x}$ *y* $\mathbf{x}_o$ *soluciones de* $|F(x,y)| = 1$. *Entonces para* $1 \leq i, j \leq n$,

$$\frac{L_i(\mathbf{x}_0)}{L_i(\mathbf{x})} - \frac{L_j(\mathbf{x}_0)}{L_j(\mathbf{x})} = (\beta_i - \beta_j)D(\mathbf{x}, \mathbf{x}_0),$$

donde $\beta_1, \ldots, \beta_n$ *dependen de* x *y son tales que la forma* $G(v,w) = (v - \beta_1 w) \cdots (v - \beta_n w)$ *es equivalente a* F.

Demostración. Seleccionemos $\mathbf{x}' \in \mathbb{Z} \times \mathbb{Z}$ con $D(\mathbf{x}', \mathbf{x}) = 1$; esto se puede porque $|F(\mathbf{x})| = 1$ tiene componentes que son primos relativos; luego $\mathbf{x}, \mathbf{x}'$ es una base para $\mathbb{Z}^2$ y así podemos escribir $\mathbf{x}_0 = a\mathbf{x} + b\mathbf{x}'$. Más aún, $D(\mathbf{x}_0, \mathbf{x}) = b$, así

$$x_0 = ax + D(\mathbf{x}_0, \mathbf{x})x' \text{ y } y_0 = ay + D(\mathbf{x}_0, \mathbf{x})y'$$

luego, para cada $i = 1, \ldots n$

$$\begin{aligned}
\frac{L_i(\mathbf{x}_0)}{L_i(\mathbf{x})} =& \frac{x_0 - \alpha_i y_0}{x - \alpha_i y} \\
=& \frac{ax + D(\mathbf{x}_0, \mathbf{x})x' - \alpha_i(ay + D(\mathbf{x}_0, \mathbf{x})y')}{x - \alpha_i y} \\
=& \frac{a(x - \alpha_i y) + D(\mathbf{x}_0, \mathbf{x})(x' - \alpha_i y')}{x - \alpha_i y} \\
=& a + D(\mathbf{x}_0, \mathbf{x})\frac{(x' - \alpha_i y')}{x - \alpha_i y} \\
=& a + D(\mathbf{x}_0, \mathbf{x})\frac{L_i(\mathbf{x}')}{L_i(\mathbf{x})},
\end{aligned}$$

consideremos $\beta_i = \frac{L_i(\mathbf{x}')}{L_i(\mathbf{x})}$, y obtenemos

$$\frac{L_i(\mathbf{x}_0)}{L_i(\mathbf{x})} = a + D(\mathbf{x}_0, \mathbf{x})\beta_i,$$

luego

$$\frac{L_i(\mathbf{x}_0)}{L_i(\mathbf{x})} - \frac{L_j(\mathbf{x}_0)}{L_j(\mathbf{x})} = a + D(\mathbf{x}_0, \mathbf{x})\beta_i - (a + D(\mathbf{x}_0, \mathbf{x})\beta_j) = D(\mathbf{x}_0, \mathbf{x})(\beta_i - \beta_j).$$

Ahora definimos

$$\begin{aligned} G(v,w) &= \pm\, F(v\mathbf{x} + w\mathbf{x}') \\ &= \pm\, F(v(x,y) + w(x',y')) \\ &= \pm\, F(vx + wx', vy + wy') \end{aligned}$$

el signo de F en $G(v,w)$ dependerá de si (x,y) es solución de $F(x,y) = 1$ o $F(x,y) = -1$, pues queremos que G sea un polinomio mónico, para esto notemos que el coeficiente líder de G es $G(1,0) = F(x,y)$.

Además, F y G son equivalentes, luego

$$\begin{aligned} G(u,v) &= \pm \prod_{i=1}^{n} L_i(v\mathbf{x} + w\mathbf{x}') \\ &= \pm \prod_{i=1}^{n} (v(x,y) + w(x',y')) \\ &= \pm \prod_{i=1}^{n} vx + wy + \alpha_i(vy + wy') \\ &= \pm \prod_{i=1}^{n} (vL_i(\mathbf{x}) + L_i(\mathbf{x}')) \\ &= \pm \prod_{i=1}^{n} (v + w\frac{L_i(\mathbf{x}')}{L_i(\mathbf{x})}) \\ &= \pm \prod_{i=1}^{n} (v - \beta_i w). \end{aligned}$$

□

En el caso cuando $x_0 = (1,0)$, tenemos $L_i(\mathbf{x}_0) = L_i(\mathbf{x}_0) = 1$, y así

$$\frac{1}{L_i(\mathbf{x})} - \frac{1}{L_j(\mathbf{x})} = D(\mathbf{x}_0, \mathbf{x})(\beta_i - \beta_j) = y(\beta_i - \beta_j)$$

para toda $\mathbf{x}$ con $|F(\mathbf{x})| = 1$, entonces $|L_1(\mathbf{x})|, \ldots, |L_n(\mathbf{x})| = 1$, ahora escogemos$j = j(\mathbf{x})$ con $|L_j(\mathbf{x})| \geq 1$, entonces

$$\frac{1}{L_i(\mathbf{x})} \geq |\beta_j - \beta_i||y| - 1$$

también $|\overline{L_j(\mathbf{x})}| \geq 1$, entonces

$$\frac{1}{|L_i(\mathbf{x})|} \geq |\overline{\beta_j} - \beta_i||y| - 1,$$

luego sumando las dos desigualdades anteriores obtenemos

$$\begin{aligned}\frac{2}{|L_i(\mathbf{x})|} \geq & (|\beta_j - \beta_i| + |\overline{\beta_j} - \beta_i|)|y| - 2 \\ \geq & |\beta_j - \beta_i + \overline{\beta_j} - \beta_i||y| - 2 \\ = & |2Re(\beta_j) - 2\beta_i||y| - 2\end{aligned}$$

y dividiendo entre 2 queda

$$\frac{1}{|L_i(\mathbf{x})|} \geq |Re(\beta_j) - \beta_i||y| - 1.$$

Ahora, escojamos un un entero $m = m(\mathbf{x})$ con $|m - Re(\beta_j)| \leq \frac{1}{2}$ para obtener

$$\frac{1}{|L_i(\mathbf{x})|} \geq (|m - \beta_i| - \frac{1}{2})|y| - 1 \text{ para } i = 1, \ldots, n. \tag{2.20}$$

Para $1 \leq i \leq n$ consideremos X_i como el conjunto de soluciones de la ecuación $|F(x,y)| = 1$ con $1 \leq y \leq Y_0$ y $|L_i(\mathbf{x})| \leq \frac{1}{2y}$.

Lema 2.26. *Sean $(x,y), (\dot{x},\dot{y}) \in X_i$ con $x \neq \dot{x}$ y $y \leq \dot{y}$. Entonces*

$$\frac{\dot{y}}{y} \geq \frac{2}{7} \operatorname{máx}(1, |\beta_i - m|)|$$

donde $\beta_i = \beta_i(\mathbf{x})$ y $m = m(\mathbf{x})$.

Demostración. Tenemos que

$$\begin{aligned}1 \leq & |D(\mathbf{x}, \dot{\mathbf{x}})| \\ \leq & \begin{Vmatrix} x - \alpha_i y & y \\ \dot{x} - \alpha_i \dot{y} & \dot{y} \end{Vmatrix} \\ \leq & |L_i(\dot{\mathbf{x}})| + \dot{y}|L_i(\mathbf{x})| \\ \leq & \frac{y}{2\dot{y}} + \dot{y}|L_i(\mathbf{x})| \\ \leq & \frac{1}{2} + \dot{y}|L_i(\mathbf{x})|\end{aligned}$$

entonces $\dot{y}|L_i(\mathbf{x})| \geq \frac{1}{2}$, luego $2\dot{y} \geq \frac{1}{L_i(\mathbf{x})}$ y de 2.20 obtenemos

$$2\dot{y} \geq (|m - \beta_i| - \frac{1}{2})|y| - 1,$$

y de aquí

$$\dot{y} \geq \frac{1}{2}(|m - \beta_i| - \frac{1}{2})|y| - \frac{1}{2},$$

lo que implica

$$\begin{aligned}\frac{\dot{y}}{y} \geq & \frac{1}{2}(|m-\beta_i| - \frac{1}{2}) - \frac{1}{2y} \\ \geq & \frac{1}{2}(|m-\beta_i| - \frac{1}{2}) - \frac{1}{2} \\ = & \frac{1}{2}|m-\beta_i| - \frac{1}{4} - \frac{1}{2} \\ = & \frac{1}{2}|m-\beta_i| - \frac{3}{4},\end{aligned}$$

la segunda desigualdad se da por que $y \geq 1$, luego como $\dot{y} \geq y$ se tiene que

$$\frac{\dot{y}}{y} \geq \text{máx}(1, \frac{1}{2}|m-\beta_i| - \frac{3}{4}) \tag{2.21}$$

ahora veamos que si $\xi \in \mathbb{R}$ es mayor que cero, entonces la desigualdad

$$\text{máx}(1, \frac{1}{2}\xi - \frac{3}{4}) \geq \frac{2}{7}\,\text{máx}(1, \xi) \tag{2.22}$$

se cumple, para esto notemos que si $\text{máx}(1, \frac{1}{2}\xi - \frac{3}{4}) = 1$ entonces $\xi \leq \frac{7}{2}$ y la desigualdad 2.22 se cumple pues $1 \geq \frac{2}{7}\,\text{máx}(1, \frac{7}{2})$, ahora en caso de que $\text{máx}(1, \frac{1}{2}\xi - \frac{3}{4}) \neq 1$ se tendría que $\xi > \frac{7}{2}$ y por lo tanto $\frac{2}{7}\xi = \frac{2}{7}\,\text{máx}(1, \xi)$, luego la desigualdad 2.22 se cumple pues cuando $\xi > \frac{7}{2}$ se tiene que $\frac{1}{2}\xi - \frac{3}{4} \geq \frac{2}{7}\xi$. Ahora podemos sustituir ξ por $|m-\beta_i|$ para obtener

$$\text{máx}(1, \frac{1}{2}|m-\beta_i| - \frac{3}{4}) \geq \frac{2}{7}\,\text{máx}(1, |m-\beta_i|)$$

y combinando esto con la desigualdad 2.21 se tiene que

$$\frac{\dot{y}}{y} \geq \frac{2}{7}\,\text{máx}(1, |m-\beta_i|)$$

tal como queríamos. □

Lema 2.27. *Supongamos que* (x, y) *satisface* $F(x, y) = 1$ *con* $y > 0$ *y* $L_i(\mathbf{x}) > \frac{1}{2y}$. *Entonces*

$$|m-\beta_i| \leq \frac{7}{2}$$

Demostración. Despejando en la desigualdad 2.20 obtenemos

$$|m-\beta_i| \leq \frac{1}{2} + \frac{1}{|L_i(\mathbf{x})|y} + \frac{1}{y} \leq \frac{1}{2} + 2 + 1 = \frac{7}{2}.$$

□

Ahora, para cada X_i no vacío sea $\mathbf{x}(i)$ el elemento de X_i cuya coordenada y sea mayor.

Consideremos X como el conjunto de soluciones de $|F(\mathbf{x})| = 1$ con $1 \leq y \leq Y_0$ donde los elementos $\mathbf{x}(1), \ldots, \mathbf{x}(n)$ han sido eliminados.

Lema 2.28. *Supongamos que la desigualdad* $M(F) \geq p^{\frac{n}{2}} n^{\frac{-n}{2n-2}}$ *se cumple para un primo* $p > (\frac{7}{2})^2$. *Sea* $\epsilon > 0$ *y* $n > n_1(p, \epsilon)$. *Entonces el conjuto* X *tiene cardinalidad*

$$|X| > \frac{n(1+\epsilon)}{1 - \frac{2\log(\frac{7}{2})}{\log p}}$$

Demostración. Sea $1 \leq i \leq n$ fijo. En el caso cuando $X_i \neq \emptyset$ ordenamos sus elementos $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_v$ de manera que $y_1 \leq y_2 \leq \cdots \leq y_v$ y por tanto $\mathbf{x}_v = \mathbf{x}(i)$.

De aplicar el lema 2.26 obtenemos

$$\frac{y_{k+1}}{y_k} \geq \frac{2}{7} \operatorname{máx}(1, |\beta_i(\mathbf{x}_k) - m(\mathbf{x}_k)|$$

para $1 \leq k \leq v-1$, por lo tanto

$$\prod_{\mathbf{x} \in X \cap X_i} \frac{2}{7} \operatorname{máx}(1, |\beta_i(\mathbf{x}_k) - m(\mathbf{x}_k)| \leq \prod_{\mathbf{x} \in X \cap X_i} \frac{y_{k+1}}{y_k} \leq \frac{y_v}{y_1} \leq y_v \leq Y_0$$

Ahora, para $\mathbf{x} \in X - X_i$ del lema 2.27 obtenemos

$$\frac{2}{7} \operatorname{máx}(1, |\beta_i(\mathbf{x}) - m(\mathbf{x})|) \leq 1$$

y por tanto

$$\prod_{\mathbf{x} \in X} \frac{2}{7} \operatorname{máx}(1, |\beta_i(\mathbf{x}) - m(\mathbf{x})| \leq Y_0 \tag{2.23}$$

La forma $G = \prod_{i=1}^{n}(v - \beta_i w)$ del lema 2.26 es equivalente a F y por lo tanto también lo es $\dot{G} = \prod_{i=1}^{n}(v - (\beta_i - m)w)$. Luego, como F es reducido se tiene $M(F) \leq M(\dot{G})$, es decir

$$M(F) \leq \prod_{i=1}^{n} \operatorname{máx}(1, |\beta_i(\mathbf{x}) - m(\mathbf{x})|),$$

ahora, de 2.23 se obtiene

$$((\frac{2}{7})^n M(F))^{|X|} \leq Y_0^n.$$

Como $M(F) \geq p^{\frac{n}{2}} n^{\frac{-n}{2n-2}}$ se cumple para un primo $p > (\frac{7}{2})^2$, se tiene que $M(F) > (\frac{7}{2})^n$ cuando $n > n_2(p)$; entonces aplicando logaritmo a la desigualdad se obtiene

$$|X| \log(\frac{2}{7})^n M(F) \leq n \log Y_0$$

para llegar a

$$|X| \leq \frac{n \log Y_0}{\log M(F) - n \log \frac{7}{2}} \tag{2.24}$$

Con A_1 como en (2.16) y (2.19) tenemos

$$A_1 = \frac{1}{a^2}(\log M(F) + \frac{1}{2}n)$$

luego con (2.11) y (2.18)

$$\log Y_0 = \frac{n}{n-\lambda}(\log M(F) + \log 2n^{\frac{1}{2}} + \frac{\log 2}{n}) + \frac{\lambda}{n-\lambda}(\log 4 + \frac{1}{a^2}(\log M(F) + \frac{n}{2}))$$

con λ como en (2.16) y (2.19) tenemos $(n^{\frac{1}{2}})$, luego

$$\log Y_0 = (1 + O(n^{-\frac{1}{2}})) \log M(F) + O(n^{\frac{1}{2}})$$

donde la constante de O depende sólo de ay b en (2.19). Luego de $\log M(F) > n \log(\frac{7}{2})$ podemos concluir que

$$\log Y_0 < (1 + \frac{\epsilon}{2}) \log M(F)$$

cuando $n > n_3(\epsilon)$, combinando esto con (2.24) obtenemos

$$|X| < n(1 + \frac{\epsilon}{2}) \frac{\log M(F)}{\log M(F) - n \log(\frac{7}{2})}.$$

Así para $n > n_1(p, \epsilon)$, de 2.3 tenemos

$$\begin{aligned} |X| <& n(1 + \frac{\epsilon}{2}) \frac{1}{1 - \frac{n \log(\frac{7}{2})}{\log M(F)}} \\ <& n(1 + \frac{\epsilon}{2}) \frac{1}{1 - \frac{\log(\frac{7}{2})}{\frac{1}{2} \log p - (\frac{\log n}{n-2})}} \\ <& n(1 + \epsilon) \frac{1}{1 - \frac{\log(\frac{7}{2})}{\frac{1}{2} \log p)}} \end{aligned}$$

□

2.4. El número de soluciones

Ahora ya podemos obtener una cota para el número de soluciones de $|F(X,Y)| = 1$. Las soluciones con $0 < y \leq Y_0$ están en X, o son alguna de las $\mathbf{x}(i)$; considerando también $\mathbf{x} = (1,0)$ tenemos que el número de soluciones de $|F(\mathbf{x})| = 1$ con $|y| \leq Y_0$ a lo mas $|X|+n+1$ (recordemos que estamos contando $\mathbf{x}$ y $-\mathbf{x}$ como una misma solución.) Luego por LOL tenemos que el número de soluciones con $|y| > Y_0$ es a lo mas $3n$ cuando n es grande. Así obtenemos que la ecuación $F(X,Y) = 1$ tiene a lo mas

$$|X| + 4n + 1$$

soluciones. Luego si $p > \frac{7}{2}^2$ y n es grande del lema 2.28 obtenemos

$$N_n(p) < n(1+2\epsilon)(\frac{1}{1-\frac{2\log(\frac{7}{2})}{\log p}} + 4),$$

donde $N_n(p)$ es una cota superior para el número de soluciones cuando la desigualdad $|D(F)| \geq p^{n(n-1)}$ se cumple; ahora juntando esto con 2.2 tenemos

$$N_n < n(1-2\epsilon)C(p)$$

donde

$$C(p) = (p+1)(\frac{1}{1-\frac{2\log(\frac{7}{2})}{\log p}} + 4).$$

Con $p = 19$ obtenemos $C(19) = 214{,}16...$, por tanto $N_n < 215n$ cuando n es grande.

Bibliografía

[BS87] E. Bombieri and W. M. Schmidt. On Thue's equation. *Invent. Math.*, 88(1):69–81, 1987.

[BS96] Edward B. Burger and Thomas Struppeck. Does $\sum_{n=0}^{\infty} 1/n!$ really converge? Infinite series and p-adic analysis or "You can sum some of the series some of the time and some of the series none of the time... but can you sum some of the series all of the time?". *Amer. Math. Monthly*, 103(7):565–577, 1996.

[BT05] F. Beukers and Sz. Tengely. An implementation of runge's method for diophantine aquations. *arXiv*, 2005. arxiv.org/pdf/math/0512418.

[Cas60] J. W. S. Cassels. On the equation $a^x - b^y = 1$. II. *Proc. Cambridge Philos. Soc.*, 56:97–103, 1960.

[Dys47] F. J. Dyson. The approximation to algebraic numbers by rationals. *Acta Math.*, 79:225–240, 1947.

[GS92] A. Grytczuk and A. Schinzel. On Runge's theorem about Diophantine equations. In *Sets, graphs and numbers (Budapest, 1991)*, volume 60 of *Colloq. Math. Soc. János Bolyai*, pages 329–356. North-Holland, Amsterdam, 1992.

[Ivo] Carlos Ivorra. *TeorÃa de NÃºmeros*. www.uv.es/ivorra/Libros/Numeros.pdf.

[Kla13] Martin Klazar. Runge's theorem on diophantine equations. *lecture on the 7-th PhD conference*, 2013. kam.mff.cuni.cz/ klazar/ostrava2.pdf.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Mat02] Keith Matthews. Thue's theorem and the Diophantine equation $x^2 - Dy^2 = \pm N$. *Math. Comp.*, 71(239):1281–1286, 2002.

[Mih04] Preda Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.*, 572:167–195, 2004.

[NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[Ran86] R. Michael Range. *Holomorphic functions and integral representations in several complex variables*, volume 108 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Rot97] K. F. Roth. Rational approximations to algebraic numbers [MR0120220 (22 #10977)]. In *Fields Medallists'lectures*, volume 5 of *World Sci. Ser. 20th Century Math.*, pages 60–66. World Sci. Publ., River Edge, NJ, 1997.

[Sch07] Andrzej Schinzel. *Andrzej Schinzel selecta. Vol. I.* Heritage of European Mathematics. European Mathematical Society (EMS), Zürich, 2007. Diophantine problems and polynomials, Edited by Henryk Iwaniec, Władysław Narkiewicz and Jerzy Urbanowicz.

[Sch08] René Schoof. *Catalan's conjecture*. Universitext. Springer-Verlag London, Ltd., London, 2008.

[SS08] A. Sankaranarayanan and N. Saradha. Estimates for the solutions of certain Diophantine equations by Runge's method. *Int. J. Number Theory*, 4(3):475–493, 2008.

[TdW89] N. Tzanakis and B. M. M. de Weger. On the practical solution of the Thue equation. *J. Number Theory*, 31(2):99–132, 1989.

[Ten03] Sz. Tengely. On the Diophantine equation $F(x) = G(y)$. *Acta Arith.*, 110(2):185–200, 2003.

[Thu09] Axel Thue. Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew. Math.*, 135:284–305, 1909.

[Tij76] R. Tijdeman. On the equation of Catalan. *Acta Arith.*, 29(2):197–209, 1976.

[Wal92] P. G. Walsh. A quantitative version of Runge's theorem on Diophantine equations. *Acta Arith.*, 62(2):157–172, 1992.

[Zan09] Umberto Zannier. *Lecture notes on Diophantine analysis*, volume 8 of *Appunti. Scuola Normale Superiore di Pisa (Nuova Serie) [Lecture Notes. Scuola Normale Superiore di Pisa (New Series)]*. Edizioni della Normale, Pisa, 2009. With an appendix by Francesco Amoroso.