Puntos de coordenadas enteras en hipérbolas

Jorge Jiménez Urroz

El tribunal:

Director de tesis:
Javier Cilleruelo Mateo

Departamento de Matemáticas
Universidad Autónoma de Madrid

A mis padres

Prefacio

Hace ya algún tiempo, Javier Cilleruelo, mi director de tesis, me brindó la oportunidad de viajar a Estados Unidos para trabajar con un excelente matemático, Andrew Granville. Dicha oportunidad se consumó a principios de Septiembre de 1993. Curiosamente fue el mismo Javier, el que durante mi estancia nos propuso el siguiente problema:

Encontrar una cota inferior del mínimo común múltiplo de k enteros en un cierto intervalo $[X, X+L]$, con L pequeño en comparación con X.

Nada más recibir el enunciado, empezamos a trabajar en lo que ha resultado ser el segundo capítulo de esta memoria.

Como tendremos oportunidad de ver, este problema se puede traducir en términos más geométricos, e intentar dar una cota a la longitud de un arco de la hipérbola $xy = N$ que contenga k puntos de coordenadas enteras. Este es, en realidad, el verdadero motivo de atacar el problema, y surge de manera natural despues del trabajo de J. Cilleruelo sobre puntos del retículo en círculos $x^2 + y^2 = R^2$. En el primer capítulo, mostramos un resultado general, en este sentido, para cónicas a las que se les puede asociar un anillo de factorización única, dedicando el resto del capítulo a la hipérbola $xy = N$.

Por otra parte, el tercer capítulo se dedica a hipérbolas cuyo "anillo asociado" no es de factorización única.

Esta tesis no habría sido posible sin Javier Cilleruelo. Sus incontables ideas, tanto en la proposición de problemas, como en su posterior método de resolución han hecho posible la consecución de esta memoria.

He de agradecer su apoyo, en las matemáticas, y en los infinitos aspectos, no menos importantes, que emergen paralelos a elaborar una tesis doctoral. Siempre estuvo cuando le necesité.

Gracias Javier, por confiar en mí.

Tuve suerte de conocer a Andrew Granville. A él le agradezco, sinceramente, su paciencia, su apoyo constante durante mis estancias en las universidades de Georgia y Michigan, una gran responsabilidad y preocupación por mi trabajo, su, a veces, dureza...Con él aprendí no sólo a trabajar en matemáticas sino también fuera del mundo de las matemáticas. Todas estas cosas han contribuido a mi formación como futuro investigador.

Thanks Andrew

A Fernando Chamizo le agradezco la lectura de esta memoria, tanto corrigiéndome en muchas ocasiones deficiencias de estilo y contribuyendo de esta forma a la clarificación de la exposición, así como dándome consejos e ideas de aquello que leía. En particular una de ellas facilitó la conclusión del Teorema 1.2. En cualquier caso, lo más grato fue su preocupación a diario por la "normal" evolución de esta tesis.

A Bernardo López por llamar mi atención sobre los números de Fekete y el diámetro transfinito, así como por anunciarme que el polinomio $H(x)$ era de sobra conocido. A Antonio Córdoba, a José Luis Fernández, a Adolfo Quirós, y a muchos otros profesores por escucharme y aconsejarme en la parte que pudiere haberles contado. A la Universidad de Georgia su hospitalidad, a Ken Ono su compañia y ánimo durante mi estancia en Georgia, a Trevor Wooley su ayuda a que pasara una temporada en la Universidad de Michigan, y su atención durante ese período. A dicha universidad le debo una grata acogida.

A mis padres, a mis hermanos, a mis amigos y entre ellos a Yolanda, María Jesús y Fernando colegas de despacho y alegrias.

Por último quisiera agradecer a Macarena Estévez su rapida y eficiente lectura de parte de la tesis...Pero sobre todo, te agradezco el día a día.

Gracias a todos.

Observaciones

Justo antes de la impresión final de esta memoria, A. Granville nos indicó que gracias a un método de I. Schur, aparentemente similar al nuestro, G. Szego, ([S], §6.7), calcula el máximo de (2.4) cuando el intervalo considerado es el $[-1, 1]$ en vez del $[0, 1]$ correspondiente al caso estudiado en nuestra memoria. Allí se incluye también, (§16.2), el diámetro transfinito de dicho intervalo, así como se hace referencia a dicha cantidad en conjuntos más generales.

Incluimos las siguientes referencias relativas a este particular:

[**Fa**] G. Faber *Tschebyscheffsche Polynome* Jour. für die reine und ange. Mathe. **150** (1919), 79–106

[**S**] I. Schur, *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome*, Jour. für die reine und ange. Mathe. **165** (1931), 52–58

[**Sz**] G. Szegö, *Orthogonal Polynimials*, Amer. Math. Soc. **23** Providence, Rhode Island (1939)

Indice

Notación

A continuación incluimos una lista de expresiones que se incluyen a lo largo de la memoria sin definición previa. La mayoría se pueden encontrar muy frecuentemente en la literatura.

$\deg F(x) :=$ Grado del polinomio $F(x)$.

$[x]$ es el mayor entero menor que x.

$f(x) \ll g(x) :=$ Existe una constante c tal que $|f(x)| \leq c|g(x)|$ para x suficientemente grande.

$f(x) \gg g(x) :=$ Existe una constante c tal que $|f(x)| \geq c|g(x)|$ para x suficientemente grande.

$f(x) = O(g(x))$ es lo mismo que "$f(x) \ll g(x)$".

$f(x) = o(g(x)) := \lim_{x\to\infty} f(x)/g(x) = 0$.

$f(x) \asymp g(x) :=$ Se cumple $c_1 g(x) \leq |f(x)| \leq c_2 g(x)$ para ciertas constantes c_1, c_2, y x suficientemente grande.

$a_n \approx b_n :=$ Se cumple $c_1 a_n \leq b_n \leq c_2 a_n$ para ciertas constantes c_1, c_2, y n suficientemente grande.

$(a_1, \cdots, a_k)$ es el máximo común divisor de todos los $a_1, \cdots, a_k$. A veces (a, b) puede denotar un punto en el plano, de coordenadas a, b.

$[a_1, \cdots, a_k]$ es el mínimo común múltiplo de $a_1, \cdots, a_k$.

$d(n)$ es el número de divisores de n.

$d_\alpha(n) = \#\{a, b \in \mathbb{Z} : N \leq a, b \leq N + N^\alpha , ab = n\}$

$r_\alpha(n) = \#\{a, b \in \mathbb{Z} : N \leq a, b \leq N + N^\alpha , a^2 + b^2 = n\}$

$\mathrm{r}_d(n) = \#\{a, b \in \mathbb{Z} : a^2 - db^2 = n\}$

Introducción

Muchos problemas aritméticos tienen una traducción geométrica en la estimación del número de puntos del retículo en curvas o regiones del plano. El más clásico es el problema del círculo, introducido por C.F. Gauss [G] en 1834. Este problema trata de estimar el número de puntos de coordenadas enteras dentro del círculo $x^2 + y^2 \leq R^2$.

Si definimos

$$r(n) = \#\{(x, y) \in \mathbb{Z} \,/\, x^2 + y^2 = n\},$$

entonces el problema del círculo se puede interpretar como el estudio en media de la función $r(n)$. A pesar de su buen comportamiento en media (Gauss obtuvo $\sum_{n \leq x} r(n) = \pi x + O\left(x^{1/2}\right)$) la función $r(n)$ es muy irregular dependiendo su valor de la factorización de n en números primos. En particular sabemos que, si

$$n = 2^{\nu} \prod_{p_j \equiv 1 (\mathrm{mod}\ 4)} p_j^{\alpha_j} \prod_{q_k \equiv 3 (\mathrm{mod}\ 4)} q_k^{\beta_k},$$

entonces $r(n) = 4 \prod_j (1 + \alpha_j)$ cuando todos los β_k son pares, y cero en otro caso. Haciendo hincapié en el significado geométrico de la función $r(n)$, la cantidad anterior, nos dirá exactamente el número de puntos de coordenadas enteras que hay en una circunferencia de radio $\sqrt{n}$. De manera natural surge el preguntarse como están repartidos dichos puntos sobre la circunferencia.

J. Cilleruelo, en su tesis doctoral, se preocupó de este particular dando varios resultados acerca de esta pregunta. Entre ellos destacaremos el siguiente:

(1) Un arco de longitud $R^{1/2 - 1/(4[k/2]+2)}$ contiene a lo más k puntos de coordenadas enteras.

Consideremos ahora otro problema clásico del retículo, el asociado a la hipérbola $xy = N$. Contar puntos bajo la gráfica de dicha curva, es equivalente a estudiar en media la función divisor

$$d(n) = \#\{(x, y) \in \mathbb{Z} \,/\, xy = n\}.$$

De nuevo un comportamiento más o menos regular en media (Dirichlet [**D**] probó $\sum_{n\leq x} d(n) = x\log x + (2\gamma - 1)x + O\left(x^{1/2}\right)$) no expresa la irregularidad de la función en sí. Como en el caso anterior podemos expresar el valor puntual de la función por medio de una fórmula sencilla en términos de la factorización de n. Así, si $n = \prod p_j^{\alpha_j}$, entonces $d(n) = \prod(1+\alpha_j)$. En este punto, y de manera análoga, sin olvidar el lado geométrico, surge la pregunta que da pie a esta memoria.

¿Podemos de alguna manera dar una cota a la longitud de un arco de hipérbola que contenga k puntos de coordenadas enteras?

Entre otros factores, la respuesta dependerá directamente de la curvatura de la zona de la curva donde nos encontremos. Del resultado principal del capítulo 1, deducimos una cota inferior para la longitud en cualquier rango, o zona, de la hipérbola.

Si nos situamos en el centro de la hipérbola, este resultado es equivalente a la cota conseguida en (1) para circunferencias, considerando una circunferencia de radio, R, como el radio de curvatura de la hipérbola, $R \approx \sqrt{N}$. De hecho la analogía llega más lejos ya que del Teorema 1.1 se deducen cotas no sólo para las hipérbolas, sino para todas las cónicas de la forma $x^2 - dy^2 = N$, tales que el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ correspondiente sea un dominio de factorización única. En particular se deduce (1) para las circunferencias.

El rango de la hipérbola en el que nuestra cota (1.1) es óptima depende del número de puntos k. En los casos $k = 2$ y 3, la cota es óptima en toda la hipérbola. Para el caso 4, una construcción mediante fracciones continuas nos permite dar la mejor cota cerca del centro de la hipérbola.

Debido a su simetría, la situación en el centro de la hipérbola es particularmente interesante. Allí es fácil ver que para la existencia de tres puntos, ya es necesaria una longitud de $N^{1/4}$. Mediante un ejemplo observamos que además dicha longitud es suficiente, y que de hecho podemos situar hasta 8 puntos de coordenadas enteras en un intervalo de longitud $cN^{1/4}$.

I. Ruzsa conjetura que en el centro de la hipérbola, para todo $\varepsilon > 0$, el número de puntos del retículo en un arco de longitud $N^{1/2-\varepsilon}$ está acotado uniformemente en N.

Introduciendo la función

$$d_\alpha(n) = \#\{(a,b) \in \mathbb{Z} \,/\, N \leq a, b \leq N + N^\alpha \,/\, ab = n\},$$

podemos estudiar en media cuántos puntos de coordenadas enteras hay en el centro de la hipérbola $xy = n$, consiguiendo un resultado que apoya la conjetura de I. Ruzsa.

La definición de $d_\alpha(n)$ fue sugerida por la función $r_\alpha(n)$ introducida por J. Cilleruelo [**C1**]. Allí la media de $r_\alpha(n)$ tiene aplicaciones al estudio de polinomios trigonométricos. En nuestro caso, gracias a que la función generatriz de la función divisor es $\zeta^2(s)$, donde $\zeta(s)$ es la función zeta de Riemann, podemos aplicar nuestros resultados sobre $d_\alpha(n)$ al estudio del momento de orden 4 de sumas parciales de $\zeta(s) = \sum 1/n^s$ sobre intervalos de pequeña longitud.

En el capítulo 2 incluimos un trabajo conjunto con A. Granville, en el que se consigue mostrar cuál es exactamente la longitud necesaria de un arco para que contenga k puntos de coordenadas enteras, cuando nos restringimos a cierto rango de la hipérbola $xy = N$, que estará lejos del centro. En este sentido, demostraremos que existe una constante c_k, y un exponente α_k, tal que si la longitud L del arco satisface

$$L < c_k N^{\alpha_k}$$

entonces el arco no contiene k puntos de coordenadas enteras, mientras que por otro lado, para infinitos valores de N, existen arcos de longitud

$$L \leq (c_k + \varepsilon) N^{\alpha_k}$$

conteniendo k puntos del retículo.

En la demostración, observamos que, si existen k puntos de coordenadas enteras, $(a_1, b_1), \cdots, (a_k, b_k)$, con $a_i b_i = N$, entonces $[a_1, \cdots, a_k] \leq N$. Luego dar una cota inferior a la longitud del arco se puede traducir en dar una cota inferior al mínimo común múltiplo M de k números en cierto intervalo $X \leq a_1 < \cdots < a_k \leq X + L$. En este contexto se consigue para cierta constante C_k

$$M \geq C_k \frac{X^k}{L^{\binom{k}{2}}}$$

mientras que para todo $\varepsilon > 0$, hay infinitos valores de X y k enteros en el intervalo $[X, X + L]$ con mínimo común múltiplo

$$M \leq (C_k + \varepsilon) \frac{X^k}{L^{\binom{k}{2}}}.$$

En el capítulo 3 nos ocupamos del estudio de hipérbolas giradas, cuyos ejes son los ejes coordenados, y queremos acotar la longitud mínima necesaria de un arco en la hipérbola $x^2 - dy^2 = N$, para que contenga k puntos de coordenadas enteras. Cuando el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ es un dominio de factorización única, sabemos dar una cota a esta longitud como caso particular del Teorema 1.1 del capítulo 1. En general, si nos aventuramos a decir que el número de puntos de coordenadas enteras pertenecientes a un arco de cierta curva, depende esencialmente de la curvatura de esa curva, deberíamos esperar, aun si no hay factorización única, obtener un resultado similar.

J. Cilleruelo y A. Córdoba estudiaron, [**C-C 1**], un problema análogo en las elipses $x^2 + dy^2 = N$. El método que utilizamos aquí, podría también usarse para las elipses dando de nuevo la cota conseguida en [**C-C 1**], sin embargo las hipérbolas son algo más esquivas, y conseguimos demostrar un resultado ligeramente más débil. Observar que, en principio, ambos casos son esencialmente distintos, ya que en el caso de las hipérbolas, la existencia de infinitas unidades en el anillo de enteros correspondiente, da lugar a infinitos puntos de coordenadas enteras sobre la hipérbola.

CAPÍTULO 1

PUNTOS DE COORDENADAS ENTERAS EN HIPÉRBOLAS

Introducción

En este capítulo damos una cota inferior a la longitud de un arco de la hipérbola $xy = N$ que contenga k puntos de coordenadas enteras. Dicha cota depende del rango en el que nos situemos, y es óptima en algunos casos particulares, lo que mostramos con ejemplos explícitos. El teorema se situa en un marco más amplio sobre dominios de factorización única con una valoración. Este enfoque nos permite deducir resultados análogos en contextos más generales.

El estudio de la hipérbola $xy = N$ esta íntimamente relacionado con la función divisor. Así, en la última sección incluimos un resultado sobre la media de una cierta función divisor, y una aplicación de éste al cálculo del momento de orden 4 de sumas del estilo $\sum 1/n^s$.

§ 1 Un resultado general.

El hecho de que el número de puntos de coordenadas enteras en arcos de $xy = N$ cuente justamente los divisores de N en cierto intervalo, será el punto de partida para acotar la longitud que debe tener un arco con k puntos del retículo.

Así, supongamos que hay k puntos $(a_1, b_1), \cdots, (a_k, b_k)$ con $a_i b_i = N$ y tal que $X \leq a_1 < \cdots < a_k \leq X + L$. En este caso el mínimo común múltiplo $[a_1, \cdots, a_k]$ que llamaremos M, cumple $M|N$. Aprovechando este hecho, vamos a enunciar nuestro resultado dentro de la aritmética, en términos del mínimo común múltiplo. En particular probaremos:

Sea $X > 0$ fijo, y sean $X \leq a_1, \cdots, a_k \leq X + L$, con mínimo común múltiplo M tal que $M^\gamma \leq X$, entonces

$$(1.1) \qquad L \geq M^{E(\gamma)} \quad \textit{donde} \quad E(\gamma) = \left(k\gamma[k\gamma] - \binom{[k\gamma]+1}{2} \right) / \binom{k}{2}$$

Notar que se cumple $E(\gamma) > \gamma^2 - \gamma(\frac{1-\gamma}{k-1})$.

Antes de demostrar (1.1), vamos a hacer ciertas observaciones sobre las condiciones del problema, y el resultado. En principio, observamos que es suficiente restringirse a k-uplas de enteros primos entre sí, es decir $(a_1, \cdots, a_k) = 1$ ya que si $(a_1, \cdots, a_k) = d$, y $[a_1, \cdots, a_k] = M$, entonces $[a_1/d, \cdots, a_k/d] = M/d$, y se tiene para cualquier $\alpha < 1$,

$$a_k - a_1 = d\left(\frac{a_k}{d} - \frac{a_1}{d}\right) \geq d\left(\frac{M}{d}\right)^\alpha > M^\alpha.$$

Por otra parte, la cota (1.1) sólo es valida cuando $\gamma \geq 1/k$. Este es de hecho el conjunto de rangos de interés. En el resto de los casos, es decir cuando $a_1 \approx M^\gamma$ con $\gamma < 1/k$, no hay más que observar que $M \leq \prod a_i$ para obtener $L \gg M^{(1-\gamma}/(k-1) > X$. Además se puede deducir que esta cota es lo mejor posible, escogiendo k enteros primos entre sí en el rango adecuado.

En el caso $\gamma = 1/k$, $E(\gamma) = 0$ es la mejor cota posible. k enteros consecutivos $a_i = n + i$, $i = 1, \cdots, k$, nos dan el ejemplo que alcanza la cota, pues el mínimo común múltiplo es como el producto, y la diferencia está acotada para todo n.

La última observación que vamos a hacer, es que en realidad es suficiente demostrar (1.1) para $\gamma \leq 1/2$, por la simetría de la hipérbola.

En efecto, un cálculo directo nos muestra que

$$E(\gamma) = 2\gamma - 1 + E(1-\gamma).$$

Por otra parte, supongamos $(a_1, \cdots, a_k) = 1$, y $[a_1, \cdots, a_k] = M$, con $a_1 \approx M^\gamma$, $\gamma > 1/2$. Entonces existen k enteros $b_1, \cdots, b_k$ tal que $a_i b_i = M$, $b_1 \approx M^{1-\gamma}$ y $[b_1, \cdots, b_k] = M$, por tanto si suponemos el resultado cierto para todo rango por debajo del $1/2$, entonces,

$$(b_1 - b_k) \geq M^{E(1-\gamma)} = M^{1-2\gamma+E(\gamma)},$$

y por tanto

$$a_k - a_1 = M/b_k - M/b_1 = \frac{M}{b_k b_1}(b_1 - b_k) \geq M^{2\gamma-1}(b_1 - b_k) \geq M^{E(\gamma)},$$

como queríamos ver.

En resumen, podemos restringir la demostración de (1.1) a rangos $1/k < \gamma \leq 1/2$, y k números primos entre sí.

Vamos a deducir este resultado a partir de un teorema un poco más general, que nos permitirá obtener resultados análogos en otros contextos.

TEOREMA 1.1.

Sea $\mathcal{K}$ el cuerpo de fracciones de un dominio de factorización única $\mathcal{A}$, y sea $\varphi : \mathcal{K} \to \mathbb{R}$ tal que

$$\text{(i)} \qquad \varphi(a) \geq 0 \quad \textit{Para todo } a \in \mathcal{A} - \{0\}$$

$$\text{(ii)} \qquad \varphi(ab) = \varphi(a) + \varphi(b) \quad \textit{Para todo } a, b \in \mathcal{K}.$$

Entonces, si $M = [a_1, \cdots, a_k]$, $\varphi(a_i) \geq \gamma\varphi(N)$ con N un múltiplo de M, y L es tal que $\varphi(a_j - a_i) \leq L$ para todo j, i, entonces

$$L \geq \varphi(N)E(\gamma), \tag{1.2}$$

donde $E(\gamma)$ está definida como en (1.1).

DEMOSTRACIÓN:

Para cada primo $p \in \mathcal{A}$, definimos la función $v_p(m)$ que asocia a cada elemento de $\mathcal{A}$ la máxima potencia de p que lo divide, extendiendo la definición a $\mathcal{K}$ de la siguiente forma, si $r = a/b$ con $a, b \in \mathcal{A}$ entonces $v_p(r) = v_p(a) - v_p(b)$.

Si ordenamos los elementos $a_1, \cdots, a_k$ de forma que para un primo fijo p, $t_i = v_p(a_i)$ sea creciente con i, obtenemos

$$v_p\left(\prod(a_j, a_i)\right) = \sum_{1 \leq i < j \leq k} t_i = \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} 1 = \sum_{i=1}^{k} t_i(k - i),$$

y por otra parte

$$v_p\left(\prod a_i\right) = \sum_{1 \leq i \leq k} t_i.$$

Ahora bien, uniendo la información local que tenemos en cada primo, podemos escribir en general $a = \prod_{p|a} p^{v_p(a)}$, y en nuestro caso nos queda

$$\prod(a_j, a_i) = \prod_{p|M} p^{\sum_{1 \leq i \leq k} t_i(k-i)}$$

$$\text{y} \qquad \prod a_i = \prod_{p|M} p^{\sum_{1 \leq i \leq k} t_i}.$$

Elevando a un cierto entero m la segunda fórmula, y multiplicando y dividiendo el resultado en la primera, obtenemos

$$\prod(a_j, a_i) = \left(\prod a_i\right)^m \prod_{p|M} p^{\sum_{1\leq i\leq k} t_i(k-i-m)}, \tag{1.3}$$

identidad válida para cualquier entero m. Gracias a esta relación entre el máximo común divisor y el tamaño de los números, y la flexibilidad que tiene en la elección del entero m, vamos a poder establecer el resultado.

De esta forma, por las propiedades de φ, (i) y (ii), deducimos

$$\varphi\left(\prod_{p|M} p^{\sum_{1\leq i\leq k} t_i(k-i-m)}\right) \geq \varphi\left(\prod_{p|M} p^{-\sum_{k-m\leq i\leq k} t_i(i-(k-m))}\right),$$

ya que $i-(k-m)\geq 0$ en ese rango de la suma. Además, como $t_i \leq t_k$, y $M=\prod_{p|M} p^{t_k}$ por la definición de los t_i, queda

$$\geq -\varphi(M)\left(\sum_{k-m\leq i\leq k}(k-i-m)\right) = -\varphi(M)\binom{m+1}{2} \geq -\varphi(N)\binom{m+1}{2},$$

de nuevo por (i) y (ii). Este hecho, junto con la hipótesis $\varphi(a_i)\geq\gamma\varphi(N)$ nos permite obtener, sustituyendo en (1.3)

$$\varphi\left(\prod(a_j,a_i)\right) \geq \varphi(N)\left(k\gamma m - \binom{m+1}{2}\right).$$

Optimizando en m, y observando que

$$\varphi(a_j-a_i) = \varphi((a_j,a_i)) + \varphi\left((a_j-a_i)/(a_j,a_i)\right) \geq \varphi((a_j,a_i)),$$

se concluye el resultado.

∎

Los siguientes corolarios, nos muestran el alcance más general del teorema

Corolario 1.1. *Sean $F_1(x),\cdots,F_k(x)$ polinomios en $\mathbb{Z}(x)$ con mínimo común múltiplo $M(x)$, y tal que $\deg(F_i(x))\geq\gamma\deg(M(x))$. Entonces*

$$\deg(F_j(x)-F_i(x)) \geq \deg(M(x))E(\gamma).$$

No hay más que elegir $\mathcal{A}=\mathbb{Z}(x)$, $\varphi(F)=\deg(F)$.

COROLARIO 1.2. *Considerar una circunferencia de radio R, centrada en el origen. En un arco de longitud $L = R^t$ tal que*

$$t < 1/2 - 1/(4[k/2] + 2),$$

como mucho hay k puntos de coordenadas enteras.

DEMOSTRACIÓN:

En primer lugar, observamos que la longitud de un arco de circunferencia, es comparable a la longitud del segmento que une los extremos del arco. A partir de aquí, no hay más que tomar $\mathcal{A} = \mathbb{Z}[i]$, $\varphi(\alpha) = \log|\alpha|$, ya que si $\alpha_1, \cdots, \alpha_k$ son tal que $\alpha_i \overline{\alpha_i} = R^2$, entonces $\varphi(\alpha) = 1/2\varphi(R^2)$ y R^2 es un múltiplo de $[\alpha_1, \cdots, \alpha_k]$.

<u>Observación:</u> De hecho este corolario es mucho más general, siendo válido el resultado para toda cónica $x^2 - dy^2 = N$, tal que $\mathbb{Z}(\sqrt{d})$ sea un dominio de factorización única, obteniendose en el caso $d > 0$ de nuevo el resultado (1.2), siempre que $\varphi(\alpha_i) \geq \gamma\varphi(N)$.

Sin embargo, el principal motivo para establecer el Teorema 1.1 en esta memoria se plasma en el siguiente corolario

COROLARIO 1.3. *La cota (1.1) es cierta en todo rango γ.*

En este caso escogemos $\mathcal{A} = \mathbb{Z}$, $\varphi(x) = \log|x|$.

Un dato a señalar es que en $\gamma = 1/2$ se obtiene

$$E(1/2) = 1/4 - 1/(8\,[(k-1)/2] + 4),$$

que, como ya mencionamos en la introducción, iguala el exponente en [**C1**].

§ 2 <u>Los casos $k = 2, 3$ y 4.</u>

Aunque el caso $k = 2$ está completamente resuelto por las observaciones que hicimos antes del Teorema 1.1, sin embargo es interesante hacer notar que en este caso, el mínimo común múltiplo M de dos números con máximo común divisor $(a_1, a_2) = d$, cumple

$$M = \frac{a_1 a_2}{d} \leq \frac{a_1 a_2}{a_1 - a_2},$$

ya que $d \leq a_2 - a_1$, y que se dará la igualdad cuando el máximo común divisor sea exactamente la diferencia de los números. Es esta sencilla observación en la que se basan todos nuestros intentos de encontrar la mejor cota para el mínimo común múltiplo de k números en un intervalo, es decir, trataremos de comparar los máximos comunes divisores de los números con sus diferencias.

Para $k = 3$, el siguiente ejemplo muestra que el Teorema 1.1 nos da la mejor cota posible para todo rango γ.

Consideramos los enteros

$$\begin{aligned} a_1 &= 4n(2n-1)\,(n+1+(2n+1)t) \\ a_2 &= a_1 + 2n - 1 \\ a_3 &= a_1 + 4n \end{aligned}$$

Con $t \approx n^{(3-6\gamma)/(3\gamma-1)}$, para cierto $1/3 < \gamma \leq 1/2$ fijo. Observamos que $(a_1, a_2, a_3) = 1$, y que, por otra parte $a_j - a_i = (a_j, a_i)$, por lo que el mínimo común múltiplo queda

$$M = \frac{\prod a_i}{\prod (a_j, a_i)} \approx \frac{n^9 t^3}{n^3} \approx n^{3/(3\gamma-1)}. \tag{1.4}$$

Por otra parte $a_1 \approx n^3 t \approx n^{3\gamma/(3\gamma-1)} \approx M^{\gamma}$, mientras que $a_j - a_i \approx n \approx M^{\gamma-1/3}$, en donde hemos usado (1.4).

Sólo falta observar, que cuando restringimos γ al conjunto $1/3 < \gamma \leq 1/2$, $E(\gamma) = \gamma - 1/3$.

El caso $k = 4$ es algo más delicado. En este caso, el ejemplo que incluimos muestra que la cota en el Teorema 1.1 es lo mejor posible, pero sólo en $\gamma = 1/2$.

Así como en los casos anteriores, los ejemplos tenían crecimiento polinómico en n, en este caso tiene crecimiento exponencial, y por otra parte creemos que no existe ningun ejemplo de crecimiento polinómico.

Este ingenioso ejemplo, de nuevo explota la idea de comparar las diferencias de los números con sus máximos comunes divisores. Para ello se utilizan las propiedades muy particulares de las convergentes a un número en su expresión en fracción continua. Este mismo ejemplo, convenientemente adaptado, ya lo habia utilizado J. Cilleruelo para el problema análogo cuando la curva es un círculo centrado en el origen.

Sean p_n/q_n las convergentes de $\sqrt{5}$ en su expresión en fracción continua $\sqrt{5} = [2; \dot{4}]$. Consideramos

$$\begin{aligned} a_1 =& p_n p_{n+2} q_{n+1} \\ a_2 =& p_{n+1} p_{n+2} q_n \\ a_3 =& p_n p_{n+1} q_{n+2} \\ a_4 =& 5 q_n q_{n+1} q_{n+2}. \end{aligned}$$

En primer lugar, observamos que $p_{n+t} | (a_i, a_j)$ o bien $q_{n+t} | (a_i, a_j)$ para algún $t \in \{0, 1, 2\}$, y que en cualquier caso

$$(a_i, a_j) \gg p_n,$$

ya que

$$\left| \frac{p_m}{q_m} - \sqrt{5} \right| = O\left(\frac{1}{q_m^2} \right), \tag{1.5}$$

y las identidades, $p_{m+1} = 4p_m + p_{m-1}$ y $q_{m+1} = 4q_m + q_{m-1}$, válidas para todo $m \geq 1$, nos permiten comparar q_{n+t} y p_{n+t} con p_n para todo $t = 0, 1, 2$. Queremos probar que $a_i - a_j \ll p_n$, pues en ese caso $(a_i, a_j) \approx p_n$ es lo más grande posible. Es suficiente verificar este hecho sólo para las diferencias con el primer número, $a_i - a_1$, siendo el caso general consecuencia de la desigualdad triangular.

Ahora bien, no hay más que usar la identidad $p_m q_{m-1} - q_m p_{m-1} = \pm 1$, cierta para todo m, para obtener, $|a_i - a_1| \ll p_n$ cuando $i = 1, 2$. Por último, controlar $a_4 - a_1$ es posible gracias a (1.5). En efecto

$$\begin{aligned} \frac{a_4 - a_1}{q_{n+1}} =& 5q_{n+2}q_n - p_{n+2}p_n = q_{n+2}q_n \left(5 - \frac{p_{n+2}}{q_{n+2}} \frac{p_n}{q_n}\right) \\ =& q_{n+2}q_n \left(5 - \left(\sqrt{5} + O\left(\frac{1}{q_n^2}\right)\right)^2\right) \ll q_n q_{n+2} \left(\frac{1}{q_n^2}\right) \leq C, \end{aligned} \tag{1.6}$$

para cierta constante C, de donde

$$a_4 - a_1 \leq C q_{n+1} \ll p_n.$$

De esta forma, por lo mencionado anteriormente, se concluye

$$(a_j, a_i) \approx p_n. \tag{1.7}$$

Para terminar observamos que $(a_i, a_j, a_l) = 1$, pues si $d | (a_i, a_j, a_l)$, entonces d es un divisor de los comunes divisores a cualesquiera dos de ellos, de donde se deduce que $d | (p_m, p_{m+1})$, o bien $d | (q_m, q_{m+1})$, que sólo puede ser si $d = 1$, pues numeradores o denominadores consecutivos de las convergentes, son primos entre sí. Ya no hay más que tener en cuenta (1.7), y que $a_i \approx p_n^3$, para obtener

$$M = \frac{\prod a_i}{\prod (a_j, a_i)} \approx p_n^6,$$

y terminar la prueba.

§ 3 El centro de la hipérbola.

Es particularmente interesante observar que, cuando uno se restringe al centro justo de la hipérbola, las cosas pueden variar drásticamente. De esta forma, mostraremos que la longitud $L \geq M^{1/4}$ es necesaria para que un arco en el centro de hipérbola contenga 3 puntos de coordenadas enteras, mientras que en la sección anterior hemos visto que un poco más alla del centro, todavía en el rango $\gamma = 1/2$, el Teorema 1.1 es lo mejor posible en los casos $k = 2, 3$ y 4

en donde, por ejemplo, para $k = 4$, se tiene $E(1/2) = 1/6$ notablemente más pequeño que el $1/4$.

Así, supongamos que hay dos puntos (x_1, y_1), (x_2, y_2) con $x_i y_i = N$ y tal que $N^{1/2} \leq x_i \leq N^{1/2} + N^{\alpha}$. Un argumento geométrico, usando que la distancia entre las rectas que unen dichos puntos con sus simétricos (y_1, x_1), (y_2, x_2) es mayor que una cierta constante, nos permite concluir que $\alpha \geq 1/4$, sin más que calcular el punto de corte de esas rectas con la hipérbola.

La pregunta está en intentar determinar si $\alpha = 1/4$ es suficiente para que un arco de esa longitud contenga $k \geq 3$ puntos de coordenadas enteras, y si es cierto, cual es el máximo número de puntos que puede contener.

Dicho de otra forma, sea k un número entero. ¿Es cierto que para alguna constante c existen infinitos valores de N , y k puntos de coordenadas enteras en la hipérbola $xy = N$, tal que $N^{1/2} \leq x < N^{1/2} + cN^{1/4}$?

Mediante un ejemplo, determinamos que la respuesta es afirmativa para $k = 4$. En efecto, el entero

$$N = n(n+1)(n-1)(n-6)(n-3)(n-4)(n-2)(n+3),$$

y sus divisores

$$\begin{aligned} x_1 =& (n-3)(n-4)(n-2)(n+3) \\ x_2 =& n(n-1)(n-3)(n-2) \\ x_3 =& n(n+1)(n-3)(n-4) \\ x_4 =& (n+1)(n-1)(n-4)(n-2), \end{aligned}$$

cumplen $x_i - N/x_i \leq an^2$ para cierta constante a. De esta forma

$$0 < x_i - \sqrt{N} < x_i - N/x_i \leq an^2 \ll N^{1/4}$$

para $i = 1, \cdots, 4$ como queríamos ver.

No se sabe la certeza del enunciado en ningun caso $k > 4$. El estudio del caso particular en el centro de la hipérbola, fue sugerido por A. Granville que trató este caso junto con C. Pomerance y P. Erdős. Este último conjeturó que podría ser ya falso para $k = 5$. Por otra parte, aparentemente I. Ruzsa va más allá, conjeturando que para todo $\varepsilon > 0$ existe un entero k, tal que sólo para un número finito de valores de N puede haber más de k puntos del retículo (x, y), con $xy = N$ y $N^{1/2} \leq x < N^{1/2} + N^{1/2-\varepsilon}$.

Si nos preocupamos de lo que pasa en media en el centro de la hipérbola, encontramos un resultado que apoya la conjetura de I. Ruzsa, en el sentido de que, veremos que casi todo n tiene menos de 2 representaciones en un arco de longitud n^α, $\alpha < 1$, en el centro de la hipérbola $xy = n$. Este tipo de medias ya fue estudiado por J. Cilleruelo para la función $r(n)$, que cuenta el número de representaciones de n como suma de dos cuadrados. La función que mide este tipo de medias para la hipérbola fue sugerido por, [C1] y el resultado conseguido es el análogo.

De esta forma, si consideramos el intervalo $I = (N, N + N^\alpha]$, definimos

$$d_\alpha(n) = \#\{(a, b) \,/\, \{a, b\} \in I\,,\ ab = n\},$$

y consideramos $\sum_n d_\alpha(n)$, de alguna manera estaremos estimando la media del número de representaciones de n por puntos en el centro de la hipérbola.

Como ya hemos mencionado, vamos a probar que de hecho casi todos los enteros tienen menos de 2 representaciones dentro del cuadrado $Q = I \times I$.

Para ver un resultado de este estilo, lo que haremos será comparar la media cuadrática de la función con su propia media, ya que si $d_\alpha(n) > k$ muchas veces, esperaríamos $\sum d_\alpha^2(n) > k \sum d_\alpha(n)$. Vamos a probar

TEOREMA 1.2. *Sea $0 < \alpha < 1$ un número real. Entonces*

$$\sum d_\alpha^2(n) = 2N^{2\alpha} + O\left(N^{3\alpha-1} \log N\right) + O\left(N^\alpha\right). \tag{1.8}$$

DEMOSTRACIÓN:

En principio observamos que

$$\sum d_\alpha(n) = N^{2\alpha} + O\left(N^\alpha\right), \tag{1.9}$$

pues dicho sumatorio cuenta, exactamente, los puntos de coordenadas enteras en Q.

En vista de (1.8) y (1.9), lo que intentaremos probar es que $d_\alpha(n) > 2$ no va a ocurrir muchas veces.

Supongamos que $d_\alpha(n) > 2$, entonces existen al menos dos representaciones no simétricas de n mediante la hipérbola $xy = n$, y dentro del cuadrado Q. Sean $ab = n = cd$, esas dos representaciones, entonces

$$\{a, b, c, d\} \in I \quad \text{y} \quad a \neq \{c, d\}.$$

Consideramos $m_1 = (a, c)$, y escribimos $a = m_1 l_1$, $c = m_1 l_2$. De $ab = cd$ deducimos que $l_1 | d$ y $l_2 | b$, por lo que para algún entero m_2 queda

$$(m_1 l_1)(m_2 l_2) = (m_1 l_2)(m_2 l_1).$$

Además, $m_1 \leq b - a \leq N^\alpha$, y lo mismo ocurre para l_1 pues es un divisor común de dos enteros en el intervalo $N, N + N^\alpha$. Si ahora tenemos en cuenta que $m_1 l_1 = a \geq N$, queda $m_1 \geq N^{1-\alpha}$ y por tanto $N^{1-\alpha} \leq m_1 \leq N^\alpha$. Una primera implicación de este hecho es que para $\alpha < 1/2$ no hay ningún entero con más de 2 representaciones en Q. Por tanto, a partir de ahora y mientras no se diga lo contrario, supondremos $\alpha \geq 1/2$. Ahora bien, supongamos que $d_\alpha(n) = j > 2$, entonces el número de representaciones de n en Q no simétricas será $j(j-2)/2$ si j es par, y $(j-1)(j-2)/2$ si j es impar, y en cualquier caso $\geq j^2/9 \gg d_\alpha(n)$, por otra parte, como acabamos de ver, dicha cantidad está acotada superiormente por el cardinal del conjunto

$$S = \{m_1, m_2, l_1, l_2 \,:\, m_i l_j \in I\{i, j\} = 1, 2,\ N^{1-\alpha} \leq m_1 \leq N^\alpha\}.$$

En este punto es conveniente que definamos $C_j = \#\{n \,:\, d_\alpha(n) = j\}$. De esta forma

$$\sum d_\alpha^2(n) = \sum j^2 C_j,$$

y del párrafo anterior se deriva

$$\sum_{j\geq 3} j^2 C_j \leq \#S.$$

Sólo nos queda dar una estimación de $\#S$. Ahora bien,

$$\#S \leq \sum_{N^{1-\alpha}\leq m_1\leq N^\alpha} \sum_{l_1\in I/m_1} \sum_{m_2\in I/l_1} \sum_{l_2\in I/m_2} 1,$$

donde hemos definido la dilatación $cI = (cN, c(N+N^\alpha)]$. Teniendo en cuenta que para todo entero k, (en particular $k=-1,0,1$), se tiene

$$\sum_{m\in cI} m^k \ll (cN)^k\,[c(N+N^\alpha)] - [cN] \ll c^{k+1}N^{\alpha+k} + (cN)^k,$$

ya que $[x]-[y] < x-y+1$, queda, tras algunas operaciones

$$\#S \ll \sum_{N^{1-\alpha}\leq m_1\leq N^\alpha} \left(\frac{N^{3\alpha-1}}{m_1} + N^{2\alpha-1} + \frac{N^{2\alpha}}{m_1^2} + \frac{N^\alpha}{m_1}\right) = O\left(N^{3\alpha-1}\log N\right).$$

Teniendo en cuenta (1.9), y que $C_1 = O(N^\alpha)$, ya que son los enteros que sólo tienen la representación en la diagonal, se obtiene para todo $0<\alpha<1$,

$$N^{2\alpha} + O(N^\alpha) = C_1 + 2C_2 + \sum_{j\geq 3} jC_j = 2C_2 + O\left(N^{3\alpha-1}\log N\right) + O(N^\alpha),$$

de donde

$$C_2 = \frac{N^{2\alpha}}{2} + O\left(N^{3\alpha-1}\log N\right) + O(N^\alpha),$$

lo que termina el resultado, por (1.10).

∎

Este teorema tiene una aplicación inmediata en el cálculo de momentos de sumas parciales de la función $\zeta(s)$, lo que veremos en la sección siguiente.

§ 4 Los momentos de $\sum 1/n^s$ en intervalos de pequeña longitud

Es bien conocida la fórmula

$$\zeta^2(s) = \sum_{n\geq 1} \frac{d(n)}{n^s}$$

válida para $\mathcal{R}e(s) > 1$. Este hecho, junto con la ecuación funcional aproximada, nos permite reducir el estudio de $\zeta^2(s)$ al comportamiento de cierto polinomio de Dirichlet $\sum_{n\leq N} d(n)/n^s$. Si a este hecho le añadimos un lema general, por el que sabemos que controlar la media cuadrática de polinomios de Dirichlet, es lo mismo que controlar la aportación que viene de los términos diagonales, podremos trasladar la información contenida en el Teorema 1.2 al cálculo del momento de orden 4 de sumas cortas del estilo $\sum 1/n^s$.

En el siguiente lema, que se deduce de un teorema más general para el estudio de la media de series de Dirichlet[1], se precisa el error cometido al estimar el momento de orden 2 de un polinomio de Dirichlet, por la aportación diagonal.

LEMA A. *Considerar* $\sum_N^{N+M} \frac{a_n}{n^s}$ *con* $|a_n| \ll n^\varepsilon$ *para todo* $\varepsilon > 0$, *y* $M \leq N$. *Entonces*

$$\int_{-T}^{T} \left| \sum_{n=N}^{N+M} \frac{a_n}{n^s} \right|^2 dt = 2T \sum_{n=N}^{N+M} \frac{|a_n|}{n^{2\sigma}} + O\left(N^{1-2\sigma+\varepsilon} M\right),$$

en donde hemos llamado $s = \sigma + it$.

DEMOSTRACIÓN:

Sea $s = \sigma + it$. Como

$$\begin{aligned} \left| \sum_{n=N}^{N+M} \frac{a_n}{n_s} \right|^2 &= \sum_{n=N}^{N+M} \frac{a_n}{n^\sigma + it} \sum_{n=N}^{N+M} \frac{\overline{a_m}}{m^{\sigma - it}} \\ &= \sum_{n=N}^{N+M} \frac{|a_n|^2}{n^{2\sigma}} + \sum_{n\neq m} \frac{a_n \overline{a_m}}{(nm)^\sigma (n/m)^{it}}, \end{aligned}$$

[1] Ver §7.1 y §7.2 en [T].

queda

$$\begin{aligned}\int_{-T}^{T}\left|\sum_{n=N}^{N+M}\frac{a_n}{n^s}\right|^2 dt =&2T\sum_{n=N}^{N+M}\frac{|a_n|^2}{n^{2\sigma}}+\sum_{n\neq m}\frac{a_n\overline{a_m}}{(nm)^\sigma}\int_{-T}^{T}\left(\frac{m}{n}\right)^{it}dt\\ =&2T\sum_{n=N}^{N+M}\frac{|a_n|^2}{n^{2\sigma}}+\sum_{n\neq m}\frac{a_n\overline{a_m}\operatorname{sen}(\log(m/n)\,T)}{(nm)^\sigma\log(m/n)}.\end{aligned}$$

Por tanto

$$R=\int_{-T}^{T}\left|\sum_{n=N}^{N+M}\frac{a_n}{n^s}\right|^2 dt-2T\sum_{n=N}^{N+M}\frac{|a_n|^2}{n^{2\sigma}}\ll\sum_{n<m}\frac{|a_n||a_m|}{(nm)^\sigma\log(m/n)}.$$

En el intervalo considerado $m\le 2n$, por lo que si escribimos $n=m-r$, entonces $r\le m/2$ y

$$\log(m/n)=-\log\left(1-\frac{r}{m}\right)>\frac{r}{m},$$

con lo que, usando $|a_n|\ll n^\varepsilon$, queda

$$R\ll N^\varepsilon\sum_{N<m\le N+M}\sum_{r\le m/2}\frac{m}{(m-r)^\sigma m^\sigma r}\ll$$

$$N^\varepsilon\sum_{N<m\le N+M}m^{1-2\sigma}\sum_{r\le m/2}\frac{1}{r}<MN^{1-2\sigma+\varepsilon},$$

como queríamos ver.

TEOREMA 1.3. *Para todo $0<\alpha<1$, se tiene*

$$\frac{1}{2T}\int_{-T}^{T}\left|\sum_{N\le n\le N+N^\alpha}\frac{1}{n^{\sigma+it}}\right|^4 dt\asymp\left(\frac{1}{2T}\int_{-T}^{T}\left|\sum_{N\le n\le N+N^\alpha}\frac{1}{n^{\sigma+it}}\right|^2 dt\right)^2,$$

cuando $N\to\infty$ y $T\ge N^{3-\alpha+\delta}$ para algún $\delta>0$.

DEMOSTRACIÓN:

Si en el lema anterior escogemos

$$a_n=\begin{cases}1 & n\in[N,N+N^\alpha]\\ 0 & \text{en el resto}\end{cases}$$

entonces

$$\frac{1}{2T}\int_{-T}^{T}\left|\sum_{N\le n\le N+N^\alpha}\frac{1}{n^{\sigma+it}}\right|^2 dt = \sum_{N\le n\le N+N^\alpha}\frac{1}{n^{2\sigma}}+O\left(\frac{N^{1+\alpha+\varepsilon-2\sigma}}{T}\right)\asymp N^{\alpha-2\sigma},$$

para $T\ge N^{1+\delta}$. Por otra parte, como

$$\left(\sum_{N\le n\le N+N^\alpha}\frac{1}{n^s}\right)^2=\left(\sum_{N\le n\le N+N^\alpha}\frac{1}{n^s}\right)\left(\sum_{N\le m\le N+N^\alpha}\frac{1}{m^s}\right)=\sum\frac{d_\alpha(k)}{k^s},$$

donde la última suma es cero cuando $k\notin\left(N^2,(N+N^\alpha)^2\right]$, sustituyendo en el Lema A

$$a_n=\begin{cases} d_\alpha(n) & n\in\left[N^2,(N+N^\alpha)^2\right]\\ 0 & \text{en el resto}\end{cases}$$

entonces,

$$\frac{1}{2T}\int_{-T}^{T}\left|\sum_{N\le n\le N+N^\alpha}\frac{1}{n^{\sigma+it}}\right|^4 dt = \sum_{N^2\le n\le (N+N^\alpha)^2}\frac{d_\alpha^2(n)}{n^{2\sigma}}+O\left(\frac{N^{3+\alpha+2\varepsilon-4\sigma}}{T}\right),$$

y teniendo en cuenta (1.8), queda

$$\frac{1}{2T}\int_{-T}^{T}\left|\sum_{N\le n\le N+N^\alpha}\frac{1}{n^{\sigma+it}}\right|^4 dt\asymp N^{2\alpha-4\sigma}$$

cuando $T\ge N^{3-\alpha+\delta}$, lo que termina la demostración.

∎

CAPÍTULO 2

Un Teorema óptimo para cierto rango

Introducción

En el capítulo anterior, hemos obtenido una cota inferior a la distancia L, que hay entre k puntos de coordenadas enteras en la hipérbola $xy = N$, y en cualquier rango $X \approx M^{\gamma}$.

Si nos restringimos a cierto rango, podemos decir no sólo el mejor exponente $E(\gamma)$ tal que $L \geq M^{E(\gamma)}$, sino también la mejor constante C_k para que $C_k M^{E(\gamma)}$ sea la longitud necesaria y suficiente de un arco de hipérbola para contener k puntos de coordenadas enteras.

Como en el capítulo anterior, nos valdremos de una intepretación más aritmética del problema, en términos del mínimo común múltiplo, para probar el resultado. Así, llamando

$$M_k = \min[a_1, \cdots, a_k],$$

donde el mínimo se toma sobre todas las k-uplas de enteros en el intervalo $X \leq a_1 < a_2 < a_k \leq X + L$, queremos encontrar una cota inferior para M_k válida para X suficientemente grande, y L pequeño en comparación con X.

Vamos a mostrar que, para una constante C_k (que definiremos más tarde), la cota

$$M_k \geq C_k \frac{X^k}{L^{\binom{k}{2}}},$$

es la mejor posible en el sentido de que para todo $\varepsilon > 0$ existen X y L, tales que

$$M_k \leq (1+\varepsilon) C_k \frac{X^k}{L^{\binom{k}{2}}}.$$

§ 1 Resultados

TEOREMA 2.1. *Para todo entero $k \geq 2$ fijo se cumple*

$$M_k \geq C_k \frac{X^k}{L^{\binom{k}{2}}}, \tag{2.1}$$

donde

$$(2.2) \qquad C_k^2 = \frac{\left(\frac{2k}{k-1}\right)^k \binom{2k-2}{k}^{(2k-1)} \prod_{m=1}^{k-2}(m!)^2}{2(k!)\prod_{m=1}^{k-1}\binom{2m}{m}^2}.$$

En el apéndice probamos la siguiente fórmula asintótica para C_k:

$$C_k = \left(4e^{-3/2}k\right)^{k^2/2-3k/2}\left(16\pi e^{13/2}\right)^{k/2} k^{7/24} e^{\alpha+O(\frac{1}{k})}$$

donde

$$\alpha = 1/12\log 2 + 1/8\log\pi - 53/24 + 5\gamma/12 + 5/4\sum_{j\geq 2}\frac{\zeta(j)-1}{j+2},$$

γ es la constante de Euler, y $\zeta(j) = \sum_{n\geq 1} n^{-j}$.

Damos los primeros valores de C_k en la siguiente tabla.

k	C_k
2	1
3	2^2
4	$2\cdot 5^2\sqrt{5}$
5	$\frac{2^6\cdot 7^3\sqrt{3\cdot 7}}{3}$
6	$2^7\cdot 3^6\cdot 7^3\sqrt{3\cdot 7}$
7	$\frac{2^{16}\cdot 3^7\cdot 11^5\cdot\sqrt{3\cdot 5\cdot 11}}{5^2}$
8	$\frac{2^{12}\cdot 3^6\cdot 11^5\cdot 13^6\cdot\sqrt{3\cdot 5\cdot 11\cdot 13}}{5}$
9	$\frac{2^{24}\cdot 3^7\cdot 5^8\cdot 11^5\cdot 13^6\cdot\sqrt{7\cdot 11\cdot 13}}{7^3}$
10	$\frac{2^{23}\cdot 3^9\cdot 5^4\cdot 11^5\cdot 13^6\cdot 17^8\cdot\sqrt{7\cdot 11\cdot 13\cdot 17}}{7^2}$

La cota inferior (2.1), es interesante sólo cuando L es pequeño en comparación con X, siendo trivial cuando L es grande. Queremos encontrar el mayor L posible tal que dicha cota es óptima. Podemos probar

Teorema 2.2. *La cota inferior (2.1) es la mejor posible en el sentido de que para todo $\varepsilon > 0$ existen X y $L \gg X^{1/\binom{k}{2}}$, tal que*

$$M_k \leq (1+\varepsilon) C_k \frac{X^k}{L^{\binom{k}{2}}}.$$

Del método que usamos se deduce que podemos establecer esta cota superior para M_k, uniformemente en el rango $L \ll X^{1/\binom{k}{2}}$. Sin embargo, un buen conocimiento acerca de la distribución de las clases de congruencia podría darnos un mejor rango para la longitud del intervalo en comparación con X.

Este es un teorema de existencia; sin embargo, los ejemplos dados en el capítulo anterior para $k = 2$ y 3 en este caso darían

$$M = \frac{a_1 a_2}{(a_1, a_2)} \leq (1+\varepsilon) \frac{X^2}{L},$$

y

$$M = \frac{a_1 a_2 a_3}{\prod_{1 \leq i < j \leq 3} (a_j, a_i)} \leq (1+\varepsilon) 4 \frac{X^3}{L^3},$$

cuando X, y L son suficientemente grandes, respectivamente.

Para $k \geq 4$, como ya mencionamos, parece poco probable encontrar ejemplos con crecimiento polinómico.

Como corolario a los Teoremas 2.1 y 2.2, conseguimos

Teorema 2.3. *Considerar la hipérbola*

$$xy = N,$$

y sea $k \geq 2$ un entero fijo. Para todo $X > 0$ y

$$L < C_k^{1/\binom{k}{2}} \frac{X^{2-\frac{2}{k-1}}}{N^{1-\frac{2}{k-1}+1/\binom{k}{2}}},$$

no hay k puntos de coordenadas enteras, (x_i, y_i), $i = 1, \cdots, k$, en la hipérbola, tales que $X \leq x_1 < x_2 < \cdots < x_k \leq X + L$.

Además, para todo $\varepsilon > 0$, podemos elegir N, $X \geq N^{1-\frac{1}{k-1}}$ y

$$L \leq (1+\varepsilon) C_k^{1/\binom{k}{2}} \frac{X^{2-\frac{2}{k-1}}}{N^{1-\frac{2}{k-1}+1/\binom{k}{2}}}$$

para que haya k puntos de coordenadas enteras, (x_i, y_i), $i = 1, \cdots, k$, en la hipérbola, tales que $X \leq x_1 < x_2 < \cdots < x_k \leq X + L$.

Observación: Estas cotas son significativas sólo cuando $X \geq N^{1/2}$. Sin embargo, el rango $X \leq N^{1/2}$ corresponde a la rama vertical de la hipérbola, y por tanto, una vez probado el Teorema 2.3, se puede deducir un resultado análogo, por simetría.

§ 2 Demostración del Teorema 2.1

Claramente, para un conjunto A de k enteros $\{a_1, \cdots, a_k\}$, se tiene

$$[a_1, \cdots, a_k] = \frac{\prod_{i=1}^k a_i}{C_A}$$

para algún entero C_A, que contiene toda la información sobre los divisores comunes a varios de ellos.

Multiplicando numerador y denominador por $\prod_{1 \leq i < j \leq k}(a_j - a_i)$, obtenemos

$$[a_1, \cdots, a_k] = \frac{\prod_{i=1}^k a_i}{\prod_{1 \leq i < j \leq k}(a_j - a_i)} N_A \tag{2.3}$$

donde

$$N_A = \frac{\prod_{1 \leq i < j \leq k}(a_j - a_i)}{C_A}.$$

En algún sentido N_A está comparando el máximo común divisor de los números con sus diferencias, como fue sugerido por el caso trivial $k = 2$.

Ahora bien, sean X y L fijos y sean $\{a_1, \cdots, a_k\}$, k enteros, de forma que $X \leq a_i \leq X + L$ para $i = 1, \cdots, k$. Podemos escribir $a_i = X + \delta_i L$ con $0 \leq \delta_1 < \delta_2 < \cdots < \delta_k \leq 1$, con lo que se obtiene

$$[a_1, \cdots, a_k] \geq \frac{X^k}{L^{\binom{k}{2}}} \frac{N_A}{\prod_{1 \leq i < j \leq k}(\delta_j - \delta_i)}.$$

Así, si queremos probar el Teorema 2.1, necesitamos dos cosas. En primer lugar maximizar

$$\prod_{1 \leq i < j \leq k} (\delta_j - \delta_i), \tag{2.4}$$

donde los δ_i se toman sobre cierto conjunto como mencionamos anteriormente, y en segundo lugar minimizar N_A.

Empezaremos maximizando (2.4).

LEMA 2.1.

$$\max \left(\prod_{1 \leq i < j \leq k} (\delta_j - \delta_i) \right)^2 = \frac{(k-1)^{(k+1)} (k-2)! \prod_{m=1}^{k-1} \binom{2m}{m}^2}{(2k)^{(k-1)} \binom{2k-2}{k}^{(2k-1)}},$$

donde el máximo se toma sobre el conjunto $0 \leq \delta_1 < \delta_2 < \cdots < \delta_k \leq 1$.

DEMOSTRACIÓN:

Sabemos que ese máximo existe, ya que es una función continua. Así, supongamos que está dado por $\eta_1, \eta_2, \cdots, \eta_k$. Entonces $\eta_1 = 0$ y $\eta_k = 1$, de lo contrario, si $\eta_1 \neq 0$ o $\eta_k \neq 1$ podríamos tomar $\delta_i = (\eta_i - \eta_1)/(\eta_k - \eta_1)$ para obtener

$$\prod (\delta_j - \delta_i) = \prod \frac{\eta_j - \eta_i}{\eta_k - \eta_1} = \frac{1}{(\eta_k - \eta_1)^{\binom{k}{2}}} \prod (\eta_j - \eta_i) > \prod (\eta_j - \eta_i),$$

donde los productos se toman sobre el conjunto $1 \leq i < j \leq k$, y llegaríamos a una contradicción.

Por tanto, tenemos que maximizar la función

$$F(\delta_2, \cdots, \delta_{k-1}) = \prod_{1 \leq i < j \leq k} (\delta_j - \delta_i).$$

F es una función diferenciable, por lo que alcanza el máximo sobre el cerrado $0 \leq \delta_2 \leq \delta_3 \leq \cdots \leq \delta_{k-1} \leq 1$. Sin embargo, si $\delta_i = \delta_j$ para algún $i \neq j$ y $\{i, j\} \in \{1, \cdots, k\}$, entonces $F = 0$, y por tanto el máximo se encuentra en un punto crítico de la función, por lo que para $2 \leq i \leq k-1$ se tiene

$$0 = \frac{1}{F} \frac{\partial F}{\partial \delta_i} (\eta_2, \cdots, \eta_{k-1}) = \sum_{j \neq i} \frac{1}{\eta_i - \eta_j}.$$

Consideramos el siguiente polinomio

$$H(x) = \prod_{i=1}^{k} (x - \eta_i).$$

El máximo que queremos encontrar es justamente su discriminante,

$$\Delta(H) = \prod_{1\leq i<j\leq k} (\eta_j - \eta_i).$$

Ahora bien,

$$H'(x) = \sum_{i=1}^{k} \prod_{j\neq i}(x - \eta_j) \quad \text{y} \quad H'(\eta_i) = \prod_{j\neq i}(\eta_i - \eta_j).$$

Además,

$$H''(x) = \sum_{i=1}^{k} \sum_{j\neq i} \prod_{l\neq j,i} (x - \eta_l) = 2 \sum_{1\leq i<j\leq k} \prod_{l\neq j,i} (x - \eta_l),$$

y por tanto

$$H''(\eta_i) = 2 \sum_{j\neq i} \prod_{l\neq j,i} (\eta_i - \eta_l) = 2H'(\eta_i) \sum_{j\neq i} \frac{1}{\eta_i - \eta_j};$$

con lo que deducimos que, para $2 \leq i \leq k-1$, $H''(\eta_i) = 0$. Teniendo en cuenta que $H''(x)$ es un polinomio de grado $k-2$, concluimos que $\eta_2, \eta_3, \cdots, \eta_{k-1}$ son todas sus raíces. Además, por definición, estas son exactamente las raíces de $H(x)$ excepto 0 y 1. Por tanto, ambos polinomios deben ser casi el mismo, en el sentido de que para alguna constante C se tiene

$$x(x-1)H''(x) = CH(x).$$

$H(x)$ es mónico, por lo que el coeficiente del término de mayor grado en $H''(x)$ es $k(k-1)$, y por tanto $C = k(k-1)$, así

$$x(x-1)H''(x) = k(k-1)H(x). \tag{2.6}$$

Dicha ecuación nos permite deducir

COROLARIO 2.1. *Las raíces de $H(x)$ son simétricas respecto de 1/2.*

Si hacemos el cambio de variable $x = (1+y)/2$, y llamamos $g(y) = H((1+y)/2)$ entonces (2.6) queda

$$(y^2 - 1)g''(y) = k(k-1)g(y).$$

Sea $g(y) = \sum_{i=0}^{k} g_i y^i$. Comparando los coeficientes en ambos lados de la ecuación, se obtiene $g_{k-1} = 0$, y para $i \leq k-2$,

$$-(i+2)(i+1)g_{i+2} = (k(k-1) - i(i-1))g_i.$$

Así, de $g_{k-1} = 0$, se deduce $g_{k-3} = 0$ y de este hecho, de nuevo por la ecuación anterior, $g_{k-5} = 0$. Iterando este proceso hasta el coeficiente de menor grado, se concluye que $g(y)$ es una función par cuando k es par, y es una función impar cuando k es impar. En otras palabras, las raíces de g son simétricas respecto del origen, lo que completa la prueba del corolario.

Volviendo a la ecuación (2.6), y comparando coeficientes en ambos lados de la igualdad, podemos encontrar explícitamente el polinomio $H(x)$ cuya expresión

$$H(x) = \sum_{j=1}^{k} (-1)^{k-j} \frac{\binom{k}{j}\binom{k-1}{j-1}}{\binom{2k-2}{k-j}} x^j, \tag{2.7}$$

puede verificarse sustituyéndola en dicha ecuación.

El discriminante del polinomio, $\Delta(H)$, puede ser determinado por medio de la resultante de $H(x)$ con $H'(x)$, ya que

$$\Delta^2(H) = |R(H(x), H'(x))|,$$

donde podemos definir la resultante de dos polinomios genéricos como sigue; Para un polinomio $f(x) = \sum_{i=0}^{n} a_i x^i$, definimos su matriz asociada de orden $l \times \{l+n\}$, para cualquier $l \in \mathbb{Z}^+$ como

$$A_{l\times\{l+n\}} = \left.\begin{pmatrix} a_n \cdots a_1 a_0 \; 0\; 0 \cdots 0 \\ 0\; a_n \cdots a_1 a_0 0 \cdots 0 \\ \vdots \quad \ddots \quad \ddots \quad \vdots \\ 0\; 0 \cdots 0\; a_n \cdots a_1 a_0 \end{pmatrix}\right\} l.$$

Sea $a_i = 0$ si $i \notin [0,n]$. Esta matriz tiene por coeficientes $a_{i,j} = a_{n-j+i}$. Entonces, definimos la resultante de dos polinomios $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{m} b_i x^i$, con matrices asociadas A y B respectivamente, como[2]

$$R(f(x), g(x)) = det \begin{pmatrix} A_{m\times\{m+n\}} \\ B_{n\times\{n+m\}} \end{pmatrix}.$$

Para encontrar la resultante de $H(x)$ con $H'(x)$, intentaremos reducir el grado del polinomio usando el siguiente

LEMA 2.2. *Sea $f \equiv f(x) = \sum_{i=0}^{n} a_i x^i$, $g \equiv g(x) = \sum_{i=0}^{m} b_i x^i$, $0 < m \leq n$, y para algún número real β y algún entero positivo l, $h \equiv h(x) = f + \beta x^l g = \sum_{i=0}^{r} c_i x^i$ donde $c_i = a_i + \beta b_{i-l}$, tal que $r \leq n$. Entonces*

(i) $$|R(f,g)| = \left|b_m^{n-r} R(g,h)\right|$$

(ii) $$R(f, cg) = c^n R(f,g) \quad c \in \mathbb{R}$$

Observación: (ii) Es verdad incluso si $g \equiv 1$.

Vamos a posponer la prueba de este lema por un momento, y veamos como usarlo en nuestro contexto.

Definimos

$$H[0] = H(x), \quad H[1] = H'(x) = \sum_{j=0}^{k-1} (-1)^{k-j-1} k \frac{\binom{k-1}{j}\binom{k-1}{j}}{\binom{2k-2}{k-j-1}} x^j$$

y

$$H[2] = kH[0] - xH[1]$$
$$H[3] = H[1] + 2H[2]$$
$$H[4] = (k-1)H[2] - (2k-3)xH[3],$$

(2.8) $$H[2l+i+1] = (k-l)H[2l+i-1] + (-1)^i 2^{1-i}(2k-2l-1)^i H[2l+i]x^i,$$

[2] Ver **[La]**

donde $i \in \{0,1\}$ y $2 \leq l < k$ en (2.8). Vamos a mostrar que

$$H[2] = \sum_{j=1}^{k-1} (-1)^{k-j} k \frac{\binom{k-1}{j}\binom{k-1}{j-1}}{\binom{2k-2}{k-j}} x^j,$$

$$H[2l+i-1] = \frac{(k-1)!(k-l)^i}{\binom{2k-2}{k}(k-l)!} \sum_{j=i}^{k-l} (-1)^{k-j+i-1} \binom{k-l+j-i}{k-l-j} \binom{2j-i}{j} x^j,$$

para $i \in \{0,1\}$, $2 \leq l \leq k$.

Los primeros casos de la fórmula se prueban directamente, y después por inducción en l.

Supongamos que es cierta hasta l, entonces

$$(k-l)H[2l-1] + 2H[2l] = \frac{(k-1)!}{\binom{2k-2}{k}(k-l-1)!} \times$$

$$\times \left\{ (-1)^{k-1} + \sum_{j=1}^{k-l} (-1)^{k-j-1} \left[\binom{k-l+j}{k-l-j}\binom{2j}{j} - 2\binom{k-l+j-1}{k-l-j}\binom{2j-1}{j} \right] x^j \right\}$$

Usando que $\binom{m}{n} = \frac{m}{m-n}\binom{m-1}{n}$ obtenemos

$$= \frac{(k-1)!}{\binom{2k-2}{k}(k-l-1)!} \times$$

$$\times \left\{ (-1)^{k-1} + \sum_{j=1}^{k-l-1} (-1)^{k-j-1} \left(\frac{k-l-j}{2j} \right) \binom{k-l+j-1}{k-l-j} \binom{2j}{j} x^j \right\}$$

$$= \frac{(k-1)!}{\binom{2k-2}{k}(k-l-1)!} \sum_{j=0}^{k-l-1} (-1)^{k-j-1} \binom{k-l+j-1}{k-l-j-1} \binom{2j}{j} x^j = H[2l+1],$$

donde hemos utilizado $\binom{m}{n} = \frac{m-n+1}{n}\binom{m}{n-1}$.

Ahora, el resultado es cierto para $H[2l]$, $H[2l+1]$, por tanto, como

$$(2k-2l-1)H[2l+1]x =$$

$$= \frac{(k-1)!}{\binom{2k-2}{k}(k-l-1)!} \sum_{j=0}^{k-l-1} (-1)^{k-j-1}(2k-2l-1) \binom{k-l+j-1}{k-l-j-1} \binom{2j}{j} x^{j+1}$$

$$= \frac{(k-1)!}{\binom{2k-2}{k}(k-l-1)!} \sum_{j=1}^{k-l} (-1)^{k-j}(2k-2l-1) \binom{k-l+j-2}{k-l-j} \binom{2j-2}{j-1} x^j$$

obtenemos, de manera similar

$$(k-l)H[2l]+(2k-2l-1)H[2l+1]x=\frac{(k-1)!}{\binom{2k-2}{k}(k-l-1)!}\times$$

$$\times\left\{\sum_{j=1}^{k-l}(-1)^{k-j}\left[(k-l)\binom{k-l+j-1}{k-l-j}\binom{2j-1}{j}-\right.\right.$$

$$\left.\left.-\ (2k-2l-1)\binom{k-l+j-2}{k-l-j}\binom{2j-2}{j-1}\right]x^j\right\}$$

$$=\frac{(k-1)!(k-l-1)}{\binom{2k-2}{k}(k-l-1)!}\left\{\sum_{j=1}^{k-l}(-1)^{k-j}\left(\frac{k-l-j}{2j-1}\right)\binom{k-l+j-2}{k-l-j}\binom{2j-1}{j}\right\}$$

$$=H[2l+2]$$

lo que prueba la fórmula en el caso general.

El grado de $H[2l+i-1]$ es $k-l$, con lo que $H[2k-1]$ tiene grado 0. Ahora, podemos aplicar el Lema 2.2 para obtener

$$|R(H[m],H[m+1])|=A_{m+1}\beta_m^{-deg(H[m+1])}\,|R(H[m+1],H[m+2])|\,,$$

donde A_m es el valor absoluto del coeficiente del término de mayor grado en $H[m]$, y $H[m+2]=\beta_m H[m]+\gamma_m H[m+1]$ segun (2.8), ya que β_m y γ_m están en las condiciones de dicho lema. Por tanto

$$|R(H[0],H[1])|=$$

$$\left\{\prod_{m=1}^{k-1}A_{2m}A_{2m-1}\prod_{j=0}^{k-2}(\beta_{2j}\beta_{2j+1})^{-(k-j-1)}\right\}|R(H[2k-2],H[2k-1])|\,.$$

Ahora bien, como

$$A_{2m}A_{2m-1}=\frac{(k-1)!^2(k-l)}{\binom{2k-2}{k}^2(k-l)!^2}\binom{2k-2l-1}{k-l}\binom{2k-2l}{k-l},$$

obtenemos

$$\prod_{m=1}^{k-1}A_{2m}A_{2m-1}=\frac{(k-1)^2}{2^{k-1}}\frac{(k-1)!^{2k-4}}{\binom{2k-2}{k}^{2k-2}(k-2)!}\prod_{m=2}^{k-3}\frac{1}{(m!)^2}\prod_{m=1}^{k-1}\binom{2j}{j}^2.$$

Por otra parte, $\beta_0 = k$, $\beta_1 = 1$, $\beta_2 = k-1$, y para $i \in \{0,1\}$, $2 \leq j < k$

$$\beta_{2j+i-1} = k - j,$$

de esta forma

$$\prod_{j=0}^{k-2} (\beta_{2j}\beta_{2j+1})^{-(k-j-1)} = \frac{\prod_{j=2}^{k-3} (j!)^2}{k^{(k-1)}(k-1)^{(k-2)}(k-2)!^{2k-5}}.$$

Además, sabemos que $\deg(H[2k-2]) = 1$, $\deg(H[2k-1]) = 0$ por lo que

$$|R(H[2k-2], H[2k-1])| = |H[2k-1]| = \frac{(k-1)!}{\binom{2k-2}{k}}.$$

Multiplicando las tres últimas ecuaciones, obtenemos

$$\Delta^2(H) = |R(H[0], H[1])| = \frac{(k-1)^{k+1}(k-2)! \prod_{m=1}^{k-1} \binom{2m}{m}^2}{(2k)^{(k-1)} \binom{2k-2}{k}^{2k-1}}.$$

Sólo falta probar el Lema 2.2:

Demostración del Lema 2.2:

Supongamos que los polinomios f, g, y h, tienen como matrices asociadas $A = (a_{i,j})$, $B = (b_{i,j})$, y $C = (c_{i,j})$ respectivamente. En principio, podemos deducir fácilmente, a partir de la definición de resultante,

$$R(f,g) = (-1)^{nm} R(g,f),$$
$$R(f,cg) = c^n R(f,g)$$

Ahora, sumando β veces la $(n-m-l+i)$-ésima fila de $B_{n\times\{n+m\}}$ a la i-ésima fila de $A_{m\times\{m+n\}}$, para $i = 1, \cdots, m$, obtenemos

$$R(f(x), g(x)) = det \begin{pmatrix} A_{m\times\{m+n\}} \\ B_{n\times\{n+m\}} \end{pmatrix} = det \begin{pmatrix} \hat{C}_{m\times\{m+n\}} \\ B_{n\times\{n+m\}} \end{pmatrix}$$

donde $\hat{C} = (\hat{c}_{i,j})$ tiene coeficientes

$$\begin{aligned} \hat{c}_{i,j} =& a_{i,j} + \beta b_{(n-m-l+i),j} = a_{n-j+i} + \beta b_{m-j+n-m-l+i} = \\ =& a_{n-j+i} + \beta b_{n-j+i-l} = c_{n-j+i} = c_{i,j}. \end{aligned}$$

Además $c_n = c_{n-1} = \cdots = c_{r+1} = 0$. Esto implica que el determinante tiene su primera columna de la siguiente forma

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ b_m \\ 0 \\ \vdots \\ 0 \end{pmatrix} ,$$

con lo que, si lo desarrollamos por su primera columna obtenemos, salvo el signo, b_m veces otro determinante con primera columna de la misma forma, y con la misma propiedad. Este proceso puede ser iterado $n-r$ veces y conseguir finalmente

$$|R(f,g)| = \pm b_m^{n-r} det \begin{pmatrix} C_{m\times\{m+r\}} \\ B_{r\times\{r+m\}} \end{pmatrix} = \left|b_m^{n-r} R(h,g)\right| = \left|b_m^{n-r} R(g,h)\right| ,$$

que completa la demostración del Lema 2.2, con lo que, el Lema 2.1 queda probado.

Observación: A las raíces del polinomio $H(x)$ se les suele llamar los números de Fekete de orden n, y están relacionados con el diámetro transfinito del intervalo $[0,1]$. Dicha cantidad se define como

$$D = \lim_{k\to\infty} \max \prod_{i<j} (\delta_j - \delta_i)^{2/k(k-1)} ,$$

y es bien conocido que

$$D = \frac{1}{4}.$$

Del Lema 2.1 se obtiene una nueva prueba de este hecho. En efecto, no hay más que observar (2.2) para obtener

$$D = \lim_{k\to\infty} \left(\frac{\prod_{m=1}^{k-2} m!}{C_k} \right)^{2/k(k-1)} ,$$

y tener en cuenta las fórmulas (A.1) y (A.2) del apéndice al final del capítulo. Para referencias ver [**F**] y el capítulo 11 de [**P**].

Despues del Lema 2.1, falta dar una cota inferior a N_A para terminar la prueba del Teorema 2.1.

LEMA 2.3.

$$\min\left(N_A\right) \geq \prod_{m=1}^{k-2} m!,$$

donde el mínimo se toma sobre todos los conjuntos A de k enteros distintos.

DEMOSTRACIÓN:

Dado un conjunto de enteros A, por (2.3) se tiene

$$N_A = \frac{[a_1, \cdots, a_k] \prod_{1 \leq i < j \leq k}(a_j - a_i)}{\prod_{i=1}^{k} a_i}. \tag{2.9}$$

Para un primo p fijo, y un número racional a/b, definimos $v_p\left(a/b\right)$ como en el Teorema 1.1.

Observamos que

$$\min\left(N_A\right) = \min\left(\prod_p p^{v_p(N_A)}\right) \geq \prod_p \min\left(p^{v_p(N_A)}\right). \tag{2.10}$$

De hecho veremos que se alcanza la igualdad. Por tanto vamos a estudiar N_A para cada primo fijo p.

Para evaluar $v_p\left(N_A\right)$ tenemos que saber cuál es la mayor potencia de p que divide a las diferencias de los números. Será conveniente para ello hacer la siguiente definición

DEFINICIÓN 2.1.

Dado un primo p, y un conjunto de k enteros $A = \{a_1, \cdots, a_k\}$, llamamos

$$A_{i,t} = \left\{a \in A \,:\, a \equiv ip^t \left(\mathrm{mod}\ p^{t+1}\right)\right\} \quad \text{para cada} \quad 1 \leq i \leq p-1,\ t \geq 0$$

y $\qquad \alpha_{i,t} = \#\left\{a \in A_{i,t}\right\}.$

Observar que $\sum_{i,t} \alpha_{i,t} = k$, donde la suma recorre los $1 \leq i \leq p-1$, y $t \geq 0$. Además, sea

$$\sigma_t = \sum_{\substack{u \geq t \\ 1 \leq i \leq p-1}} \alpha_{i,u} = \# \left\{ a \in A \, : \, p^t | a \right\}$$

Con esta definición podemos probar

PROPOSICIÓN 2.1.

(2.11)

$$v_p\left(N_A\right) = \sum_{t \geq 1} \binom{\sigma_t - 1}{2} + \sum_{\substack{t \geq 0 \\ 1 \leq l \leq p-1}} \left\{ \binom{\alpha_{l,t}}{2} + v_p \left(\prod_{a_j \neq a_i \in A_{l,t}} \left(\frac{a_j - a_i}{p^{t+1}} \right) \right) \right\}$$

DEMOSTRACIÓN:

Ordenamos los elementos $a_i \in A$ como en el Teorema 1.1, es decir, si llamamos $t_i = v_p\left(a_i\right)$, entonces $t_i \leq t_j$ siempre que $i \leq j$. Así, por (2.9)

$$v_p\left(N_A\right) = v_p\left(\left[a_1, \cdots, a_k\right]\right) + v_p \left(\prod_{1 \leq i < j \leq k} \left(a_j - a_i\right) \right) - v_p \left(\prod_{i=1}^{k} a_i \right).$$

Ahora $v_p\left(\left[a_1, \cdots, a_k\right]\right) = t_k$ y

$$v_p \left(\prod_{i=1}^{k} a_i \right) = \sum_{i=1}^{k} t_i.$$

Además, $p^{t_i} | \left(a_j - a_i\right)$ por lo que podemos escribir

$$v_p \left(\prod_{1 \leq i < j \leq k} \left(a_j - a_i\right) \right) = \sum_{1 \leq i < j \leq k} t_i + v_p \left(\prod_{1 \leq i < j \leq k} \left(\frac{a_j - a_i}{p^{t_i}} \right) \right).$$

Observar que $v_p\left(\left(a_j - a_i\right)/p^{t_i}\right) \geq 0$ y sólo es distinto de cero en caso de que $a_j \equiv a_i \left(\bmod\, p^{t_i+1}\right)$; en otras palabras, sólo cuando a_j, a_i, pertenezcan al mismo conjunto $A_{l,t}$, y en ese caso $p^{t_i+1} | \left(a_j - a_i\right)$, y se tiene $v_p\left(\left(a_j - a_i\right)/p^{t_i}\right) = 1 + v_p\left(\left(a_j - a_i\right)/p^{t_i+1}\right) \geq 1$. Además

$$\sum_{1 \leq i < j \leq k} t_i = \sum_{i=1}^{k-1} t_i \sum_{i < j \leq k} 1 = \sum_{i=1}^{k-1} t_i(k-i).$$

Todo esto nos da

$$v_p(N_A) = \sum_{i=1}^{k-1} t_i(k-i-1) + \sum_{\substack{t\geq 0\\ 1\leq l\leq p-1}} \left\{ \binom{\alpha_{l,t}}{2} + v_p\left(\prod_{a_j \neq a_i \in A_{l,t}} \left(\frac{a_j - a_i}{p^{t+1}} \right) \right) \right\}.$$

Ahora, por la definición de σ_t vemos que si $i > k - \sigma_t$ entonces $t_i \geq t$, y por tanto, para $k - \sigma_{t_j} < i \leq k - \sigma_{t_{j+1}}$, se tiene $t_i = t_j$. De esta forma, si r es el menor entero tal que $t_{k-1} = t_r$, deducimos

$$\begin{aligned}\sum_{i=1}^{k-1} t_i(k-i-1) =& \sum_{j=1}^{r-1} t_j \sum_{k-\sigma_{t_j}+1 \leq i \leq k-\sigma_{t_{j+1}}} (k-i-1) + t_r \sum_{k-\sigma_{t_r}+1\leq i\leq k-1} (k-i-1)\\ =& \sum_{j=1}^{r-1} \left(t_j \sum_{\sigma_{t_{j+1}}-1\leq i\leq \sigma_{t_j}-2} i \right) + t_r \sum_{1\leq i\leq \sigma_{t_r}-2} i.\end{aligned}$$

Teniendo en cuenta que

$$\sum_{1\leq i\leq n-2} i = \binom{n-1}{2},$$

y que por ello

$$\sum_{\sigma_{t_{j+1}}-1\leq i\leq \sigma_{t_j}-2} i = \binom{\sigma_{t_j}-1}{2} - \binom{\sigma_{t_{j+1}}-1}{2},$$

un simple argumento nos permite concluir

$$\sum_{i=1}^{k-1} t_i(k-i-1) = \sum_{j=1}^{r} (t_j - t_{j-1}) \binom{\sigma_{t_j}-1}{2},$$

donde hemos llamado $t_0 = 0$. Ahora, $\sigma_t = \sigma_{t_j}$ para $t_{j-1} < t \leq t_j$, $\sigma_t = 0$ si $t > t_k$, y si $t_k > t_r$ entonces $\sigma_{t_k} = 1$. Así, la última suma es

$$= \sum_{t\geq 1} \binom{\sigma_t - 1}{2},$$

que completa la demostración de la proposición.

Corolario 2.2. *N_A es un entero*

De nuestra prueba se deduce que $v_p(N_A) \geq 0$ para todo primo p. Esto demuestra el resultado, ya que cualquier racional con esa propiedad, es de hecho un entero.

Observación: Si $p \geq k-1$, podemos[3] escoger A tal que $\sigma_1 \leq 2$ y $\alpha_{i,t} \leq 1$ para todo $\{i,t\}$, con lo que $v_p(N_A)=0$. Por tanto, a partir de ahora, si no se indica lo contrario, nos restringiremos a $p<k-1$. De otra forma, los resultados serían triviales.

Por la fórmula (2.11), vemos que para entender $v_p(N_A)$ debemos saber que sucede en cada clase $A_{i,t}$. Necesitaremos el siguiente

LEMA 2.4. *Para cualesquiera $m+1$ enteros $g_0, g_1, \cdots, g_m$ y un primo, p, podemos encontrar g_j tal que*

$$v_p\left(\prod_{\substack{0\leq i\leq m\\ i\neq j}} (g_j-g_i)\right) \geq v_p(m!).$$

DEMOSTRACIÓN:

Vamos a probar el resultado por inducción en m. Para $m \leq p-1$ el resultado es trivial. Así, supongamos $m \geq p$. Por el principio del palomar, existe a, $0 \leq a \leq p-1$ tal que

$$\#\{j \,:\, g_j \equiv a \,(\mathrm{mod}\ p)\} \geq \left[\frac{m}{p}\right]+1.$$

Sea $h_j=(g_j-a)/p$ para cada uno de esos j. Si están todos los $m+1$ enteros, entonces

$$v_p\left(\prod_{1\leq i\leq m} (g_0-g_i)\right) = v_p\left(\prod_{1\leq i\leq m} p(h_0-h_i)\right) \geq m \geq v_p(m!).$$

En otro caso, por la hipótesis de inducción, existe $g_j \equiv a\,(\mathrm{mod}\ p)$ tal que

$$v_p\left(\prod_{\substack{0\leq i\leq m\\ i\neq j}} (g_j-g_i)\right) = v_p\left(\prod_{\substack{0\leq i\leq m\\ g_i\equiv a (\mathrm{mod}\ p)\\ i\neq j}} p(h_j-h_i)\right) \geq \left[\frac{m}{p}\right] + v_p\left(\left[\frac{m}{p}\right]!\right);$$

[3] Por ejemplo $a_k \equiv 2p\left(\mathrm{mod}\ p^2\right)$, $a_i \equiv i\,(\mathrm{mod}\ p)$ para $i=1,\cdots,k-1$.

pero entonces el resultado se sigue de

$$v_p(m!) = \sum_{l\geq 1}\left[\frac{m}{p^l}\right] = \left[\frac{m}{p}\right] + v_p\left(\left[\frac{m}{p}\right]!\right).$$

Este lema tiene una bonita consecuencia.

COROLARIO 2.3. *Sean $g_1, g_2, \cdots, g_n$, n enteros, entonces*

$$\prod_{1\leq i<j\leq n}\left(\frac{g_j-g_i}{j-i}\right)$$

es también un entero.

DEMOSTRACIÓN:

Procedemos por inducción. El resultado es trivial para $n=2$, así, supongamos que es cierto para $n-1$ términos. Sea p un primo, y escojamos g_r mediante el Lema 2.4 (con $m=n-1$) para obtener

$$v_p\left(\prod_{1\leq i<j\leq n}\left(\frac{g_j-g_i}{j-i}\right)\right) =$$

$$= v_p\left(\frac{\prod_{i,j\neq r}(g_j-g_i)}{\prod(j-i)}\right) + v_p\left(\frac{\prod_{i\neq r}(g_r-g_i)}{(n-1)!}\right) \geq 0+0=0,$$

usando la hipótesis de inducción y el Lema 2.4, respectivamente. Esto nos da el resultado como en el Corolario 2.2.

Ya tenemos la maquinaria suficiente para probar

PROPOSICIÓN 2.2. *Existe un conjunto $A = \{a_1, a_2, \cdots, a_k\}$ de enteros con $v_p(N_A)$ minimal, tal que*

(i) $\alpha_{i,t} \geq \alpha_{I,T}$ *si* $t \leq T$

(ii) Para cada $1 \leq i \leq p-1$ *y* $t \geq 0$ *se tiene*

$$A_{i,t} = \left\{ip^t,\ ip^t+p^{t+1},\ ip^t+2p^{t+1}, \cdots, ip^t+(\alpha_{i,t}-1)p^{t+1}\right\}$$

(iii) Podemos elegir a_{k+1} tal que $\hat{A} = A\bigcup\{a_{k+1}\}$ tiene $v_p\left(N_{\hat{A}}\right)$ minimal sobre los conjuntos de $k+1$ enteros, y para el cual se cumple (i) y (ii).

DEMOSTRACIÓN:

(i) A lo largo de la prueba, supondremos que tenemos un conjunto A de k enteros con $v_p(N_A)$ mínimo. Supongamos que

$$A_{i,t} = \left\{ip^t + g_j p^{t+1} \,:\, 1 \le j \le \alpha_{i,t}\right\} \quad \text{y}$$
$$A_{I,T} = \left\{Ip^T + G_J\, p^{T+1} \,:\, 1 \le J \le \alpha_{I,T}\right\},$$

con $\alpha_{i,t} < \alpha_{I,T}$ y $t \le T$. Sea B idéntico a A excepto con $A_{i,t}$ y $A_{I,T}$ reemplazados por

$$B_{i,t} = \left\{ip^t + G_J\, p^{t+1} \,:\, 1 \le J \le \alpha_{I,T}\right\} \quad \text{y}$$
$$B_{I,T} = \left\{Ip^T + g_j p^{T+1} \,:\, 1 \le j \le \alpha_{i,t}\right\}.$$

Por la Proposición 2.1, se tiene, haciendo $\sigma'_v = \sigma_v - \alpha_{I,T}$ para $t < v \le T$,

$$v_p(N_B) - v_p(N_A) = \sum_{t<v\le T} \left\{ \binom{\sigma'_v + \alpha_{i,t} - 1}{2} - \binom{\sigma'_v + \alpha_{I,T} - 1}{2} \right\} \le 0,$$

que nos lleva a una contradicción.

Observar que si $t = T$, entonces $v_p(N_B) - v_p(N_A) = 0$ y por tanto podemos reordenar los conjuntos $A_{i,t}$ con t fijo para que $\alpha_{i,t}$ sea decreciente también en i.

Antes de seguir con (ii) y (iii), hagamos la siguiente

DEFINICIÓN 2.2. *Para un conjunto de k enteros, $A = \{a_1, a_2, \cdots, a_k\}$, y un entero, $a_{k+1} \equiv i_0 p^{t_0} \left(\mathrm{mod}\, p^{t_0+1}\right)$, consideramos el conjunto $\hat{A} = A \bigcup \{a_{k+1}\}$ con $\hat{\sigma}_t$, $\hat{\alpha}_{i,t}$ los números correspondientes a $\hat{A}$ en la Definición 2.1. Además llamaremos*

$$D_{a_{k+1}} = v_p\left(N_{\hat{A}}\right) - v_p(N_A).$$

Por la fórmula (2.11) se tiene

$$D_{a_{k+1}} = \sum_{1\le t\le t_0} (\hat{\sigma}_t - 2) + v_p\left(\prod_{a_j \in A_{i_0,t_0}} \frac{(a_{k+1} - a_j)}{p^{t_0+1}}\right) + \hat{\alpha}_{i_0,t_0} - 1. \tag{2.12}$$

Para probar (ii) y (iii) procederemos por inducción en k. La proposición es claramente cierta para $k = 2$, y la suponemos cierta hasta k. Ahora, supongamos que tenemos $A = \{a_1, a_2, \cdots, a_k\}$ con $v_p(N_A)$ mínimo, y satisfaciendo (i) y (ii); y B un conjunto de $k+1$ enteros con $v_p(N_B)$ mínimo y $\beta_{i,t}$, η_t sus correspondientes números en la Definición 2.1. Entonces, consideramos el par (i_0, t_0) para el cual $\beta_{i_0,t_0} > \alpha_{i_0,t_0}$ y $\beta_{i,t} \leq \alpha_{i,t}$ para todo par (i,t) tal que $t \leq t_0$, o si $t = t_0$ entonces $i < i_0$. Sea b_0 un elemento de B_{i_0,t_0} para el cual

$$D_{b_0} = \max_{b \in B_{i_0,t_0}} D_b.$$

(Aquí hemos usado la Definición 2.2 con $A = B \setminus \{b\}$ y $\hat{A} = B$, para cada b). Entonces, por (2.12) con esta elección particular de b_0 como a_{k+1}, y el Lema 2.4 obtenemos

$$D_{b_0} \geq \sum_{1 \leq t \leq t_0} (\eta_t - 2) + v_p\left((\beta_{i_0,t_0} - 1)!\right) + \beta_{i_0,t_0} - 1,$$

ya que, escribiendo $b = i_0 p^{t_0} + g p^{t_0+1}$ para todo b en B_{i_0,t_0}, $b_0 = i_0 p^{t_0} + g_0 p^{t_0+1}$, se tiene

$$v_p\left(\prod_{b_0 \neq b \in B_{i_0 t_0}} \frac{(b_0 - b)}{p^{t_0+1}}\right) = v_p\left(\prod_{b_0 \neq b \in B_{i_0,t_0}} (g_0 - g)\right).$$

Por otro lado, eligiendo $a_{k+1} = i_0 p^{t_0} + (\alpha_{i_0,t_0} + 1)p^{t_0+1}$, tenemos para $\hat{A} = A \bigcup \{a_{k+1}\}$

$$D_{a_{k+1}} = \sum_{1 \leq t \leq t_0} (\sigma_t - 1) + v_p\left(\alpha_{i_0,t_0}!\right) + \alpha_{i_0,t_0},$$

donde hemos usado que, en ese caso, $\hat{\sigma}_t = \sigma_t + 1$ cuando $t \leq t_0$ y $\hat{\alpha}_{i_0,t_0} = \alpha_{i_0,t_0} + 1$. Y por tanto, como, para $t \leq t_0$

$$\sigma_t = k - \sum_{\substack{1 \leq u < t \\ 1 \leq i \leq p-1}} \alpha_{i,u} < k + 1 - \sum_{\substack{1 \leq u < t \\ 1 \leq i \leq p-1}} \beta_{i,u} = \eta_t,$$

obtenemos

$$D_{a_{k+1}} \leq D_{b_0}.$$

De esta forma,

$$v_p\left(N_B\right) = v_p\left(N_{B\setminus\{b_0\}}\right) + D_{b_0} \geq v_p\left(N_A\right) + D_{a_{k+1}} = v_p\left(N_{\hat{A}}\right).$$

$\hat{A}$ tiene $v_p\left(N_{\hat{A}}\right)$ mínimo y satisface (ii). Por tanto, quizás debamos aplicar el proceso en (i) para conseguir que nuestro conjunto tenga $\alpha_{i,t}$ decreciente, y terminar la demostración.

De la prueba de la Proposición 2.2, podemos deducir que para cada primo $p \leq k-1$, existe un entero u_p tal que si A es un conjunto de k enteros como en la proposición, y tomamos $\hat{A} = A \bigcup \{a_{k+1}\}$ donde

$$a_{k+1} \equiv u_p \left(\mathrm{mod}\ p^{E(k,p)}\right) \quad \text{con} \quad E(k,p) = 2\left[\frac{k}{p-1}\right], \tag{2.13}$$

entonces $\hat{A}$ es como en la proposición. En efecto, vemos, por la definición de D_a, que para $\hat{A}$ podemos elegir cualquier $\tilde{a}_{k+1} \equiv a_{k+1} \left(\mathrm{mod}\ p^E\right)$ para E suficientemente grande, y el valor de $v_p\left(N_{\hat{A}}\right)$ no varía. Para encontrar un E particular en esas condiciones, necesitamos $v_p\left(\hat{a}_{k+1} - a_j\right) = v_p\left(a_{k+1} - a_j\right)$ para cualquier j. Se puede probar que $E(k,p)$ es suficientemente grande usando que A es como en la Proposición 2.2.

Entonces, por el Teorema chino del resto, deducimos la existencia de k enteros $r_1, r_2, \cdots, r_k$ tal que si $A = \{a_1, \cdots, a_k\}$ con

$$a_i \equiv r_i \left(\mathrm{mod}\ P_l\right),$$

donde $P_l = \prod_{p \leq l} p^{E(k,p)}$, entonces $v_p\left(N_A\right)$ es mínimo para todo $p \leq l$.

En el siguiente lema veremos que, de hecho, cada $r_i = i - 1$.

LEMA 2.5. *Si $A = \{a_1, \cdots, a_k\}$ con $0 < a_i \equiv i-1\,(\mathrm{mod}\ P_l)$, para $1 \leq i \leq k$ entonces $v_p\left(N_A\right)$ es mínimo para todo $p \leq l$.*

DEMOSTRACIÓN:

Procederemos por inducción en k. El resultado es claramente cierto para $k = 2$. Sea $p \leq l$, y supongamos que $A = \{0, \cdots, k-1\}$ tiene $v_p\left(N_A\right)$ minimal. Después de la Proposición 2.2, lo único que nos falta probar es que para

$\hat{A} = A \bigcup \{a_{k+1}\}$, se tiene

$$D_{a_{k+1}} \geq D_k.$$

Escribimos k en base p como $k = \sum_{i=r}^{R} \kappa_i p^i$ con $\kappa_r, \kappa_R \neq 0$. Entonces, se tiene[4]

$$\sum_{1 \leq i \leq p-1} \alpha_{i,t} = (p-1)\left[\frac{k}{p^{t+1}}\right] + \kappa_t \quad \text{si } t \neq r, R;$$
$$\sum_{1 \leq i \leq p-1} \alpha_{i,r} = (p-1)\left[\frac{k}{p^{r+1}}\right] + \kappa_r - 1;$$
$$\sum_{1 \leq i \leq p-1} \alpha_{i,R} + \alpha_{1,R+1} = \kappa_R + 1;$$

y por tanto $\sigma_t = \left[\frac{k}{p^t}\right]$ si $t \leq r$, y $\sigma_t = \left[\frac{k}{p^t}\right] + 1$ si $t > r$. Entonces, observando que $\alpha_{\kappa_r,r} = \left[\frac{k}{p^{r+1}}\right]$, obtenemos

$$D_k = \sum_{1 \leq t \leq r} (\sigma_t - 1) + v_p\left(\left[\frac{k}{p^{r+1}}\right]!\right) + \left[\frac{k}{p^{r+1}}\right] = -r + \sum_{t \geq 1} \left[\frac{k}{p^t}\right].$$

Por otra parte, si $a_{k+1} \equiv i_0 p^{t_0} \left(\text{mod } p^{t_0+1}\right)$, entonces, como $\alpha_{i,t} \geq \left[\frac{k}{p^{t+1}}\right]$, obtenemos para $t_0 \geq r$,

$$\begin{aligned} D_{a_{k+1}} &\geq \sum_{1 \leq t \leq r} \left(\left[\frac{k}{p^t}\right] - 1\right) + \sum_{r < t \leq t_0} \left[\frac{k}{p^t}\right] + v_p\left(\left[\frac{k}{p^{t_0+1}}\right]!\right) + \left[\frac{k}{p^{t_0+1}}\right] = \\ &= -r + \sum_{t \geq 1} \left[\frac{k}{p^t}\right] = D_k; \end{aligned}$$

mientras que para $t_0 < r$,

$$\begin{aligned} D_{a_{k+1}} &\geq \sum_{1 \leq t \leq t_0} \left(\left[\frac{k}{p^t}\right] - 1\right) + \sum_{t_0 < t \leq r} \left[\frac{k}{p^t}\right] + v_p\left(\left[\frac{k}{p^{t_0+1}}\right]!\right) + \left[\frac{k}{p^{t_0+1}}\right] = \\ &= -t_0 + \sum_{t \geq 1} \left[\frac{k}{p^t}\right] > D_k. \end{aligned}$$

Que demuestra el resultado para cualquier primo p dado. No hay más que aplicar el teorema chino del resto para completar la prueba del Lema 2.5.

[4]Esto es verdad para una elección particular del elemento congruente con $0(\text{mod } p)$, sin embargo, por la Proposición 2.2, el resultado es cierto para cualquier elección de ese elemento.

El Lema 2.3 entonces se sigue de (2.10) ya que, para este particular conjunto A, tenemos

$$v_p\left(N_A\right) = v_p\left(\prod_{m=1}^{k-2} m!\right).$$

Este hecho termina la prueba del Teorema 2.1.

∎

§ 3 <u>Demostración de los Teoremas 2.2 y 2.3</u>

Para probar el Teorema 2.2 mostraremos, en primer lugar, que de hecho la igualdad se cumple en el Lema 2.3, en otras palabras, por el Lema 2.5, con $l = k-2$

$$\min \prod_{p \leq k-2} p^{v_p(N_A)} = \prod_{p \leq k-2} p^{v_p\left(\prod_{m=1}^{k-2} m!\right)}.$$

Así, por (2.10), necesitamos encontrar un conjunto A de k enteros como en el Lema 2.5 y tal que $v_p\left(N_A\right) = 0$ para $p > k-2$. Además, si queremos conseguir la cota exacta en el Teorema 2.2, este conjunto debe maximizar (2.4) al mismo tiempo.

Empecemos con

LEMA 2.6.

$$\min(N_A) = \prod_{m=1}^{k-2} m!,$$

DEMOSTRACIÓN:

Supongamos que tenemos un conjunto de $k-1$ enteros $A = \{a_1, \cdots, a_{k-1}\}$, con $a_i \equiv i-1 \pmod{P_{k-2}}$ y $N_A = \prod_{m=1}^{k-3} m!$. Entonces, para probar el Lema 2.6, tenemos que encontrar $a_k \equiv k-1 \pmod{P_{k-2}}$ y tal que para $\hat{A} = A \bigcup \{a_k\}$, $v_p\left(N_{\hat{A}}\right) = 0$ para todo $p \geq k-1$. Consideramos un primo $p \geq k-1$. Por la observación despues de la Proposición 2.1, sabemos como elegir las clases de congruencia $\hat{A}_{i,t}$, para que $v_p\left(N_{\hat{A}}\right) = 0$ y vemos que esta elección es equivalente a

$$(*) \qquad v_p\left((a_i, a_j, a_l)\right) = 0$$

$$(**) \qquad v_p\left(a_j - a_i\right) = v_p\left((a_j, a_i)\right)$$

donde $i < j < l \leq k$.

Si llamamos $d_{j,i} = a_j - a_i$, y escribimos

$$d_{j,i} = \delta_{j,i}\mu_{j,i} \tag{2.14}$$

donde $\delta_{j,i}$ es[5] el mayor divisor de $d_{j,i}$ primo con P_{k-2}, para que se cumpla (*) es suficiente con que

$$(\delta_{j,i}, \delta_{l,i}) = 1, \tag{2.15}$$

ya que si $p|(a_i, a_j, a_l)$ entonces divide a sus diferencias. Por otra parte, como $v_p\left(\delta_{j,i}\right) = v_p\left(a_j - a_i\right)$, para cumplir (**) debemos tener $v_p\left(\delta_{j,i}\right) = v_p\left((a_j, a_i)\right)$, para todo primo $p \geq k-1$, que es equivalente a

$$\delta_{j,i}|a_i, \tag{2.16}$$

para $j = i+1, \cdots, k$. En resumen, para obtener el resultado en el Lema 2.6, tenemos que encontrar k enteros que cumplan (2.15) y (2.16).

Una vez que tenemos un método para probar el Lema 2.6, si queremos probar el Teorema 2.2 todavía necesitamos que los números, $a_1, \cdots a_k$, estén distribuidos de cierta forma sobre el intervalo, para que (2.4) sea máximo. Probaremos ambas cosas, es decir, el Lema 2.6 y el Teorema 2.2, gracias al siguiente lema de criba:

LEMA 2.7. *Sean $d_1 < d_2 < \cdots < d_s$, u, enteros, $P = \prod_{p \leq l} p^{m_p}$ donde el producto recorre los primos p menores o iguales que l, y m_p son números enteros. Considerar un intervalo I, y sea*

$$R_n = \left\{r \in I \,:\, r \equiv u \,(mod\ P)\ ,\ (r - d_i, n) = 1\ ,\ i = 1, \cdots, s\right\},$$

[5] Se deduce de la definición de P_{k-2}, que de hecho $\mu_{j,i} = (d_{j,i}, P_{k-2})$

para cualquier entero n.

Si n es tal que $(n, P) = 1$, entonces

$$\#R_n = \frac{|I|}{P} \prod_{p|n} \left(1 - \frac{\Delta(p)}{p}\right) + O\left(d^{s}(n)\right),$$

donde $\Delta(m) = \#\{a \,:\, d_i \equiv a \,(\mathrm{mod}\; m)\}$ y $d(n)$ es la función divisor.

DEMOSTRACIÓN:

Escribimos $n = \nu_1 \nu_2$, donde ν_1 es el mayor divisor de E tal que

$$\left(\nu_1, \prod_{1 \leq i < j \leq s} (d_j - d_i)\right) = 1.$$

Entonces, $(r - d_i, E) = 1$ es lo mismo que $(r - d_i, \nu_1) = 1$ y $(r - d_i, p) = 1$, para todo $p|\nu_2$. Además, sean $D_{1,p}, D_{2,p}, \cdots, D_{\Delta(p),p}$, aquellos valores modulo p, que son congruentes con algun d_j. Cuando $d_j \equiv d_i \,(\mathrm{mod}\; p)$, entonces $p|(r - d_j)$ si y sólo si $p|(r - d_i)$, por lo que se tiene

$$\{r \,:\, (r - d_i, p) = 1\,,\, i = 1, \cdots, s\} = \{r \,:\, (r - D_{i,p}, p) = 1\,,\, i = 1, \cdots, \Delta(p)\},$$

y por tanto

$$R_n = R_{\nu_1} \bigcap_{p|\nu_2} \{(r - D_{i,p}, p) = 1\,,\, i = 1, \cdots, \Delta(p)\}.$$

Usando la función de Möbius, $\mu(n)$, que cumple[6]

$$\sum_{d|n} \mu(d) = \begin{cases} 0 & \text{if } n \neq 1 \\ 1 & \text{if } n = 1 \end{cases}$$

Podemos escribir

$$\#R_n = \sum_{r \in R_n} 1 = \sum_{\substack{r \in I \\ r \equiv u (\mathrm{mod}\; P)}} \prod_{j=1}^{s} \sum_{m_{j,\nu_1} | (r - d_j, \nu_1)} \mu(m_{j,\nu_1}) \prod_{p|\nu_2} \prod_{i=1}^{\Delta(p)} \sum_{m_{i,p} | (r - D_{i,p}, p)} \mu(m_{i,p}).$$

[6]Ver **[H-W]**

Para cualesquiera conjuntos finitos A_i, $i = 1, \cdots, t$, y $f(n)$ una función, se tiene

$$\prod_{i=1}^{t} \sum_{m_i \in A_i} f(m_i) = \sum \prod_{i=1}^{t} f(m_i), \tag{2.17}$$

donde la suma a la derecha de la igualdad recorre todas las posibles t-uplas $\{m_1, \cdots, m_t\}$ tal que $m_i \in A_i$. De esta forma, si tomamos $A_i = S_{i,l} = \{m_{i,l} : m_{i,l} | (r - d_i, l)\}$, nuestra última expresión para $\# R_n$ queda

$$= \sum_{\substack{r \in I \\ r \equiv u (\mathrm{mod}\ P)}} \sum \prod_{j=1}^{s} \mu(m_{j,\nu_1}) \sum \prod_{p|\nu_2} \prod_{i=1}^{\Delta(p)} \mu(m_{i,p}),$$

en donde, en la primera suma $m_{j,\nu_1} \in S_{j,\nu_1}$ para $j = 1, \cdots, s$, mientras que en la segunda $m_{i,p} \in S_{i,p}$ para los primos p tal que $p|\nu_2$ e $i = 1, \cdots, \Delta(p)$. Cambiando el orden de sumación, queda

$$= \sum \prod_{p|\nu_2} \prod_{i=1}^{\Delta(p)} \mu(m_{i,p}) \prod_{j=1}^{s} \mu(m_{j,\nu_1}) \sum_{r \in \mathcal{R}} 1, \tag{2.18}$$

donde, la primera suma es sobre todas las colecciones de $m_{i,p}|p$, $m_{1,\nu_1}|\nu_1$ con p recorriendo los primos $p|\nu_2$, e $i = 1, \cdots, \Delta(p)$ y $j = 1, \cdots, s$, y en la última $\mathcal{R}$ se define como

$$\mathcal{R} = \{r \in I : r \equiv u\,(\mathrm{mod}\ P)\} \bigcap_{j=1}^{s} \{r \equiv d_j\,(\mathrm{mod}\ m_{j,\nu_1})\} \bigcap_{\substack{i=1 \\ p|\nu_2}}^{\Delta(p)} \{r \equiv D_{i,p}\,(\mathrm{mod}\ m_{i,p})\}.$$

Ahora bien, como $D_{j,p} \not\equiv D_{i,p}\,(\mathrm{mod}\ p)$ si $j \neq i$, se tiene $(m_{i,p}, m_{j,p}) = 1$ para todo $p|\nu_2$, y por tanto, todos los módulos son primos entre sí, pues ν_1, ν_2 y P son primos entre sí. Así, podemos aplicar el teorema chino del resto para obtener, en la última suma

$$\sum_{r \in \mathcal{R}} 1 = \frac{|I|}{P \prod_{p|\nu_2} \prod_{i=1}^{\Delta(p)} m_{i,p} \prod_{j=1}^{s} m_{j,\nu_1}} + O(1).$$

Ahora bien, el número de posibles colecciones $\{m_{i,p}, m_{j,\nu_1}\}$ que sumamos en (2.18), será contar para cada primo $p|\nu_2$ todas las posibles colecciones de $\Delta(p)$

divisores de p, mientras que para ν_1 contaremos las posibles s-uplas de divisores de ν_1, por tanto, queda

$$\sum \prod_{p|\nu_2} \prod_{i=1}^{\Delta(p)} \mu(m_{i,p}) \prod_{j=1}^{s} \mu(m_{j,\nu_1}) \ll \prod_{p|\nu_2} 2^{\Delta(p)}(d(\nu_1))^s \leq d^s(n)$$

ya que $\Delta(p) \leq s$, y la función divisor es multiplicativa.

Así, para (2.18) obtenemos, usando que $\mu(n)$ es una función multiplicativa, y teniendo en cuenta que los módulos son primos entre sí,

$$= \frac{|I|}{P} \sum \frac{\mu\left(\prod_{j=1}^{s} m_{j,\nu_1}\right)}{\prod_{j=1}^{s} m_{j,\nu_1}} \prod_{p|\nu_2} \frac{\mu\left(\prod_{i=1}^{\Delta(p)} m_{i,p}\right)}{\prod_{i=1}^{\Delta(p)} m_{i,p}} + O\left(d^s(n)\right),$$

y por (2.17)

$$= \frac{|I|}{P} \sum \frac{\mu\left(\prod_{j=1}^{s} m_{j,\nu_1}\right)}{\prod_{j=1}^{s} m_{j,\nu_1}} \prod_{p|\nu_2} \sum \frac{\mu\left(\prod_{i=1}^{\Delta(p)} m_{i,p}\right)}{\prod_{i=1}^{\Delta(p)} m_{i,p}} + O\left(d^s(n)\right),$$

donde, en la primera suma $m_{j,\nu_1}|\nu_1$, $j = 1, \cdots, s$ y en la segunda, $m_{i,p}|p$, $i = 1, \cdots, \Delta(p)$ para cada $p|\nu_2$.

Teniendo en cuenta de nuevo que los módulos son primos entre sí, observamos que para $M_p = (\prod_{i=1}^{\Delta(p)} m_{i,p})$ y $M = (\prod_{j=1}^{s} m_{j,\nu_1})$, se tiene $M_p|p$ y $M|\nu_1$, con lo que nos queda

$$= \frac{|I|}{P} \left(\sum_{M|\nu_1} \frac{\mu(M)}{M} \sum_{m_1 \cdots m_s = M} 1 \right) \prod_{p|\nu_2} \left(\sum_{M_p|p} \frac{\mu(M_p)}{M_p} \sum_{m_1 \cdots m_{\Delta(p)} = M_p} 1 \right) + \\ + O\left(d^s(n)\right).$$

Ahora, si M es libre de cuadrados, entonces

$$\sum_{m_1 \cdots m_t = M} 1 = \prod_{p|M} t$$

y por tanto,

$$f_t(N) = \sum_{M|N} \frac{\mu(M)}{M} \sum_{m_1 \cdots m_t = M} 1 = \sum_{M|N} \mu(M) \prod_{p|M} \frac{t}{p}$$
$$= \prod_{p|N} \left(1 - \frac{t}{p}\right).$$

La última igualdad se puede verificar directamente haciendo la multiplicación. Esto termina la prueba del Lema (2.7).

COROLARIO 2.4. *Dado un entero k, para todo $\varepsilon > 0$ existen X, L, y un conjunto de k enteros $A = \{a_1, \cdots, a_k\}$ con $X \leq a_1 < a_2 < \cdots < a_k \leq X + L$, tal que*

$$[a_1, \cdots, a_k] \leq (1+\varepsilon) C_k \frac{X^k}{L^{\binom{k}{2}}},$$

donde C_k es como en (2.2).

DEMOSTRACIÓN:

Sea $H(x)$ el polinomio en (2.7) y $0 = \eta_1 < \eta_2 < \cdots < \eta_k = 1$ sus raíces. Sea $P = \prod_{p \leq k-2} p^{E(k,p)}$, donde $E(k,p)$ es como en (2.13).

Supongamos que tenemos $j < k$ enteros, $0 = d_{1,1} < d_{2,1} < \cdots < d_{j,1}$ con $P \ll d_{2,1}$, y $d_{i,1} \equiv i - 1 \pmod{P}$, tal que

$$\frac{d_{i,1}}{d_{2,1}} = \frac{\eta_i}{\eta_2} + o(1)$$

cuando $d_{2,1} \to \infty$, y llamando $d_{i,l} = d_{i,1} - d_{l,1} = \delta_{i,l}\mu_{i,l}$ como en (2.14), se tiene

$$(\delta_{i,l}, \delta_{m,n}) = 1, \tag{2.19}$$

para $i, l, m, n \leq j$. Vamos a aplicar el Lema 2.7 con $d_i = d_{i,1}$ para $i = 1, \cdots, j$, $m_p = E(k,p)$, $l = k-2$, $u = j$, $I = \frac{\eta_{j+1}}{\eta_2} d_{2,1} \pm \sqrt{d_{2,1}}$, y $n = \prod_{1 \leq l < i \leq j} \delta_{i,l}$.

Como $p|n$ implica $p|(d_{i,1} - d_{l,1})$ para algunos i, l, y se cumple (2.19) por hipótesis, deducimos $\Delta(p) = j - 1$ para todo $p|n$. Además

$$\delta_{i,l} \leq d_{i,1} - d_{l,1} = \frac{\eta_i - \eta_l}{\eta_2} d_{2,1} + O(\sqrt{d_{2,1}}) \leq c d_{2,1}$$

para alguna constante c, por lo que

$$d(n) = d\left(\prod_{1 \leq l < i \leq j} \delta_{i,l}\right) = O(d_{2,1}^{\epsilon})$$

para todo $\epsilon > 0$.

Por otra parte

$$\prod_{p|n}\left(1-\frac{j-1}{p}\right) \geq \prod_{p\leq cd_{2,1}}\left(1-\frac{j-1}{p}\right) \sim \frac{1}{\log^{j-1}(d_{2,1})}.$$

Por tanto,

$$\sum_{r\in R_n} 1 = \frac{\sqrt{d_{2,1}}}{P}\prod_{p|n}\left(1-\frac{j-1}{p}\right) + O(d^j(n)) > \frac{d_{2,1}^{1/2-o(1)}}{P} - O\left(d_{2,1}^{\epsilon}\right) > 0,$$

si $d_{2,1} > P^{2+\epsilon}$. En ese caso, podemos elegir

$$r = d_{1+j,1} = \frac{\eta_{j+1}}{\eta_2}d_{2,1} + O(\sqrt{d_{2,1}}),$$

y tal que (2.19) se cumple para $i, l, m, n \leq j+1$. Resumiendo, si empezamos con $d_{2,1} \gg P^{2+\epsilon}$, y $d_{2,1} \equiv 1 \,(\mathrm{mod}\, P)$, y repetimos el anterior proceso $k-1$ veces, obtenemos $d_{2,1} < d_{3,1} < \cdots < d_{k,1}$ que serán las diferencias de nuestros números con el primero, a_1.

Por tanto, eligiendo $a_1 \equiv 0 \,(\mathrm{mod}\, P)$, los enteros $a_i = a_1 + d_{i,1}$, $d_{1,1} = 0$, alcanzarán el mínimo de $v_p(N_A)$ para $p \leq k-2$. Además, para ver si alcanzan ese mínimo también cuando $p \geq k-1$, tenemos que comprobar que se cumple (*) y (**), que es lo mismo que probar que $\delta_{j,i}|a_i$ para todo $1 \leq i \leq k$ y $j \geq i+1$ ya que, por el Lema 2.7, sabemos que $(\delta_{j,i}, \delta_{l,m}) = 1$. En otras palabras, necesitamos

$$a_1 + d_{i,1} = a_i \equiv 0 \left(\mathrm{mod}\ \prod_{j=i+1}^{k} \delta_{j,i}\right).$$

Como $(\delta_{j,i}, \delta_{l,m}) = (E, P) = 1$, podemos aplicar el teorema chino del resto para obtener una solución a_1 (mod EP). Por tanto, para esos k enteros, N_A tiene el valor del Lema 2.6. Además,

$$d_{2,1} = \eta_2 d_{k,1} + O(\sqrt{d_{k,1}}),$$

luego

$$a_j - a_i = \frac{\eta_j - \eta_i}{\eta_2} d_{2,1} + O(\sqrt{d_{2,1}}) = (\eta_j - \eta_i) d_{k,1} + O(\sqrt{d_{k,1}}).$$

Sea $d_{k,1} = L$. Para todo $\varepsilon' > 0$, tomando L suficientemente grande, (dependiendo de k), se tiene

$$\prod_{1 \le i < j \le k} (a_j - a_i) \ge \Delta(H) L^{\binom{k}{2}} (1 - \varepsilon')$$

donde $\Delta(H)$ es el discriminante de $H(x)$, y

$$\prod_{i=1}^{k} a_i \le X(X+L)^{k-1} = X^k + O(X^{k-1}L) \le X^k(1+\varepsilon'),$$

cuando[7] $L = o(X)$.

Así,

$$[a_1, \cdots, a_k] = \frac{\prod_{i=1}^{k} a_i}{\prod_{1 \le i < j \le k} (a_j - a_i)} N_A \le (1+\varepsilon) C_k \frac{X^k}{L^{\binom{k}{2}}}$$

para

$$\varepsilon > \frac{2\varepsilon'}{1-\varepsilon'},$$

lo que termina la prueba del Teorema 2.2.

∎

COROLARIO 2.5. *Sea $k \ge 2$ un entero fijo. Para todo $X > 0$ y para todo*

$$L < C_k^{\frac{1}{\binom{k}{2}}} \frac{X^{2-\frac{2}{k-1}}}{N^{1-\frac{2}{k-1}+\frac{1}{\binom{k}{2}}}},$$

no hay k puntos de coordenadas enteras (a_i, b_i), $i = 1, \cdots, k$ en la hipérbola $xy = N$, tales que $X \le a_1 < a_2 < \cdots < a_k \le X + L$.

Además, para todo $\varepsilon > 0$, podemos elegir N, $X \ge N^{1-\frac{1}{k-1}}$ y

$$L \le (1+\varepsilon) C_k^{\frac{1}{\binom{k}{2}}} \frac{X^{2-\frac{2}{k-1}}}{N^{1-\frac{2}{k-1}+\frac{1}{\binom{k}{2}}}},$$

[7] Esto siempre es cierto cuando $k \ge 3$ por la elección de a_1 y las diferencias entre los números.

para que haya k puntos de coordenadas enteras, (a_i, b_i), en la hipérbola tales que $X \leq a_1 < a_2 < \cdots < a_k \leq X + L$.

DEMOSTRACIÓN:

Si tenemos k puntos de coordenadas enteras (a_i, b_i), $i = 1, \cdots, k$ tales que $X \leq a_1 < a_2 < \cdots < a_k \leq X + L$, entonces $b_i | N$, y $x - l \leq b_1 < b_2 \cdots < b_k \leq x$ para $x = N/X$ y $x - l = N/(X + L)$ así, por el Teorema 2.1

$$N \geq [b_1, \cdots, b_k] \geq C_k \frac{x^k}{l^{\binom{k}{2}}},$$

o bien

$$l \geq C_k^{1/\binom{k}{2}} \frac{x^{2/(k-1)}}{N^{1/\binom{k}{2}}},$$

y usando $x - l \leq x$ tenemos

$$L = \frac{N}{x-l} - \frac{N}{x} = \frac{lN}{(x-l)x} \geq C_k^{1/\binom{k}{2}} \frac{N^{1-\frac{1}{\binom{k}{2}}}}{x^{2-\frac{2}{k-1}}} = C_k^{1/\binom{k}{2}} \frac{X^{2-\frac{2}{k-1}}}{N^{1-\frac{2}{k-1}+\frac{1}{\binom{k}{2}}}}.$$

Procedemos análogamente, usando el Teorema 2.2, para obtener la segunda parte del corolario.

∎

En este apéndice damos una fórmula para el comportamiento asintótico de la constante C_k, definida en (2.2) mediante la expresión

$$C_k^2 = \frac{1}{2k!}\left(\frac{2k}{k-1}\right)^k \frac{\binom{2k-2}{k}^{2k-1}}{\binom{2k-2}{k-1}^2} \prod_{m=1}^{k-2} \frac{(m!)^2}{\binom{2m}{m}^2}.$$

Concretamente veremos que

$$C_k^2 = \left(4e^{-3/2}k\right)^{k^2-3k} \left(16\pi e^{13/2}\right)^k k^{7/12} e^{\alpha+O(1/k)}, \tag{A.1}$$

donde

$$\alpha = 1/6\log 2 + 1/4\log\pi - 53/12 + 5\gamma/6 + 5/2\sum_{j\geq 2}\frac{\zeta(j)-1}{j+2},$$

γ es la constante de Euler, y $\zeta(j) = \sum_{n\geq 1} n^{-j}$.

C_k^2 consiste en un producto de binomios. Por tanto, para calcular su comportamiento asintótico, intentaremos usar la fórmula de Stirling. Sin embargo, esta fórmula es buena cuando el factorial es de un número suficientemente grande, por lo que debemos encontrar un método alternativo de calcular el último producto en C_k, pues contiene términos pequeños.

Observando que se da la siguiente identidad,

$$\left(\prod_{m=1}^{l}(2m)!\right)^2 = 2^l l! \prod_{m=1}^{2l} m!,$$

que se sigue de $(2m)! = 2m(2m-1)!$, podemos reducir el estudio de ese último producto a calcular una fórmula asintótica para $\prod_m m!$. Ahora bien, se tiene

$$\begin{aligned}\prod_{m=1}^{l-1} m! = \prod_{m=1}^{l-1} m^{l-m} = \left(\prod_{m=1}^{l-1} m\right)^{l+1/2} \prod_{m=1}^{l-1} m^{-m-1/2}\\ =(l-1)!^{l+1/2}\prod_{m=1}^{l-1} m^{-m-1/2},\end{aligned}$$

y usando la identidad

$$l^{f(l)} \prod_{m=1}^{l-1} m^{f(m)-f(m+1)} = \prod_{m=2}^{l} \left(\frac{m}{m-1}\right)^{f(m)},$$

cierta para cualquier polinomio $f(x)$, podemos obtener el término principal en el producto de factoriales, quedando un producto de términos muy cercanos a 1, que podremos estimar usando el desarrollo del logaritmo. En efecto, sea $f(x) = x^2/2$, entonces $f(m) - f(m+1) = -m - 1/2$, y

$$\prod_{m=1}^{l-1} m! = \frac{l!^{l+1/2}}{l^{(l+1)^2/2}} \prod_{m=2}^{l} \left(\frac{m}{m-1}\right)^{m^2/2}.$$

Ahora, consideramos

$$\begin{aligned}
\sum_{m=2}^{l} m^2 \log\left(\frac{m}{m-1}\right) &= -\sum_{m=2}^{l} m^2 \log\left(1-\frac{1}{m}\right) = \sum_{m=2}^{l} m^2 \sum_{j\geq 1} \frac{1}{jm^j} \\
&= \sum_{m=2}^{l} m + \frac{1}{2}\sum_{m=2}^{l} 1 + \frac{1}{3}\sum_{m=2}^{l}\frac{1}{m} + \sum_{m=2}^{l}\sum_{j\geq 4}\frac{1}{jm^{j-2}} \\
&= \left(\frac{l(l+1)}{2} - 1\right) + \frac{1}{2}(l-1) + \frac{1}{3}(\log l + \gamma - 1) + \\
&\quad + \sum_{m=2}^{l}\sum_{j\geq 2}\frac{1}{(j+2)m^j} + O\left(\frac{1}{l}\right),
\end{aligned}$$

donde hemos usado el hecho

$$\sum_{m=1}^{l} \frac{1}{m} = \log l + \gamma + O\left(\frac{1}{l}\right).$$

Cambiando el orden de sumación, y observando que

$$\sum_{j\geq 2}\frac{1}{j+2}\sum_{m\geq l+1}\frac{1}{m^j} < \sum_{j\geq 2}\frac{1}{j+2}\int_l^\infty \frac{1}{t^j}dt < \sum_{j\geq 2}\frac{1}{l^{j-1}} = O\left(\frac{1}{l}\right),$$

obtenemos

$$\begin{aligned}
\prod_{m=2}^{l}\left(\frac{m}{m-1}\right)^{m^2} &= \exp\left(\sum_{m=2}^{l} m^2 \log\left(\frac{m}{m-1}\right)\right) \\
&= l^{1/3}\exp\left(l^2/2 + l - 11/6 + \gamma/3 + \sum_{j\geq 2}\frac{\zeta(j)-1}{j+2} + O\left(\frac{1}{l}\right)\right).
\end{aligned}$$

Esto nos permite obtener el comportamiento asintótico del producto de factoriales, y por tanto, para completar el correspondiente a C_k, sólo tenemos que aplicar la fórmula de Stirling,[8]

$$m! = \sqrt{2\pi} m^{m+1/2} e^{-m+1/(12m)+O(1/m^2)},$$

que es cierta para todo $m \geq 1$, y el hecho,

$$(k+a)^k = k^k e^{a-a^2/2k+O(1/k^2)}.$$

Observación: En particular hemos obtenido la fórmula

$$\prod_{m=1}^{l-1} m! = \eta^{1/2} \left(\sqrt{2\pi}\right)^l \left(e^{-3/2} l\right)^{l^2/2-1/12+O(1/l)}, \tag{A.2}$$

donde

$$\eta = \sqrt{2\pi} \exp\left(-23/12 + \gamma/3 + \sum_{j\geq 2} \frac{\zeta(j)-1}{j+2}\right).$$

[8]Ver **[Ed]** por ejemplo.

CAPÍTULO 3

La hipérbola $x^2 - dy^2 = N$

Introducción

Si giramos 45 grados nuestra hipérbola $xy = N$, uno debería pensar en obtener de nuevo resultados similares a los obtenidos hasta ahora, y así es el caso, ya que la hipérbola que se obtiene es $x^2 - y^2 = N$, y no hay más que observar que $x^2 - y^2 = (x - y)(x + y)$ para traducirlo de nuevo a un problema de divisores.

Este es el caso más sencillo de hipérbolas, con ejes los ejes coordenados. Vamos a ocuparnos del caso más general, $x^2 - dy^2 = N$, y usando la factorización única en ideales en cuerpos cuadráticos, obtendremos un resultado análogo al obtenido en el capítulo 1 para anillos de factorización única.

§ 1 Resultado y definiciones

Sea $d > 1$ un entero libre de cuadrados. Consideramos el cuerpo de números $\mathbb{Q}(\sqrt{d})$ con anillo de enteros $\mathcal{A}$, y sea h_2 el número de elementos del grupo de clases de orden menor o igual que 2. Podemos probar[9]

TEOREMA 3.1. *a) En un arco de la hipérbola, $x^2 - dy^2 = N$, de longitud N^α con $\alpha \le 1/4 - 1/(8\left[\frac{k}{4h_2}\right] + 4)$, no hay más de k puntos de coordenadas enteras.*

b) Si además, algún divisor de d, $d_1 \neq 1, -d$, es representable mediante la hipérbola, entonces el resultado se puede mejorar hasta $\alpha \le 1/4 - 1/(8\left[\frac{k}{2h_2}\right] + 4)$.

Por simplicidad, vamos a considerar $d \equiv 1 \pmod 4$, siendo el caso general idéntico salvo obvias modificaciones.

Consideramos la función aritmética

$$\mathrm{r}_d(N) = \#\{x, y \in \mathbb{Z} \,/\, x^2 - dy^2 = N\}.$$

Esta función se puede interpretar como el número de puntos de coordenadas enteras que hay en la hipérbola, $x^2 - dy^2 = N$. De manera obvia podemos asignar a cada punto de coordenadas enteras, un elemento en el anillo de enteros $\mathcal{A}$ de $\mathbb{Q}(\sqrt{d})$ de norma N, y viceversa. De esta forma, podemos concluir que si

[9] Sin pérdida de generalidad podemos suponer N positivo.

$\mathrm{r}_d(N) > 1$ entonces $\mathrm{r}_d(N) = \infty$, ya que, si $\xi \in \mathcal{A}$ corresponde a una representación de N, entonces $\mu\xi$ corresponderá a una representación distinta de N para toda unidad μ de $\mathcal{A}$. Nuestra afirmación se concluye del hecho de que para todo k entero, ε^k es una unidad, donde ε es la unidad fundamental[10] de $\mathcal{A}$.

Parece claro pues, que para contar representaciones de N, basta contar ciertas representaciones, y luego multiplicar por unidades. Es conveniente por tanto introducir la siguiente definición; Decimos que dos representaciones ξ_1, ξ_2, están relacionadas, si existe una unidad μ tal que $\mu\xi_1 = \xi_2$.

Vamos a centrarnos en un arco de pequeña longitud de la hipérbola, que por simetría podemos suponer que está en el primer cuadrante.

Si dicho arco es suficientemente pequeño, no podrá tener dos representaciones relacionadas, ya que estamos multiplicando por unidades. Más concretamente, sea un arco de hipérbola Γ. Definimos

$$L(\Gamma) = \max_{\{p_1,p_2\}\in\Gamma} \left|(x_1 + y_1\sqrt{d}) - (x_2 + y_2\sqrt{d})\right|$$

donde[11] $p_i = (x_i, y_i)$, y consideramos las funciones aritméticas $\mathrm{r}_{d,\Gamma}$, $\mathrm{r}^*_{d,\Gamma}$ que cuentan las representaciones de N que se encuentran en Γ, y aquellas que además son no relacionadas, respectivamente. Entonces

LEMA 1. *Para todo arco Γ con $L(\Gamma) \leq N^{1/2}$ se tiene*

$$\mathrm{r}_{d,\Gamma} = \mathrm{r}^*_{d,\Gamma}.$$

DEMOSTRACIÓN:

En efecto, sea $\xi = x + y\sqrt{d} > \sqrt{N}$ por estar en el primer cuadrante. Entonces, si $\{\xi, \mu\xi\}$ están en Γ para alguna unidad μ, se tiene

$$\mu = \frac{\mu\xi}{\xi} = 1 + \frac{\mu\xi - \xi}{\xi} \leq 1 + N^{-1/2}L(\Gamma)$$

[10]Si $d \equiv 5 \pmod 8$, y ε es la unidad fundamental de $\mathcal{A}$ entonces en ε^{3k}, $k \in \mathbb{Z}$ no intervienen semienteros.

[11]Si el arco Γ no estuviese en el primer cuadrante, definimos $L(\Gamma) = L(\overline{\Gamma})$ donde $\overline{\Gamma}$ es el arco simétrico a Γ y contenido en el primer cuadrante.

mientras que, por otro lado $\mu \geq \varepsilon > 1 + \sqrt{d}$. Uniendo ambas desigualdades, deducimos el resultado. Si Γ no estuviese completamente contenido en ningún cuadrante, un razonamiento similar nos llevaría de nuevo al mismo resultado, salvo constantes.

Así, en arcos de longitud menor que $N^{1/2}$, sólo tendremos que preocuparnos de representaciones no relacionadas.

§ 2 <u>Demostración del Teorema 3.1</u>

Sea la factorización de N en números primos

$$N = \prod_{\left(\frac{d}{q_j}\right)=-1} q_j^{\beta_j} \prod_{\left(\frac{d}{r_j}\right)=0} r_j^{\delta_j} \prod_{\left(\frac{d}{p_j}\right)=1} p_j^{\alpha_j},$$

donde el primer producto recorre los primos q_j tales que d no es residuo cuadrático, el segundo es sobre los primos que dividen a d, y el último sobre aquellos tal que d es residuo cuadrático, hecho que representamos mediante el símbolo de Legendre.

Supongamos que N tiene una representación $x + y\sqrt{d}$ en la hipérbola. Considerando ideales en el anillo de enteros $\mathcal{A}$ se obtiene

$$< x+y\sqrt{d} >< x-y\sqrt{d} >=< N >= \prod_{\left(\frac{d}{q_j}\right)=-1} < q_j >^{\beta_j} \prod_{\left(\frac{d}{r_j}\right)=0} \mathcal{R}_j^{2\delta_j} \prod_{\left(\frac{d}{p_j}\right)=1} \wp_{j,1}^{\alpha_j}\wp_{j,2}^{\alpha_j},$$

ya que $< q >$ es primo siempre que $\left(\dfrac{d}{q}\right) = -1$, y $< p >= \wp_1\wp_2$, o $< r >= \mathcal{R}^2$ cuando $\left(\dfrac{d}{p}\right) = 1$, o $\left(\dfrac{d}{r}\right) = 0$ respectivamente. Además se cumple la ecuación de normas

$$\mathrm{N}(< x + y\sqrt{d} >) = \mathrm{N}(< x - y\sqrt{d} >) = N,$$

de donde se deduce

$$< x + y\sqrt{d} >= \prod_{\left(\frac{d}{q_j}\right)=-1} < q_j >^{\beta_j/2} \prod_{\left(\frac{d}{r_j}\right)=0} \mathcal{R}_j^{\delta_j} \prod_{\left(\frac{d}{p_j}\right)=1} \wp_{j,1}^{\gamma_j}\wp_{j,2}^{\alpha_j-\gamma_j},$$

para algunos $0 \leq \gamma_j \leq \alpha_j$.

Observamos en primer lugar que si $\mathrm{r}_d(N) > 1$ entonces los β_k tienen que ser pares. Además, si $\mathcal{R}_j \in E_{\mu(j)}$, y $\wp_{j,1} \in E_{\nu(j)}$, donde $E_1, \cdots, E_h$ son los elementos del grupo de clases de $\mathcal{A}$, entonces $\wp_{j,2} \in E_{\nu(j)}^{-1}$ y tiene que cumplirse

$$\prod E_{\mu(j)}^{\delta_j} E_{\nu(j)}^{2\gamma_j-\alpha_j} = E_1, \tag{3.1}$$

ya que el ideal $\prod \mathcal{R}_j^{\delta_j} \wp_{j,1}^{\gamma_j} \wp_{j,2}^{\alpha_j-\gamma_j}$ debe ser principal. De esta forma, hemos encontrado una correspondencia entre las representaciones de N no relacionadas, y conjuntos de enteros γ_j menores que α_j y que cumplen (3.1). De hecho, dados ciertos γ_j en esas condiciones, hemos encontrado una representación, no sólo de N, sino de algún divisor suyo, hecho que veremos más adelante.

Supongamos que hay $k+1$ representaciones de N en un arco Γ. La diferencia entre representaciones distintas de N, y por tanto la longitud de Γ, estará acotada inferiormente por el tamaño de los "comunes divisores" que tengan las representaciones. Intentaremos encontrar factores comunes gracias a nuestra correspondencia con los conjuntos de exponentes $\{\gamma_j\}$.

Consideramos los elementos del grupo de clase

$$\prod E_{\nu(j)}^{\gamma_{j,1}-\gamma_{j,s}},$$

donde los $\gamma_{j,i}$ corresponden al primo j-ésimo de la i-ésima representación. Elevando al cuadrado

$$\begin{aligned}\left(\prod E_{\nu(j)}^{\gamma_{j,1}-\gamma_{j,s}}\right)^2 &= \left(\prod E_{\mu(j)}^{\delta_j} E_{\nu(j)}^{2\gamma_{j,1}-\alpha_j}\right)\left(\prod (E_{\mu(j)}^{\delta_j} E_{\nu(j)}^{2\gamma_{j,s}-\alpha_j}\right)^{-1}\\ &= E_1,\end{aligned}$$

por tanto, todos los elementos considerados son de orden 2. Si llamamos h_2 al número de elementos del grupo de clase de orden menor o igual que 2, habrá al menos $C_1 = [m/h_2] + 1$ elementos de los anteriores, donde $[x]$ es el mayor entero menor que x, que son iguales, o en otras palabras, "dividiendo" ambos elementos da la identidad, es decir

$$\prod E_{\nu(j)}^{\gamma_{j,l}-\gamma_{j,s}} = E_1 \tag{3.2}$$

para todos los $1 \leq l, s \leq C_1$, (quizá ordenando las representaciones convenientemente). Sean ξ_l, ξ_s dos representaciones tal que se cumple (3.2). Entonces,

$$
\begin{aligned}
< x_s + y_s\sqrt{d} >= & \prod_{\left(\frac{d}{q_j}\right)=-1} < q_j >^{\beta_j/2} \prod_{\left(\frac{d}{r_j}\right)=0} \mathcal{R}_j^{\delta_j} \prod_{\left(\frac{d}{p_j}\right)=1} \wp_{j,1}^{\gamma_j} \wp_{j,2}^{\alpha_j-\gamma_j} \\
=< & \prod_{\left(\frac{d}{q_j}\right)=-1} q_j^{\beta_j/2} > \prod_{\left(\frac{d}{r_j}\right)=0} \mathcal{R}_j^{\delta_j} \prod_{\left(\frac{d}{p_j}\right)=1} \wp_{j,1}^{\min(\gamma_{j,s},\gamma_{j,l})} \wp_{j,2}^{\alpha_j-\max(\gamma_{j,s},\gamma_{j,l})} \times \\
\times & \prod_{\left(\frac{d}{p_j}\right)=0 \text{ o } 1} \wp_{j,1}^{\frac{|\gamma_{j,s}-\gamma_{j,l}|+(\gamma_{j,s}-\gamma_{j,l})}{2}} \wp_{j,2}^{\frac{|\gamma_{j,s}-\gamma_{j,l}|-(\gamma_{j,s}-\gamma_{j,l})}{2}} \\
= & \mathcal{I}_1\mathcal{I}_2\mathcal{I}_3.
\end{aligned}
$$

Análogamente, encontramos para ξ_l

$$< x_l + y_l\sqrt{d} >= \mathcal{I}_1\mathcal{I}_2\mathcal{I}_3^{-1},$$

donde $\mathcal{I}_3\mathcal{I}_3^{-1} \in E_1$. Además, $\mathcal{I}_1$ es principal, y por (3.2) $\mathcal{I}_3$ también lo es, de lo que concluimos que $\mathcal{I}_2$ es principal, y

$$
\begin{aligned}
< x_s + y_s\sqrt{d} > &= < (u_{s,l} + v_{s,l}\sqrt{d})(a_{s,l} + b_{s,l}\sqrt{d}) > \\
< x_l + y_l\sqrt{d} > &= < (u_{s,l} + v_{s,l}\sqrt{d})(a_{s,l} - b_{s,l}\sqrt{d}) > .
\end{aligned}
$$

donde

$$\mathrm{N}(< a_{s,l} + b_{s,l}\sqrt{d} >) = \prod p_j^{|\gamma_{j,s}-\gamma_{j,l}|}. \tag{3.3}$$

Ahora bien, si dos ideales principales son iguales, sus representantes están relacionados, de donde deducimos que existe un entero $\delta_{s,l}$, tal que[12]

$$\varepsilon^{\delta_{s,l}}(a_{s,l} - b_{s,l}\sqrt{d})(x_s + y_s\sqrt{d}) = (a_{s,l} + b_{s,l}\sqrt{d})(x_l + y_l\sqrt{d}), \tag{3.4}$$

[12]Pudiera ser que $a_{s,l} + b_{s,l}\sqrt{d}$ represente $-\prod p_j^{|\gamma_{j,s}-\gamma_{j,l}|}$, en cuyo caso deberíamos repetir el argumento sustituyendo $a_{s,l} - b_{s,l}\sqrt{d}$ por $-(a_{s,l} - b_{s,l}\sqrt{d})$.

Además, podemos escoger $|\delta_{s,l}| \leq 1$, ya que en caso contrario, elegiríamos el representante $a_{s,l}+b_{s,l}\sqrt{d} = \varepsilon^{[\delta_{s,l}/2]}(a_{s,l}+b_{s,l}\sqrt{d})$, siendo en este caso su conjugado $a_{s,l} - b_{s,l}\sqrt{d} = \varepsilon^{-[\delta_{s,l}/2]}(a_{s,l} - b_{s,l}\sqrt{d})$.

Para terminar la prueba, necesitamos que la función $\delta_{s,l}$, se haga cero las más veces posibles. Vamos a ver que al menos de cada tres valores uno es cero. Para ello veremos que, para todo $1 \leq \{i,l,s\} \leq C_1$, $\delta_{i,s}+\delta_{s,l}-\delta_{i,l}$ es par. En efecto, si multiplicamos (3.4) por $(a_{i,s}+b_{i,s}\sqrt{d})(a_{i,l}+b_{i,l}\sqrt{d})$ obtenemos

$$
\begin{aligned}
&\varepsilon^{\delta_{s,l}}(a_{s,l}-b_{s,l}\sqrt{d})(a_{i,l}+b_{i,l}\sqrt{d})\varepsilon^{\delta_{i,s}}(a_{i,s}-b_{i,s}\sqrt{d})(x_i+y_i\sqrt{d}) = \\
=&\varepsilon^{\delta_{s,l}}(a_{s,l}-b_{s,l}\sqrt{d})(a_{i,l}+b_{i,l}\sqrt{d})(a_{i,s}+b_{i,s}\sqrt{d})(x_s+y_s\sqrt{d}) \\
=&(a_{s,l}+b_{s,l}\sqrt{d})(a_{i,s}+b_{i,s}\sqrt{d})(a_{i,l}+b_{i,l}\sqrt{d})(x_l+y_l\sqrt{d}) \\
=&(a_{s,l}+b_{s,l}\sqrt{d})(a_{i,s}+b_{i,s}\sqrt{d})\varepsilon^{\delta_{i,l}}(a_{i,l}-b_{i,l}\sqrt{d})(x_i+y_i\sqrt{d}),
\end{aligned}
$$

donde hemos usado varias veces (3.4). De esta forma, hemos conseguido un elemento $u+v\sqrt{d} = (a_{s,l}-b_{s,l}\sqrt{d})(a_{i,l}+b_{i,l}\sqrt{d})(a_{i,s}-b_{i,s}\sqrt{d})$, tal que

$$\varepsilon^{\delta_{s,l}+\delta_{i,s}-\delta_{i,l}}(u+v\sqrt{d}) = u - v\sqrt{d}.$$

Por otra parte, multiplicando ideales,

$$< u+v\sqrt{d} >= \prod(\wp_{j,1}\wp_{j,2})^{|\gamma_{j,l}-\gamma_{j,s}|+|\gamma_{j,i}-\gamma_{j,s}|+|\gamma_{j,i}-\gamma_{j,l}|} =< r >,$$

donde $r \in \mathbb{Z}$. Por tanto, existe un entero k tal que $(u+v\sqrt{d}) = \varepsilon^k r$, o de otra forma,

$$\varepsilon^{\delta_{s,l}+\delta_{i,s}-\delta_{i,l}+k} r = u - v\sqrt{d} = \varepsilon^{-k} r$$

que sólo es posible si $\delta_{s,l}+\delta_{i,s}-\delta_{i,l} = 2k$.

Ordenemos los valores $\delta_{1,l}$ de forma que $\delta_{1,l} = 0$ si $2 \leq l \leq l_0$, y $|\delta_{1,l}| = 1$ si $l_0 < l \leq C_1$. Entonces $\delta_{s,l} = 0$ tanto para los $1 \leq \{s,l\} \leq l_0$ así como para los $l_0 < \{s,l\} \leq C_1$. Como $\max\{l_0, C_1 - l_0\} \geq [\frac{C_1-1}{2}] + 1 = C_2$, observamos que, $\delta_{s,l} = 0$ al menos para $\binom{C_2}{2}$ pares $\{s,l\}$. En esos casos, podemos escribir (3.4) como

$$\frac{x_s+y_s\sqrt{d}}{x_l+y_l\sqrt{d}} = \frac{a_{s,l}+b_{s,l}\sqrt{d}}{a_{s,l}-b_{s,l}\sqrt{d}}.$$

En primer lugar, como ambas representaciones están en Γ, se tiene[13]

$$\frac{x_s + y_s\sqrt{d}}{x_l + y_l\sqrt{d}} = 1 + \frac{(x_s + y_s\sqrt{d}) - (x_l + y_l\sqrt{d})}{x_l + y_l\sqrt{d}} \leq 1 + L(\Gamma)N^{-1/2}.$$

Por otra parte, por (3.3), se tiene[14]

$$a_{s,l} + b_{s,l}\sqrt{d} \geq \prod p_j^{\frac{|\gamma_{j,s}-\gamma_{j,l}|}{2}}, \quad 0 \leq a_{s,l} - b_{s,l}\sqrt{d} \leq \prod p_j^{\frac{|\gamma_{j,s}-\gamma_{j,l}|}{2}}.$$

Ahora bien, como $a_{s,l} + b_{s,l}\sqrt{d} \neq a_{s,l} - b_{s,l}\sqrt{d}$ la desigualdad es estricta, y por ser $a_{s,l}, b_{s,l}$ números enteros, deducimos

$$a_{s,l} + b_{s,l}\sqrt{d} \geq \prod p_j^{\frac{|\gamma_{j,s}-\gamma_{j,l}|}{2}} + \sqrt{d}.$$

Uniendo las dos últimas desigualdades obtenemos

$$L(\Gamma)N^{-1/2} \geq \sqrt{d} \prod p_j^{-\frac{|\gamma_{j,s}-\gamma_{j,l}|}{2}}.$$

Multiplicando las desigualdades análogas de los $\binom{C_2}{2}$ pares con $\delta_{s,l} = 0$ nos queda

$$\left(L(\Gamma)N^{-1/2}\right)^{\binom{C_2}{2}} \geq K \prod p_j^{-\sum_{1\leq s<l\leq C_2} \frac{|\gamma_{j,s}-\gamma_{j,l}|}{2}} \tag{3.5}$$

para cierta constante K que depende de d. Ahora bien, el máximo de $\sum_{1\leq s<l\leq C_2} |\gamma_{j,s} - \gamma_{j,l}|$ se alcanza cuando la mitad de los $\gamma_{j,s}$ son cero, y la otra mitad α_j, y en ese caso

$$\sum_{1\leq s<l\leq C_2} |\gamma_{j,s} - \gamma_{j,l}| = \alpha_j[C_2/2](C_2 - [C_2/2])$$

Sustituyendo en (3.5), y utilizando $\prod p_j^{\alpha_j} \leq N$ obtenemos el resultado de la primera parte del teorema.

[13] Observar que la cota será mejor, dependiendo de lo lejos que esté el arco Γ del centro de la hipérbola, pues $x_l + y_l\sqrt{d} \gg \sqrt{n}$.

[14] Quizá fuera necesario considerar la fracción inversa, $(x_l + y_l\sqrt{d})/(x_s + y_s\sqrt{d})$

Para mejorar nuestra cota, suponemos que estamos en las hipótesis de la parte b) del teorema. En tal caso, existe un entero positivo $l|d^2$, $l \neq m^2$ que es representable por la hipérbola. Esto es cierto, ya que para $d_1 > 0$ y $d_1|d$, se tiene o bien $x^2 - dy^2 = d_1$, o $x^2 - dy^2 = -d_1$, en cuyo caso $(dy)^2 - dx^2 = d_1 d$.

Ahora bien, para todo $p|l$ entonces $p|d$, luego $< l >$ es completamente ramificado en $\mathcal{A}$, por tanto existe un ideal $\mathcal{L}$ de $\mathcal{A}$ tal que $< l >= \mathcal{L}^2$, mientras que por ser representable

$$< x + y\sqrt{d} >< x - y\sqrt{d} >=< l >= \mathcal{L}^2,$$

para algún par (x, y). Tomando normas en la igualdad anterior obtenemos, $\mathrm{N}(< x+y\sqrt{d} >) = \mathrm{N}(< x-y\sqrt{d} >) = l$, luego $< x+y\sqrt{d} >=< x-y\sqrt{d} >= \mathcal{L}$. Por tanto existe una unidad μ tal que $(x + y\sqrt{d}) = \mu(x - y\sqrt{d})$ y de nuevo podemos suponer $\mu = \varepsilon$, la unidad fundamental, razonando como en (3.4), ya que $x + y\sqrt{d} \neq x - y\sqrt{d}$ por no ser l un cuadrado perfecto. Para terminar el razonamiento, no hay más que multiplicar (3.4) por $x - y\sqrt{d}$ siempre que $\delta_{s,l} = 1$, obteniendo quizá para un nuevo $a_{s,l} + b_{s,l}\sqrt{d}$, y para todos los $\binom{C_1}{2}$ pares s, l

$$\frac{x_s + y_s\sqrt{d}}{x_l + y_l\sqrt{d}} = \frac{a_{s,l} + b_{s,l}\sqrt{d}}{a_{s,l} - b_{s,l}\sqrt{d}},$$

donde en algunos casos $\mathrm{N}(< a_{s,l} + b_{s,l}\sqrt{d} >) = l\prod p_j^{|\gamma_{j,s}-\gamma_{j,l}|}$. El resto del razonamiento es análogo y concluye la parte b) del teorema.

∎

<u>Observacion:</u> Por último, notar que este truco utilizado para mejorar el resultado en el teorema, puede ser utilizado para encontrar unidades en el anillo de enteros $\mathcal{A}$. Así, supongamos que tenemos una solución no trivial a, $x^2 - dy^2 = n$, con n tal que $p|n$ implica $p|d$, entonces, n ramifica completamente, y deducimos que

$$x + y\sqrt{d} = \mu(x - y\sqrt{d}) \tag{3.6}$$

con lo que hemos encontrado μ, una unidad del anillo $\mathcal{A}$. Además, si encontramos el menor $x + y\sqrt{d} > \sqrt{n}$ que representa a un cierto $n \neq m^2$ en esas condiciones, entonces hemos encontrado la unidad fundamental del anillo, ya que si en (3.6), $\mu = \varepsilon^{2k+1}$, $k \geq 1$, consideramos $u + v\sqrt{d} = \varepsilon^{-k}(x + y\sqrt{d}) < x + y\sqrt{d}$, mientras que por (3.6) $u + v\sqrt{d} = \varepsilon(u - v\sqrt{d})$ y por tanto $u + v\sqrt{d} > \sqrt{n}$ con lo que llegamos a una contradicción.

[B-H] D. Berend and J.E. Harmse, *Gaps Between Consecutive Divisors of Factorials* , Ann. Inst. Fourier. Grenoble **13.3** (1993), 569–583

[B-S] Z.I. Borevich and I.R. Shafarevich, *Number Theory* , Academic Press New York (1966)

[C1] J. Cilleruelo, *Representación de enteros como suma de dos cuadrados* , Tesis. Universidad Autónoma, Madrid (1989)

[C2] J. Cilleruelo, *Arcs containing no three lattice points* , Acta Arith. **lix.1** (1991), 87–90

[C-C 1] J. Cilleruelo and A. Córdoba, *Trigonometric Polynomials and Lattice Points* , Proc. of Amer. Math. Soc. **115.4** (1992), 899–905

[C-C 2] J. Cilleruelo and A. Córdoba, *La Teoría de los Números* , Mondadori, Madrid (1992)

[C-C 3] J. Cilleruelo and A. Córdoba, *Lattice Points on Ellipses* , Duke Math. Jour. **76.3** (1994), 741-750

[D] P.G.L. Dirichlet, *Über die Bestimmung der Mittleren Werte Der Zahlentheorie* , Abh. Königl. Preuss. Akad. Wiss (1849), 69–83

[Ed] H. M. Edwards, *Riemanns Zeta Function* , Pure and Applied Math. **58** Academic Press New York (1974)

[F] M. Fekete, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Z. **17** (1923) 228–249

[**G**] C. F. Gauss, *De Nexu Inter Multitudinem Classium, In Quas Formae Binariae Secundi Gradus Distribuuntur, Earumque Determinantem* , Werke Bd 2

[**Gr**] G. Grekos, *Sur le nombre de points entiers dune courbe convexe* , Bull. Sc. math. 2^e série **112** (1988), 235–254

[**H-T**] R.R. Hall and G. Tenenbaum, *Divisors* , Cambridge Univ. Press. Cambridge (1988)

[**H-W**] G. H. Hardy and E.M. Wright, *Introduction to the theory of numbers,* 4th ed. Clarendon Press. Oxford (1960)

[**He1**] D.R. Heath-Brown, *The Divisor Function at Consecutive Integers* , Mathematika **31** (1984), 141–149

[**He2**] D.R. Heath-Brown, *Consecutive almost-primes* Journal Indian Math. Soc. **52** (1987), 39–49

[**Hi**] A. Hildebrand, *On a conjecture of Balog* , Proc. A.M.S. **95.4** (1985), 517–523

[**Hu**] Hua l. Keng, *Introduction to Number Theory* , Springer Verlag Berlin (1982)

[**I-M**] H. Iwaniec and C.J. Mozzochi, *On the divisor and circle problem* , Jour. Number Theory **29** (1988), 60–93

[**K**] E. Krätzel, *Lattice Points* , Kluwer Acad. Publ. Berlin (1988)

[**La**] S. Lang, *Algebra* , Addison-Wesley: Reading Massachusets (1965)

[**Le**] H. W. Lenstra, Jr. *Divisors in residue classes* , Math. of Comp. **42.165** (1984), 331–340

[**P**] Chr. Pommerenke, *Univalent Functions*, Vandenhoeck & Ruprecht in Göttingen. Studia Mathematica Bd **xxv** (1975)

[**S-T**] I.N. Stewart and D.O. Tall, *Algebraic Number Theory* , Chapman and Hall London (1987)

[**T**] E.C Titchmarsh, *The Theory of The Riemann Zeta-Function* , Clarendon Press (2Ed Revised by D.R. Heath-Brown) Oxford (1986)

[**V**] M. D. Vose, *Integers with consecutive divisors in small ratio* , Jour. Number Theory **19** (1984), 233–238

[**W**] D. T. Walker, *On the diofantine equation* $mX^2 - nY^2 = \pm 1$, Amer. Math. Monthly **74** (1967), 504–513

Reunido el Tribunal que suscribe en el día de la fecha, acordó calificar la presente Tesis Doctoral con la censura de APTO 'Cum Laude' (unan.)

Madrid, 14-7-1995

Las firmas están al principio de la Tesis