UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE CIENCIAS

SECCIÓN DE POSGRADO Y SEGUNDA ESPECIALIZACIÓN PROFESIONAL

DISTRIBUCIÓN DE LOS ENTEROS COPRIMOS A UN ENTERO DADO

TESIS PARA OPTAR EL GRADO DE MAESTRO EN CIENCIAS CON MENCIÓN EN MATEMÁTICA APLICADA

ELABORADA POR

JUAN CARLOS ROJAS COLUNCHE

ASESOR

OSWALDO JOSÉ VELÁSQUEZ CASTAÑÓN

LIMA - PERÚ

2014

Dedicatoria

Dedico este trabajo a Dios y a mi madre, María V. Colunche Delgado,
que han sido la luz y el camino para dar este paso.

Agradecimientos

Agradeciendo antes que todo a Dios, nuestro padre, y aunque es difícil valorar el apoyo que nos brindan las personas que estan cerca nuestro, quisiera dar las gracias en primer lugar a mi madre, María V. Colunche Delgado. Definitivamente es y a sido siempre la persona que más me a apoyado en todos los aspectos de mi vida.
Quisiera agradecer también a mi (algo numerosa) familia y mis amigos, los cuales directa e indirectamente han contribuído conmigo y con mi labor académica a lo largo de todos estos años. Un agradecimiento especial a los profesores que han contribuído directamente con la dirección y revisado de este trabajo, prestándome valiosas ideas, sugerencias y sacándome en más de una ocasión de algún apuro: a Oswaldo Velásquez, que ha sido mi asesor y motivador lo largo de su elaboración, y que me introdujo en la fascinante área de la teoría de números; Johel Beltrán, que me dictó un excelente curso de probabilidades y aceptó gustoso su revisión; a Arnol Chadozeau, cuyo trabajo inspira en gran medida el presente y a Félix Escalante, que también ofreció su valiosa revisión y sugerencias.

Muchas gracias.

Índice general

DISTRIBUCIÓN DE LOS ENTEROS COPRIMOS A UN ENTERO DADO.

El presente trabajo se divide en dos partes, siendo la primera una introducción al estudio de algunas técnicas de análisis probabilístico aplicado a la teoría de números, y la segunda una exposición de la aplicación de algunos de éstos al problema de la mayoración de los momentos centrales de grado k de los enteros coprimos a un entero dado n en intervalos de longitud h. Respecto de la primera parte, presentamos en ésta una exposición de algunos conceptos y técnicas del análisis combinatorio y también de la teoría de probabilidades. Así mismo, presentamos una introducción a la aplicación de estos conceptos a la teoría de números y algunos resultados al respecto. A modo de ejemplo, exponemos la prueba del Teorema de Hardy – Ramanujan, del que se puede inferir que la función $\omega(n)$, que cuenta la cantidad de divisores primos de un entero n, tiene orden normal $\log\log n$, como también la prueba de la existencia de una base asintótica de orden 2 en $\mathbb{N}$ tal que su número de elementos menores o iguales a n es $o(n^{\varepsilon})$ cuando $n \to +\infty$, para cualquier $\varepsilon > 0$.
En la segunda parte del trabajo, detallamos el problema de la acotación uniforme en k de los momentos

$$M_k(q;h) = \sum_{n=1}^{q} \left(\sum_{i=1}^{h} [(n+i,q) = 1] - h\frac{\varphi(q)}{q} \right)^k$$

de los coprimos con q en intervalos enteros de longitud h. Para tal fin, aproximamos este problema al de una ley binomial de parámetros h, P usando las técnicas de la primera parte del trabajo. Para este tipo de ley binomial, establecemos la estimativa

$$\mu_k(h,P) \ll C^{k/2}k^{k/2}\left(k + hP(1-P)\right)^{k/2}.$$

A seguir, usamos técnicas de análisis combinatorio para mostrar, en la parte final del trabajo que

$$M_k(q;h) \ll qC^{k/2}k^{k/2}\left(k + h\frac{\varphi(q)}{q}\right)^{k/2},$$

donde C es una constante absoluta y q se asume sin factores cuadrados.

DISTRIBUTION OF THE COPRIME INTEGERS TO A GIVEN INTEGER.

The present work is divided into two parts, the first being an introduction to some methods of probabilistic analysis applied to number theory, and the second a exposition of an application from these to the problem of bounding the central moments of k grade of the coprimes integers to a given integer n in h-length intervals. About the first part, we show some concepts and methods from combinatory analysis as well as probabilistic theory. Also, we show an introduction to appliances of these to number theory and some results about them. For instance, we expose the Hardy-Ramanujan theorem's proof, which implies that the $\omega(n)$ function, that counts the amount of prime divisors for an integer n, has the normal order $\log\log n$, as well as the proof of the existence of a asintotic base of order 2 in $\mathbb{N}$ such that the amount of its elements being nor mayor than n is $o(n^{\varepsilon})$ when $n \to +\infty$, for all $\varepsilon > 0$. In the second part we detail the problem of the uniform bounding in k for de moments

$$M_k(q;h) = \sum_{n=1}^{q} \left(\sum_{i=1}^{h} [(n+i,q) = 1] - h\frac{\varphi(q)}{q} \right)^k$$

of the coprimes with q in integer intervals of h length. To this purpose, we aproximate the problem to a binomial law with parameters (h,k) by using the first part of the text. For this type of probabilistic law we get the equation

$$\mu_k(h,P) \ll C^{k/2}k^{k/2}\left(k + hP(1-P)\right)^{k/2}.$$

Then, we use combinatorial methods to show, at the last part of the work, that

$$M_k(q;h) \ll qC^{k/2}k^{k/2}\left(k + h\frac{\varphi(q)}{q}\right)^{k/2},$$

where C is an absolute constant and q is asumed to be without any square factor.

Introducción

¿Cómo aplicar el método estadístico-probabilístico para el estudio de una función aritmética? Quizá sea esta la pregunta que surge al observar algunos resultados acerca del comportamiento de ciertas funciones aritméticas que han llamado la atención de numerososos eminentes matemáticos durante la historia, al observar que los valores que éstas toman aparecen en forma tan impredecible e irregular que parecen haber sido resultado de un juego de azar. Por ejemplo, H. Cramér [7] modela una sucesión S considerándola como elemento de una clase C de sucesiones que forman parte de las posibles realizaciones de un juego de azar, consistiendo éste en un conjunto infinito de urnas U_n, $n \in \mathbb{N}$, cada una de las cuales tiene una probabilidad P_n de ser blanca o negra, éxito o fracaso. En palabras del autor, *"It is then in many cases possible to prove that, with a probability = 1, a certain relation R holds in C,* i.e. *that in a definite mathematical sense "almost all" sequences of C satisfy R. Of course we cannot in general conclude that R holds for que particular sequence S, but results suggested in this way may sometimes afterwards be rigorously proved by other methods"*. Por ejemplo, si observamos que del teorema del número primo,

$$\frac{\pi(x)}{x} \sim \frac{1}{\log x}$$

cuando $x \to \infty$, podría ser natural considerar $P_n = 1/\log n$ a ser la opción más conveniente para el estudio de los números primos, y tratar de conjeturar posibles resultados acerca de éstos.

El modo impredecible e irregular en que aparecen los valores de una función aritmética puede ser abordado, probabilísticamente, de un modo ligeramente distinto: quizás sean estos, efectivamente, el resultado de un juego de azar. Luego, nos encontraríamos ante un conjunto de *observaciones*, observaciones de una variable aleatoria, valores que pueden aproximar el comportamiento de la variable, y quizá también viceversa. Es probable que el lector familarizado con el uso de técnicas de análisis estadístico se sienta en un terreno familiar. El uso de un número finito, limitado de observaciones para el estudio y la predicción de resultados más generales forma parte esencial de esta rama de

la ciencia, resumida bajo el título de *inferencia estadística*. Es con esta motivación que en la primera parte del trabajo hacemos una introducción, quizá algo superficial, al uso de las técnicas de análisis combinatorio y probabilístico al estudio de ciertos problemas de teoría de números, como por ejemplo la prueba del teorema de Hardy y Ramanujan, presentada por Turán, y también la respuesta afirmativa al problema de Sidon dada por Erdős. Estos muestran dos facetas distintas en cuanto a la aplicación de resultados de teoría de probabilidades se refiere. A grandes rasgos, el primer resultado consiste (con algunas variaciones) en expresar primero el problema de teoría de números como uno probabilístico en espacios de probabilidad finitos, construyendo las variables aleatorias X_n que modelan el problema de acuerdo a las características de la función o sucesión aritmética en estudio. Por lo general, las características probabilísticas de X_n no son lo suficientemente adecuadas, haciendo imposible la aplicación de las herramientas de teoría probabilística de manera directa para su estudio. Algunos problemas técnicos que se presentan tienen que ver con el concepto probabilístico de *independencia*, o con el hecho de que tales X_n no pueden ser definidas en todo $\mathbb{Z}^+$, ya que es posible ver que

No existe una medida de probabilidad $\mathcal{P}$ definida en $\mathbb{Z}^+$ tal que, para todo $m \in \mathbb{Z}^+$,

$$\mathcal{P}(m\mathbb{Z}^+) = \frac{1}{m}.$$

En vista de estos inconvenientes, es que se transfiere el estudio de las funciones X_n al estudio de ciertas funciones Y_n, éstas variables aleatorias definidas en un espacio de probabilidad Ω y con un comportamiento probabilístico más adecuado. Es decir, las variables X_n son ahora *observaciones* de Y_n. Desde luego, los resultados que se puedan obtener para Y_n no son válidos para la sucesión aritmética en estudio. Sin embargo, un trabajo con técnicas de análisis combinatorio puede acercarnos algún resultado similar para el objeto original.

El segundo presenta una marcada diferencia respecto al anterior: en éste se usan las herramientas de la teoría de probabilidades directamente para probar la existencia de una base aditiva de orden 2 para $\mathbb{N}$. Tal cosa necesita por supuesto de la previa construcción de un espacio de probabilidad y la definición de variables aleatorias independietes adecuados que nos brinden resultados directos para el problema de existencia. Este método, muy usado para probar la existencia de ciertos objetos matemáticos de diversa índole, incluso en teoría de grafos, tiene quizás una desventaja: la existencia del objeto es probada, más su definición explícita es muy complicada en la mayoría de casos.

En la segunda parte del presente trabajo, basada en el artículo *Sur la répartition des*

entiers premiers à un entier sans petit facteur premier de A. Chadozeau [4], abordamos el estudio de los momentos centrales de grado k de los enteros coprimos con un entero dado q en intervalos de longitud h cuando $h \leq P^-(q)$, donde $P^-(q)$ representa el menor factor primo de q, empleando las ideas de los capítulos anteriores. Para hacer la analogía probablística, empezamos notando que la sucesión de coprimos con q tiene densidad $P = \varphi(q)/q$ y que podemos expresar el número de coprimos con q en el intervalo $[\![n+1, n+h]\!]$ como

$$X = \sum_{i=1}^{h} X_i(n),$$

donde $X_i(n) = 1$ si $(n+i, q) = 1$ y 0 en caso contrario. Es decir, como una suma de variables aleatorias en un espacio de probabilidad finito. Así, en vista del parecido evidente, tomamos como punto de partida el estudio de una variable aleatoria de la forma

$$Y = \sum_{i=1}^{h} Y_i,$$

donde Y_i son variables aleatorias independientes con $P\{Y_i = 1\} = P$, $P\{Y_i = 0\} = 1 - P$, siendo probable que el comportamiento de Y nos de luces para el propio de X. El estudio de los momentos de grado k de los enteros coprimos con q respecto de su valor promedio, a saber

$$M_k(q; h) = \sum_{n=1}^{q} \left(\sum_{i=1}^{h} [(n+i, q) = 1] - h\frac{\varphi(q)}{q} \right)^k$$

tiene una profunda relación con el estudio de la *función de Jacobsthal*, definida por

$$C(r) := \max_{\omega(q)=r} g(q) - 1,$$

donde

$$g(q) := \min \left\{ m : \min_{1 \leq i \leq m} (a+i, q) = 1, \, \forall a \in \mathbb{N} \right\}$$

es el menor número m tal que cualquier intervalo $[\![a+1, a+m]\!]$ de longitud m en $\mathbb{N}$ posee almenos algún coprimo con q, y $\omega(q)$ es el número de factores primos de q. Una rápida inspección de la función $g(q)$ muestra que si $q = \prod_{i=1}^{\omega(q)} p_i^{\alpha_i}$ es su factorización en producto de pontencias de primos, entonces

$$g(q) = g\left(\prod_{i=1}^{\omega(q)} p_i \right);$$

es decir que $g(q)$ depende solamente de los factores primos, más no de las potencias de éstos. Luego, el máximo en la definición de $C(r)$ puede ser considerado sobre los enteros

q sin factores cuadrados. De este modo, consideramos en el trabajo esta hipótesis sobre q, siendo éste el caso de mayor interés como acabamos de ver.

A. Chadozeau ([5]) nos muestra una reseña de algunos trabajos en relación a la acotación optimal para las funciónes g y C, como por ejemplo la conjeturas $C(r) < r^2$ (conjetura de Jacobsthal) y

$$g(q) \ll \frac{q}{\varphi(q)} \log q, \tag{1}$$

la acotación conjeturable más fuerte en relación a g. Es posible ver que el abordaje de dos de las conjeturas de Erdös, a saber las acotaciones

$$\sum_{i=1}^{\varphi(q)} (a_{i+1} - a_i)^\gamma \ll_\gamma \varphi(q) \left(\frac{q}{\varphi(q)}\right)^\gamma$$

para todo entero positivo $q \in \mathbb{N}$ y todo real $\gamma > 0$, donde $1 = a_1 < a_2 < \cdots$ son los enteros coprimos q, y la acotación uniforme

$$\sum_{i=1}^{\varphi(q)} e^{x(a_{i+1}-a_i)\varphi(q)/q} < \varphi(q)$$

para algún real $x > 0$, ambas estrechamente ligadas a (1), pasan por la acotación de los momentos centrales $M_k(q; h)$.

Estudiaremos primero los momentos centrales de grado k de la variable aleatoria Y, que tiene una distribución binomial de parámetros (h, P), probando que

$$\mu_k(h, P) = \sum_{j \geq 0} (hP(1-P))^j \, R_{k,j}(p)$$

donde $R_{k,j}$ son los denomidados *polinomios de Romanovsky*. Acotaciones sobre la norma de éstos nos permitirán luego acotar, uniformemente en h, k, $\mu_k(h, P)$, por

$$\mu_k(h, P) \ll \left(Ck\left(k + hP(1-P)\right)\right)^{k/2}.$$

Este resultado motiva de modo positivo el pensar que una acotación similar puede ser posible para los momentos $M_k(q; h)$. El proceso de adaptar los resultados acerca de una ley binomial a el estudio de los coprimos con q requiere fundamentalmente de la acotación de las covarianzas de las variables X_i

$$\mathbb{E}\left[\prod_{i \in I}(X_i - P)\right] = P^{\operatorname{card} I} \sum_{s=0}^{\operatorname{card} I} (-1)^{\operatorname{card} I - s} \binom{\operatorname{card} I}{s} \prod_{p|q} \frac{1 - s/p}{(1-1/p)^s},$$

objetivo que es motivo del último capítulo, con el cual mostramos la acotación

$$\mathbb{E}\left[\prod_{i \in I}(X_i - P)\right] \ll P^{\operatorname{card} I} \left(C \frac{\operatorname{card} I}{P^-(q) \log P^-(q)}\right)^{\operatorname{card} I/2}$$

para una constante absoluta C. Finalmente, el resultado para los momentos $M_k(h;P)$ es la acotación uniforme en h, $q \geq 2$ sin factores cuadrados, con $h \leq P^-(q)$,

$$\frac{M_k(q;h)}{q} \ll \left(Ck\left(k + h\frac{\varphi(q)}{q}\right)\right)^{k/2},$$

donde C es una constante absoluta.

Notaciones

Denotamos con $\mathbb{N}$ al conjunto de los números enteros mayores o iguales a 0, denominado conjunto de *números naturales*. Denotaremos con $\mathbb{Z}^+$ el conjunto de los enteros estrictamente positivos.
Dada una proposición P, denotamos con $[P]$ el valor de verdad de P, esto es

$$[P] = \begin{cases} 1, & \text{si } P \text{ es verdadera} \\ 0, & \text{en caso contrario.} \end{cases}$$

Dados los enteros m y n, denotaremos con $m|n$ la propiedad de que m es divisor de n. La notación $p|n$ indica que p es un número primo (divisor de n), en tanto que $p^m||n$ indica que p es primo y p^m es divisor de n, mas p^{m+1} no lo es. Respecto de los índices en sumatorias, debemos mencionar que la presencia de paréntesis indica suma sobre n-uplas ordenadas. Por ejemplo, las notaciones

$$\sum_{\substack{s_i \\ (1\leq i\leq n)}} \quad , \quad \sum_{\substack{(s_i) \\ 1\leq i\leq n}}$$

significan que la sumatoria se considera sobre todas las n-uplas ordenadas $(s_1, \ldots, s_n)$. Respecto del producto, recalcamos que el producto sobre un cojunto vacío de índices tiene, por convención, el valor de 1. Por otro lado, las notaciones clásicas o, O y la notación de Vinogradof $\ll$ serán usadas en el sentido usual. Esto es, para las funciones $f : \mathbb{R} \to \mathbb{R}$, $g : \mathbb{R} \to [0, +\infty)$,

- Usaremos la notación $f \sim g$ cuando $f(x)/g(x) \to 1$ cuando $x \to +\infty$. En este caso diremos que f y g son *asintóticamente equivalentes*.

- usamos la notación $f = O(g)$ para decir que existe una constante $M > 0$ tal que $|f(x)| \leq Mg(x)$, para todo $x \in \mathbb{C}$. La acotación $f = O(g)$ cuando $x \to \infty$ significa que $|f(x)| \leq Mg(x)$ para cuando x es suficientemente grande. Esto lo denotamos usualmente con $f \ll g$. Esta notación puede extenderse al caso $f : \mathbb{C} \to \mathbb{C}$ considerando $|x|$ suficientemente grande.

- La notación $f = o(g)$ cuando $x \to \infty$ significa que $f(x)/g(x) \to 0$ cuando $x \to \infty$.
- La notación $f(x) = h(x) + O(g(x))$ significa que $f(x) - h(x) = O(h(x))$, esto es, $|f(x) - h(x)| \leq Mg(x)$ para x suficientemente grande. Análogamente, la notación $f(x) = h(x) + o(g(x))$ hace referencia a la ecuación $f(x) - h(x) = o(g(x))$, esto es, $\lim_{x\to\infty} (f(x) - h(x))/g(x) = 0$.

Para una sucesión $(a_n) \subset \mathbb{R}$, la notación $a_n \uparrow L$ ($a_n \downarrow L$), donde $L \in \mathbb{R} \cup \{\pm\infty\}$ significa que (a_n) es creciente (decreciente) y que $\lim_{n\to\infty} a_n = L$.
Usaremos las notaciones convencionales para las funciones aritméticas más conocidas de la teoría de números. Por ejemplo,

$$\begin{aligned} \pi(x) &= \text{card}\{p \leq x,\ p \text{ es primo}\}, \\ \omega(n) &= \sum_{p|n} 1. \end{aligned}$$

Usaremos las letras n, i, j, k para denotar números enteros, salvo mención explícita de lo contrario.
La notación (m, n) denotará, salvo clara mención en lo contrario, al máximo común divisor de los enteros my n. $[\![a, n]\!]$ denotará el intervalo $\{a, a + 1, \cdots, b\}$ en $\mathbb{N}$. Los signos $\lfloor a \rfloor$ y $\lceil a \rceil$ denotan el máximo entero menor o igual que a y el mínimo entero mayor o igual que a respectivamente.
Para un conjunto finito A, denotamos por $\text{card}\, A$ o $|A|$ el número de elementos de A.
Dado un conjunto $A \subset \mathbb{N}$, definimos la *función característica* de A a ser la función $1_A : \mathbb{N} \to \mathbb{R}$ definida como $1_A(x) = [x \in A]$, para todo $x \in \mathbb{N}$. Evidentemente lo mismo se puede definir en el caso en que $A \subset \mathbb{R}^n$. Además, si $a = (a_n)_{n\in\mathbb{N}}$ es una sucesión de números naturales creciente, podemos definir su función característica 1_a mediante

$$1_a(x) = [\exists n \in \mathbb{N}, x = a_n].$$

Es posible ver que si $A = \{a_n,\ n \in \mathbb{N}\}$, entonces $1_A = 1_a$. De este modo, nos referiremos indistintamente a la función característica de una sucesión o del conjunto de elementos de ésta. Del mismo modo, para $B \subset \mathbb{N}$ escribiremos $a \cap B$, $a \cup B$ para referirnos a los conjuntos $A \cap B$ y $A \cup B$ respectivamente.

Capítulo 1

Preliminares

1.1. Números combinatorios

Dado un conjunto finito A , una enumeración (u ordenación) de A es una aplicación biyectiva $\sigma : [\![1, \operatorname{card} A]\!] \to A$. Es común denotar con $A = \{a_1, \cdots, a_k\}$, donde $k = \operatorname{card} A$ para indicar que en el conjunto A se ha **fijado** una enumeración σ con $\sigma(1) = a_1, \cdots, \sigma(k) = a_k$, usualmente arbitraria, pero fija. Del mismo modo, un *conjunto (partición, par, etc.) ordenado* es un par (A, σ), donde A es un conjunto y σ es una enumeración de A. Cuando no es necesario especificar o mencionar σ, mas sí el hecho de que la enumeración considerada es importante, o susceptible a modificaciones, como por ejemplo en caso de hacerse un conteo sobre las posibles formas de ordenamiento de los elementos de A, es común usar la notación $(a_1, \ldots, a_k)$, con $k = \operatorname{card} A$, para denotar el conjunto ordenado (A, σ), donde se entiende que $a_1 = \sigma(1)$, $\ldots$, $a_k = \sigma(k)$. Usaremos la notación estándar para los *números combinatorios*

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{si } 0 \leq k \leq n, \\ (-1)^{n-k} \frac{(-k-1)!}{(-n-1)!(n-k)!} & \text{si } k \leq n < 0, \\ 0 & \text{en otro caso.} \end{cases} \tag{1.1}$$

Mencionamos algunas propiedades usuales de los números combinatorios, que listamos en la siguiente proposición.

Proposición 1.1.1. *Se cumplen:*

i) $\binom{n}{b}\binom{b}{j} = \binom{n-j}{b-j}\binom{n}{j}$.

ii) $\binom{n}{b} = \binom{n-1}{b} + \binom{n-1}{b-1}$.

iii) $b\binom{n}{b} = n\binom{n-1}{b-1} = (n-b+1)\binom{n}{b-1}$ *(Ley de absorción).*

Consideremos ahora $n \in \mathbb{N}$ y una $k-upla$ $s = (s_1, \ldots, s_k) \in \mathbb{N}^k$ tal que $\sum_i s_i = n$ y $s_i \geq 1$ para todo i. Definimos el número combinatorio $\binom{n}{s}$ por

$$\binom{n}{s} = \frac{n!}{\prod_{i=1}^{k} s_i!}. \tag{1.2}$$

Es posible ver que $\binom{n}{s}$ mide el número de particiones ordenadas $(A_1, \ldots, A_k)$ del conjunto $[\![1, n]\!]$ tales que $\operatorname{card} A_i = s_i$, para todo $1 \leq i \leq k$. En el caso particular de (s_1, s_2), tenemos

$$\binom{n}{(s_1, s_2)} = \frac{n!}{s_1! s_2!} = \binom{n}{s_1} = \binom{n}{s_2},$$

que es también el número de maneras de escojer un conjunto con s_1 elementos de $[\![1, n]\!]$. Observemos que $s_2 = n - s_1$ queda automáticamente definido a partir de s_1, por lo que es usual denotar

$$\binom{n}{s_1} = \binom{n}{(s_1, s_2)},$$

no habiendo contradicción alguna con las definiciones anteriores.
Enunciamos ahora el *teorema del multinomio*, el cual generaliza la *fórmula del binomio de Newton*, y expresa la expansión de la $n-$ésima potencia de una suma de k elementos.

Proposición 1.1.2 (Teorema del multinomio)**.** *Para $a_i \in \mathbb{C}$, $1 \leq i \leq k$ se tiene*

$$\left(\sum_{i=1}^{k} a_i\right)^n = \sum_{\substack{s=(s_i)\subset\mathbb{N}^k \\ \sum s_i = n}} \binom{n}{s} \prod_{j=1}^{k} a_j^{s_j}$$

Demostración. Presentamos una prueba, o un esbozo de una, usando argumentos de análisis combinatorio: será suficiente ver que para cada $s = (s_1, \ldots, s_k) \in \mathbb{N}^k$ con $\sum_i s_i = n$, el término $a_1^{s_1} a_2^{s_2} \ldots a_k^{s_k}$ aparece $\binom{n}{s}$ veces en el desarrollo de la potencia. Para esto, vemos que la expresión $\left(\sum_{i=1}^{k} a_i\right)^n$ es un producto de n factores idénticos:

$$\left(\sum_{i=1}^{k} a_i\right)^n = (a_1 + \cdots + a_k) \ldots (a_1 + \cdots + a_k).$$

Podemos enumerar cada uno de los n factores, identificándolos con el conjunto $[\![1, n]\!]$. Cualquier término de la suma resultante puede ser obtenido escogiendo un a_i de cada factor (n en total) y multiplicando éstos. Ahora bien, para cada partición ordenada $(A_1, \ldots, A_k)$ (posiblemente $A_i = \emptyset$ para algún i) de $[\![1, n]\!]$, con $\operatorname{card} A_i = s_i$ para $1 \leq i \leq k$, podemos construir el término $a_1^{s_1} a_2^{s_2} \ldots a_k^{s_k}$ escogiendo a_1 de cada uno de los

factores identificados con elementos A_1, a_2 de los factores identificados con elementos de A_2, etc. Luego, el término $a_1^{s_1}a_2^{s_2}\dots a_k^{s_k}$ aparece una vez por cada partición ordenada $(A_1,\dots,A_k)$. Esto es, $\binom{n}{s}$ veces, lo que demuestra el resultado. □

En el caso que $a_i = 1$, para todo $i = 1,\dots,n$, tenemos el siguiente resultado.

Corolario 1.1.3. *Para $k, n \geq 1$, $k, n \in \mathbb{N}$ se tiene*

$$k^n = \sum_{\substack{c=(c_i)\subset\mathbb{N}\\ \sum c_i = n}} \binom{n}{c}.$$

El siguiente tipo especial de números utilizado con frecuencia en el análisis combinatorio son los llamados *números de Stirling de segunda especie*, denotados para $k, n \in \mathbb{N}$ por $\left\{{n \atop k}\right\}$, y definidos como el número de formas de particionar un conjunto con n elementos en k partes disjuntas. Es claro que entonces

$$\left\{{n \atop k}\right\} = 0, \text{ si } k > n.$$

A seguir, mencionaremos algunos resultados de nuestro interés. El lector interesado en un estudio detallado puede consultar, por ejemplo, [20, Chapitre V], [5, Appendice. A].

Proposición 1.1.4. *Tenemos la siguiente fórmula explícita para los números de Stirling:*

$$\left\{{n \atop k}\right\} = \sum_{j=0}^{k}(-1)^{k-j}\frac{j^{n-1}}{(j-1)!(k-j)!} = \frac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n$$

Demostración. Ver [20, p. 38]. □

Proposición 1.1.5. *Se cumple*

$$k!\left\{{n \atop k}\right\} = \sum_{\substack{s_i\geq 1\\ (1\leq i\leq k)\\ \sum_i s_i = n}} \binom{n}{s}$$

Demostración. Fijada una colección $(s_1,\dots,s_k)\subset\mathbb{N}$ tal que $s_i \geq 1$ para todo $1 \leq i \leq k$ y $\sum_i s_i = n$, el número de particiones (ordenadas) $(A_1,\dots,A_k)$ de $[\![1,n]\!]$ tales que $\operatorname{card} A_i = s_i$ para todo i es

$$\binom{n}{s} = \binom{n}{s_1,\dots,s_k} = \frac{n!}{\prod_{i=1}^k s_i!};$$

luego, el número total de particiones ordenadas $(A_1,\dots,A_k)$ de $[\![1,n]\!]$ es

$$\sum_{\substack{s_i\geq 1\\ (1\leq i\leq k)\\ \sum_i s_i = n}} \frac{n!}{\prod_{i=1}^k s_i!} = \sum_{\substack{s_i\geq 1\\ (1\leq i\leq k)\\ \sum_i s_i = n}} \binom{n}{s}.$$

Ahora, como $\left\{ {n \atop k} \right\}$ es el número de particiones (no ordenadas) de $[\![1, n]\!]$ en k partes, el número de particiones ordenadas sería $k!\left\{ {n \atop k} \right\}$, de donde

$$k!\left\{ {n \atop k} \right\} = \sum_{\substack{s_i \geq 1 \\ (1 \leq i \leq k) \\ \sum_i s_i = n}} \binom{n}{s},$$

como queríamos probar. □

Proposición 1.1.6. *Para n, k números naturales con $k \leq n$ se cumple*

$$k!\left\{ {n \atop k} \right\} \leq k^n$$

Demostración. Denotemos por

$$S = \{f : [\![1, n]\!] \to [\![1, k]\!];\ f \text{ es sobreyectiva}\}$$

y

$$F = \{f : [\![1, n]\!] \to [\![1, k]\!];\ f \text{ es función}\}.$$

Es claro que $\operatorname{card} S \leq \operatorname{card} F = k^n$. Fijadas una partición $A = \{A_i,\ 1 \leq i \leq k\}$ de $[\![1, n]\!]$ y una enumeración $\sigma(1), \ldots, \sigma(k)$ de $[\![1, k]\!]$, éstas definen una única aplicación sobreyectiva $f_{A,\sigma} : [\![1, n]\!] \to [\![1, k]\!]$ por la relación

$$f_{A,\sigma}(x) = \sigma(i),\ \text{para todo } x \in A_i.$$

Toda aplicación sobreyectiva de $[\![1, n]\!]$ en $[\![1, k]\!]$ es también de la forma $f_{A,\sigma}$, para algún par (A, σ), y como el número de enumeraciones σ de $[\![1, k]\!]$ es $k!$, entonces el número de elementos de S es $k!\left\{ {n \atop k} \right\}$. Luego,

$$k!\left\{ {n \atop k} \right\} = \operatorname{card} S \leq \operatorname{card} F = k^n.$$

□

Dada una sucesión $a = (a_i) \in \mathbb{R}$, decimos que la función f es una *función generatríz* para a si

$$f(x) = \sum_{n \geq 0} a_n \frac{x^n}{n!},$$

siendo la suma convergente para x en una vecindad abierta de 0. Será de utilidad el siguiente resultado, que nos brinda la función generatríz de los números de Stirling de segunda especie.

Proposición 1.1.7. *Fijado $k \in \mathbb{N}$, la función $f(x) = \dfrac{(e^x-1)^k}{k!}$ es función generatriz para los números de Stirling $\left\{ {n \atop k} \right\}$, $n \in \mathbb{N}$, i.e,*

$$\sum_{m\geq 0} \left\{ {m \atop k} \right\} \frac{x^m}{m!} = \frac{(e^x-1)^k}{k!}, \tag{1.3}$$

para todo $x \in \mathbb{R}$.

Demostración. La prueba de este resultado puede encontrarse en [20, p. 40]. □

1.2. Las funciones Γ y $\mathbb{\Gamma}$

Recordamos algunas propiedades básicas de la *función Gamma*, definida para $x \in \mathbb{R}\setminus(\mathbb{Z}^- \cup \{0\})$ por

$$\Gamma(x) = \int_0^{+\infty} e^{-t}t^x dt.$$

Para un estudio detallado de las propiedades de esta importante función, ver [17]. Mencionamos sin embargo algunos resultados que usaremos en el presente trabajo. Primero, $\Gamma(1) = 1$ y se tiene la fórmula de recursión $\Gamma(x+1) = x\Gamma(x)$, por lo que

$$\Gamma(n) = (n-1)!$$

para todo número narutal $n \geq 1$. Este resultado muestra que la función Γ es una extensión analítica del factorial de un número natural. Las siguientes acotaciones muestran el comportamiento de $\Gamma(t)$ para valores grandes de t.

Proposición 1.2.1 (Fórmula de Stirling)**.** *Se tiene, para todo $x \in \mathbb{R}\setminus(\mathbb{Z}^- \cup \{0\})$*

$$\Gamma(x) = \sqrt{2\pi}x^{x-1/2}e^{-x+\theta(x)/(12x)},$$

donde $0 < \theta(x) < 1$ es una constante dependiente de x. Como consecuencia, $n! = n\Gamma(n) = \sqrt{2\pi}n^{n+1/2}e^{-n+\theta(n)/12n}$ y

$$\Gamma(x) \sim \sqrt{2\pi}x^{x-1/2}e^{-x}$$

cuando $x \to +\infty$.

Demostración. Ver [17, pp. 20–24]. □

Proposición 1.2.2 (Fórmula de multiplicación de Gauss)**.** *Se tiene, para todo $x \in \mathbb{R}\setminus(\mathbb{Z}^- \cup \{0\})$*

$$\Gamma\left(\frac{x}{2}\right)\Gamma\left(\frac{x+1}{2}\right) = \frac{\sqrt{\pi}}{2^{x-1}}\Gamma(x).$$

Demostración. Ver [17, pp. 20–24]. □

Definimos ahora la noción de *doble factorial* de un número $n \in \mathbb{N}$ por

$$n!! = \begin{cases} \frac{n!}{2^{n/2}(n/2)!}, & n \text{ es par;} \\ 0, & n \text{ es impar.} \end{cases}$$

Notemos que $n!!$ está definido por la fórmula de recurrencia: $0!! = 1$, $1!! = 0$ y

$$(2n+2)!! = (2n+1)(2n)!!.$$

De modo análogo a como la función Γ es una extensión analítica de la noción de factorial, nos abocamos ahora a definir la función $\mathbb{\Gamma}$ por

$$\mathbb{\Gamma}(t+1) = \Gamma\left(\frac{t+1}{2}\right)\frac{2^{t/2}}{\sqrt{2}} = \frac{\Gamma(t+1)}{2^{t/2}\Gamma(t/2+1)}, \tag{1.4}$$

la cual es una extensión analítica de la noción de doble factorial. Para ver esto, sólo notemos que

$$\mathbb{\Gamma}(n+1) = \frac{\Gamma(n+1)}{2^{n/2}\Gamma(n/2+1)} = \frac{n!}{2^{n/2}(n/2)!} = n!! \tag{1.5}$$

para todo número natural par n. Además, de la Fórmula de Stirling para Γ podemos deducir la siguiente

Proposición 1.2.3 (Fórmula de Stirling)**.** *Para todo $n \in \mathbb{N}$ se tiene*

$$(2n)!! = \mathbb{\Gamma}(2n+1) \leq e^{1/24}\sqrt{2}\,(2n/e)^n\,.$$

Además,

$$\mathbb{\Gamma}(t+1) \sim \sqrt{2}\left(\frac{t}{e}\right)^{t/2}$$

cuando $t \to \infty$.

Demostración. Primero, de (1.5) y (1.4) tenemos

$$(2n)!! = \mathbb{\Gamma}(2n+1) = \frac{(2n)!}{2^n n!},$$

y usando la fórmula de Stirling para $(2n)!$ y $n!$ obtenemos

$$(2n)!! \;=\; \frac{\sqrt{2\pi}(2n)^{2n+1/2}e^{-2n}e^{\theta_1/24n}}{2^n\sqrt{2\pi}n^{n+1/2}e^{-n}e^{\theta_2/12n}} = \sqrt{2}(2n)^n e^{-n}e^{\theta_1/24n-\theta_2/12n},$$

y como $\theta_1/24n - \theta_2/12n \leq 1/24n \leq 1/24$ entonces

$$(2n)!! \leq e^{1/24n}\sqrt{2}\left(\frac{2n}{e}\right)^n \leq e^{1/24}\sqrt{2}\left(\frac{2n}{e}\right)^n.$$

Hemos probado así la primera afirmación de la proposición. Para probar la segunda, usamos (1.4) y la fórmula de recusión de Γ para obtener

$$\mathbb{\Gamma}(t+1) = \frac{\Gamma(t+1)}{2^{t/2}\Gamma(t/2+1)} = \frac{t\Gamma(t)}{2^{t/2}(t/2)\Gamma(t/2)}.$$

Usando nuevamente la fórmula de Stirling para $\Gamma(t)$ y $\Gamma(t/2)$ en la última expresión tendremos

$$\mathbb{\Gamma}(t+1) = \frac{t\sqrt{2\pi}t^{t-1/2}e^{-t}e^{\theta_1/12t}}{2^{t/2}(t/2)\sqrt{2\pi}(t/2)^{t/2-1/2}e^{-t/2}e^{\theta_2/6t}} = \sqrt{2}\left(\frac{t}{e}\right)^{t/2} e^{\theta_1/12t-\theta_2/6t},$$

y por tanto

$$\mathbb{\Gamma}(t+1) \sim \sqrt{2}\left(\frac{t}{e}\right)^{t/2}$$

cuando $t \to +\infty$, como se quería demostrar. □

1.3. La Integral de Riemann-Stieltjes

El propósito es describir brevemente una noción de integración ligeramente más general que la integral de Riemann. Consideremos un intervalo $[a,b]$ de $\mathbb{R}$. Por una partición de $[a,b]$ entendemos un conjunto ordenado en forma creciente

$$P = \{a = a_0 < a_1 < \ldots < a_n = b\}$$

de puntos de $[a,b]$. Por la *norma de* P entendemos el número

$$\|P\| = \max_{1\leq i\leq n} (a_i - a_{i-1}).$$

Dadas las particiones P y Q, decimos que Q es un *refinamiento* de P si $P \subset Q$. Decimos que Q es *más fina que* P si $\|Q\| \leq \|P\|$. Es claro que si Q es un refinamiento de P entonces es más fina que P.

Sean f, α funciones reales definidas en $[a,b] \subset \mathbb{R}$. Para $P = \{a = x_0 < x_1 < \ldots < x_n = b\}$ partición de $[a,b]$, una suma de la forma

$$S(P,f,\alpha) = \sum_{k=1}^{n} f(t_k)\Delta\alpha_k,$$

donde $t_k \in [x_{k-1}, x_k]$ y $\Delta\alpha_k = \alpha(x_k) - \alpha(x_{k-1})$ es llamada *suma de Riemann-Stieltjes de* f *con respecto de* α. Decimos que f es *integrable respecto de* α *en* $[a,b]$, si existe un número L tal que para todo $\varepsilon > 0$, existe una partición P_0 de $[a,b]$ tal que, para toda partición P más fina que P_0, y para cada elección de puntos $t_k \in [x_{k-1}, x_k]$ se tiene

$$|S(P,f,\alpha) - L| < \varepsilon.$$

En caso afirmativo, el número L es único, y lo denotaremos con $\int_a^b f(x)d\alpha(x)$. En el caso que $\alpha(x) = x$, estamos en el caso de la integral de Riemann. Al igual que en este caso, cuando $a = \pm\infty$ o $b = \pm\infty$ se definen las integrales impropias como el límite de integrales definidas en intervalos finitos. Por ejemplo,

$$\int_a^{+\infty} f(x)d\alpha(x) = \lim_{M\to+\infty} \int_a^M f(x)d\alpha(x),$$

y

$$\int_{-\infty}^{+\infty} f(x)d\alpha(x) = \int_{-\infty}^{c} f(x)d\alpha(x) + \int_c^{+\infty} f(x)d\alpha(x),$$

siempre que los límites existan.

Este concepto de integral suele ser útil para expresar sumas finitas como integrales y aplicar los resultados que tenemos disponibles en ésta. Por ejemplo, consideremos una sucesión creciente $a = (a_n)_{n\in\mathbb{N}}$ en $\mathbb{Z}^+$ y f una función integrable según Riemann. Sea

$$F_a(x) = \text{card}\{n \in \mathbb{N};\ 1 \leq a_n \leq x\}$$

a ser el número de elementos de la sucesión a menores o iguales que x. Entonces, para $0 \leq x < y$,

$$\int_x^y f(t)dF_a(t) = \sum_{x<a_n\leq y} f(a_n).$$

En el caso particular en que $a_n = n$, tenemos $F_a(x) = \lfloor x \rfloor$, de donde

$$\int_x^y f(t)d\lfloor t \rfloor = \sum_{x<n\leq y} f(n),$$

mientras que si a fuera la sucesión de números primos, tendriamos $F_a(x) = \pi(x)$, y así

$$\int_x^y f(t)d\pi(t) = \sum_{x<p\leq y} f(p).$$

El siguiente es el conocido teorema de integración por partes, válido también en el contexto de la integral de Riemann-Stieltjes, y muy útil en el cálculo y acotación de sumas.

Proposición 1.3.1 (Integración por partes)**.** *Sea $[a, b] \subset \mathbb{R}\cup\{\pm\infty\}$. Si f es integrable en $[a, b]$ respecto de α entonces α es integrable en $[a, b]$ respecto de f y se cumple*

$$\int_a^b \alpha(x)df(x) = \alpha(x)f(x)\Big|_a^b - \int_a^b f(x)d\alpha(x).$$

Demostración. Ver [1] □

Como un ejemplo elemental de aplicación del anterior resultado tenemos que si $f : [0, +\infty) \to \mathbb{R}$ es una función diferenciable, con derivada integrable según Riemann, entonces

$$\begin{aligned}\sum_{y<n\leq x} f(n) &= \int_y^x f(t)d\lfloor t\rfloor \\ &= f(t)\lfloor t\rfloor\Big|_x^y - \int_x^y \lfloor t\rfloor df(t) \\ &= f(y)\lfloor y\rfloor - f(x)\lfloor x\rfloor - \int_x^y \lfloor t\rfloor f'(t)dt.\end{aligned}$$

Finalmente, los siguientes tres clásicos resultados de teoría de números serán también herramientas para nuestro trabajo.

Teorema 1.3.2 (Teorema del número primo)**.** *Se cumple*

$$\frac{\pi(N)}{N} \sim \frac{1}{\log N}$$

cuando $N \to +\infty$*, donde*

$$\pi(N) = \text{card}\{p \leq N;\ p \text{ es primo}\}.$$

Demostración. Para una prueba analítica ver, por ejemplo, [1, Capítulo 13]. □

Un resultado más débil, pero suficientemente útil para algunas aplicaciones en el trabajo establece que

$$\frac{\pi(N)}{N} \ll \frac{1}{\log N}.$$

Puede verse la demostración en [1, teorema 4.6]

Teorema 1.3.3 (Mertens)**.** *Para* $N \geq 2$ *se tiene*

$$\sum_{p\leq N} \frac{\log p}{p} = \log N + O(1).$$

Demostración. Ver [16, p. 14]. □

Teorema 1.3.4. *Para* $N \geq 2$ *se cumple*

$$\sum_{p\leq N} \frac{1}{p} = \log\log N + O(1).$$

Demostración. Ver [1, Teorema 4.12]. □

Teorema 1.3.5 (Fórmula de Mertens)**.** *Para $N \geq 2$ se cumple*

$$\prod_{p \leq N} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log N} \left(1 + O\left(\frac{1}{\log N}\right)\right),$$

donde γ denota la constante de Euler definida por

$$\gamma = \lim_{n \to +\infty} \left(\sum_{i=1}^{n} \frac{1}{i} - \log n\right).$$

Así,

$$\prod_{p \leq N} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log N}$$

cuando $N \to +\infty$.

Demostración. Ver [16, p.17]. □

Capítulo 2

Modelo probabilístico

El presente capítulo tiene la intención de exponer algunos resultados propios de la teoría de probabilidades, junto con algunos ejemplos de aplicación de éstos a la teoría de números. Si bien es cierto que no es posible aplicar aquella de manera inmediata, es con frecuencia el análisis combinatorio el que permite la aplicación de algunos resultados. En todo caso, son los resultados de la teoría probabilística los que inspiran algunos en teoria de números, dando inicio a la teoría probabilística de números.

2.1. Resultados de teoría de probabilidades

Citamos en esta sección las definiciones básicas y algunos teoremas de la Teoría de la Probabilidad que serán importantes a lo largo del trabajo. Los detalles de éstos pueden ser encontrados en [6], [9].

Definición 2.1.1. Decimos que $(\Omega,\ \mathcal{F},\ P)$ es un *espacio de probabilidad* cuando $\Omega \neq \emptyset$, $\mathcal{F}$ es una σ-álgebra en Ω y P es una *medida de probabilidad* definida en $\mathcal{F}$, esto es, $P : \mathcal{F} \to \mathbb{R}^+$ es una función satisfaciendo

i) $P(\Omega) = 1$,

ii) Si $\{A_n,\ n \in \mathbb{N}\}$ es una familia numerable de conjuntos disjuntos de $\mathcal{F}$ entonces

$$P\left(\bigcup_{n\in\mathbb{N}} A_n\right) = \sum_{n\in\mathbb{N}} P\left(A_n\right).$$

Los conjuntos $A \in \mathcal{F}$ serán llamados *eventos*.

En caso la σ-álgebra $\mathcal{F}$ sea el conjunto potencia o sea claro por el contexto de cual se trata, escribiremos simplemente (Ω, P).

Denotaremos con $\mathcal{B}$ al σ-álgebra en $\mathbb{R}$ generada por los intervalos abiertos (σ-álgebra de Borel). A los elemtos de $\mathcal{B}$ les llamaremos *borelianos*.

Definición 2.1.2. Sea $(\Omega, \mathcal{F}, P)$ un espacio de probabilidad. Una función $X : \Omega \to \mathbb{R}^n$ $\mathcal{B}$-medible, esto es,

$$X^{-1}(B) \in \mathcal{F}, \quad \text{para todo } B \in \mathcal{B},$$

será llamada *variable aleatoria*. X será llamada integrable cuando

$$\int_\Omega |X| dP < +\infty,$$

donde la integral es entendida en el sentido de Lebesgue. Una exposición de ésta y sus propiedades pueden ser encontradas en [19].

Definida una variable aleatoria integrable X en $(\Omega, \mathcal{F}, P)$, definimos su *esperanza* a ser

$$\mathbb{E}[X] = \int_\Omega X dP.$$

$\mathbb{E}$ es así un operador lineal y representa el promedio de los valores que puede tomar X en Ω. Podemos ver que para $A \in \mathcal{F}$,

$$P(A) = \mathbb{E}[1_A]$$

donde 1_A es la función característica de A. También definimos los *momentos* de X a ser $\mathbb{E}\left[X^k\right]$ en caso ésta exista. Serán de utilidad los llamados *momentos centrales de grado* k a ser

$$\mu_k(X) = \mathbb{E}\left[(X - \mathbb{E}[X])^k\right],$$

que miden el grado de desviación de X respecto de su media $\mathbb{E}[X]$. El caso particular en que $k = 2$ es muy usado en análisis estadístico. El momento central de grado 2 lo llamamos *varianza*, y vendría a ser

$$\mu_2(X) = \mathbb{E}\left[(X - \mathbb{E}[X])^2\right] = \mathbb{E}[X^2] - \mathbb{E}[X]^2.$$

Por otro lado, X define una medida de probabilidad μ_X en $(\mathbb{R}, \mathcal{B})$ definida para $B \in \mathcal{B}$ arbitrario, por

$$\mu_X(B) = P\{X \in B\}.$$

Llamaremos frecuentemente *la ley de* X a la medida μ_X.
También X define una σ-álgebra $\mathcal{F}_X$ en Ω definida por

$$\mathcal{F}_X = \left\{X^{-1}(B),\ B \in \mathcal{B}\right\}.$$

Notemos que, por definición de variable aleatoria,

$$\mathcal{F}_X \subset \mathcal{F},$$

además de que X es medible respecto de $\mathcal{F}_X$. De hecho, $\mathcal{F}_X$ es la menor σ-álgebra respecto de la cual X es medible.
Una propiedad sobre los elementos de Ω se dice que se cumple casi ciertamente, lo que denotaremos *c.c* cuando lo haga en un conjunto de medida 1. De este modo, dos variables aleatorias X_1, X_2 definidas en $(\Omega, \mathcal{F}, P)$ son *iguales casi ciertamente* cuando

$$P\{X_1 \neq X_2\} = 0.$$

Dada una medida μ en $\mathbb{R}$, definimos su *función de distribución* a ser la función $F_\mu : \mathbb{R} \to [0,1]$ definida por

$$F_\mu(x) = \mu(-\infty, x].$$

En caso que μ sea la ley de alguna variable aleatoria $X : \Omega \to \mathbb{R}$, nos referiremos a F_μ como la *función de distribución* de X, y la denotaremos con F_X. Así,

$$F_X(x) = \mu_X(-\infty, x] = P\{X \leq x\}.$$

Tenemos las siguientes propiedades de las funciones de distribución.

Proposición 2.1.1. *Si F_μ es la función de distribución de la medida de probabilidad μ en $\mathbb{R}$ entonces se cumple que*

i) F_μ *es no decreciente.*

ii) $\lim_{x\to+\infty} F_\mu(x) = 1$, $\lim_{x\to-\infty} F_\mu(x) = 0$.

iii) F *es una función continua por la derecha.*

iv) $\mu(\{x\}) = F_\mu(x) - \lim_{y\to x^-} F_\mu(y)$, *en particular si* F_μ *es continua se tiene que* $\mu(\{x\}) = 0$.

Demostración. Ver [9, p. 10]. □

Además, las propiedades descritas en la proposición anterior describen completamente a las funciones de distribución.

Teorema 2.1.2. *Si $F : \mathbb{R} \to \mathbb{R}$ es una función que satisface las propiedades (i), (ii) y (iii) de la proposición anterior, entonces F es la función de distribución de alguna variable aleatoria.*

Demostración. Ver [9, p. 10]. □

En vista de este resultado, una función que satisface las propiedades (i), (ii) y (iii) de la proposición 2.1.1 será llamada *función de distribución*. Un estudio amplio de las funciones de distribución puede ser encontrado en [6].
El concepto de independiencia es uno de los conceptos centrales en teoría probabilística. La idea de que la probabilidad de éxito de el lanzamiento de una moneda no depende en absoluto del resultado del lanzamiento de otra, o de la misma en un momento posterior induce a abstraer este concepto de un modo matemático. Así, dos eventos A y B se dicen *independientes* cuando

$$P(A \cap B) = P(A)P(B).$$

En general, la definición de independencia para σ-álgebras es como sigue: una familia finita de σ-álgebras F_i, $i \in I$ (I finito) se dice *independiente* cuando cualquier colección A_i, $i \in I$, con $A_i \in F_i$ se tenga

$$P\left(\bigcap_{i\in I} A_i\right) = \prod_{i\in I} P\left(A_i\right).$$

Una familia de σ-álgebras F_i, $i \in I$ (I no necesariamente finito)se dice independiente cuando cualquier subfamilia finita lo sea. Las definiciones de independencia pueden trasladarse también a las variables aleatorias mediante el uso del σ-álgebra generada por éstas. Así, una familia finita de variable aleatorias X_i, $i \in I$ se dice *independientes* cuando sus σ-álgebras generadas lo sean. Esto es equivalente a afirmar que

$$P\left(\bigcap_{i\in I}\{X_i \in B_i\}\right) = \prod_{i\in I} P\{X_i \in B_i\}$$

para toda colección finita $B_i \in B$, $i \in I$.

Proposición 2.1.3. *Sean X_i, $i \in \{1, ..., n\}$ variables aleatorias independientes en un espacio de probabilidad $(\Omega, \mathcal{F}, P)$. Entonces*

$$\mathbb{E}\left[\prod_{i=1}^{n} X_i\right] = \prod_{i=1}^{n} \mathbb{E}\left[X_i\right].$$

Demostración. Ver [9, p. 46]. □

Si tenemos dos variables aleatorias X, Y, decidir su independencia o no es en general un problema muy difícil. Definimos la covarianza de X e Y a ser

$$\operatorname{cov}[X, Y] = \mathbb{E}\left[(X - E[X])\,(Y - E[Y])\right] = \mathbb{E}\left[XY\right] - E[X]E[Y].$$

En el caso que X e Y son independientes se cumple $\operatorname{cov}[X,Y] = 0$. De este modo, $\operatorname{cov}[X,Y]$ es una medida del grado de correlación entre las variables X e Y. En general, definimos la covarianza de un conjunto finito X_i, $i \in I$ de variables aleatorias a ser

$$\operatorname{cov}[X_i, i \in I] = \mathbb{E}\left[\prod_{i\in I}(X_i - \mathbb{E}[X_i])\right],$$

que es 0 en caso las variables X_i sean independientes.

Lema 2.1.4. *A y B son eventos independientes si, y sólo si, 1_A y 1_B son variables aleatorias independientes.*

Demostración. Si denotamos con $\sigma(A)$ y $\sigma(B)$ los σ-álgebras generados por 1_A y 1_B respectivamente, entonces

$$\sigma(A) = \{\emptyset, \Omega, A, A^c\}, \qquad \sigma(A) = \{\emptyset, \Omega, A, A^c\}$$

Si 1_A y 1_B son independientes, es claro que A y B lo son, pues $A \in \sigma(A)$ y $B \in \sigma(B)$. Para la implicación contraria, analicemos los elementos de la forma $C \cap D$, donde $D \in \sigma(A)$ y $D \in \sigma(B)$. Los casos en que $C = \emptyset$, Ω o $D = \emptyset$, Ω puede verse sin problema que $p(C \cap D) = P(C)P(D)$. Los siguientes casos los conforman las expresiones $A \cap B$, $A \cap B^c$, $A^c \cap B$ y $A^c \cap B^c$. En el primer caso, por hipótesis tenemos que $P(A \cap B) = P(A)P(B)$. Para el segundo, vemos que

$$P(A) = P\left(A \cap B^c\right) + P(A \cap B) = P\left(A \cap B^c\right) + P(A)P(B),$$

y así

$$P\left(A \cap B^c\right) = P(A)\left(1 - P(B)\right) = P(A)P(B^c).$$

El mismo razonamiento se aplica para probar que A^c y B son independientes, así como A^c y B^c. Los elementos $\emptyset$ reduce cualquier intersección a un conjunto de probabilidad 0 mientras que Ω no la afecta, por lo que la prueba está concluída. □

Observación 2.1.1. Como consecuencia de la proposición anterior, si A y B son eventos independientes, entonces también lo son A^c y B^c. Es posible ver que si las variables aleatorias X e Y son independientes y $f, g : \mathbb{R} \to \mathbb{R}$ son funciones continuas, entonces $f(X)$ y $g(Y)$ son también variables aleatorias independientes. Ésto es consecuencia de que, por la continuidad de f y g, $\sigma(f(X)) \subset \sigma(X)$ y $\sigma(g(Y)) \subset \sigma(Y)$. Si X e Y son independientes, podemos ver que

$$\begin{aligned}
\operatorname{Var}[X+Y] &= \mathbb{E}\left[(X+Y)^2\right] - \mathbb{E}[X+Y]^2 \\
&= \mathbb{E}[X^2 + 2XY + Y^2] - \left(\mathbb{E}[X]^2 + 2\mathbb{E}[X]\mathbb{E}[Y] + \mathbb{E}[Y]^2\right) \\
&= \mathbb{E}[X^2] + 2\mathbb{E}[X]\mathbb{E}[Y] + \mathbb{E}[Y^2] - \left(\mathbb{E}[X]^2 + 2\mathbb{E}[X]\mathbb{E}[Y] + \mathbb{E}[Y]^2\right) \\
&= \mathbb{E}[X^2] + \mathbb{E}[Y^2] - \mathbb{E}[X]^2 - \mathbb{E}[Y]^2 = \operatorname{Var}[X] + \operatorname{Var}[Y].
\end{aligned}$$

En general, si X_i, $i \in I$ (I finito) son independientes,

$$\text{Var}\left[\sum_{i\in I} X_i\right] = \sum_{i\in I} \text{Var}[X_i].$$

Denotamos, para una familia numerable $\mathcal{A} = \{A_n,\ n \in \mathbb{N}\}$ de elementos de $\mathcal{F}$,

$$\liminf_{n\in\mathbb{N}} A_n = \bigcup_{n=1}^{\infty} \bigcap_{k\geq n} A_k,$$

y también

$$\limsup_{n\in\mathbb{N}} A_n = \bigcap_{n=1}^{\infty} \bigcup_{k\geq n} A_k,$$

llamados el *límite inferior* y el *límite superior*, respectivamente, de la familia $\mathcal{A}$. Observemos que $\liminf_{n\in\mathbb{N}} A_n$ es el conjunto de todos los elementos que pertenecen a todos salvo una familia finita de los conjuntos A_n, mientras que $\limsup_{n\in\mathbb{N}} A_n$ es el conjunto de todos los elementos que pertenecen a una cantidad infinita de los conjuntos A_n. De este modo, es claro que $\liminf_{n\in\mathbb{N}} A_n \subset \limsup_{n\in\mathbb{N}} A_n$.

Lema 2.1.5 (Borel-Cantelli)**.** *Sean A_n, $n \in \mathbb{N}$ eventos en un espacio de probabilidad $(\Omega, \mathcal{F}, P)$ tales que*

$$\sum_{n=1}^{+\infty} P\left(A_n\right) < +\infty.$$

Entonces,

$$P\left(\limsup_{n\in\mathbb{N}} A_n\right) = 0.$$

Demostración. Ver [9, p. 65]. □

El siguiente resultado puede verse también como consecuencia de la desigualdad de Markov ([9, p. 29]).

Proposición 2.1.6 (Desigualdad de Chebyshev)**.** *Si ϕ es una función estrictamente positiva y creciente en $(0, +\infty)$, con $\phi(-x) = \phi(x)$, y X es una variable aleatoria tal que $E[\phi(X)] < \infty$ entonces, para $a > 0$:*

$$\phi(a)P\{|X| \geq a\} \leq \mathbb{E}[\phi(X)].$$

Demostración. Ver [6, p. 51]. □

Como una consecuencia de este teorema, si consideramos la función $\phi(x) = x^2$, tenemos que para $a \in \mathbb{R}$,

$$a^2 P\{|X| \geq a\} \leq \mathbb{E}[X^2].$$

Algo más interesante es que si $Y = (X - \mathbb{E}[X])^2$ y $\lambda > 0$, entonces $\mathbb{E}[Y] = \mathrm{Var}[X]$, y si aplicamos la desigualdad de Chebychev para $a = \lambda^2 \mathbb{E}[Y]$,

$$P\{Y \geq \lambda^2 \mathbb{E}[Y]\} \leq \frac{\mathbb{E}[Y]}{\lambda^2 \mathbb{E}[Y]} = \frac{1}{\lambda^2},$$

o sea

$$P\{|X - \mathbb{E}[X]| > \lambda \sqrt{\mathrm{Var}[X]}\} \leq \frac{1}{\lambda^2}. \tag{2.1}$$

Teorema 2.1.7 (Ley fuerte de los grandes números)**.** *Sea* (Y_n) *una sucesión de variables aleatorias independientes definidas en un espacio de probabilidad* $(\Omega, \mathcal{F}, P)$ *tales que* $\mathbb{E}[Y_n] = 0$*, para todo* $n \in \mathbb{N}$*. Sea* $(a_n) \subset \mathbb{R}^+$ *creciente tal que* $a_n \to +\infty$ *cuando* $n \to +\infty$*. Si*

$$\sum_{n=1}^{+\infty} \frac{\mathrm{Var}\,[Y_n]}{a_n^2} < +\infty,$$

entonces

$$\frac{1}{a_n} \sum_{i=1}^{n} Y_i \to 0$$

con probabilidad 1*.*

Demostración. Ver [10, p. 189]. □

La siguiente es una versión ligeramente distinta de la ley de los grandes números.

Teorema 2.1.8 (Ley de los grandes números)**.** *Sea* (X_n) *una sucesión de variables aleatorias independientes, con* $\mathbb{E}[X_n] > 0$*, para todo* $n \in \mathbb{N}$*. Supongamos también que* $\sum_{1 \leq i \leq n} \mathbb{E}[X_i] \uparrow +\infty$ *cuando* $n \to \infty$ *y que*

$$\sum_{n \geq 1} \frac{\mathrm{Var}\,(X_n)}{\left(\sum_{j \leq n} \mathbb{E}[X_j]\right)^2} < +\infty.$$

Entonces

$$\lim_{n \to +\infty} \frac{\sum_{j \leq n} X_j}{\sum_{j \leq n} \mathbb{E}[X_j]} = 1$$

con probabilidad 1*.*

Demostración. Usamos la Ley Fuerte de los Grandes Números (teorema 2.1.7) con

$$a_n = \sum_{i=1}^{n} \mathbb{E}[X_i],$$

$$Y_i = X_i - \mathbb{E}[X_i],$$

de donde obtenemos el resultado. □

La noción de convergencia casi cierta no es la única en teoría de probabilidades. La siguiente es una noción muy útil de convergencia para variables aleatorias, la cual sólo depende de las funciones de distribución que éstas definen en $\mathbb{R}$.

Definición 2.1.3. Sean μ, μ_n, $n \in \mathbb{N}$ medidas de probabilidad en $\mathbb{R}$. Decimos que μ_n converge débilmente a μ, y denotamos

$$\mu_n \Rightarrow \mu,$$

si

$$\mu_n(f) \to \mu(f),$$

cuando $n \to +\infty$, para toda función $f : \mathbb{R} \to \mathbb{R}$ uniformemente continua y limitada. Decimos que una sucesión de variables aleatorias X_n converge débilmente a otra variable X (todas definidas en el mismo espacio de probabilidad) cuando sus leyes μ_{X_n} lo hagan a μ_X.

Proposición 2.1.9. *Sean μ, μ_n, $n \in \mathbb{N}$ medidas de probabilidad en $\mathbb{R}$. $\mu_n \Rightarrow \mu$ si, y sólo si,*

$$F_{\mu_n}(z) \to F_\mu(z),$$

cuando $n \to +\infty$, para todo z punto de continuidad de F_μ.

Demostración. Ver [3, p. 16, teorema 2.1]. □

Para un estudio bastante extenso acerca de la convergencia de variables aleatorias y resultados acerca de ésta se puede consultar [3].

2.2. Teoría probabilística de números

Presentamos en esta sección algunas ideas para aproximar un problema de teoría de números, por lo general el estudio de cierta función aritmética, mediante el empleo de conceptos propios de teoría probabilística. El objetivo es aplicar las diferentes herramientas de esta teoría para conjeturar algunos resultados acerca de la sucesión aritmética en estudio. Sin embargo, como iremos viendo, no es en general posible el expresar un problema aritmético en forma de uno probabilístico sin perder conceptos cruciales en el camino, por ejemplo el de independencia, que tan requerido es por las herramientas probabilísticas. Es así como el empleo de este tipo de herramientas tiene que remitirse en algunos casos a ser una guía, y los resultados que con éstas se obtienen una motivación para buscar resultados similares mediante el uso de herramientas

diseñadas para trabajar con conjuntos finitos. Tales herramientas son, por supuesto, las del análisis combinatorio.
Hay, sin embargo, un tipo de problemas en los que no es imposible utilizar resultados probabilísticos directamente: los problemas de existencia, como veremos en la sección 2.2.5.

2.2.1. Densidad

Consideremos un subconjunto $A \subset \mathbb{N}$. Queremos estudiar la idea de la probabilidad de que un número entero z pertenezca a A. Un primer y evidente intento sería el definir una adecuada medida de probabilida P en $\mathbb{Z}^+$. Ésta, por cierto, no podría ser arbitraria. Para que sea interesante desde el punto de vista numérico, debería respetar algunas ideas intuitivas básicas. Una de ellas es, por ejemplo, si $A = 2\mathbb{Z}^+$ es el conjunto de los número pares, se debería tener $P(A) = 1/2$, ya que en cierto modo, uno de cada dos números es par. De un modo más general, la probabilidad de que un número sea múltiplo de un entero m tendría que ser $1/m$. El siguiente resultado muestra que tales condiciones no son esperables de una medida de probabilidad.

Proposición 2.2.1. *No existe una medida de probabilidad P definida en $\mathbb{Z}^+$ tal que, para todo $m \in \mathbb{Z}^+$,*

$$\mathcal{P}(m\mathbb{Z}^+) = \frac{1}{m}. \tag{2.2}$$

Demostración. Probemos el resultado por contradicción. Sea P una medida de probabilidad en $\mathbb{Z}^+$ tal que (2.2) se cumple para todo $m \in \mathbb{Z}^+$. Observemos que para $a, b \in \mathbb{Z}^+$, con $(a, b) = 1$ tenemos que

$$a\mathbb{Z}^+ \cap b\mathbb{Z}^+ = ab\mathbb{Z}^+,$$

de donde

$$P\left(a\mathbb{Z}^+ \cap b\mathbb{Z}^+\right) = \frac{1}{ab} = P\left(a\mathbb{Z}^+\right) P\left(b\mathbb{Z}^+\right),$$

por lo que los conjuntos $a\mathbb{Z}^+$ y $b\mathbb{Z}^+$ son independientes. Luego, por la proposición 2.1.4 los eventos

$$\mathbb{Z}_a^+ := \mathbb{Z}^+ \setminus \left(a\mathbb{Z}^+\right),\ \mathbb{Z}_b^+ := \mathbb{Z}^+ \setminus \left(b\mathbb{Z}^+\right),$$

son también independientes. Así,

$$P\left(\mathbb{Z}_a^+ \cap \mathbb{Z}_b^+\right) = \left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right).$$

Dado $m \in \mathbb{Z}^+$ arbitrario, para $p > m$ primo tenemos que $m \in \mathbb{Z}_p^+$. Luego para $N > m$ cualquiera se tenemos

$$\{m\} \subset \bigcap_{m<p\leq N} \mathbb{Z}_p^+,$$

por lo que, como $(p, q) = 1$ para $p \neq q$ primos,

$$P\{m\} \leq P\left(\bigcap_{m<p\leq N} \mathbb{Z}_p^+\right) = \prod_{m<p\leq N}\left(1 - \frac{1}{p}\right).$$

Usamos entonces la fórmula de Mertens (teorema 1.3.5) para concluir que

$$0 \leq P\{m\} \leq \lim_{N\to+\infty} \prod_{m<p\leq N}\left(1 - \frac{1}{p}\right) = 0$$

para todo $m \in \mathbb{Z}^+$. De la aditividad de la medida de probabilidad P tendríamos entonces que

$$P\{\mathbb{Z}^+\} = \sum_{m\in\mathbb{Z}^+} P\{m\} = 0,$$

lo que es una contradicción. Esto prueba la proposición. □

La proposición 2.28 muestra que no es posible definir una medida de probabilidad en $\mathbb{Z}^+$ que satifaga 2.2. El siguiente concepto es, como mostraremos, una mejor aproximación en este sentido, aunque no es una medida en sentido estricto.

Definición 2.2.1 (Densidad)**.** Sea $A \subset \mathbb{Z}^+$. Decimos que A tiene *densidad (natural)* si el límite

$$\delta(A) = \lim_{N\to+\infty} \frac{|A \cap [\![1, N]\!]|}{N} \tag{2.3}$$

existe. En este caso, $\delta(A)$ será llamada la *densidad* de A.

Observación 2.2.1. En el caso de una sucesión creciente $a = (a_n)_{n\in\mathbb{N}} \subset \mathbb{Z}^+$, diremos que a tiene densidad α cuando $\delta(A) = \alpha$ donde $A = \{a_n, n \in \mathbb{N}\}$. Esto es,

$$\alpha = \lim_{N\to+\infty} \frac{|a \cap [\![1, N]\!]|}{N}.$$

Ejemplo 2.2.1. El conjunto de los números primos tiene densidad 0. En efecto, del teorema del número primo (teorema 1.3.2), si

$$\pi(N) = \operatorname{card} A_N = |\{p; p \leq N\}|,$$

entonces

$$\lim_{N\to+\infty} \frac{\pi(N)\log N}{N} = 1.$$

Luego, como

$$\frac{\pi(N)}{N} \ll \frac{1}{\log N} \to 0$$

entonces $\lim_{N\to+\infty} \pi(N)/N = 0$, lo que muestra lo afirmado.

Notemos que la idea de densidad respeta la idea intuitiva de cuantos múltiplos de m debería haber en $\mathbb{Z}^+$. Podemos observar que:

i) Para un entero positivo r, el conjunto rZ tiene densidad $1/r$. Para verificar esto, notamos que

$$|\{n \in \mathbb{N}; nr \leq N\}| = \left\lfloor \frac{N}{r} \right\rfloor,$$

y por tanto

$$\frac{1}{r} - \frac{1}{N} = \frac{N/r - 1}{N} \leq \frac{1}{N}|\{n \in \mathbb{N}; nr \leq N\}| \leq \frac{1}{r},$$

y haciendo $N \to \infty$ obtenemos el resultado. De igual modo, la densidad de la progresión aritmética $A = \{a_0 + nr,\ n \in \mathbb{Z}^+\}$ posee densidad $1/r$. En efecto, observamos que

$$|\{n;\ a_0 + rn \leq N\}|\,| = |\{n;\ nr \leq N - a_0\}| = \left\lfloor \frac{N - a_0}{r} \right\rfloor,$$

de donde

$$\frac{1}{N}\,|\{n;\ a_0 + rn \leq N\}| = r + O\left(\frac{1}{N}\right).$$

Haciendo $N \to +\infty$, obtenemos que la densidad de A es r.

ii) Una sucesión estrictamente creciente (a_n) de $\mathbb{Z}^+$ tiene densidad α si, y sólo si,

$$\lim_{n \to +\infty} \frac{n}{a_n} = \alpha.$$

En efecto, supongamos primero que (a_n) tiene densidad α. Entonces, observando que

$$\frac{1}{a_N}|\{n;\ a_n \leq a_N\}| = \frac{N}{a_N},$$

tenemos haciendo $N \to +\infty$ que $N/a_N \to \alpha$. Para la otra implicación, observemos que para $N \in \mathbb{N}$ existe $n \in \mathbb{N}$ tal que $a_n \leq N < a_{n+1}$. De este modo,

$$\frac{1}{N}\,|\{i;\ a_i \leq N\}| = \frac{n}{N} \geq \frac{n}{a_{n+1} - 1}. \tag{2.4}$$

Denotemos

$$\eta_n = \frac{n+1}{a_{n+1}} - \frac{n}{a_{n+1} - 1} = \frac{a_{n+1} - (n+1)}{a_{n+1}\,(a_{n+1} - 1)};$$

como $a_n \geq n$ para todo $n \in \mathbb{N}$, entonces

$$0 \leq \eta_n \leq \frac{1}{a_{n+1} - 1} \to 0,$$

cuando $n \to +\infty$. Observando finalmente que, por la definición de η_n y (2.4),

$$\frac{n+1}{a_{n+1} - 1} - \eta_n = \frac{n}{a_{n+1} - 1} \leq \frac{|a \cap [\![1, N]\!]|}{N} \leq \frac{n}{a_n},$$

y haciendo $n \to +\infty$ obtenemos que

$$\lim_{N\to+\infty} \frac{|a \cap [\![1, N]\!]|}{N} = \alpha.$$

Esto es lo que queríamos probar.

iii) Existen sucesiones crecientes en $\mathbb{Z}^+$ que no tienen densidad. Para un ejemplo de tales sucesiones, definamos

$$A = \bigcup_{k=0}^{+\infty} \{n;\ 10^k \leq n < 2 \cdot 10^k\}.$$

Definamos, para cada N,

$$A_N = A \cap [\![1, N]\!].$$

Entonces, tenemos que

$$|A_{10^m-1}| = \sum_{k=0}^{m-1} 10^k = \frac{1}{9}\left(10^m - 1\right),$$

$$|A_{2\cdot 10^m-1}| = \frac{1}{9}\left(10^m - 1\right) + 10^m = \frac{5}{9}\left(2 \cdot 10^m - 1\right) + \frac{4}{9}.$$

Luego, tenemos que el límite definido en (2.3) no existe.

iv) La unión finita de conjuntos de densidad 0 es también un conjunto de densidad 0. También todo subconjunto de un conjunto de densidad 0 tiene también densidad 0, así como la union e intersección finita de conjuntos con densidad 0 es también un conjunto de densidad 0.

v) Teniendo en cuenta que un subconjunto de $\mathbb{N}$ tiene densidad 0 si, y sólo si, su complemento tiene densidad 1, y del ítem anterior, entonces la unión e intersección finita de conjuntos con densidad 1 tiene también densidad 1.

Vayamos ahora con una interpretación probabilística del concepto de densidad: definamos los espacios de probabilidad (las σ-álgebras son el conjunto potencia respectivo) (Ω_N, ν_N), donde

$$\Omega_N = [\![1, N]\!]$$

y ν_N es la medida de probabilidad natural, es decir, para $C \subset \Omega_N$,

$$\nu_N(C) = \frac{|C|}{N} = \frac{1}{N}\sum_{x\in C} 1.$$

Entonces, la densidad de A es

$$\delta(A) = \lim_{N\to+\infty} \nu_N(A \cap \Omega_N),$$

en caso el límite exista; es decir, el límite de las medidas de las restricciones de A a los conjuntos Ω_N. Si consideramos a la función característica 1_A, observamos que

$$\nu_N(A \cap \Omega_N) = \sum_{n \in \Omega_N} \nu_N(\{n\}) 1_A|_{\Omega_N}(n) = \mathbb{E}[1_A|_{\Omega_N}].$$

Luego, la densidad de A puede ser entendida como el límite de las esperanzas de las restricciones de su función característica a Ω_N cuando $N \to +\infty$, las cuales son variables aleatorias. Claramente, lo mismo puede decirse en el caso en que A es una sucesión creciente de números naturales.

2.2.2. Función de distribución y orden normal

Consideremos una sucesión $a = (a_n) \subset \mathbb{N}$ creciente de números naturales, y su función característica $f : \mathbb{N} \to \mathbb{R}$. La densidad de a puede interpretarse como el límite de las esperanzas de una sucesión de variables aleatorias f_N definidas en sendos espacios de probabilidad finitos (Ω_N, μ_N), a saber, $f_N = f|_{\Omega_N}$, $N \in \mathbb{N}$, como vimos en la sección anterior. Con este punto de vista, podemos interpretar la existencia de una función de distribución para a a ser el límite de las funciones distribución de las variables f_N. La teoría de la probabilidad tiene un concepto más preciso para este hecho.

Definición 2.2.2. Sea $a \subset \mathbb{N}$ una sucesión aritmética, f su función característica y F una función de distribución. Sean $f_N = f|_{\Omega_N}$, donde $\Omega_N = \{1, ..., N\}$. Decimos que a tiene la *función distribución límite* (o simplemente *función distribución*) F cuando

$$F_N \Rightarrow F,$$

donde F_N son las funciones distribución de las variables aleatorias f_N, definidas para $z \in \mathbb{R}$ por

$$F_N(z) = \mu_N\left(\{n; f_N(n) \leq z\}\right).$$

Esto es, $F_N(z) \to F(z)$ cuando $N \to +\infty$ para todo z punto de continuidad de F (ver la definición 2.1.9).

A modo de ejemplo, veamos la relación entre el concepto de densidad y el de función distribución límite.

Ejemplo 2.2.2. Es equivalente decir que una sucesión de enteros tiene densidad α a afirmar que su función característica 1_A tiene la función de distribución F definida por

$$F(z) = \begin{cases} 0 & , z < 0; \\ 1 - \alpha & , 0 \leq z < 1; \\ 1 & , z \geq 1. \end{cases}$$

Probaremos el caso $\alpha \neq 0$, en el que 1 no es punto de continuidad de F. En efecto,

- Supongamos primero que $A = \{a_n;\ n \in \mathbb{N}\}$ tiene densidad α. Es claro que para $z < 0$, $F_N(z) = 0$ y que para $z \geq 1$: $F_N(z) = 1$ para todo $N \in \mathbb{Z}^+$ pues $0 \leq 1_A \leq 1$, por tanto $\lim_{N\to\infty} F_N(z) = F(z)$ en estos casos. Ahora, sea $0 \leq z < 1$. De la definición de función de distribución, debemos probar que

$$\lim_{N\to\infty} F_N(z) = 1 - \alpha,$$

donde F_N son las funciones distribución de las restricciones de 1_A a $\Omega_N = [\![1, N]\!]$. Notemos que

$$F_N(z) = \mu_N\{1_A \leq z\} = \mu_N\{1_A = 0\} = 1 - \mu_N\{1_A = 1\}, \tag{2.5}$$

y haciendo $N \to +\infty$,

$$\lim_{N\to+\infty} F_N(z) = 1 - \lim_{N\to+\infty} \mu_N\{1_A = 1\} = 1 - \alpha,$$

que es lo que queríamos probar.

- Para la otra implicación es suficiente ver (2.5) y hacer $N \to +\infty$. Así tenemos lo que habíamos afirmado.

El concepto de "casi ciertamente" en teoría de la probabilidad puede ser naturalmente entendido también en el contexto de la teoría de números. Una propiedad sobre los números enteros positivo se dice válida *casi cietamente*, denotado con *c.c*, cuando lo sea excepto en un conjunto de densidad 0. Un concepto más útil (pero más debil) para el estudio de funciones aritméticas con crecimiento irregular es el concepto de orden normal.

Definición 2.2.3 (Orden normal)**.** Sea $f : \mathbb{N} \to \mathbb{R}$ una función aritmética. Decimos que la función $g : \mathbb{N} \to \mathbb{R}$ es un *orden normal* de f cuando, para todo $\varepsilon > 0$, existe un conjunto $A_\varepsilon \subset \mathbb{N}$ con densidad 1 (que depende de ε) tal que

$$|f(n) - g(n)| \leq \varepsilon |g(n)|,$$

para todo $n \in A_\varepsilon$.

Observación 2.2.2. Es posible que una función f tenga varios órdenes normales.

Observación 2.2.3. La definición de orden normal es equivalente a la siguiente: dado $\varepsilon > 0$, el conjunto de los $n \in \mathbb{N}$ tales que

$$|f(n) - g(n)| > \varepsilon g(n) \tag{2.6}$$

tiene densidad 0. Esto es equivalente a afirmar, por definición de densidad, que el conjunto de los $n \leq x$ que cumplen (2.6) tiene cardinal $o(x)$ cuando $x \to +\infty$.

Observación 2.2.4. La expresión

$$f = (1 + o(1))g \qquad c.c$$

equivale a decir que g es un orden normal para f.

Proposición 2.2.2. *Sean f, g funciones aritméticas positivas. Entonces g es un orden normal de f si, y sólo si, las funciones distribución H_N de f/g, esto es,*

$$H_N(z) = \mu_N \left\{ n \leq N;\ \frac{f(n)}{g(n)} \leq z \right\}$$

convergen débilmente a la función de distribución $H := 1_{[1,+\infty)}$.

Demostración. Primero veamos que si g es un orden normal de f entonces las funciones H_N convergen débilmente a H. Será suficiente ver, por la Proposición 2.1.9, que

$$H_N(z) \to H(z)$$

para todo $z \neq 1$.

- Si $z > 1$, sea $\varepsilon > 0$ tal que $z > 1+\varepsilon$. Como por hipótesis, la densidad de los enteros n para los que $|f(n)/g(n) - 1| > \varepsilon$ es 0, entonces la densidad de los enteros n para los que $f(n)/g(n) - 1 > \varepsilon$ (que son una parte de aquellos), también es 0. Por consiguiente, la densidad de los enteros n tales que $f(n)/g(n) \leq 1 + \varepsilon < z$ es 1, lo que por definición implica que $H_N(z) \to 1$ cuando $N \to +\infty$.

- Si ahora $z < 1$, sea $\varepsilon > 0$ tal que $z < 1 - \varepsilon$. Por hipótesis, la densidad de los enteros n para los que $|f(n)/g(n) - 1| > \varepsilon$ es 0. Luego, la densidad de los que cumplen $f(n)/g(n) < 1 - \varepsilon$ también es 0. Luego, como $z < 1 - \varepsilon$, entonces la densidad de los enteros n tales que $f(n)/g(n) < z$ es también 0, lo que por definición significa que $H_N(z) \to 0$ cuando $z < 1$.

De este modo, hemos probado la primera implicación. Para ver la implicación contraria, notamos que, para $\varepsilon > 0$, $1 - \varepsilon$ y $1 + \varepsilon$ son puntos de continuidad de H. Luego, por hipótesis, la densidad de los enteros n tales que

$$\frac{f(n)}{g(n)} \leq 1 - \varepsilon$$

es 0, que equivale a decir que la de aquellos para los que

$$1 - \varepsilon < \frac{f(n)}{g(n)}$$

es 1. También la densidad de los enteros n tales que

$$\frac{f(n)}{g(n)} \leq 1 + \varepsilon$$

es 1, de donde podemos concluír que la densidad de los enteros n tales que

$$\left| \frac{f(n)}{g(n)} - 1 \right| < \varepsilon$$

es 1. Esto prueba que g es un orden normal de f, y por tanto la proposición. □

2.2.3. El teorema de Hardy-Ramanujan

Estudiaremos en esta sección el comportamiento promedio de la función

$$\omega(n) = |\{n;\ p \mid n\}| = \sum_{p|n} 1,$$

que cuenta el número de divisores primos de un entero n desde un punto de vista probabilístico. En 1917 Hardy y Ramanujan [13] probaron, junto con resultados similares para $d(n)$ (el número de divisores de n) y $\Omega(n)$ (el número de divisores primos contando su multiplicidad), que el orden normal de la función $\omega(n)$ es $\log\log n$. La prueba era de naturaleza técnica y no utilizaba ideas probabilísticas en su desarrollo. En 1937 Turán presentó una prueba más simple a un problema algo más preciso, que discutiremos en esta sección, junto con algunas ideas probabilísticas acerca del tema. Como es típico en este tipo de pruebas, se hace uso intensivo de resultados combinatorios para seguir ideas probabilísticas. Analicemos el siguiente modelo probabilístico:
Definamos las funciones $X_p : \mathbb{Z}^+ \to \mathbb{R}$ (p primo) por

$$X_p(n) = \begin{cases} 1, & p \mid n; \\ 0, & \text{otro caso.} \end{cases} \tag{2.7}$$

Tales X_n son la función característica de la sucesión $a = p\mathbb{Z}^+$. Observemos que tal sucesión tiene densidad $1/p$, por lo que las esperanzas de $X_p|_{\Omega_N}$ convergen a $1/p$ cuando $N \to +\infty$. Además,

$$\omega(n) = \sum_{p|n} 1 = \sum_{p \leq n} X_p(n).$$

Restringidas a $\Omega_N = [\![1, N]\!]$, las funciones X_p son variables aleatorias. y por tanto

$$\omega_N = \omega|_{\Omega_N} = \sum_p X_p$$

es una variable aleatoria también. Si nos fijamos, es "esperable" que las variables aleatorias X_p sean independientes. De cierto modo, el hecho de que un entero m sea dividible

por un primo p_1 "no depende"de que lo sea por un primo p_2. Así, estas funciones pueden ser vistas como observaciones a variables aleatorias independientes Y_p definidas en un espacio de probabilidad (Ω, ν) tales que

$$\nu\{Y_p = 1\} = \frac{1}{p}, \quad \nu\{Y_p = 0\} = 1 - \frac{1}{p}.$$

Tales variables aleatorias modelan las funciones X_p. Observemos que para $N \in \mathbb{N}$, para cada $n \in \Omega_N$ tenemos

$$\omega_N(n) = |\{p;\ p|n\}| = \sum_{p \leq N} X_p(n),$$

de donde ω se puede interpretar como una variable aleatoria en cada Ω_N, y la variable aleatoria

$$Y = \sum_{p \leq N} Y_p.$$

puede mostrarnos algunos resultados posibles para ω. Para ser un poco más precisos, Si usamos las herramientas probabilísticas para Y_p podemos observar que del teorema 1.3.4

$$\begin{aligned} \mathbb{E}[Y] &= \sum_{p \leq N} \mathbb{E}[Y_p] = \sum_{p \leq N} \frac{1}{p} \\ &= \log\log N + O(1). \end{aligned} \tag{2.8}$$

Además, como las variables Y_p son independientes,

$$\mathrm{Var}[Y] = \sum_{p \leq N} \mathrm{Var}[Y_p],$$

y por tanto

$$\begin{aligned} \mathrm{Var}[Y] &= \sum_{p \leq N} E[Y_p^2] - E[Y_p]^2 = \sum_{p \leq N} E[Y_p] - E[Y_p]^2 \\ &= \sum_{p \leq N} \frac{1}{p} - \sum_{p \leq N} \frac{1}{p^2} \\ &= \log\log N + O(1) \end{aligned} \tag{2.9}$$

ya que $\sum_{p \leq N} 1/p = \log\log(N) + O(1)$ y $\sum_{p \leq N} 1/p^2 < +\infty$. Observemos que el término $O(1)$ es un término pequeño. De hecho, $O(1) = o\left(f(N)\right))$ para cualquier función tal que $f(N) \to +\infty$ cuando $N \to +\infty$. Consideremos una función $\Psi(N) > 0$. Si usamos la desigualdad (2.1) para $\lambda = \Psi(N) > 0$ tenemos

$$\nu\left\{|Y - E[Y]| > \Psi(N)\sqrt{\mathrm{Var}[Y]}\right\} \leq \frac{1}{\Psi(N)^2}.$$

Las estimativas (2.8) y (2.9) motivan el conjeturar que

$$\frac{1}{N}\left|\left\{n \leq N : |\omega(n) - \log\log N| > \Psi(N)\sqrt{\log\log(N)}\right\}\right| = O\left(\frac{1}{\psi(N)^2}\right).$$

Veremos en la prueba del teorema 2.2.6 que esta afirmación es cierta, y que implica que

$$\frac{1}{N}\left|\left\{n \leq N : |\omega(n) - \log\log n| > \Psi(n)\sqrt{\log\log(n)}\right\}\right| = O\left(\frac{1}{\psi(N)^2}\right). \tag{2.10}$$

Sea $\varepsilon > 0$. Si $\Psi(N) \to +\infty$ cuando $N \to +\infty$, por ejemplo en el caso que $\Psi(N) = \varepsilon\sqrt{\log\log N}$, tendríamos que

$$\frac{1}{N}\left|\left\{n \leq N : \left|\frac{\omega(n)}{\log\log n} - 1\right| > \varepsilon\right\}\right| = O\left(\frac{1}{\log\log N}\right),$$

y por tanto $\log\log(N)$ es un orden normal para la función ω. La desigualdad 2.10 es conocida como teorema de Hardy-Ramanujan, y como hemos visto, implica que $\log\log$ es un orden normal para ω.

Requeriremos de los siguientes lemas:

Lema 2.2.3. *Sea $f : \mathbb{R}^+ \to \mathbb{R}^+$ tal que $f(x) > \delta$ para $x \geq x_0$, con $\delta > 0$. Entonces el número de enteros positivos $n \leq x$ tales que*

$$|\log\log x - \log\log n| \geq f(x) \tag{2.11}$$

es $o(x)$ cuando $x \to +\infty$.

Demostración. En efecto, sea $n \leq x$ tal que (2.11) se cumple. Entonces

$$\log\left(\frac{\log x}{\log n}\right) \geq f(x),$$

de donde

$$\log x \geq (\log n)\, e^{f(x)},$$

y de esto

$$n \leq x^{\left(\frac{1}{e^{f(x)}}\right)}.$$

Para $x \geq x_0$, $1/e^{f(x)} < 1/(e^{\delta}) = 1 - \lambda$, para algún $\lambda > 0$, de donde el número de enteros n que cumplen (2.11) no excede $x^{1-\lambda}$, que es $o(x)$ cuando $x \to +\infty$. □

Lema 2.2.4. *Se cumplen:*

$$\frac{1}{x}\sum_{n\leq x}\omega(n) = \log\log x + O(1), \tag{2.12}$$

y

$$\frac{1}{x}\sum_{n\leq x}\omega(n)^2 = (\log\log x)^2 + O(\log\log x). \tag{2.13}$$

Demostración. Primero notemos que

$$\frac{1}{x}\sum_{n\leq x}\omega(n)=\frac{1}{x}\sum_{n\leq x}\sum_{p|n}1=\frac{1}{x}\sum_{p\leq x}\sum_{k=1}^{\lfloor x/p\rfloor}1=\sum_{p\leq x}\frac{1}{p}+\frac{1}{x}O\left(1\right)$$

y como, por el teorema 1.3.4,

$$\sum_{p\leq x}\frac{1}{p}=\log\log x+O(1),$$

obtenemos

$$\sum_{n\leq x}\omega(n)=x\log\log x+O(x)+O(1)=x\log\log x+O(x). \tag{2.14}$$

Probaremos la otra afirmación siguiendo las ideas de Hardy [12]. Observemos primero que

$$\omega(n)\left(\omega(n)-1\right)=\sum_{\substack{pq|n\\p\neq q}}1=\sum_{pq|n}1-\sum_{p^2|n}1,$$

y así

$$\begin{aligned}\sum_{n\leq x}\omega(n)^2 &= \sum_{n\leq x}\omega(n)+\sum_{n\leq x}\sum_{pq|n}1-\sum_{n\leq x}\sum_{p^2|n}1\\ &= \sum_{n\leq x}\omega(n)+\sum_{pq\leq x}\left\lfloor\frac{x}{pq}\right\rfloor-\sum_{p^2\leq x}\left\lfloor\frac{x}{p^2}\right\rfloor\\ &= x\log\log x+O(x)+\sum_{pq\leq x}\left\lfloor\frac{x}{pq}\right\rfloor-\sum_{p^2\leq x}\left\lfloor\frac{x}{p^2}\right\rfloor\end{aligned}$$

por (2.14). Así,

$$\frac{1}{x}\sum_{n\leq x}\omega(n)^2=\log\log x+O(1)+\frac{1}{x}\sum_{pq\leq x}\left\lfloor\frac{x}{pq}\right\rfloor-\frac{1}{x}\sum_{p^2\leq x}\left\lfloor\frac{x}{p^2}\right\rfloor$$

y como

$$\frac{1}{x}\sum_{pq\leq x}\left\lfloor\frac{x}{pq}\right\rfloor=\sum_{pq\leq x}\frac{1}{pq}+O(1),$$

y

$$\frac{1}{x}\sum_{p^2\leq x}\left\lfloor\frac{x}{p^2}\right\rfloor\leq\sum_{p^2\leq x}\frac{1}{p^2}\leq\sum_{p\in\mathbb{N}}\frac{1}{p^2}<+\infty,$$

entonces

$$\frac{1}{x}\sum_{n\leq x}\omega(n)^2=\log\log x+O(1)+\sum_{pq\leq x}\frac{1}{pq} \tag{2.15}$$

Para el sumando restante, notamos que

$$\left(\sum_{p\leq\sqrt{x}}\frac{1}{p}\right)^2\leq\sum_{pq\leq x}\left(\frac{1}{pq}\right)\leq\left(\sum_{p\leq x}\frac{1}{p}\right)^2, \tag{2.16}$$

por lo que nos enfocaremos en acotar ambos extremos de esta desigualdad.

- Por el teorema 1.3.4 tenemos

$$\sum_{n\leq\sqrt{x}}\frac{1}{p}=\log\log\sqrt{x}+O(1)=\log\log x+O(1),$$

pues $\log\log x-\log\log\sqrt{x}=-\log\left(\frac{1}{2}\right)$, por tanto

$$\left(\sum_{p\leq\sqrt{x}}\frac{1}{p}\right)^2=(\log\log x+O(1))^2=(\log\log x)^2+O(\log\log x). \tag{2.17}$$

- También, otra vez del teorema 1.3.4,

$$\left(\sum_{p\leq x}\frac{1}{p}\right)^2=(O(\log\log x+O(1))^2=(\log\log x)^2+O(\log\log x). \tag{2.18}$$

Tomando en cuenta (2.18), (2.17) y notando que por (2.16) tenemos

$$\left|\sum_{pq\leq x}\frac{1}{pq}-(\log\log x)^2\right|\leq \text{máx}\left\{\left|\left(\sum_{p\leq x}\frac{1}{p}\right)^2-(\log\log x)^2\right|,\left|\left(\sum_{p\leq\sqrt{x}}\frac{1}{p}\right)^2-(\log\log x)^2\right|\right\},$$

entonces

$$\sum_{pq\leq x}\frac{1}{pq}=(\log\log x)^2+O(\log\log x).$$

Remplazando en (2.15) tenemos finalmente que

$$\frac{1}{x}\sum_{n\leq x}\omega(n)^2=(\log\log x)^2+O(\log\log x),$$

lo que prueba el lema. □

Proposición 2.2.5. *El orden normal de la función $\omega(n)$ es $\log\log n$.*

Demostración. Veamos en principio que cada una de las siguientes afirmaciones implica la siguiente.

i) Para todo $\varepsilon>0$, el número de enteros positivos $n\leq x$ tales que

$$|\omega(n)-\log\log x|>\varepsilon\log\log x \tag{2.19}$$

es $o(x)$ cuando $x\to+\infty$.

ii) Para todo $\varepsilon>0$, el número de enteros positivos $n\leq x$ tales que

$$|\omega(n)-\log\log n|>\varepsilon\log\log x \tag{2.20}$$

es $o(x)$ cuando $x\to+\infty$.

iii) Para todo $\varepsilon > 0$, el número de enteros positivos $n \leq x$ tales que

$$|\omega(n) - \log\log n| > \varepsilon \log\log n \tag{2.21}$$

es $o(x)$ cuando $x \to +\infty$.

Mostraremos primero que (i) implica (ii). Sea $\varepsilon > 0$. Notemos que para n cumpliendo (2.20) tenemos

$$\varepsilon \log\log x < |\omega(n) - \log\log n| \leq |\omega(n) - \log\log x| + |\log\log x - \log\log n|.$$

Luego, si n cumple (2.20) entonces n cumple

$$\frac{\varepsilon}{2} \log\log x \leq |\omega(n) - \log\log x|, \tag{2.22}$$

excepto para aquellos n tales que

$$|\log\log x - \log\log n| \geq \frac{\varepsilon}{2} \log\log x,$$

que son en número $o(x)$ por el lema 2.2.3 . Luego, como el el número de los n cumpliendo (2.22) es $o(x)$ por (i), tenemos que el número de n cumpliendo (2.20) es $o(x)$. Esto prueba que (i) implica (ii).
Veamos ahora que (ii) implica (iii). Para esto, notemos que los n que cumplen (2.21) satisfacen

$$|\omega(n) - \log\log n| > \varepsilon \log\log n \geq \frac{\varepsilon}{2} \log\log x \tag{2.23}$$

excepto para aquellos n tales que

$$\varepsilon \log\log n < \frac{\varepsilon}{2} \log\log x.$$

i.e.,

$$\log\log x - \log\log n > \frac{1}{2} \log\log x.$$

El número de éstos es nuevamente por el lema 2.2.3, $o(x)$. También el número de los que satisfacen (2.23) es $o(x)$ por (ii). Esto prueba que (ii) implica (iii).

Observemos que, por definición, (iii) equivale a decir que $\log\log n$ es un orden normal de $\omega(n)$, por lo que es suficiente mostrar que (i) se cumple. Sean $\varepsilon > 0$ y

$$B_\varepsilon = \{n \leq x;\ n \text{ cumple } (2.19)\}.$$

Así, para los elementos $n \in B_\varepsilon$ se tiene

$$1 \leq \frac{(\omega(n) - \log\log x)^2}{\varepsilon^2 (\log\log x)^2}.$$

Luego, usando (2.12) y (2.13),

$$\begin{aligned}
\frac{1}{x}\sum_{n\in B_\varepsilon} 1 &\leq \frac{1}{\varepsilon^2 x}\sum_{n\leq x}\frac{(\omega(n)-\log\log x)^2}{(\log\log x)^2}\\
&= \frac{1}{\varepsilon^2 x}\sum_{n\leq x}\frac{\omega(n)^2-2\omega(n)\log\log x+(\log\log x)^2}{(\log\log x)^2}\\
&= \frac{1}{\varepsilon^2(\log\log x)^2}\left(\frac{1}{x}\sum_{n\leq x}\omega(n)^2-\frac{2\log\log x}{x}\sum_{n\leq x}\omega(n)+\frac{(\log\log x)^2}{x}\right)\\
&= \frac{1}{\varepsilon^2(\log\log x)^2}\big((\log\log x)^2+O(\log\log x)-2\log\log x\,(\log\log x+O(1))\\
&\quad +(\log\log x)^2\big)\\
&= \frac{O(\log\log x)}{\varepsilon^2(\log\log x)^2}\\
&= o(1),
\end{aligned}$$

como queríamos probar. □

Siguiendo las mimas ideas probamos el teorema de Hardy-Ramanujan, que tiene por caso particular al anterior.

Teorema 2.2.6 (Hardy-Ramanujan)**.** *Sea $\Psi:\mathbb{Z}^+\to\mathbb{R}^+$ una función tal que $\psi(t)\to+\infty$ cuando $t\to+\infty$. Entonces el número de los enteros $n\leq x$ que cumplen*

$$|\omega(n)-\log\log n|>\Psi(n)\sqrt{\log\log n}$$

es $O\left(x/\Psi(x)^2\right)$. Luego, el conjunto

$$\left\{n;\ |\omega(n)-\log\log n|\leq\Psi(n)\sqrt{\log\log n}\right\}$$

tiene densidad 1*.*

Demostración. La idea de la demostración es, como dijimos antes, la de la proposición 2.2.5. En lo que sigue de ella denotaremos por ψ a una función positiva $\psi:\mathbb{Z}^+\to\mathbb{R}$ tal que

$$\psi(x)\to+\infty$$

cuando $x\to+\infty$. Notemos primero que cada una de las siguientes afirmaciones implica la siguiente.

i) Para todo ψ el número de enteros positivos $n\leq x$ tales que

$$|\omega(n)-\log\log N|>\Psi(N)\sqrt{\log\log N} \tag{2.24}$$

es $o(x)$.

ii) Para todo ψ el número de enteros positivos $n \leq x$ tales que

$$|\omega(n) - \log\log n| > \Psi(N)\sqrt{\log\log N} \tag{2.25}$$

es $o(x)$.

iii) Para todo ψ el número de enteros positivos $n \leq x$ tales que

$$|\omega(n) - \log\log n| > \Psi(n)\sqrt{\log\log n} \tag{2.26}$$

es $o(x)$.

En efecto, vemos primero que si n cumple (2.25) entonces

$$\begin{aligned} \Psi(x)\sqrt{\log\log x} &< |\omega(n) - \log\log n| \\ &\leq |\omega(n) - \log\log N| + |\log\log N - \log\log n|, \end{aligned}$$

luego n cumple (2.24) para $\Psi/2$, i.e.,

$$\frac{1}{2}\Psi(x)\sqrt{\log\log x} < |\omega(n) - \log\log x|$$

excepto aquellos tales que

$$|\log\log x - \log\log n| > \frac{1}{2}\Psi(x)\sqrt{\log\log x},$$

que son $o(x)$ por el lema 2.2.3. Esto prueba que (i) implica (ii). Ahora veamos que (ii) implica (iii). El método es completamente análogo. Sea $n_0 > 0$ tal que

$$\Psi(n) > 1 \tag{2.27}$$

para todo $n \geq n_0$. Entonces, para $n \geq n_0$ que satisface (2.26) tenemos

$$|\omega(n) - \log\log n| > \Psi(n)\sqrt{\log\log n} \geq \frac{1}{2}\sqrt{\log\log x}$$

excepto para aquellos $n \geq n_0$ para los que

$$\Psi(n)\sqrt{\log\log n} < \frac{1}{2}\sqrt{\log\log x}.$$

Pero como $\Psi(n) > 1$ para n$\geq n_0$, éstos n satisfacen

$$\log\log n < \frac{1}{4}\log\log x,$$

y el número de éstos es, por el lema 2.2.3, $o(x)$. El número de enteros $n \leq n_0$ es también $o(x)$, por lo que (ii) implica (iii). De este modo, será suficiente ver que se cumple (i)

para probar la proposición. Sea Ψ una función creciente, positiva, tal que $\Psi(n) \to +\infty$ cuando $n \to +\infty$. Sea

$$B_x = \{n \leq x;\ |\omega(n) - \log\log x| > \Psi(x)\sqrt{\log\log x}\}.$$

Entonces,

$$\begin{aligned}
\sum_{n\in B_x} 1 &\leq \sum_{n\in B_x} \frac{(\omega(n) - \log\log n)^2}{\Psi(x)^2 \log\log x} \leq \sum_{n\leq x} \frac{(\omega(n) - \log\log n)^2}{\Psi(x)^2 \log\log x} \\
&= \frac{1}{\Psi(x)^2 \log\log x} \sum_{n\leq x} \left(\omega(n)^2 - 2\omega(n)\log\log x + \log\log x^2\right) \\
&= \frac{1}{\Psi(x)^2 \log\log x} \left(\sum_{n\leq x} \omega(n)^2 - 2\log\log x \sum_{n\leq x} \omega(n) + xO\left(\log\log x\right)\right).
\end{aligned}$$

Usando entonces el lema 2.2.4, tenemos que

$$\sum_{n\in B} 1 = O\left(\frac{x}{\Psi(x)^2}\right) = o(x),$$

que es lo que queríamos probar. □

Finalizamos la sección con una breve discusión acerca del estudio de una función aritmética aditiva en general sugerida por Tenebaum[16]. Consideremos una función aditiva $f : \mathbb{N} \to \mathbb{R}$, esto es, que cumple

$$f(mn) = f(m) + f(n),$$

para todo $m, n \in \mathbb{Z}^+$ con $(m, n) = 1$. Sea $N \in \mathbb{N}$. Para $n \leq N$, de la aditividad de f podemos expresar

$$f(n) = \sum_{p^m \| n} f\left(p^m\right) = \sum_{p\leq N} \sum_{m=1}^{\infty} f\left(p^m\right) \xi_{p^m}(n),$$

donde

$$\xi_{p^m}(n) = \begin{cases} 1 & , p^m \| n; \\ 0 & , \text{otro caso.} \end{cases}.$$

Notemos esta suma es siempre una suma de finitos términos. Ahora bien, observemos que las funciones ξ_{p^m}, $p^m \leq N$ pueden ser vistas como variables aleatorias definidas en el espacio de probabilidad (Ω_N, μ_N), tomando valores 1 o 0. Tenemos

$$\begin{aligned}
E_N[\xi_{p^m}] &= \mu_N\{n;\ p^m \mid n,\ p^{m+1} \nmid n\} \\
&= \frac{1}{N}\left(\left\lfloor \frac{N}{p^m} \right\rfloor - \left\lfloor \frac{N}{p^{m+1}} \right\rfloor\right) \\
&= \frac{1}{p^m} - \frac{1}{p^{m+1}} + O\left(\frac{1}{N}\right),
\end{aligned}$$

de donde

$$\mu_N\{\xi_{p^m} = 1\} = \left(1 - p^{-1}\right) p^{-m} + O\left(N^{-1}\right).$$

También, para $p \neq q$,

$$\begin{aligned}
\mathbb{E}\left[\xi_{p^m}\xi_{q^\mu}\right] &= \frac{1}{N}\left(\left\lfloor\frac{N}{p^m q^\mu}\right\rfloor - \left\lfloor\frac{N}{p^{m+1}q^\mu}\right\rfloor - \left\lfloor\frac{N}{p^m q^{\mu+1}}\right\rfloor + \left\lfloor\frac{N}{p^{m+1}q^{\mu+1}}\right\rfloor\right) \\
&= \left(1 - p^{-1}\right) p^{-m}\left(1 - q^{-1}\right) q^{-\mu} + O(N^{-1}) \\
&= E\left(\xi_{p^m}\right) E\left(\xi_{q^\mu}\right) + O\left(N^{-1}\right).
\end{aligned}$$

Esto nos dice que las variables aleatorias ξ_{p^m} son *asintóticamente independientes*. Podemos interpretar este hecho diciendo que la función f puede ser expresada en la forma

$$f = \sum \zeta_p,$$

donde las funciones ζ_p son variables aleatorias independientes definidas en un espacio de probabilidad abstracto Ω tales que

$$P\left\{\zeta_p = f\left(p^m\right)\right\} = \left(1 - p^{-1}\right) p^{-m}.$$

En este punto, es necesario notar en el caso en que $f\left(p^m\right)$ coincida para diferentes valores de m, la probabilidad se entiende como la suma de los valores respectivos.
Los dos siguientes resultados muestran que, bajo ciertas condiciones, el comportamiento de la función f es aproximado por $\sum \zeta_p$.

Teorema 2.2.7 (Desigualdad de Turán-Kubilius)**.** *Existe una función $\varepsilon : \mathbb{R}^+ \to \mathbb{R}$, con $\varepsilon(x) \to 0$ cuando $x \to +\infty$, tal que para toda función $f : \mathbb{N} \to \mathbb{C}$ aditiva se tiene*

$$\frac{1}{x}\sum_{n \leq x} |f(n) - A(x)|^2 \leq (2 + \varepsilon(x))\, B(x)^2,$$

donde

$$A(x) = \sum_{p^m \leq x} f\left(p^m\right) p^{-m}\left(1 - p^{-1}\right), \; B(x)^2 = \sum_{p^m \leq x} |f(p^m)|^2 p^{-m}.$$

Demostración. Ver [16, p. 302]. □

Teorema 2.2.8. *Con la notación y las hipótesis del teorema 2.2.7, si*

$$B = o(A),$$

entonces A es un orden normal de f.

Demostración. Ver [16, p. 305]. □

En el caso de ω, ésta es una función aditiva. En este caso tenemos que

$$A(N) = \sum_{p \leq N} \frac{1}{p} = \log\log N + O(1)$$

y también

$$B(N)^2 = \log\log N + O(1)$$

por lo que

$$B = o(A).$$

Luego, del teorema 2.2.8, $\log\log + O(1)$ es un orden normal para la función ω, por lo que $\log\log$ es un orden normal para ω.
Una exposición completa de esta prueba puede ser encontrada en [16, pp. 302–306].

2.2.4. Conteo de primos

Mostraremos ahora una aproximación al conteo de primos usando las ideas de la teoría de la probabilidad. Consideramos las funciones X_p definidas como en (2.7). Como hicimos antes, interpretamos X_p como (observaciones a) variables aleatorias independientes tales que

$$P\{X_p = 1\} = \frac{1}{p},\ P\{X_p = 0\} = 1 - \frac{1}{p}.$$

Observamos que para $N \in \mathbb{N}$, un entero positivo n con $\sqrt{N} < n \leq N$ es primo si, y sólo si,

$$p \nmid n, \text{ para todo primo } p \leq \sqrt{N},$$

propiedad conocida como *la criba de Eratóstenes*. Luego,

$$\begin{aligned} \left\{\sqrt{N} < n \leq N;\ n \text{ es primo}\right\} &= \left\{\sqrt{N} < n \leq N;\ X_p(n) = 0,\ \forall\, p \leq \sqrt{N}\right\} \\ &= \bigcap_{p \leq \sqrt{N}} \{X_p = 0\}, \end{aligned}$$

de donde, asumiendo la independencia de las variables aleatorias X_p,

$$\begin{aligned} \frac{1}{N}\left|\{\sqrt{N} < n \leq N;\ n \text{ es primo }\}\right| &= P \bigcap_{p \leq \sqrt{N}} \{X_p = 0\} \\ &= \prod_{p \leq \sqrt{N}} P\{X_p = 0\} \\ &= \prod_{p \leq \sqrt{N}} \left(1 - \frac{1}{p}\right). \end{aligned}$$

Usamos la fórmula de Mertens (teorema 1.3.5) para concluir que

$$\frac{1}{N}\left|\{\sqrt{N} < n \leq N;\ n \text{ es primo }\}\right| \sim \frac{2e^{-\gamma}}{\log N},$$

donde γ denota la constante de Euler. Luego, tendríamos

$$\frac{1}{N}\left(\pi(N) - \pi(\sqrt{N})\right) \sim \frac{2e^{-\gamma}}{\log N},$$

y notando que

$$\frac{\frac{\pi(\sqrt{N})}{N}}{\frac{2e^{-\gamma}}{\log N}} \leq \frac{\frac{\sqrt{N}}{N}}{\frac{2e^{-\gamma}}{\log N}} = \frac{\log N}{2e^{-\gamma}\sqrt{N}} \to 0$$

cuando $N \to +\infty$, tenemos entonces que

$$\frac{\pi(N)}{N} \sim \frac{2e^{-\gamma}}{\log N}.$$

Notemos que esta es una aproximación al teorema del número primo (teorema 1.3.2). Sin embargo,

$$2e^{-\gamma} \neq 1.$$

2.2.5. El problema de Sidon

En esta sección presentamos una aplicación, una solución probabilística a un problema de teoría aditiva de números. El método usado es un método muy poderoso para aplicar teoría probabilística en la prueba de existencia de objetos matemáticos en diferentes áreas. Este método consiste en construir un espacio de probabilidad adecuado al problema de estudio, y probar que las propiedades del objeto a encontrar son satisfechas con probabilidad positiva en este espacio. De este modo, tal objeto existe. En nuestro caso, el problema que nos motiva a escribir esta sección tiene por objeto a encontrar una base A de orden 2 de $\mathbb{Z}^+$ tal que

$$\text{card}\{a \in A;\ n - a \in A\} = o\left(n^{\varepsilon}\right),$$

para algún $\varepsilon > 0$. Esto es, un conjunto $A \subset \mathbb{N}$ tal que

i) A es una base de orden 2 de $\mathbb{N}$ (ver definición 2.2.4).

ii) $r_A(n) = \text{card}\{(a \in A;\ n - a \in A\} = o(n^{\varepsilon})$, para todo $\varepsilon > 0$.

En (1956), Erdős presentó una respuesta afirmativa, y de hecho más precisa, a este problema, denominado *problema de Sidon*. Algunos resultados de análisis combinatorio pueden ser consultados en [10, Chapter III].

Definición 2.2.4. *Sea $A \subset \mathbb{N}^+$. Decimos que A es una base aditiva de orden k si para todo $n \in \mathbb{N}^+$ suficientemente grande, existen $a_i \in A$, $i = 1 \ldots, k$ tales que*

$$n = a_1 + \cdots + a_k.$$

En lo que sigue de la sección denotaremos con (α_n) a una sucesión de números positivos con $0 < \alpha_n < 1$, $\lim_{n \to +\infty} \alpha_n = 0$

$$\alpha_{n+1} \leq \alpha_n \tag{2.28}$$

para todo $n \geq n_0$. Consideremos en lo que sigue un espacio de probabilidad $(\Omega, \mathcal{F}, P)$ y variables aleatorias independientes X_n tales que

$$P\{X_n = 1\} = \alpha_n, \ P\{X_n = 0\} = 1 - \alpha_n, \ \text{ para } n \in \mathbb{N}. \tag{2.29}$$

Se puede ver [11] para una justificación de la existencia de tales variables aleatorias. A continuación, construimos un conjunto de sucesiones basados en el conjunto Ω, de modo que probar la existencia de una determinada sucesión se reduzca al problema de encontrar determinado subconjunto de Ω. Definamos, para cada $w \in \Omega$, los conjuntos aleatorios

$$A(w) = \{n \in \mathbb{N}; \ X_n(w) = 1\} \subset \mathbb{N},$$

y

$$A_N(w) = A(w) \cap [\![1, N]\!].$$

De este modo, para $w \in \Omega$ se puede saber si un entero n es un elemento de $A(w)$ observando $X_n(w)$, pues

$$1_{A(w)}(n) = X_n(w).$$

Podríamos decir que cada sucesión $A(w)$ es el resultado de un juego de azar sobre los enteros positivos: para cada entero $n \in \mathbb{Z}^+$, se tiene una moneda X_n, con probabilidad de éxito (cara) de α_n. n es un elemento de la sucesión si y sólo si $X_n = 1$ (cara). ¿Cómo deben escogerse los α_n de modo que las sucesiones resultantes tengan algunas propiedades deseadas? Veamos un ejemplo.

Ejemplo 2.2.3 (Modelamiento de los cuadrados)**.** *Con las notaciones anteriores, si*

$$\alpha_n = \frac{1}{2\sqrt{n}}$$

entonces

$$\operatorname{card} A_N(\omega) \sim \sqrt{N}$$

con probabilidad 1 *en* Ω.

Demostración. Nuestra herramienta básica será la ley de los grandes números. Primero, verifiquemos que las variables aleatorias X_n verifican las hipótesis del teorema 2.1.8 (ley de los grandes números). Para esto, notemos que

$$E[X_n] = E[X_n^2] = \frac{1}{2\sqrt{n}}$$

y

$$\mathrm{Var}[X_n] = E[X_n] - E[X_n]^2 = \frac{1}{2\sqrt{n}}\left(1 - \frac{1}{2\sqrt{n}}\right).$$

Luego,

$$\sum_{n=1}^{+\infty} \frac{\mathrm{Var}[X_n]}{\left(\sum_{i=1}^n E[X_i]\right)^2} = \sum_{n=1}^{+\infty} \frac{\frac{1}{2\sqrt{n}}\left(1 - \frac{1}{2\sqrt{n}}\right)}{\left(\sum_{i=1}^n \frac{1}{2\sqrt{i}}\right)^2} \leq \sum_{n=1}^{+\infty} \frac{1}{\sqrt{n}} \frac{1}{\left(\sum_{i=1}^n \frac{1}{2\sqrt{i}}\right)^2}. \tag{2.30}$$

También

$$\sum_{n\leq N} E[X_n] = \sum_{n\leq N} \frac{1}{2\sqrt{n}} \sim \sqrt{N} \tag{2.31}$$

cuando $N \to +\infty$. En efecto, tenemos que

$$\begin{aligned} \lim_{N\to+\infty} \frac{1}{\sqrt{N}} \sum_{n=1}^{N} \frac{1}{2\sqrt{n}} &= \lim_{N\to+\infty} \frac{1}{2} \sum_{n=1}^{N} \frac{1}{N} \frac{1}{\sqrt{\frac{n}{N}}} \\ &= \int_0^1 \frac{1}{2\sqrt{x}} dx = 1, \end{aligned}$$

lo que prueba (2.31). Remplazando en (2.30) obtenemos, para algún $C > 0$,

$$\sum_{n=1}^{+\infty} \frac{\mathrm{Var}[X_n]}{\left(\sum_{i=1}^n E[X_i]\right)^2} \leq C \sum_{n=1}^{+\infty} \frac{1}{\sqrt{n^3}} < +\infty.$$

Como además

$$\sum_{n=1}^{+\infty} E[X_n] = \sum_{n=1}^{+\infty} \frac{1}{\sqrt{n}} = +\infty,$$

aplicamos el teorema 2.1.8 y nos da

$$\lim_{n\to+\infty} \frac{\sum_{j=1}^n X_j}{\sum_{j=1}^n E[X_j]} = 1 \ c.c \tag{2.32}$$

Como

$$\sum_{n=1}^{N} X_n(w) = |\{n;\ X_n(w) = 1,\ 1 \leq n \leq N\}| = \mathrm{card}\, A_N, \tag{2.33}$$

de (2.32), (2.33) y (2.31) tenemos que

$$|A(w) \cap [\![1, N]\!]| = |\{n;\ X_n(w) = 1,\ 1 \leq n \leq N\}| \sim \sqrt{N}\ c.c.,$$

que es lo que se quería demostrar. □

Ahora mostraremos la respuesta al problema de Sidon. Veremos que escogiendo adecuadamente los α_n es posible encontrar un subconjunto de $\Omega' \subset \Omega$ con medida positiva (de hecho con medida 1) tal que, para $\omega \in \Omega'$, $A(w)$ satisface las condiciones requeridas, es decir, es una base de orden dos suficientemente "pequeña".

Denotemos, para $n \in \mathbb{N}$,

$$r_n(w) = \sum_{1 \le i < n/2} X_i(w) X_{n-i}(w). \tag{2.34}$$

Para $w \in \Omega$,observemos que para $1 \le i \le n/2$, $X_i(w)X_{n-i}(w) = 1$ equivale a decir que tanto i como $n-i$ son elementos de $A(w)$, osea que $n = i + n - i$ es suma de dos elementos distintos de $A(w)$. Del mismo modo, n es suma de dos elementos en $A(w)$ cuando $X_i(w)X_{n-i}(w) = 1$ para algún $1 \le i \le n/2$. Luego $r_n(w)$ es el número de formas de expresar n como suma de dos enteros en $A(w)$. Más precisamente,

$$\begin{aligned} r_n(w) &= \left|\{(a', a'') \in A(w)^2;\ n = a' + a'',\ a' < a''\}\right| \\ &= \left|\{i \in A(w); 1 \le i \le n/2, n - i \in A(w)\}\right|. \end{aligned}$$

Denotemos ahora $\lambda_n = E[r_n]$, el promedio sobre todos los $A(w)$ del número de maneras expresar n como suma de dos elementos distintos de $A(w)$. De la independencia de las variables aleatorias X_n tenemos

$$\lambda_n = \sum_{1 \le i \le n/2} E[X_i]E[X_{n-i}] = \sum_{1 \le i < n/2} \alpha_i \alpha_{n-i}. \tag{2.35}$$

También denotemos

$$\lambda'_n = \sum_{1 \le i < n/2} \frac{\alpha_i \alpha_{n-i}}{1 - \alpha_i \alpha_{n-i}}. \tag{2.36}$$

Lema 2.2.9. *Si (α_n) cumple (2.28) entonces*

$$\lambda_n \sim \lambda'_n$$

cuando $n \to +\infty$.

Demostración. Observemos en primer lugar que $\lambda'_n \ge \lambda_n$, y también

$$\begin{aligned} 0 \le \frac{\lambda'_n}{\lambda_n} - 1 &= \frac{1}{\lambda_n} \left(\sum_{1 \le i \le n/2} \alpha_i \alpha_{n-i} \left((1 - \alpha_i \alpha_{n-i})^{-1} - 1 \right) \right) \\ &= \frac{1}{\lambda_n} \left(\sum_{1 \le i \le n/2} \alpha_i \alpha_{n-i} \left(\frac{\alpha_i \alpha_{n-i}}{1 - \alpha_i \alpha_{n-i}} \right) \right). \end{aligned} \tag{2.37}$$

Sea $0 < \varepsilon < 1/2$. De las condiciones en (2.28) tenemos, para algún $n_0 > 0$, que si $n \geq 2n_0$ y $1 \leq i \leq n/2$ entonces

$$\alpha_i \alpha_{n-i} \leq \alpha_{n-i} \leq \alpha_{n/2} < \varepsilon,$$

de donde

$$\frac{1}{\alpha_i \alpha_{n-i}} - 1 = \frac{\alpha_i \alpha_{n-i}}{1 - \alpha_i \alpha_{n-i}} \leq 2\varepsilon.$$

Remplazando esto en (2.37), obtenemos que

$$0 \leq \frac{\lambda'_n}{\lambda_n} - 1 \leq 2\varepsilon \frac{\sum_{1 \leq i < n/2} \alpha_i \alpha_{n-i}}{\lambda_n} = 2\varepsilon,$$

para todo $n \geq 2n_0$. Esto prueba el lema. □

Lema 2.2.10. *Consideremos, en (2.29),*

$$\alpha_n = \alpha \sqrt{\frac{\log n}{n}}$$

para $n \geq 2$, y $\alpha_1 = 1/2$, donde $\alpha > 0$ es tal que se cumple (2.28). Entonces

$$\lambda_n \sim \frac{1}{2} \alpha^2 \pi \log n$$

cuando $n \to +\infty$.

Demostración. Se sigue de [10, lema 11] en el caso que $c = c' = 1/2$ y observando que $\Gamma(1/2) = \sqrt{\pi}$. □

Lema 2.2.11. *Para $d, n \in \mathbb{N}$ tenemos que*

$$P\{r_n = d\} \leq \frac{(\lambda'_n)^d}{d!} e^{-\lambda_n}.$$

Demostración. Ver [10, p. 148]. □

Lema 2.2.12. *Consideremos*

$$0 \leq V \leq \xi \leq U.$$

Entonces

$$\sum_{0 \leq d \leq V} \frac{\xi^d}{d!} \leq \left(\frac{e\xi}{V} \right)^V, \tag{2.38}$$

y

$$\sum_{d \geq U} \frac{\xi^d}{d!} \leq \left(\frac{e\xi}{U} \right)^U. \tag{2.39}$$

Demostración. Notemos que

$$\sum_{0\le d\le V}\frac{\xi^d}{d!}=\sum_{0\le d\le V}\frac{V^d}{d!}\left(\frac{\xi}{V}\right)^d\le\left(\frac{\xi}{V}\right)^V\sum_{0\le d\le V}\frac{V^d}{d!}\le\left(\frac{\xi}{V}\right)^V e^V,$$

lo que prueba (2.38). Por otro lado,

$$\sum_{d\ge U}\frac{\xi^d}{d!}=\sum_{d\ge U}\frac{U^d}{d!}\left(\frac{\xi}{U}\right)^d\le\left(\frac{\xi}{U}\right)^U\sum_{d\ge U}\frac{U^d}{d!}\le\left(\frac{\xi}{U}\right)^U e^U.$$

Con esto tenemos probado (2.39) y por tanto el lema. □

El siguiente teorema responde afirmativamente al problema de Sidon.

Teorema 2.2.13. *Existen $A\subset\mathbb{N}$, c_1 y $c_2>0$ tales que*

$$c_1\log n\le\left|\{i\in A;\ 1\le i\le n/2,\ n-a\in A\}\right|\le c_2\log n, \tag{2.40}$$

para todo $n\ge n_0$.

Demostración. Como es de esperarse, el método consiste en escoger adecuadamente las probabilidades α_n. Sean

$$\alpha_n=\alpha\sqrt{\frac{\log n}{n}} \tag{2.41}$$

y $\{X_n,\ n\in\mathbb{N}\}$ variables aleatorias independientes definidas en un espacio de probabilidad (Ω,P) como en (2.29), es decir

$$\{X_n=1\}=\alpha_n=\alpha\sqrt{\frac{\log n}{n}},\qquad P\{X_n=0\}=1-P\{X_n=1\},$$

donde

$$\alpha=\left(\frac{1}{2}\left(1+2/\pi\right)\right)^{\frac{1}{2}}.$$

Notemos que entonces $0<\alpha<1$ y que

$$\frac{1}{2}\pi\alpha^2=\frac{1}{4}\pi\left(1+\frac{2}{\pi}\right)>\frac{5}{4}>1.$$

Denotemos

$$A(w)=\{n;\ X_n(w)=1\},$$

r_n, λ_n y λ'_n como en (2.34), (2.35) y (2.36) respectivamente.
Probaremos que existen constantes positivas c_1, c_2 tales que $A(w)$ satisface (2.40) para algún $w\in\Omega$. Notemos que como la función $x\to\log x/x$ es decreciente en $[3,+\infty]$ y

$$\frac{\log n}{n}<1$$

para todo $n \geq 1$, entonces (α_n) cumplen la condición (2.28). El objetivo será usar el lema de Borel-Cantelli (lema 2.1.5) para probar que el conjunto de los $w \in \Omega$ tales que existen $c_1(w) > 0$, $c_2(w) > 0$ cumpliendo, para algún $n_0(w) > 0$,

$$c_1(w) \log n < r_n(w) < c_2 \log n \qquad \text{para todo} \qquad n \geq n_0(w) \tag{2.42}$$

tiene probabilidad 1 en Ω. Observemos que la existencia de constantes $c_1(w) > 0$ y $c_2(w) > 0$ cumpliendo (2.42) es equivalente a la de constantes $c_1'(w) > 0$ y $c_2'(w) > 0$ tales que, para algún $n_0'(w) > 0$,

$$c_1(w)\lambda_n'(w) < r_n(w) < c_2'(w)\lambda_n'(w). \tag{2.43}$$

para todo $n \geq n_0'(w)$. Esto es consecuencia de que, por los lemas 2.2.9 y 2.2.10,

$$\lambda_n' \sim \lambda_n \sim \frac{1}{2}\pi \log n$$

cuando $n \to +\infty$. Para probar (2.43) usaremos el lema de Borel-Cantelli. Antes que todo, sabemos, por el lema 2.2.10, que $\lambda_n / \log n \sim (1/2)\pi\alpha^2 > 1$, de donde tenemos que

$$\lambda_n > \log n(1 + \delta),$$

para algún $\delta > 0$ y para todo $n \geq n_0$. Luego,

$$e^{-\lambda_n} = O\left(n^{-1-\delta}\right) \text{ para todo } n \geq n_0. \tag{2.44}$$

Veamos que el conjunto de los $\omega \in \Omega$ para los que existen constantes $c_1(\omega) > 0$, $c_2(\omega) > 0$ y $n_0(\omega) \in \mathbb{N}$ tales que

$$r_n(w) \leq c_2(w)\lambda_n'(w)$$

para todo $n \geq n_0(\omega)$ tiene probabilidad 1. Será suficiente ver, por el lema 2.1.5, que

$$\sum_{n=1}^{+\infty} P\{w;\ c_2\lambda_n' > r_n(w)\} < +\infty,$$

para algún $c_2 > 0$. Escojamos $c_2 = e$. Considerando que $r_n(w)$ sólo toma valores enteros, y los lemas 2.2.11 y 2.2.12, tenemos

$$\begin{aligned}
\sum_{n=1}^{+\infty} P\{r_n > c_2\lambda_n'\} &= \sum_{n=1}^{+\infty} \sum_{d > c_2\lambda_n'} P\{r_n = d\} \\
&\leq \sum_{n=1}^{+\infty} \sum_{d > c_2\lambda_n'} \left(\frac{(\lambda_n')^d}{d!} e^{-\lambda_n}\right) \\
&\leq \sum_{n=1}^{+\infty} e^{-\lambda_n} \left(\frac{e\lambda_n'}{c_2\lambda_n}\right)^{c_2\lambda_n'} = O\left(\sum_{n=1}^{+\infty} e^{-\lambda_n}\right);
\end{aligned}$$

y usando (2.44) entonces

$$\sum_{n=1}^{+\infty} P\{r_n > c_2\lambda'_n\} \leq \sum_{n=1}^{+\infty} O\left(n^{-1-\delta}\right) < +\infty.$$

Usamos el lema de Borel-Cantelli, de donde

$$P\left(\lim_{n\geq 1}\sup\{r_n > c_2\lambda'_n\}\right) = 0,$$

i.e.,

$$P\left(\lim_{n\geq 1}\inf\{r_n \leq c_2\lambda'_n\}\right) = 1,$$

por lo que dado w en un conjunto de probabilidad 1, existe un $n_1(w)$ tal que

$$r_n(w) \leq c_2 \log n \text{ para todo } n \geq n_1.$$

Usemos ahora un argumento similar para mostrar que existe $c_1 > 0$ tal que para w en un conjunto de probabilidad 1 se tiene

$$c_1 \log n \leq r_n(w) \text{ para todo } n \geq n_2(w),$$

Consideremos $0 < c_1 < 1$, de modo que $c_1\lambda'_n < \lambda'_n$. De modo análogo al caso anterior, usando los lemas 2.2.12 y 2.2.10 tenemos

$$\begin{aligned}
\sum_{n=1}^{+\infty} P\{R_n < c_1\lambda'_n\} &= \sum_{n=1}^{+\infty} \sum_{1\leq d\leq c_1\lambda'_n} P\{r_n = d\} \\
&\leq \sum_{n=1}^{+\infty} \sum_{1\leq d\leq c_1\lambda'_n} \frac{(\lambda'_n)^d}{d!} e^{-\lambda_n} \\
&\leq \sum_{n=1}^{+\infty} e^{-\lambda_n} \left(\frac{e\lambda'_n}{c_1\lambda'_n}\right)^{c_1\lambda'_n} \\
&= \sum_{n=1}^{+\infty} e^{-\lambda_n} \left(\frac{e}{c_1}\right)^{c_1\lambda'_n} \qquad (2.45)
\end{aligned}$$

Sabemos que $\lambda'_n \sim \lambda_n$ y que $\lambda_n = O(\log n)$, por lo que, para alguna constante $K > 0$,

$$\left(\frac{e}{c_1}\right)^{c_1\lambda'_n} \leq \left(\frac{e}{c_1}\right)^{Kc_1 \log n}. \qquad (2.46)$$

Como $t \log t \to 0$ cuando $t \to 0$, entonces

$$\lim_{n\to+0} \left(\frac{e}{t}\right)^t = \lim_{n\to+0} \frac{e^t}{e^{t\log t}} = 1,$$

por lo que, como

$$e^{\frac{1}{2}\frac{\delta}{K}} > 1,$$

existe $0 < c_1 < 1$ tal que

$$\left(\frac{e}{c_1}\right)^{c_1} < e^{\frac{1}{2}\frac{\delta}{K}}.$$

De esto y (2.46) tenemos

$$\left(\frac{e}{c_1}\right)^{c_1\lambda'_n} \leq \left(\frac{e}{c_1}\right)^{c_1 K \log n} \leq e^{\frac{1}{2}\delta \log n} = n^{\frac{\delta}{2}}$$

para n suficientemente grande. Remplazando esto en (2.45) y usando(2.44) tenemos

$$\sum_{n=1}^{+\infty} P\{R_n < c_1\lambda'_n\} \leq \sum_{n=1}^{+\infty} e^{-\lambda'_n} n^{\frac{\delta}{2}} \leq \sum_{n=1}^{+\infty} n^{-1-\delta/2} < +\infty.$$

Luego, del lema de Borel-Cantelli,

$$P\left(\lim_n \inf\{c_1 < r_n\}\right) = 1,$$

por lo que dado $w \in \lim\inf_n\{c_1 < r_n\}$, existe $n_2(w)$ tal que

$$c_1\lambda'_n < r_n(w) \text{ para todo } n \geq n_2(w).$$

Así, (2.40) se cumple para todo $w \in \lim_n\{c_1\lambda'_n \leq r_n\} \cap \lim\inf_n\{r_n \leq c_2\lambda'_n\}$, que es un conjunto de probabilidad 1. En particular, existe $w \in \Omega$ tal que

$$c_1\lambda'_n \leq r_n(w) \leq c_2\lambda'_n \text{ para todo } n \geq n_0(w).$$

Como dijimos antes, esto es equivalente a probar la existencia de constantes $C_1 > 0$, $C_2 > 0$ tales que

$$C_1 \log n \leq r_n(w) \leq C_2 \log n$$

para todo $n \geq n_0(w)$. Recordando que

$$r_n(w) = \left|\{(a', a'') \in A(w)^2;\ n = a' + a'',\ a' < a''\}\right|,$$

el teorema está probado para $A = A(w)$. □

2.3. Modelo probabilístico del problema

Presentamos en esta sección una aproximación probabilística al problema de la distribución de los enteros coprimos a un entero dado siguiendo las ideas de los capítulos anteriores, en las cuales cierta propiedad aritmética P acerca de los números naturales puede ser estudiada considerando al hecho de que P sea válida o no en éstos como un conjunto de *observaciones* de los valores de una variable aleatoria X definida en cierto

espacio de probabilidad Ω, por lo general tomando valores 0 o 1, de acuerdo a si P es cierta o no.

Consideremos un entero natural $q \in \mathbb{N}$. El número de enteros positivos coprimos con q y menores que q está dado por $\varphi(q)$. Luego la media de éstos sería $\varphi(q)/q$. Se podría decir que "la probabilidad de que un entero sea coprimo con q es $p = \varphi(q)/q$". Consideremos un intervalo $I = [\![n+1, n+h]\!]$ de longitud h en $\mathbb{N}$. El número de enteros coprimos con q en $[\![n+1, n+h]\!]$ sería, en promedio, $h\varphi(q)/q$. Estamos interesados en estudiar la desviación del número de coprimos con q en un intervalo de longitud h respecto de este valor promedio. El número de coprimos con h en el intervalo $[\![n+1, n+h]\!]$ está dado por

$$\sum_{i=1}^{h} [(n+i, q) = 1].$$

Así, definimos

$$M_k(q; h) = \sum_{n=1}^{q} \left(\sum_{i=1}^{h} [(n+i, q) = 1] - h\frac{\varphi(q)}{q} \right)^k \tag{2.46}$$

a ser el momento de grado k del número de coprimos con q en un intervalo de longitud h.

Ahora planteemos el problema siguiendo un camino probabilístico: consideremos la sucesión a de los enteros coprimos con q. Podemos observar que a tiene densidad

$$\delta(a) = \frac{\varphi(q)}{q}.$$

Definamos las funciones X_i, $1 \leq i \leq h$ por

$$X_i(n) = \begin{cases} 1, & (n+i, q) = 1, \\ 0, & (n+i, q) \neq 1, \end{cases}$$

que indican si $n+i$ es coprimo o no con q. Así, X_i son variables aleatorias definidas en el espacio de probabilidad finito $([\![1, q]\!], \nu_q)$, donde para $A \subset [\![1, q]\!]$

$$\nu_q(A) = \frac{\operatorname{card} A}{q}.$$

Podemos observar que de este modo, el número de coprimos con q en $[\![n+1, n+h]\!]$ sería

$$X(n) = \sum_{i=1}^{h} X_i(n),$$

que es también una variable aleatoria en $[\![1, q]\!]$. También podemos ver que

$$E[X_i] = \frac{1}{q} \sum_{n=1}^{q} X_i(n) = \frac{\varphi(q)}{q} = P,$$

de donde X_i son variables aleatorias tales que

$$P\{X_i = 1\} = P, \qquad P\{X_i = 0\} = 1 - P,$$

y por tanto $X = \sum_{i=1}^{h} X_i$ es una variable aleatoria, con $E[X] = hP = h\varphi(q)/q$. Luego,

$$\frac{1}{q} M_k(q; h) = \frac{1}{q} \sum_{n=1}^{q} \left(X(n) - E[X]\right)^k = \mu_k[X],$$

es decir, los momentos centrales de los coprimos con q son los momentos centrales de grado k de X. Así, una acotación de los coprimos se traduce en un acotación de los mismos de una variable aleatoria. Si damos una rápida inspección de X ,es inmediata su semejanza con una variable aleatoria con distribución binomial de parámetros (h, k). Y decimos su semejanza, pues falta un ingrediente básico para tal cosa: la independencia de las variables aleatorias X_i. Podemos ver por ejemplo [10, pp. 107–109] para una discusión general acerca de este fenómeno. Sin embargo, si asumimos que $h \leq P^-(q)$, donde $P^-(q)$ es el menor divisor primo de q, es posible intuir que para $i, j \in [\![1, h]\!]$ los eventos $n + i$ es coprimo con q y $n + j$ es coprimo con q son independientes, ya que $n+i$ y $n+j$ no comparten ningún divisor de primo de q. Este razonamiento puede ser formalizado en la acotación

$$\operatorname{cov}[X_i, X_j] \ll \frac{P^2}{P^-(q) \log P^-(q)}$$

siendo esta acotación un caso particular de la proposición 4.0.9 para el caso $I = \{i, j\}$, en el que $t = \operatorname{card} I = 2$. Este resultado muestra que tal covarianza no depende de i, j a la vez que es pequeño para valores grandes de $P^-(q)$. Tal resultado puede interpretarse heurísticamente con el hecho que si $i, j \leq h \leq P^-(q)$ entonces los eventos $(n+i, q) = 1$ y $(n + j, q) = 1$ son independientes.

El razonamiento anterior conduce a modelar las variables X_i mediante el uso de variables aleatorias Y_i, éstas sí independientes. Así X_i pueden ser consideradas como observaciones de Y_i, definidas en un espacio de probabilidad Ω, tomando valores 0 o 1, tales que

$$P\{Y_i = 1\} = P, \qquad P\{Y_i = 0\} = 1 - P.$$

Observemos que

$$X(n) = \sum_i X_i(n) = \operatorname{card}\left\{i \in [\![1, h]\!];\, X_i(n) = 1\right\},$$

que es el número de coprimos con q en el intervalo $[\![n + 1, n + h]\!]$ serían considerados observaciones de la variable aleatoria $Y = \sum_{i=1}^{n} Y_i$, es decir de

$$\operatorname{card}\left\{i \in [\![1, h]\!];\, Y_i = 1\right\}.$$

Debido a la asumpción de la independencia de Y_i, Y es una variable aleatoria con ley binomial, de parámetros (h, P). De este modo, es de esperar que una acotación de los momentos centrales de grado k de una ley binomial de parámetros (h, P) conlleve a acotaciones similares para los momentos $M_k(q; h)$.

Si denotamos con

$$\mu_k(h, P) = \mu_k(Y) = \mathbb{E}\left[(Y - hP)^k\right],$$

a los momentos centrales de una ley binomial de parámetros (h, P), probaremos el siguiente resultado: existe una constante $c > 0$ absoluta tal que

$$\mu_k(h, P) \ll (ck)^{k/2} \left(k + hP(1 - P)\right)^{k/2}$$

para todo $k \geq 0$. Considerando que $M_k(q; h)$ es el momento estadístico de la variable aleatoria $\sum_{i=1}^{h} Y_i$ calculado a partir de las observaciones X_i, por comparación resulta natural el siguiente resultado, que es el objetivo de lo que sigue del trabajo: para una constante absoluta $c > 0$ se tiene

$$M_k(q; h) \ll (ck)^{k/2} \left(k + h\frac{\varphi(q)}{q}\right)^{k/2},$$

uniformemente en $k \geq 0$, $h \geq 0$ y q tales que $P^-(q) \geq h$, donde q se asume sin factores cuadrados.

Como ya hemos comentado, al no ser posible la aplicación directa de herramientas probabilísticas, el camino, a veces largo y técnico, consiste en soportar los cálculos mediante el uso de técnicas de análisis combinatorio. A continuación definiremos los conceptos necesarios para abordar el estudio de los momentos de las variables X_i. Los siguientes conceptos son para una sucesión a módulo q en general. Dado $q \in \mathbb{N}$, una sucesión

$$1 \leq a_1 < a_2 < \ldots < a_r \leq q,$$

y definiendo para $m \in \mathbb{N}$, $i \in [\![0, r - 1]\!]$

$$a_{rm+i} = qm + a_i.$$

De este modo hemos definido una sucesión creciente $a = (a_i)_i \subset \mathbb{N}$, de modo que $P = \delta(a) = r/q$. En el problema de interés, tales a_i vendrían a ser los enteros coprimos con q. Usaremos los indicadores

$$e_n = [n \in a]$$

para $n \in \mathbb{N}$. A continuación, fijamos algunas notaciones útiles para el estudio de la sucesión a:

- $E_n(l) = \operatorname{card} a \cap (n + [\![0, l-1]\!]) = \sum_{i \in I} e_{n+i}$, que mide el número de elementos de a en el intervalo $n + I$, donde $I = [\![0, l-1]\!]$.
- $F_j(l) = \operatorname{card}\{n \in [\![1, q]\!];\ E_n(l) = j\}$. Notemos que para $j > l$ tal número sería 0, pues $E_n(l) \leq l$, por lo que consideraremos el caso en que $j \leq l$.
- $M_k(l) = \sum_{n=1}^{q} (E_n(l) - lP)^k$, donde $P = \delta(a) = r/q$. Desde un punto de vista estadístico, M_k mide la desviación de la cantidad de elementos de a en un intervalo de longitud l respecto del promedio $l\delta(a) = Pl$.

Las definiciones de E_n, F_n y $M_k(l)$ pueden ser entendidas de un modo más general. Definimos, para $I \subset [\![1, q]\!]$

- $E_n(I) = \operatorname{card}\{a_i :\ \text{existe } j \in I \text{ con } a_i = n + j\}$.
- $F_j(I) = \operatorname{card}\{n \in [\![1, q]\!];\ E_n(I) = j\}$.
- También
$$M_k(I) = \sum_{n=1}^{q} (E_n(I) - P \operatorname{card} I)^k \tag{2.47}$$

Notemos que en caso que $I = [\![0, k-1]\!]$ se tiene $E_n(I) = E_n(k)$. También que

$$M_k(I) = \sum_{j=0}^{\operatorname{card} I} (j - P \operatorname{card} I)^k F_j(I), \tag{2.48}$$

pues $E_n(I)$ toma el valor j para $F_j(I)$ valores de n. Para un estudio más efectivo de $F_j(I)$ definamos, para $J \subset I$

$$F_J^*(I) = \operatorname{card}\{n \in [\![1, q]\!] :\ E_n(I) = \operatorname{card} J = E_n(J)\},$$

que mide la cantidad de elementos $n \in [\![1, q]\!]$ para los cuales

$$a \cap (n + I) = a \cap (n + J) = n + J.$$

De este modo, observando que para $n \in [\![1, q]\!]$: $E_n(I) = j$ si y sólo si existe $J \subset I$ tal que $E_n(I) = E_n(J) = \operatorname{card} J = j$, y en este caso J es único, tenemos que

$$F_j(I) = \sum_{\substack{J \subset I \\ |J| = j}} F_J^*(I). \tag{2.49}$$

Respecto de $F_J^*(I)$ tenemos que

$$F_J^*(I) = \operatorname{card}\{n \in [\![1, q]\!];\ n + J \subset a,\ (n + I \backslash J) \cap a = \emptyset\}.$$

Observando que $n+J \subset a$ y $(n+I\backslash J)\cap a = \emptyset$ si y sólo si $n+j \in a$ para todo $j \in J$ y $n+i \notin a$ para todo $j \in I\backslash J$, lo que es equivalente al hecho de que $e_{n+j} = 1$, $1-e_{n+i} = 1$ para todo $j \in J$ y $i \in I\backslash J$, si y sólo si

$$\prod_{j\in J} e_{n+j} \prod_{i\in I\backslash J} (1-e_{n+i}) = 1,$$

tenemos que

$$F_J^*(I) = \sum_{n=1}^{q} \prod_{j\in J} e_{n+j} \prod_{i\in I\backslash J} (1-e_{n+i})\,. \tag{2.50}$$

También observemos que como $I\backslash I = \emptyset$ entonces

$$F_I^*(I) = \sum_{n=1}^{q} \prod_{i\in I} e_{n+i}, \tag{2.51}$$

que es el número de enteros $n \leq q$ para los cuales todos los enteros $n+i$, $i \in I$ es coprimo con q.

Lema 2.3.1. *Para $I \subset \mathbb{N}$ finito, $a_i \in \mathbb{C}$, $i \in I$, tenemos*

$$\prod_{i\in I}(1-a_i) = \sum_{J\subset I}(-1)^{|J|}\prod_{j\in J} a_j.$$

Demostración. Será suficiente considerar el caso en que $I = [\![1,m]\!]$. El lema se sigue por inducción sobre m. Para $m=1$ el resultado es claro. Supongámoslo cierto para m. Para $m+1$ tenemos, por hipótesis inductiva,

$$\prod_{i=1}^{m+1}(1-a_i) = (1-a_{m+1})\prod_{i=1}^{m}(1-a_i) = (1-a_{m+1})\left(\sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\prod_{j\in J} a_j\right),$$

y por tanto

$$\begin{aligned}
\prod_{i=1}^{m+1}(1-a_i) &= \sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\prod_{j\in J} a_j - \sum_{J\subset[\![1,m]\!]}(-1)^{|J|}a_{m+1}\prod_{j\in J} a_j \\
&= \sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\prod_{j\in J} a_j + \sum_{J\subset[\![1,m]\!]}(-1)^{|J|+1}\prod_{j\in J\cup\{m+1\}} a_j \\
&= \sum_{J\subset[\![1,m+1]\!]}(-1)^{|J|}\prod_{j\in J} a_j,
\end{aligned}$$

probando el lema. □

Bueno, ahora probamos el siguiente lema que será de utilidad en la prueba del teorema principal del trabajo.

Lema 2.3.2. *Se cumple*

$$F_J^*(I) = \sum_{J' \subset I \setminus J} (-1)^{\operatorname{card} J'} F^*_{J \cup J'} (J \cup J') .$$

Demostración. De (2.50) tenemos

$$F_J^*(I) = \sum_{n=1}^{q} \prod_{j \in J} e_{n+j} \prod_{i \in I \setminus J} (1 - e_{n+i}) ,$$

y usando el lema 2.3.1 para $\prod_{i \in I \setminus J} (1 - e_{n+i})$ tenemos

$$\begin{aligned} F_J^*(I) &= \sum_{n=1}^{q} \prod_{j \in J} e_{n+j} \left(\sum_{J' \subset I \setminus J} (-1)^{\operatorname{card} J'} \prod_{j \in J'} e_{n+j} \right) \\ &= \sum_{J' \subset I \setminus J} (-1)^{\operatorname{card} J'} \sum_{n=1}^{q} \prod_{i \in J} e_{n+i} \prod_{j \in J'} e_{n+j} \\ &= \sum_{J' \subset I \setminus J} (-1)^{\operatorname{card} J'} \sum_{n=1}^{q} \prod_{j \in J \cup J'} e_{n+j}. \end{aligned}$$

Notando que de (2.51) tenemos, para $J' \subset I \setminus J$

$$F_{J \cup J'} (J \cup J') = \sum_{n=1}^{q} \prod_{i \in J \cup J'} e_{n+j},$$

entonces

$$F_J^*(I) = \sum_{J' \subset I \setminus J} (-1)^{\operatorname{card} J'} F^*_{J \cup J'} (J \cup J') .$$

□

De los resultados anteriores, podemos expresar los momentos centrales en la forma

$$\begin{aligned} M_k(I) &= \sum_{j=0}^{\operatorname{card} I} (E_n(I) - P \operatorname{card} I)^k \\ &= \sum_{j=0}^{\operatorname{card} I} (j - P \operatorname{card} I)^k F_j(I) \\ &= \sum_{j=0}^{\operatorname{card} I} (j - P \operatorname{card} I)^k \sum_{\substack{J \subset I \\ |J| = j}} F_J^*(I) \\ &= \sum_{j=0}^{\operatorname{card} I} (j - P \operatorname{card} I)^k \sum_{\substack{J \subset I \\ |J| = j}} \sum_{J' \subset I \setminus J} (-1)^{\operatorname{card} J'} F^*_{J \cup J'} (J \cup J') . \end{aligned}$$

¿Cuál es la ventaja de expresar $M_k(I)$ en función de $F^*_{J\cup J'}(J \cup J')$? ¿Qué significan, en general, $F^*_J(J)$? Una mirada a la definición de $F_J(J)$ nos indica que mide el número de n para los que

$$a \cap (n + J) = n + J,$$

es decir que todos los elementos de $n + J$ son elementos de la sucesión. Esto es, si $X_j(n) = [(n + j, q)] = 1$,

$$F^*_J(J) = \mathbb{E}\left[\prod_{j\in J} X_j\right].$$

Capítulo 3

Momentos centrales de una ley binomial

Pasamos ahora al estudio de los momentos centrales de la variable aleatoria

$$Y = Y_1 + \cdots + Y_h$$

donde Y_i, $i = 1, \ldots, h$ son variables aleatorias independientes con

$$P(Y_i = 1) = P, \qquad P(Y_i = 0) = 1 - P.$$

Esta variable Y define una ley binomial de parámetros (h, P), esto es , para $j \in \mathbb{N}$,

$$P(Y = j) = \binom{h}{j} P^j (1 - P)^{h-j}.$$

El k-ésimo momento de Y a ser, como es usual,

$$\mu_k(h, P) = \mu_k[Y] = \mathbb{E}\left(Y - \mathbb{E}(Y)\right)^k.$$

Proposición 3.0.3. *Consideremos una variable aleatoria Y con ley binomial de parámetros (h, P). Entonces*

i) $\mathbb{E}[Y] = hP$.

ii) $\mu_2(h, P) = hP(1 - P)$.

En general, notando que

$$P\left(\left(Y - \mathbb{E}(Y)\right)^k = \left(j - \mathbb{E}(Y)\right)^k\right) = P\left(Y = j\right) = \binom{h}{j} P^j (1 - P)^{h-j}$$

y considerando que $\mathbb{E}(Y) = hP$, tenemos

$$\begin{aligned} \mu_k(h, P) &= \sum_{j=0} P\left(\{Y = j\}\left(j - \mathbb{E}[Y]\right)^k\right) \\ &= \sum_{j=0} (j - hP)^k \binom{h}{j} P^j (1 - P)^{k-j}. \end{aligned}$$

Proposición 3.0.4 (Romanovsky)**.** *Para $k \geq 1$ tenemos*

$$\mu_{k+1}(h,P) = khP(1-P)\mu_{k-1}(h,P) + P(1-P)\frac{\partial \mu_k}{\partial P}(h,P).$$

Demostración. Ver [18]. □

Proposición 3.0.5. *Para $k \geq 0$ se tiene*

$$\mu_k(h,P) \in \mathbb{Z}[P][hP(1-P)].$$

Demostración. El resultado es válido para $k = 0$ pues, $\mu_0(h,P) = 1$. Consideremos ahora $k \geq 1$. Probaremos el resultado por inducción sobre k. Primero, recordemos que $\mu_1(h,P) = 0 \in \mathbb{Z}[P][hP(1-P)]$. También $\mu_2(h,P) = hP(1-P) \in \mathbb{Z}[P][hP(1-P)]$. Ahora, supongamos que para todo $i \leq k$ se tenga $\mu_i(h,P) \in \mathbb{Z}[P][hP(1-P)]$. Analicemos el caso $k+1$. De la proposición 3.0.4 tenemos

$$\mu_{k+1}(h,P) = khP(1-P)\mu_{k-1}(h,P) + P(1-P)\frac{\partial \mu_k}{\partial P}(h,P),$$

y considerando que por hipótisis inductiva $\mu_{k-1}(h,P) \in \mathbb{Z}[p][hP(1-P)]$, entonces será suficiente probar que $P(1-P)\frac{\partial \mu_k}{\partial P}(h,P) \in \mathbb{Z}[P][hP(1-P)]$. Para esto, de la hipótesis inductiva, existen polinomios $\bar{R}_{k,j} \in \mathbb{Z}[P]$ tales que

$$\mu_k(h,P) = \sum_{j\geq 0} \bar{R}_{k,j}(P)\left(hP(1-P)\right)^j,$$

por lo que

$$P(1-P)\frac{\partial \mu_k}{\partial P}(h,P) = \sum_{j\geq 0}\left[P(1-P)\bar{R}'_{k,j}(P) + (1-2P)\bar{R}_{k,j}(P)\right]\left(hP(1-P)\right)^j,$$

y por tanto $P(1-P)\frac{\partial \mu_k}{\partial P}(h,P) \in \mathbb{Z}[P][hP(1-P)]$, probando con esto la proposición. □

Como una consecuencia tenemos la siguiente proposición.

Proposición 3.0.6. *Para $k \geq 0$ tenemos*

$$\mu_k(h,P) = \sum_{j\geq 0}\left(hP(1-P)\right)^j R_{k,j}(P),$$

donde los polinomios $R_{k,j}$ están definidos recursivamente por las ecuaciones

i) $R_{0,j} = \delta(j)$, $R_{1,j} = 0$, $R_{k,0} = \delta(k)$ para $j,k \in \mathbb{N}$ arbitrarios.

ii)

$$R_{k+1,j}(x) = kR_{k-1,j-1}(x) + j(1-2x)R_{k,j}(x) + x(1-x)\frac{\partial}{\partial x}R_{k,j}(x). \tag{3.1}$$

Demostración. De la proposición 3.0.5 tenemos que $\mu_k(h,P) \in \mathbb{Z}[P][hP(1-P)]$, por lo que existen (únicos) polinomios $\bar{R}_{k,j} \in \mathbb{Z}[P]$ tales que

$$\mu_k(h,P) = \sum_{j\geq 0} \bar{R}_{k,j}(P)\left(hP(1-P)\right)^j. \tag{3.2}$$

Probaremos que los polinomios $\bar{R}_{k,j}$ son los polinomios de Romanovsky.

- Primero, tenemos que $\mu_0(h,P) = 1$, de donde $\bar{R}_{0,0}(x) = 1$.

- Veamos que $\bar{R}_{k,0} = \bar{R}_{0,k} = 0$ para $k \geq 1$. En efecto, como $\mu_0(h,P) = 1$, entonces $\bar{R}_{0,k} = 0$. Para ver que $\bar{R}_{k,0} = 0$ notemos que $\mu_k(h,P)$ es múltiplo de $hP(1-P)$. En efecto, usaremos inducción sobre $k \geq 1$. Si $k = 1$ entonces $\mu_k(h,P) = 0$. Si $k = 2$, entonces $\mu_k(h,P) = hP(1-P)$. Suponiendo la propiedad válida para todo $1 \leq j \leq k$, tenemos para $k+1$, de la proposición 3.0.4,

  $$\mu_{k+1} = khP(1-P)\mu_{k-1}(h,P) + P(1-P)\frac{\partial \mu_k}{\partial P}(h,P).$$

  Será suficiente probar que $P(1-P)\frac{\partial \mu_k}{\partial P}(h,P)$ es múltiplo de $hP(1-P)$. De la hipótesis inductiva, tenemos

  $$\mu_k(h,P) = \sum_{j\geq 1} \bar{R}_{k,j}(P)\left(hP(1-P)\right)^j,$$

  de donde

  $$\frac{\partial \mu_k}{\partial P}(h,P) = \sum_{j\geq 1}\left[\bar{R}'_{k,j}(P)\left(hP(1-P)\right)^j + j\left(hP(1-P)\right)^{j-1}h(1-2P)\bar{R}_{k,j}(P)\right],$$

  y por tanto $P(1-P)\frac{\partial \mu_k}{\partial P}(h,P)$ es, efectivamente, múltiplo de $hP(1-P)$, concluyendo por el principio de inducción que $\mu_k(h,P)$ es múltiplo de $hP(1-P)$ para todo $k \geq 1$. De este modo, el término independiente respecto de $hP(1-P)$ es 0, i.e, $\bar{R}_{k,0} = 0$, que es lo que queríamos probar.

- Probemos ahora que los polinomios $R_{k,j}$ satisfacen la ecuación (3.1). Usando nuevamente la proposición 3.0.4 tenemos

  $$\begin{aligned}\mu_{k+1}(h,P) &= khP(1-P)\sum_{j\geq 0}\bar{R}_{k-1,j}(P)\left(hP(1-P)\right)^j \\ &\quad + P(1-P)\frac{\partial}{\partial P}\sum_{j\geq 0}\bar{R}_{k,j}(P)\left(hP(1-P)\right)^j,\end{aligned}$$

  de donde

  $$\begin{aligned}\mu_{k+1}(h,P) &= k\sum_{j\geq 0}\bar{R}_{k-1,j}(P)\left(hP(1-P)\right)^{j+1} + \\ &\quad + \sum_{j\geq 0}\bar{R}_{k,j}(P)P(1-P)j\left(hP(1-P)\right)^{j-1}h(1-2P),\end{aligned}$$

$$= \sum_{j\geq 0} \left(k\bar{R}_{k-1,j-1}(P) + j(1-2P)\bar{R}_{k,j}(P) + P(1-P)\bar{R}'_{k,j}(P)\right)(hP(1-P))^j .$$

Luego, como $\mu_{k+1}(h,P) = \sum_{j\geq 0} \bar{R}_{k+1,j}(P)\,(hP(1-P))^j$ entonces de la igualdad polinomial anterior

$$\bar{R}_{k+1,j}(P) = k\bar{R}_{k-1,j-1}(P) + j(1-2P)\bar{R}_{k,j} + P(1-P)\bar{R}'_{k,j}(P),$$

como queríamos probar.

Los tres ítems prueban el resultado. □

La proposición anterior justifica un estudio más o menos detallado de los polinomios $R_{k,j}$, llamados *polinomios de Romanovsky*. Como vemos, si queremos una acotación para los momentos $\mu_k(h,P)$, la tarea consiste en hallar una acotación adecuada para las normas de $R_{k,j}$.

3.1. Polinomios de Romanovsky

En este capítulo estudiamos las propiedades principales de los polinomios $R_{i,j}$, llamados *polinomios de Romanovsky*, relacionadas con los momentos centrales de una ley binomial como acabamos de ver, y definidos según las ecuaciones en (i) y (ii) de la proposición 3.0.6.

Veremos a continuación algunas propiedades importantes de tales polinomios.

Proposición 3.1.1. *Para $k, j \in \mathbb{N}$ se tiene:*

i) $R_{k,j}(1-x) = (-1)^k R_{k,j}(x)$;

ii) $R_{k,j} \in \mathbb{Z}[x(1-x)]$ *para k par, y* $R_{k,j} \in (1-2x)\mathbb{Z}[x(1-x)]$ *para k impar.*

iii) $\deg R_{k,j} \leq k-2j$ *para* $1 \leq j \leq k/2$ *y* $\deg R_{k,j} = 0$ *para* $j > k/2$.

iv) $R_{2k,k}(x) = (2k)!!$ *para* $k \geq 1$.

Demostración. Usaremos la ecuación (3.1) e inducción para probar la proposición. Empezamos probando i). Notemos que para todo $j \in \mathbb{N}$

$$R_{0,j}(1-x) = \delta(j) = (-1)^0(x).$$

Ahora suponemos que para todo $l \leq k$ y para todo $j \in \mathbb{N}$ se tiene

$$R_{l,j}(1-x) = (-1)^l R_{l,j}(x),$$

y para $k+1$ tendríamos

$$\begin{aligned} R_{k+1,j}(1-x) &= kR_{k-1,j-1}(1-x) + (-1)j(1-2x)R_{k,j}(1-2x) + \\ &\quad +(1-x)(x)R'_{k,j}(1-x) \\ &= (-1)^{k+1}kR_{k-1,j-1}(x) + (-1)^{k+1}jx(1-x)R_{k,j}(x) + \\ &\quad +x(1-x)R'_{k,j}(1-x) \end{aligned}$$

Pero $R_{k,j}(1-x) = (-1)^k R_{k,j}(x)$, y usando la regla de la cadena entonces

$$R'_{k,j}(1-x) = (-1)^{k+1}R'_{k,j}(x);$$

Reemplazando esto en (3.3) nos da

$$\begin{aligned} R_{k+1,j}(1-x) &= (-1)^{k+1}kR_{k-1,j-1}(x) + (-1)^{k+1}j(1-2x)R_{k,j}(x) + \\ &\quad +(-1)^{k+1}x(1-x)R'_{k,j}(x) \\ &= (-1)^{k+1}R_{k+1,j}(x) \end{aligned}$$

para todo $j \in \mathbb{N}$, probando la parte (i). Ahora probamos la parte (ii). Usaremos inducción sobre el conjunto de los enteros $i \in \mathbb{N}$ tales que (ii) es cierto para el impar $2i-1$ y para el par $2i$. Para $i = 0, 1$ el resultado es cierto por verificación directa. Supongamos ahora (hipótesis inductiva) que para $1 \leq l \leq i$ se cumple:

$$R_{2i-1,j} \in (1-2x)\mathbb{Z}[x(1-x)] \qquad \text{y} \qquad R_{2i,j} \in \mathbb{Z}[x(1-x)].$$

Para el caso $i+1$ tenemos $2(i+1)-1 = 2i+1$ y $2(i+1) = 2i+2$. Luego, de la ecuación (3.1),

$$R_{2i+1}(x) = 2iR_{2i-1,j-1}(x) + j(1-2x)R_{2i,j}(x) + x(1-x)R'_{2i,j}(x). \tag{3.3}$$

Como $R_{2i,j}(x) \in \mathbb{Z}[x(1-x)]$, denotemos $R_{2i,j}(x) = p(x(1-x))$. Entonces

$$R'_{2i,j}(x) = (1-2x)p'(x(1-x)) \in (1-2x)\mathbb{Z}[x(1-x)].$$

Además, por hipótesis inductiva,

$$R_{2i-1,j-1}(x) \in (1-2x)\mathbb{Z}[x(1-x)] \qquad \text{y} \qquad (1-2x)R_{2i,j}(x) \in (1-2x)\mathbb{Z}[x(1-x)],$$

y de (3.3) concluímos que

$$R_{2(i+1)-1}(x) \in (1-2x)\mathbb{Z}[x(1-x)],$$

probando que (ii) es cierto para el impar $2i-1$. Prosiguiendo con la prueba, otra vez de (3.1) tenemos

$$R_{2i+2,j}(x) = (2i+1)R_{2i,j-1}(x) + j(1-2x)R_{2i+1,j}(x) + x(1-x)R'_{2i+1,j}(x). \tag{3.4}$$

Suponiendo que $R_{2i+1,j}(x) = (1-2x)q(x(1-x))$, entonces

$$(1-2x)R_{2i+1,j}(x) = (1-2x)^2 q(x(1-x))$$

y así

$$R'_{2i+1,j}(x) = -2q(x(1-x)) + (1-2x)^2 q'(x(1-x));$$

notando también que $(1-2x)^2 = 1-4x(1-x) \in \mathbb{Z}[x(1-x)]$ tenemos esto implica que $R_{2i+1,j}(x)$, $(1-2x)R'_{2i+1,j}(x) \in \mathbb{Z}[x(1-x)]$, y por consiguiente, de (3.4), concluímos que

$$R_{2(i+1),j}(x) \in \mathbb{Z}[x(1-x)],$$

probándose que (ii) es cierto para el par $2(i+1)$. Esto prueba (ii).

Probamos ahora (iii) por inducción sobre k. Para $k = 2$, si $1 \leq j \leq k/2 = 1$ entonces $j = 1$ y

$$R_{k,j}(x) = R_{0,0}(x) + (1-2x)R_{1,1}(x) + x(1-x)R'_{1,1}(x) = 1,$$

de donde $\deg R_{2,1}(x) = 0 = 2-2(1)$. Si por el contrario tenemos $j > k/2 = 1$, entonces

$$R_{2,j}(x) = R_{0,j-1}(x) + j(1-2x)R_{1,j}(x) + x(1-x)R'_{1,j}(x) = 0,$$

pues $j-1 > 0$ y $R_{1,j} = 0$. Supongamos ahora que (iii) es cierto para todo $k \leq k_0$. Consideremos el caso k_0+1. Primero, sea $j > (k_0+1)/2$. Entonces $j-1 > (k_0-1)/2$ y $j > k_0/2$, de donde $R_{k_0-1,j-1}(x) = 0$ y $R_{k_0,j}(x) = 0$, por lo que

$$R_{k_0+1,j} = kR_{k_0-1,j-1}(x) + j(1-2x)R_{k_0,j}(x) + x(1-x)R'_{k_0,j}(x) = 0.$$

El caso $1 \leq j \leq (k_0+1)/2$ es análogo.

Ahora probemos (iv). Para $k = 0$ tenemos que $R_{0,0}(x) = 1 = 0!!$. Para $k = 1$,

$$R_{2,1}(x) = R_{0,0}(x) + (1-2x)R_{1,1}(x) + x(1-x)R'_{1,1}(x),$$

pero como $R_{1,1}(x) = 0$ entonces $R_{2,1}(x) = 1 = 2!!$. Procediendo por inducción sobre k, supongamos que $R_{2k,k} = (2k)!!$. Entonces de (3.1)

$$R_{2(k+1),k+1}(x) = (2k+1)R_{2k,k}(x) + (k+1)(1-2x)R_{2k+1,k+1}(x) + x(1-x)R'_{2k+1,k+1}(x);$$

pero como $k+1 > (2k+1)/2$ entonces $R_{2k+1,k+1}(x) = 0$, de donde

$$R_{2(k+1),k+1}(x) = (2k+1)R_{2k,k} = (2k+1)(2k)!! = (2(k+1))!!$$

por la hipótesis inductiva. Esto termina la prueba de la proposición. □

Consideremos ahora en $\mathbb{Z}[x]$ la norma $\|\cdot\|_1$ definida por

$$\left\|\sum_{i=0}^{n} a_i x^i\right\|_1 = \sum_{i=0}^{n} |a_i|.$$

Notemos que para $p, q \in \mathbb{Z}[x]$ tenemos que $\|p(x)q(x)\|_1 \leq \|p(x)\|_1\|q(x)\|_1$ y también $\|p'(x)\|_1 \leq \deg p\|p(x)\|_1$. En efecto, para un polinomio $p(x) = \sum_{i=0}^{m} a_i x^i$ de grado m tenemos que $p'(x) = \sum_{i=1}^{m} i a_i x^{i-1}$, de donde

$$\|p'\|_1 = \sum_{i=1}^{m} |i a_i| \leq m \sum_{i=0}^{m} |a_i| = \deg p \|p\|_1.$$

Proposición 3.1.2. *Para $k, j \geq 1$ se tiene que*

$$\|R_{k+1,j}\|_1 \leq k \|R_{k-1,j-1}\|_1 + (2k - j) \|R_{k,j}\|_1 .$$

Demostración. De (3.1) tenemos, para $k \geq 1$

$$\begin{aligned}
\|R_{k+1,j}(x)\|_1 &= \left\|kR_{k-1,j-1}(x) + j(1-2x)R_{k,j}(x) + x(1-x)R'_{k,j}(x)\right\|_1 \\
&\leq k \|R_{k-1,j-1}(x)\|_1 + j \|1-2x\|_1 \left\|R_{k,j(x)}\right\|_1 + \|x(1-x)\|_1 \left\|R'_{k,j}(x)\right\|_1 \\
&= k \|R_{k-1,j-1}(x)\|_1 + 3j \|R_{k,j}(x)\|_1 + 2(k-2j) \|R_{k,j}(x)\|_1 \\
&= k \|R_{k-1,j-1}\|_1 + (2k-j) \|R_{k,j}\|_1 ,
\end{aligned}$$

que es lo que queríamos probar. □

Denotaremos en lo que sigue, para $i, j \in \mathbb{N}$,

$$r_{i,j} = \frac{1}{\Gamma(i+2j+1)} R_{i+2j,j}(0) = \frac{R_{i+2j,j}(0)}{(i+2j)!!}. \tag{3.5}$$

y también por

$$T_{i,j} = \Gamma(2i-2j+1)\binom{k-j-1}{j-1} = \begin{cases} (2i-2j)!!\binom{i-j-1}{j-1}, & \text{si } i \geq j, \\ 0, & \text{en otro caso.} \end{cases} \tag{3.6}$$

Tales números nos servirán para acotar las normas $\|R_{i,j}\|$, cosa que haremos a continuación.

Proposición 3.1.3. *Para $i, j \geq 1$ tenemos*

$$T_{i,j} \leq \left(\frac{4(i-j)}{e}\right)^{i-j} \tag{3.7}$$

Demostración. Usamos la proposición 1.2.3 para obtener

$$\Gamma(2(i-j)+1) \leq e^{1/24}\sqrt{2}\left(\frac{2(i-j)}{e}\right)^{i-j},$$

y observando que también

$$\binom{i-j-1}{j-1} \leq 2^{i-j-1},$$

entonces

$$T_{i,j} = \Gamma(2i-2j+1)\binom{k-j-1}{j-1} \leq e^{1/24}\sqrt{2}\left(\frac{2(i-j)}{e}\right)^{i-j} 2^{i-j-1} = \frac{e^{1/24}}{\sqrt{2}}\left(\frac{4(i-j)}{e}\right)^{i-j}.$$

□

Lema 3.1.4. *Se tiene:* $T_{i,0} = \delta(i)$. *Además,* $T_{i,j} = 0$ *para* $2j > i$ *y la fórmula de recurrencia, para* $i, j \geq 1$,

$$T_{i+1,j} = iT_{i-1,j-1} + (2i-j)T_{i,j}.$$

Demostración. Primero, observando que $\binom{i-1}{-1} = \delta(i)$, tenemos que $T_{i,0} = \delta(i)$. A continuación, si $2j > i$ entonces $i-j-1 < j-1$, de donde $\binom{i-j-1}{j-1} = 0$. De este modo, $T_{i,j} = 0$ para $2j > i$. Esto también implica que $T_{0,j} = 0$ para $j \geq 1$. Ahora, consideremos $i \geq 1$, $j \geq 1$. Probaremos la propiedad recursiva faltante. Si $i \leq j$, entonces $\binom{i-j-1}{j-1} = 0$, puesto que $i-j-1 < 0 \leq j-1$. De este modo, si $i < j$, tenemos que $T_{i-1,j-1} = T_{i,j} = T_{i+1,j} = 0$, cumpliéndose la propiedad deseada. Consideremos el caso $i \geq j \geq 1$. Será importante tener en cuenta que

$$T_{i-1,j-1} = \Gamma(2(i-1)-2(j-1)+1)\binom{i-1-(j-1)+1}{j-1-1} = \Gamma(2i-2j+1)\binom{i-j+1}{j-1}.$$

Usando la propiedad de recurrencia $\Gamma(n+1+2) = (n+1)\Gamma(n)$ tenemos que

$$\begin{aligned} T_{i+1,j} &= \Gamma(2i-2j+1+2)\binom{i-j-1+1}{j-1} \\ &= (2i-2j+1)\Gamma(2i-2j+1)\binom{i-j-1+1}{j-1}; \end{aligned}$$

usando la propiedad

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

y repartiendo el producto obtenemos

$$\begin{aligned} T_{i+1,j+1} &= (2i-2j+1)\left(\Gamma(2i-2j+1)\binom{i-j-1}{j-1} + \Gamma(2i-2j+1)\binom{i-j-1}{j-2}\right) \\ &= (2i-2j+1)T_{i,j} + (2i-2j+1)T_{i-1,j-1} \\ &= (2i-j)T_{i,j} + (2i-2j+1)T_{i-1,j-1} - (j-1)T_{i,j}. \end{aligned} \tag{3.8}$$

Notemos que de la propiedad de absorción,

$$\begin{aligned}(j-1)T_{i,j} &= \mathbb{\Gamma}(2i-2j+1)(j-1)\binom{i-j-1}{j-1} \\ &= \mathbb{\Gamma}(2i-2j+1)\,(i-j-1-(j-1)+1)\binom{i-j-1}{j-2} \\ &= (i-2j+1)T_{i-1,j-1},\end{aligned}$$

y reemplazando esto en (3.8) tenemos

$$\begin{aligned}T_{i+1,j} &= (2i-j)T_{i,j}+(2i-2j+1)T_{i-1,j-1}-(i-2j+1)T_{i-1,j-1} \\ &= iT_{i-1,j-1}+(2i-j)T_{i,j},\end{aligned}$$

como queríamos probar. □

Finalmente, tenemos la acotación adecuada para las normas de los polinomios de Romanovsky.

Proposición 3.1.5. *Para $i, j \in \mathbb{N}$ tenemos*

$$\|R_{i,j}\|_1 \leq T_{i,j}.$$

Luego, de (3.7),

$$\|R_{i,j}\|_1 \leq T_{i,j} \leq \left(\frac{4(i-j)}{e}\right)^{i-j}.$$

Demostración. Del lema 3.1.4 y la definición de $R_{i,j}$ tenemos que $\|R_{0,0}\|_1 = T_{0,0} = 1$. Para $j \geq 1$ se tiene $R_{0,j} = R_{j,0} = 0$, de donde $\|R_{0,j}\|_1 \leq T_{0,j} \geq 0$ y también $\|R_{j,0}\|_1 = 0 \leq T_{j,0}$. Por inducción, suponiendo que $\|R_{i,j}\|_1 \leq T_{i,j}$, para todo $i \leq k$, usando la ecuación (3.1)

$$\begin{aligned}\|R_{k+1,j}\|_1 &= \left\|kR_{k-1,j-1}+j(1-2x)R_{k,j}+x(1-x)R'_{k,j}\right\|_1 \\ &\leq k\|R_{k-1,j-1}\|_1+j\|1-2x\|_1\|R_{k,j}\|_1+\|x(1-x)\|_1\|R_{k,j}\|_1 \\ &\leq kT_{k-1,j-1}+3jT_{k,j}+2\|R'_{k,j}\|_1,\end{aligned}$$

y como

$$\|R'_{k,j}\|_1 \leq \deg R_{k,j}\|R_{k,j}\| \leq (k-2j)T_{k,j},$$

entonces

$$\|R_{k+1,j}\|_1 \leq kT_{k-1,j-1}+3jT_{k,j}+2(k-2j)T_{k,j} = kT_{k-1,j-1}+(2k-j)T_{k,j},$$

y por tanto, del lema 3.1.4 otra vez, $\|R_{k,j}\| \leq T_{k,j}$. □

Para concluir con la sección, presentamos un par de resultados más acerca de los polinomios de Romanovsky que nos darán una idea más precisa de su comportamiento.

Lema 3.1.6. *Sean i, j números naturales. Entonces*

i) $r_{0,j} = 1$ *y* $r_{i,0} = \delta(i)$.

ii) Si $i, j \geq 1$ *entonces*

$$r_{i,j} = r_{i,j-1} + j\frac{\Gamma(i+2j)}{\Gamma(i+2j+1)}r_{i-1,j}.$$

Demostración. Para probar i) notamos que por la definición de $r_{i,j}$ (ver (3.5)) tenemos

$$r_{0,j} = \frac{R_{2j,j}(0)}{\Gamma(2j+1)} = \frac{(2j)!!}{(2j)!!} = 1.$$

También

$$r_{i,0} = \frac{R_{i,0}(0)}{\Gamma(i+1)} = \delta(i).$$

Ahora probamos (ii). Usando (3.1) y la definición dada en la ecuación (3.5) tenemos

$$\begin{aligned} r_{i,j} &= \frac{1}{\Gamma(i+2j+1)}R_{i+2j,j} \\ &= \frac{1}{\Gamma(i+2j+1)}\left((i+2j-1)R_{i+2j-2,j-1}(0) + jR_{i+2j-1,j}(0)\right). \end{aligned} \tag{3.9}$$

Notando que

$$\Gamma(i+2j+1) = (i+2j)!! = (i+2j-1)\,(i+2(j-1))!! = (i+2j-1)\Gamma(i+2j-1)$$

tenemos entonces

$$\begin{aligned} r_{i,j} &= \frac{1}{(i+2j-1)\Gamma(i+2j-1)}\left((i+2j-1)R_{i+2j-2,j-1}(0) + jR_{i+2j-1,j}(0)\right) \\ &= \frac{R_{i+2j-2,j-1}}{\Gamma(i+2j-1)} + \frac{j}{\Gamma(i+2j+1)}R_{i+2j-1,j}(0) \\ &= r_{l,j-1} + \frac{j}{\Gamma(i+2j+1)}R_{i+2j-1,j}(0); \end{aligned}$$

y finalmente, notando que por definición de $r_{i-1,j}$ tenemos

$$R_{i+2j-1,j}(0) = r_{i-1,j}\Gamma(i+2j),$$

entonces

$$r_{i,j} = r_{i,j-1} + j\frac{\Gamma(i+2j)}{\Gamma(i+2j+1)}r_{i-1,j},$$

que es lo que queríamos probar. □

Corolario 3.1.7. *Tenemos que*

$$r_{i,j} = \sum_{1\leq l\leq j} l\frac{\Gamma(2l+i)}{\Gamma(2l+i+1)}R_{i-1,l}.$$

Demostración. Aplicamos el lema 3.1.6 recursivamente en j. □

Proposición 3.1.8. *Existe una constante $c>0$ absoluta tal que*

$$r_{i,j} \geq c^i \alpha^{i/2}\frac{j^{3i/2}}{i!}.$$

uniformemente en $\alpha \in (0,1]$ y $0 \leq \alpha i \leq j$.

Demostración. Del corolario 3.1.7 se cumple

$$r_{i,j} = \sum_{1\leq l\leq j} l\frac{\Gamma(2l+i)}{\Gamma(2l+i+1)}R_{i-1,l}.$$

Recordemos que de la fórmula de Stirling (proposición 1.2.3) tenemos que

$$\Gamma(t+1) \sim \sqrt{2}\left(\frac{t}{e}\right)^{t/2},$$

por lo que también

$$\Gamma(t) \sim \sqrt{2}\left(\frac{t-1}{e}\right)^{(t-1)/2}.$$

De estos dos resultados obtenemos

$$\frac{\Gamma(t)}{\Gamma(t+1)} \sim \frac{\left(\frac{t-1}{e}\right)^{(t-1)/2}}{\left(\frac{t}{e}\right)^{t/2}} = \left(\left(1-\frac{1}{t}\right)^t\right)^{1/2} e^{1/2}\left(\frac{1}{t-1}\right)^{1/2}.$$

Tomando en cuenta que $(1-1/t)^t \to e^{-1}$ cuando $t\to+\infty$ entonces

$$\frac{\Gamma(t)}{\Gamma(t+1)} \sim (t-1)^{-1/2} \sim t^{-1/2}$$

cuando $t\to+\infty$, por lo que

$$\sqrt{\frac{t}{3}}\frac{\Gamma(t)}{\Gamma(t+1)} \sim \frac{1}{\sqrt{3}}$$

cuando $t\to+\infty$. Sea

$$K = \min_{t\geq 1}\sqrt{\frac{t}{3}}\frac{\Gamma(t)}{\Gamma(t+1)} > 0;$$

entonces

$$r_{i,j} \geq \sum_{1\leq l\leq j} l\frac{K\sqrt{3}}{\sqrt{2l+i}}r_{i-1,l} \geq \sum_{\alpha i\leq l\leq j} l\frac{\sqrt{3}K}{\sqrt{2l+i}}r_{i-1,l},$$

y como para $\alpha i \leq l$ se tiene

$$\frac{l}{\sqrt{2l+i}} \geq \frac{l}{\sqrt{2\alpha i+i}} = \sqrt{l}\sqrt{\frac{l}{i}}\frac{1}{\sqrt{2\alpha+1}} \geq \sqrt{l}\sqrt{\alpha}\frac{1}{\sqrt{2\alpha+1}}$$

entonces

$$r_{i,j} \geq \sum_{\alpha i \leq l \leq j} K\sqrt{\alpha}\sqrt{l}\sqrt{\frac{3}{2\alpha+1}}r_{i-1,l} \geq \sqrt{\alpha}K\sum_{\alpha i \leq l \leq j}\sqrt{l}r_{i-1,l} \tag{3.10}$$

para todo $i \geq 1$ (notar que $3/(2\alpha+1) \geq 1$). Denotemos con

$$C = \left(K\frac{1-e^{-3/2}}{3/2}\right) > 0.$$

Probaremos que para todo $\alpha \in (0,1]$ y $j \geq \alpha i$ se tiene

$$r_{i,j} \geq C^i \alpha^{i/2}\frac{j^{3i/2}}{i!}.$$

La desigualdad es válida para $i = 0$ pues ambos miembros de ésta son iguales a 1. Asumamos $i \geq 1$. Supongamos que para todo $\alpha \in (0,1]$, $l \geq \alpha(i-1)$ se tiene

$$r_{l-1,j} \geq C^{l-1}\alpha^{(l-1)/2}\alpha^{(l-1)/2}\frac{j^{3(l-1)/2}}{(l-1)!}.$$

Sea $\alpha \in (0,1]$, $\alpha i \leq j$. De (3.10), como $\alpha(i-1) \leq \alpha i \leq i$ tenemos

$$\begin{aligned} r_{l,j} &\geq K\sqrt{\alpha}\sum_{\alpha i \leq l \leq j}\sqrt{l}C^{i-1}\alpha^{(i-1)/2}\frac{i^{3(i-3)/2}}{(i-1)!} \\ &= K\alpha^{1/2}\frac{C^{i-1}}{(i-1)!}\sum_{\lceil \alpha i \rceil \leq l \leq j} i^{3i/2-1}. \end{aligned}$$

Como la función $x \mapsto x^{3i/2-1}$ es creciente entonces

$$\begin{aligned} r_{i,j} &\geq K\alpha^{i/2}\frac{C^{i-1}}{(i-1)!}\int_{\lceil \alpha i \rceil - 1}^{j} x^{3i/2-1}dx \\ &= \frac{2}{3}K\alpha^{i/2}\frac{C^{i-1}}{i!}\left(j^{3i/2} - (\lceil \alpha i \rceil - 1)^{3i/2}\right) \\ &= \alpha^{i/2}\frac{C^{i-1}}{i!}j^{3i/2}\frac{K}{3/2}\left(1 - \left(\frac{\lceil \alpha i \rceil - 1}{j}\right)^{3i/2}\right). \end{aligned}$$

Finalmente, notemos que como $j \geq \lceil i \rceil$ y $i \geq \lceil \alpha i \rceil$ entonces

$$\left(\frac{\lceil \alpha i \rceil - 1}{j}\right)^{3i/2} \leq \left(\left(1 - \frac{1}{\lceil \alpha i \rceil}\right)^{\lceil \alpha i \rceil}\right)^{3l/(2\lceil \alpha i \rceil)} \leq e^{-3i/(2\lceil \alpha i \rceil)} \leq e^{-3/2},$$

por lo que

$$\frac{K}{3/2}\left(1 - \left(\frac{\lceil \alpha i \rceil - 1}{j}\right)^{3i/2}\right) \geq \frac{K}{3/2}\left(1 - e^{-3/2}\right) = C,$$

probándose la proposición. □

Corolario 3.1.9. *Para una constante absoluta $C > 0$ se tiene: para todo $j \geq 0$ y $k \geq 2j \in \mathbb{N}$*

$$R_{k,j}(0) \geq C^k k^j \frac{j^{2(k-2j)}}{(k-2j)!}. \tag{3.11}$$

Demostración. Sea $i = k - 2j \geq 0$. De la proposición 3.1.8 tenemos

$$r_{i,j} \geq C_1^i \alpha^{i/2} \frac{j^{3i/2}}{i!},$$

para todo $\alpha \in (0, 1/3]$ y $j \leq \alpha i \geq 0$, donde

$$r_{i,j} = \frac{1}{\Gamma(i+2j+1)} R_{i+2j,j}(0),$$

donde C_1 es una constante absoluta. En el peor de los casos, podemos asumir $C < 1$. Escogiendo

$$\alpha = \text{mín}\left\{\frac{1}{2}, \frac{j}{i}\right\} \geq \frac{j}{2j+i}$$

observamos que $\alpha i \leq j$ para todo $j \geq 1$ y $i \geq 0$. Veamos que (3.11) se cumple.

- Si $i = 0$ entonces $1 = r_{0,j} \geq 1 = C^0 \frac{j^0}{2j^0 0!}$.
- Si $i \geq 1$ entonces

  $$r_{i,j} \geq C_1^i \left(\frac{j}{i+2j}\right)^{i/2} \frac{j^{3i/2}}{i!} = C_1^i \frac{j^{2i}}{k^{k/2-j} i!} = \frac{1}{C_1^{2j} k^{k/2}} C_1^k k^j \frac{j^{2(k-2j)}}{(k-2j)!}.$$

  Recordando que, por definición,

  $$r_{i,j} = \frac{1}{\Gamma(2j+i+1)} R_{2j+1,j}(0) = \frac{1}{\Gamma(k+1)} R_{k,j}(0),$$

  entonces

  $$Rk, j(0) \geq \frac{\Gamma(k+1)}{C_1^{2j} k^{k/2}} C_1^k k^j \frac{j^{2(k-2j)}}{(k-2j)!} \geq \frac{\Gamma(k+1)}{k^{k/2}} C_1^k k^j \frac{j^{2(k-2j)}}{(k-2j)!}$$

  ya que $C_1 < 1$. Será suficiente probar que, para una constante $C_2 > 0$,

  $$\frac{\Gamma(k+1)}{k^{k/2}} \geq C_2^k;$$

  para esto, de la fórmula de Stirling

  $$\Gamma(k+1)/k^{k/2} \sim \sqrt{2}/e^{k/2} \geq \left(\frac{1}{\sqrt{e}}\right)^k,$$

  lo que prueba el resultado.

□

3.2. Acotación de los momentos centrales

Finalizamos el capítulo con la acotación de los momentos centrales $\mu_k(h,P)$, que es consecuencia de la acotación de las normas de $R_{k,j}$. Ésta acotación servirá como inspiración para probar algo similar para los momentos centrales $M_k(h;P)$.

Proposición 3.2.1. *Para una constante $C > 4/e$ se tiene*

$$\mu_k(h,P) \ll C^{k/2}k^{k/2}hP(1-P)\left(k+hP(1-P)\right)^{\lfloor k/2\rfloor-1}.$$

uniformemente en $k \geq 1$. En consecuencia,

$$\mu_k(h,P) \ll C^{k/2}k^{k/2}\left(k+hP(1-P)\right)^{k/2}.$$

Demostración. De la proposición (3.0.6) y notando que $R_{k,0}(x) = 0$ y $R_{k,j}(x) = 0$ para $j > k/2$ tenemos

$$\begin{aligned}
|\mu_k(h,P)| &\leq \sum_{j=1}^{\lfloor k/2\rfloor}(hP(1-P))^j\,|R_{k,j}(P)| \\
&\leq \sum_{j=1}^{\lfloor k/2\rfloor}(hP(1-P))^j\,\|R_{k,j}\|_1 \\
&\leq \sum_{j=1}^{\lfloor k/2\rfloor}(hP(1-P))^j\,T_{k,j};
\end{aligned}$$

además, tomando en cuenta (3.7) tenemos

$$\begin{aligned}
|\mu_k(h,P)| &\leq \sum_{j=1}^{\lfloor k/2\rfloor}(hP(1-P))^j\left(\frac{4}{e}\right)^{k-j}(k-j)^{k-j} \\
|\mu_k(h,P)| &\leq \sum_{j=1}^{\lfloor k/2\rfloor}(hP(1-P))^j\left(\frac{4}{e}\right)^{k-j}(k)^{k-j} \\
&\leq \left(\frac{4}{e}\right)^k k^k\sum_{j=1}^{\lfloor k/2\rfloor}\left(\frac{hP(1-P)}{k}\right)^j \\
&= \left(\frac{4}{e}\right)^k k^{k-1}hP(1-P)\sum_{j=0}^{\lfloor k/2\rfloor-1}\left(\frac{hP(1-P)}{k}\right)^j.
\end{aligned}$$

Como por la fórmula del binomio de Newton $\sum_{j=0}^{m}x^i \leq (1+x)^m$, entonces, para

cualquier $c > 4/e$

$$\begin{aligned}
\mu_k(h,P) &\leq \left(\frac{4}{e}\right)^k k^{k-1} hP(1-P)\left(\frac{k+hP(1-P)}{k}\right)^{\lfloor k/2\rfloor -1} \\
&= \left(\frac{4/e}{c}\right)^k c^k k^{k-\lfloor k/2\rfloor} hP(1-P)\left(k+hP(1-P)\right)^{\lfloor k/2\rfloor -1} \\
&\leq \left(\frac{4/e}{c}\right)^k k^{1/2} c^k k^{k-\lfloor k/2\rfloor} hP(1-P))\left(k+hP(1-P)\right)^{\lfloor k/2\rfloor -1};
\end{aligned}$$

y como para $(4/ec) < 1$ tenemos $(4/ec)^k k^{1/2} \ll 1$, entonces se sigue lo que queremos probar. □

Capítulo 4

Teorema principal

Sea $q \in \mathbb{N}$ y

$$1 \leq a_1 < a_2 < \ldots < a_n < \cdots$$

los números naturales coprimos con q, es decir, $(a_n, q) = 1$ para todo $n \in \mathbb{N}$. Podemos ver que para $m \in \mathbb{N}$, $i \in [\![0, \varphi(q) - 1]\!]$ tenemos

$$a_{\varphi(q)m+i} = mq + a_i$$

y de este modo la densidad de a sería

$$\delta(a) = P = \frac{\varphi(q)}{q}.$$

Probamos en esta sección el siguiente teorema:

Teorema 4.0.2. *Para una constante absoluta $C > 0$ tenemos*

$$M_k(q; h) \ll q \left(Ck \left(k + h\frac{\varphi(q)}{q} \right) \right)^{k/2}$$

uniformemente en $k \geq 0$, $h \geq 1$ verificando $P^-(q) \geq h$ y q sin factores cuadrados.

Éste es el análogo al teorema 3.2.1 para la variable $X = \sum_{i=1}^{h} X_i$, donde $X_i(n) = [(n + i, q) = 1]$.

Primero particularizaremos los conceptos definidos en la sección 2.3 para este caso. Así, usaremos las definiciones de e_n, $F_j(I)$, $F_J(I)$, $F_J^*(I)$ y $M_k(I)$ definidos en la sección 2.3. Definimos también el polinomio m_k mediante

$$m_k(h, x, y) = \sum_{j=0}^{h} (j - hx)^k \binom{h}{j} y^j (1 - y)^{h-j} \tag{4.1}$$

Podemos ver que

$$m_k(h, P, P) = \mu_k(h, P).$$

Lema 4.0.3. *Tenemos la siguiente igualdad polinomial:*

$$m_k(h,x,y) = \sum_{t\geq 0} \binom{k}{t} (h(y-x))^k \, \mu_{k-t}(h,y).$$

Demostración. Expresamos

$$(j-hx)^k = (j-hy+hy-hx)^k = \sum_{l=0}^{k} \binom{k}{l} (j-hx)^{k-l} (hy-hx)^l,$$

y reemplazando en (4.1) entonces

$$\begin{aligned} m_k(h,x,y) &= \sum_{j=0}^{h} (j-hx)^k \binom{h}{j} y^j (1-y)^{h-j} \\ &= \sum_{l=0}^{k} (h(y-x))^l \binom{k}{l} \sum_{j=0}^{h} \binom{h}{j} (j-hy)^{k-l} y^j (1-y)^{h-j} \\ &= \sum_{l=0}^{k} (h(y-x))^l \binom{k}{l} m_{k-l}(h,y,y). \end{aligned}$$

□

Si reemplazamos $x = y = P$, hemos expresado μ_k en función de los momentos de grado menor μ_{k-l}.
Recordemos que de (2.51)

$$F_I^*(I) = \sum_{n=1}^{q} \prod_{i\in I} e_{n+i}$$

donde $e_{n+i} = [(n+i,q) = 1]$ son los indicadores que muestran si $n+i$ es o no coprimo con q. Si planteamos esto usando las variables aleatorias X_i tendríamos

$$F_I^*(I) = \sum_{n=1}^{q} \prod_{i\in I} X_i(n)$$

es el número de enteros $n \leq q$ para los cuales todos los números $n+i$, $i \in I$ son coprimos con q. Luego,

$$\frac{F_I^*(I)}{q} = \frac{1}{q} \sum_{n=1}^{q} \prod_{i\in I} X_i(n)$$

vendría a ser la esperanza del producto $\prod_{i\in I} X_i$. Tales números $F_J^*(J)$ eran importantes porque los momentos de grado k se expresaban en última instancia como un polinomio en éstas, a saber

$$M_k(I) = \sum_{j=0}^{\operatorname{card} I} (j - P \operatorname{card} I)^k \sum_{\substack{J\subset I \\ |J|=j}} \sum_{J'\subset I\setminus J} (-1)^{\operatorname{card} J'} F_{J\cup J'}^* (J\cup J'). \tag{4.2}$$

Recordemos que el objetivo es analizar el caso en que $I = [\![1, h]\!]$, pues deseamos analizar el número de coprimos con q en intervalos de longitud h. Habíamos hecho un comentario sobre la condición $h \leq P^-(q)$, que era la condición natural de independencia de los X_i. Tenemos el siguiente resultado.

Lema 4.0.4. *Sean $q \in \mathbb{N}$ y $I \subset [\![1, P^-(q)]\!]$. Entonces*

$$\frac{1}{q} F_I^*(I) = \mathbb{E}\left[\prod_{i \in I} X_i\right] = \prod_{p|q} \left(1 - \frac{\operatorname{card} I}{p}\right).$$

Demostración. De la expresión (2.51) tenemos que

$$F_I^*(I) = \sum_{n=1}^{q} \prod_{i \in I} e_{n+i},$$

donde $e_{n+i} = [(n+i, q) = 1]$. Observemos que

$$[(n+i, q) = 1] = \prod_{p|q} [(n+i, p) = 1],$$

por lo que

$$\begin{aligned} F_I^*(I) &= \sum_{n=1}^{q} \prod_{i \in I} \prod_{p|q} [(n+i, p) = 1] \\ &= \prod_{p|q} \left(\sum_{n=1}^{p} \prod_{i \in I} [(n+i, p) = 1] \right). \end{aligned}$$

Notemos que para cada $p|n$, para cada $n \in [\![1, p]\!]$: $(n+i, p) = 1$ para todo i, excepto en aquellos que $n + i = p$ o $n + i = 2p$. Como $\operatorname{card} I \leq P^-(q) \leq p$, el número de estos últimos es exactamente $\operatorname{card} I$, de donde

$$\sum_{n=1}^{p} \prod_{i \in I} [(n+i, p) = 1] = p - \operatorname{card} I.$$

Luego,

$$F_I^*(I) = \prod_{p|q} (p - \operatorname{card} I) = \prod_{p|q} p \prod_{p|q} \left(1 - \frac{\operatorname{card} I}{p}\right) = q \prod_{p|q} \left(1 - \frac{\operatorname{card} I}{p}\right).$$

□

Es de interés observar que el lema 4.0.4 muestra que la esperanza del producto

$$\prod_{i \in I} X_i = \prod_{p|q} \left(1 - \frac{\operatorname{card} I}{p}\right)$$

depende de I sólo a travéz de su cardinalidad, lo que a su vez muestra nuevamente el carater "independiente" de las variables aleatorias X_i en el caso en que $i \in [\![1, P^-(q)]\!]$. Podemos decir que este hecho es de cierto modo natural y predecible pues cada variable aleatoria X_i se considera como una aproximación a Y_i. Además, como el interés es calcular los momentos

$$m_k(q,h) = q\mathbb{E}\left[(X - \mathbb{E}[X])^k\right]$$

los cuales en última instancia se reducen a un polinomio en esperanzas de productos de variables X_i, y éstas dependen sólo del número de factores, podemos resumir la información e identificar $\prod_{i\in I} X_i$ con el polinomio $y^{\operatorname{card} I}$ definiendo la forma lineal $\mathbb{E}_{\text{obs}}$ en el conjunto de polinomios $\mathbb{R}[y]$ mediante

$$\mathbb{E}_{\text{obs}}[y^m] = \mathbb{E}\left[\prod_{i\in I} X_i\right] = \frac{1}{q}\sum_{n=1}^{q}\prod_{i\in I}[(n+i,q)=1] = \prod_{p|q}\left(1 - \frac{m}{p}\right), \tag{4.3}$$

donde $I \subset [\![1, P^-(q)]\!]$ es cualquier conjunto con cardinal m. De este modo $\mathbb{E}_{\text{obs}}[y^m]$ es la esperanza de un producto de m variables X_i. Así,

$$F_I^*(I) = q\,\mathbb{E}_{\text{obs}}\left[y^{\operatorname{card} I}\right].$$

Por ejemplo, observamos que

$$\begin{aligned}
\mathbb{E}\left[\prod_{i\in I}(X_i - P)\right] &= \mathbb{E}\left[\sum_{J\subset I}(-1)^{\operatorname{card} I\setminus J} P^{\operatorname{card} I\setminus J}\prod_{i\in J} X_i\right] \\
&= \sum_{J\subset I}(-1)^{\operatorname{card} I\setminus J} P^{\operatorname{card} I\setminus J}\mathbb{E}\left[\prod_{i\in J} X_i\right] \\
&= \sum_{J\subset I}(-1)^{\operatorname{card} I\setminus J} P^{\operatorname{card} I\setminus J}\,\mathbb{E}_{\text{obs}}\left[y^{\operatorname{card} I\setminus J}\right] \\
&= \mathbb{E}_{\text{obs}}\left[(y-P)^{\operatorname{card} I}\right].
\end{aligned}$$

Así las covarianzas de las variables aleatorias X_i se calculan mediante $\mathbb{E}_{\text{obs}}\left[(y-P)^t\right]$. El siguiente resultado es una consecuencia directa de la ecuación (4.2) y la definición de $\mathbb{E}_{\text{obs}}$.

Lema 4.0.5. *Sea $q \in \mathbb{N}$ y $I \subset [\![1, P^-(q)]\!]$. Entonces*

$$M_k(I) = q\,\mathbb{E}_{\text{obs}}\left(m_k\left(\operatorname{card} I, P, Y\right)\right).$$

En particular, $M_k(I) = M_k(q; \operatorname{card} I)$.

Demostración. De los lemas 2.3.2 y 4.0.4 tenemos que

$$\begin{aligned} F_J^*(I) &= \sum_{J'\subset I\setminus J} (-1)^{\operatorname{card} J'} F^*_{J\cup J'}(J\cup J') \\ &= \sum_{J'\subset I\setminus J} (-1)^{\operatorname{card} J'} q\,\mathbb{E}_{\text{obs}}\left[y^{\operatorname{card} J\cup J'}\right]. \end{aligned}$$

Denotemos con $j = \operatorname{card} J$. Por cada $j' \in [\![0, \operatorname{card}(I\setminus J) = \operatorname{card} I - j]\!]$ hay exactamente $\binom{\operatorname{card} I-j}{j'}$ subconjuntos $J' \subset I\setminus J$, de donde

$$\begin{aligned} F_J^*(I) &= q \sum_{j'=0}^{\operatorname{card} I-j} \binom{\operatorname{card} I - j}{j'} (-1)^{j'}\,\mathbb{E}_{\text{obs}}\left[y^{j+j'}\right] \\ &= q\,\mathbb{E}_{\text{obs}}\left[y^j \sum_{j'=0}^{\operatorname{card} I-j} \binom{\operatorname{card} I - j}{j'} (-1)^{j'} y^{j'}\right] \\ &= q\,\mathbb{E}_{\text{obs}}\left[y^j (1-y)^{\operatorname{card} I-j}\right]. \end{aligned} \tag{4.4}$$

Recordemos que de (2.49) tenemos

$$F_j(I) = \sum_{\substack{J\subset I \\ \operatorname{card} J=j}} F_J(I),$$

y de (4.4) entonces

$$\begin{aligned} F_j(I) &= \sum_{\substack{J\subset I \\ \operatorname{card} J=j}} q\,\mathbb{E}_{\text{obs}}\left[y^j(1-y)^{\operatorname{card} I-j}\right] \\ &= q\,\mathbb{E}_{\text{obs}}\left[y^j(1-y)^{\operatorname{card} I-j}\right] \sum_{\substack{J\subset I \\ \operatorname{card} J=j}} 1 \\ &= q\binom{\operatorname{card} I}{j}\,\mathbb{E}_{\text{obs}}\left[y^j(1-y)^{\operatorname{card} I-j}\right]. \end{aligned}$$

Finalmente, de (2.48),

$$\begin{aligned} M_k(I) &= \sum_{j=0}^{\operatorname{card} I} (j - P\operatorname{card} I)^k F_j(I) \\ &= q \sum_{j=0}^{\operatorname{card} I} (j - P\operatorname{card} I)^k \binom{\operatorname{card} I}{j}\,\mathbb{E}_{\text{obs}}\left[y^j(1-y)^{h-j}\right], \end{aligned}$$

y de la definición de $m_k(h, P, y)$ y la linealidad de $\mathbb{E}_{\text{obs}}$ entonces obtenemos que

$$M_k(I, q) = q\,\mathbb{E}_{\text{obs}}\left[m_k\left(\operatorname{card} I, P, y\right)\right],$$

probando la proposición. □

En el caso en que $I = [\![1, h]\!]$ tenemos $\operatorname{card} I = h$, y de las proposición 3.0.6 y el lema 4.0.3 tenemos la siguiente consecuencia inmediata.

Lema 4.0.6. *Se cumple*

$$M_k(q;h) = q \sum_{t\geq 0} \sum_{j\geq 0} \binom{k}{t} h^{t+j}\, \mathbb{E}_{\text{obs}}\left[(y-P)^t y^j (1-y)^j R_{k-t,j}(y)\right].$$

El siguiente lema es una aplicación del teorema de integración por partes para la integral de Riemann-Stieltjes, presentado en la sección de preliminares.

Lema 4.0.7. *Tenemos la siguiente acotación:*

$$\sum_{p\geq p_1} \frac{1}{(p-1)^2} \ll \frac{1}{p_1 \log p_1},$$

donde la suma está extendida sobre los enteros $p \in \mathbb{N}$ primos.

Demostración. La prueba está basada en el teorema de integración por partes para la integral de Riemman-Stieltjes. Tenemos

$$\begin{aligned}
\sum_{p\geq p_1} \frac{1}{(p-1)^2} &= \int_{p_1}^{+\infty} \frac{1}{(x-1)^2} d\pi(x) \\
&= \left| -\frac{1}{(x-1)} \pi(x) \Big|_{p_1}^{+\infty} + 2\int_{p_1}^{+\infty} \frac{\pi(x)}{(x-1)^3} dx \right| \\
&\leq \left| \lim_{N\to+\infty} \frac{\pi(N)}{(N-1)^2} - \frac{\pi(p_1)}{(p_1-1)^2} \right| + \left| \int_{p_1}^{+\infty} \frac{\pi(x)}{x} \frac{x}{(x-1)^3} dx \right| \\
&\leq \lim_{N\to+\infty} \frac{\pi(N)}{(N-1)^2} + \frac{\pi(p_1)}{(p_1-1)^2} + \int_{p_1}^{+\infty} \frac{\pi(x)}{(x-1)^3} dx.
\end{aligned}$$

Observemos que, para $x \geq 2$,

$$1 \geq \frac{x-1}{x} = 1 - \frac{1}{x} \geq \frac{1}{2},$$

de donde

$$\frac{1}{(x-1)^2} \leq \frac{1}{4x^2}, \qquad \frac{1}{(x-1)^3} \leq \frac{1}{8x^3}.$$

Luego,

$$\sum_{p\geq p_1} \frac{1}{(p-1)^2} \ll \lim_{N\to+\infty} \frac{\pi(N)}{N}\frac{1}{N} + \frac{\pi(p_1)}{p_1^2} + \int_{p_1}^{+\infty} \frac{\pi(x)}{x}\frac{1}{x^2} dx.$$

Como $\pi(x) \leq 6x/(\log x)$ (ver [1, teorema 4.6]), entonces

$$\begin{aligned}
\sum_{p\geq p_1} \frac{1}{(p-1)^2} &\ll \lim_{N\to+\infty} \frac{1}{N\log N} + \frac{1}{p_1 \log p_1} + \int_{p_1}^{+\infty} \frac{1}{x^2 \log x} dx \\
&\leq \frac{1}{p_1 \log p_1} + \frac{1}{\log p_1} \int_{p_1}^{+\infty} \frac{1}{x^2} dx \\
&= 2\frac{1}{p_1 \log p_1},
\end{aligned}$$

como se quería probar. □

A continuación empezamos la tarea de acotar las esperanzas $\mathbb{E}_{\text{obs}}\left[(y-P)^t y^j (1-y)^j\right]$. Como observamos antes, el primer término en este producto es la covarianza entre t variables X_i. La proposición 4.0.9 acota éstas y es la pieza fundamental en las acotaciones siguientes. Básicamente se trata de una aplicación directa del teorema 4.0.8, cuya prueba trataremos en el siguiente capítulo.

Proposición 4.0.8. *Sean K, $K' > 0$ en $\mathbb{R}$, $t \in \mathbb{N}$, $x \in (\mathbb{R}\backslash\{1\})^m$ y $X = (x_i/(1-x_i))_{1\le i\le m}$. Si $t\|X\|_\infty \le K$ y $t\|X\|^2 \le K'$ entonces*

$$\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}\frac{1-sx_i}{(1-sx_i)^s} \ll_{K,K'} \left(Ct\|X\|^2\right)^{t/2}$$

para alguna constante $C = C_{K,K'} > 0$.

Demostración. Se desarrolla en detalle en el capítulo 5. □

Proposición 4.0.9. *Para todo $t \in \mathbb{N}$, $q \in \mathbb{N}$ tales que $t \le P^-(q)$ y q sin factores cuadrados se tiene*

$$\mathbb{E}_{\text{obs}}\left((y-P)^t\right) \ll P^t\left(c\frac{t}{P^-(q)\log P^-(q)}\right)^{t/2}$$

para una constante absoluta $c > 0$ y uniformemente en p, q.

Demostración. De la fórmula del binomio de Newton tenemos que

$$\begin{aligned}\mathbb{E}_{\text{obs}}\left[\left(\frac{y}{P}-1\right)^t\right] &= \mathbb{E}_{\text{obs}}\left[\sum_{s=0}^{t}(-1)^{t-s}\left(\frac{y}{p}\right)^s\right]\\ &= \sum_{s=0}^{t}(-1)^{t-s}P^{-s}\,\mathbb{E}_{\text{obs}}\left[y^s\right]\\ &= \sum_{s=0}^{t}(-1)^{t-s}P^{-s}\prod_{p|q}\left(1-\frac{s}{p}\right). \qquad (4.5)\end{aligned}$$

Ahora bien, de la fórmula de Euler (ver [1, teorema 2.4]) y la definición de p tenemos

$$\varphi(q) = q\prod_{p|q}\left(1-\frac{1}{p}\right),$$

de donde

$$\prod_{p|q}\left(1-\frac{1}{p}\right)^s = \left(\prod_{p|q}\left(1-\frac{1}{p}\right)\right)^s = \left(\frac{\varphi(q)}{q}\right)^s = P^s,$$

y reemplazando en (4.5) entonces

$$\mathbb{E}_{\text{obs}}\left[\left(\frac{y}{P}-1\right)^t\right] = \sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{p|q}\frac{1-s/p}{(1-1/p)^s}.$$

Sean $p_1 < p_2 < \ldots < p_m$ los divisores primos de q. Consideremos

$$x = \left(\frac{1}{p_1}, \ldots, \frac{1}{p_m}\right) \in (\mathbb{C}\backslash\{1\})^m,$$

y

$$X = \left(\frac{1/p_1}{1-1/p_1}, \ldots, \frac{1/p_m}{1-1/p_m}\right) = \left(\frac{1}{p_1-1}, \ldots, \frac{1}{p_m-1}\right).$$

A fin de aplicar el teorema 4.0.8 observemos que, usando la proposición 4.0.7,

$$\|X\|^2 = \sum_{i=1} \frac{1}{(p_i-1)^2} \leq \sum_{p \geq p_1} \frac{1}{(p-1)^2} \ll \frac{1}{p_1 \log p_1},$$

y también $t \leq P^-(q)$. Aplicando la proposición 4.0.8 obtenemos

$$\sum_{s=0}^{t} (-1)^{t-s} \binom{t}{s} \prod_{p|q} \frac{1-s/p}{(1-1/p)^s} \ll \left(C \frac{t}{P^-(q) \log P^-(q)}\right)^{t/2}$$

para una constante absoluta $C > 0$, que es lo queríamos demostrar. □

Recordando que $\operatorname{cov}[X_i, X_j] = \mathbb{E}_{\text{obs}}[(y-P)^2]$, (tendríamos $t = 2$) resulta

$$\operatorname{cov}[X_i, X_j] \ll \frac{P^2}{P^-(q) \log P^-(q)},$$

que muestra el carácter independiente de X_i, X_j para valores grandes de $P^-(q)$.
A continuación, extenderemos el alcance de esta proposición a polinomios más allá de $(y-P)^t$. Tenemos los dos siquientes resultados.

Lema 4.0.10. *Sean $m, n \in \mathbb{N}$, $q \in \mathbb{N}$ sin factores cuadrados, tales que $t+m \leq P^-(q)$. Entonces*

$$\mathbb{E}_{\text{obs}}\left((y-P)^t y^m\right) \ll (cP)^{t+m} \frac{t^{t/2}}{\left(P^-(q) \log P^-(q)\right)^{t/2}}$$

uniformemente en t, m, q y para una constante absoluta $c > 0$.

Demostración. Escribimos $y = (y-P) + p$, de donde

$$y^m = \sum_{i=0}^{m} \binom{m}{i} (y-P)^i P^{m-i},$$

y de este modo, de la linealidad de $\mathbb{E}_{\text{obs}}$

$$\mathbb{E}_{\text{obs}}\left[(y-P)^t y^m\right] = P^{t+m} \sum_{i=0}^{m} \binom{m}{i} \mathbb{E}_{\text{obs}}\left[\left(\frac{y}{P}-1\right)^{t+i}\right].$$

Del lema 4.0.9 tenemos entonces que, uniformemente y para una constante $C > 0$ absoluta,

$$\mathbb{E}_{\text{obs}}\left[(y-P)^t y^m\right] \ll P^{t+m}\sum_{i=0}^{m}\binom{m}{i}C^{t+i}\frac{(ti)^{(t+i)/2}}{(P^-(q)\log P^-(q))^{(t+i)/2}}$$
$$\ll P^{t+m}C^t\frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}}\sum_{i=0}^{m}\binom{m}{i}\left(1+\frac{i}{t}\right)^{t/2}\left(\frac{t+i}{P^-(q)\log P^-(q)}\right)^{k/2},$$

y como $t+i \le t+m \le P^-(q)$ y $(1+i/t)^t \le e^i$ entonces

$$\mathbb{E}_{\text{obs}}\left[(y-P)^t y^m\right] \ll C^{t+m}P^{t+m}\frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}},$$

probando el resultado. □

Lema 4.0.11. *Para una constante absoluta $C > 0$ se tiene*

$$\mathbb{E}_{\text{obs}}\left((y-P)^s y^m R(y)\right) \ll C^{s+m+r}P^{s+m}\|R\|_1\frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}},$$

uniformemente en $(s,m) \in \mathbb{N}^2$ y $R \in \mathbb{R}[x]$ con $\deg R = r$ satisfaciendo $s+m+r \le P^-(q)$.

Demostración. Sea

$$R = \sum_{i=0}^{r}\alpha_i x^i.$$

Entonces de la linealidad de $\mathbb{E}_{\text{obs}}$ tenemos

$$\mathbb{E}_{\text{obs}}\left[(y-P)^s y^m R(y)\right] = \sum_{i=0}^{r}\alpha_i\,\mathbb{E}_{\text{obs}}\left[(y-P)^s y^{m+i}\right],$$

y como $s+i+m \le s+m+r \le P^-(q)$, aplicando el corolario 4.0.10 se tiene que existe una constante absoluta $C > 0$ tal que, uniformemente en $s, m \in \mathbb{N}$

$$\begin{aligned}\mathbb{E}_{\text{obs}}\left((y-P)^s y^m R(y)\right) &\ll \sum_{i=0}^{r}|\alpha_i|C^{s+m+i}P^{s+m+i}\frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}}\\ &\ll C^{s+m+r}P^{s+m}\left(\sum_{i=0}^{r}|\alpha_i\right)\frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}}\\ &= C^{s+m+r}P^{s+m}\|R\|_1\frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}}.\end{aligned}$$

□

Teorema 4.0.12. *Para una constante absoluta $c > 0$ tenemos*

$$M_k(q;h) \ll q\,(ck)^{k/2}\left(k+h\frac{\varphi(q)}{q}\right)^{k/2}$$

uniformemente en $k \ge 0$, $h \ge 1$ y $q \in \mathbb{N}$ tales que $P^-(q) \ge h$ y $q \ge 2$ sin factores cuadrados.

Demostración. De la definición de $M_k(h;P)$ tenemos, si $h \leq k$,

$$M_k(h;P) = \sum_{n=1}^{q} \left(\sum_{i=1}^{h} [(n+i,q)=1] - hP \right)^k \leq qh^k \leq qk^k \leq qk^{k/2} \left(k+hP\right)^{k/2}.$$

Ahora consideremos el caso $k \leq h \leq P^-(q)$. De la proposición 3.0.6 y el lema 4.0.3 tenemos

$$m_k(h,x,y) = \sum_{t\geq 0} \binom{k}{t} \left(h(y-x)\right)^t \sum_{j\geq 0} \left(hy(1-y)\right)^j R_{k-t,j}(y),$$

donde los polinomios $R_{i,j}$ son los polinomios de Romanovsky. De este modo, aplicando el lema 4.0.3 y recordando que $R_{i,j} = 0$ para $2j > k-t$ tenemos

$$\begin{aligned} M_k(q;h) &= q\,\mathbb{E}_{\text{obs}}\left(m_k(h,P,y)\right) \\ &= q \sum_{t\geq 0}\sum_{j\leq 0} \binom{k}{t} h^{t+j}\,\mathbb{E}_{\text{obs}}\left((y-P)^t y^j (1-y)^j R_{k-t,j}(y)\right) \\ &= q \sum_{t+2j\leq k} \binom{k}{t} h^{t+j}\,\mathbb{E}_{\text{obs}}\left[(y-P)^t y^j (1-y)^j R_{k-t,j}(y)\right] \\ &\leq q \sum_{t+2j\leq k} 2^k h^{t+j}\,\mathbb{E}_{\text{obs}}\left[(y-P)^t y^j (1-y)^j R_{k-t,j}(y)\right] \qquad (4.6) \end{aligned}$$

Ahora bien, por ser $R_{i,j}$ los polinomios de Romanovsky tenemos $\deg R_{k-t,j} \leq k-t-2j$. Del lema 4.0.11 para $R = y^j R_{k-t,j}$, $m = j$, $r = j+k-t-2j$ y $s = t$, como

$$s+m+r = t+j+j+k-t-2j = k \leq h \leq P^-(q)$$

entonces

$$\mathbb{E}_{\text{obs}}\left[(y-P)^t \left(y(1-y)\right)^j R_{k-t,j}(y)\right] \ll C^k P^{t+j} \left\|(1-y)^j R_{k-t,j}(y)\right\| \frac{t^{t/2}}{\left(P^-(q)\log P^-(q)\right)^{t/2}}.$$

Observamos que

$$\begin{aligned} \left\|(1-y)^j R_{k-t,j}(y)\right\| &\leq \|(1-y)^j\|\,\|R_{k-t,j}(y)\| \leq 2^j \|R_{k-t,j}(y)\| \\ &\leq 2^j \left(\frac{4}{e}(k-t-j)\right)^{k-t-j} \leq 2^j 2^{k-j} k^{k-t-j} = 2^k k^{k-t-j}, \end{aligned}$$

por lo que

$$\mathbb{E}_{\text{obs}}\left[(y-P)^t y^j (1-y)^j R_{k-t,j}(y)\right] \ll (2C)^k P^{t+j} \frac{t^{t/2} k^{k-t-j}}{\left(P^-(q)\log P^-(q)\right)^{t/2}};$$

reemplazando en (4.6), entonces

$$M_k(q;h) \ll (4C)^k q \sum_{t+2j\leq k} \frac{(hP)^{t+j} t^{t/2}}{\left(P^-(q)\log P^-(q)\right)^{t/2}} k^{k-t-j}.$$

Notemos que $P^-(q)\log P^-(q) \geq P^-(q)\log 2 \geq h\log 2 \geq hP\log 2$, y también $t^{t/2} \leq k^{t/2}$, por lo que

$$\begin{aligned} M_k(q;h) &\ll (4C)^k q \sum_{t+2j\leq k} \left(\frac{1}{\log 2}\right)^{t/2} (hP)^{t/2+j} t^{t/2} k^{k-t/2+j} \\ &\leq (4C)^k q k^k \sum_{t+2j\leq k} \left(\frac{hP}{k\log 2}\right)^{(t+2j)/2}. \end{aligned}$$

Ahora, para cada $\mu \in [\![0,k]\!]$ existen a lo más k pares ordenados (j,t) verificando $t+2j=\mu$, de donde

$$M_k(q;h) \ll k(4C)^k q k^k \sum_{\mu\leq k} \left(\frac{hP}{k\log 2}\right)^{\mu/2}.$$

Como $k \ll (1+1/C)^k$,

$$\begin{aligned} \sum_{\mu\leq k} \left(\frac{hP}{k\log 2}\right)^{\mu/2} &\leq \left(\sum_{\mu\leq k} \left(\frac{1}{\log 2}\right)^{\mu/2}\right)\left(\sum_{\mu\leq k} \left(\frac{hP}{k}\right)^{\mu/2}\right) \\ &\leq \left(1+\left(\frac{1}{\log 2}\right)^{1/2}\right)^k \left(1+\left(\frac{hP}{k}\right)^{1/2}\right)^k \\ &\leq 3^k \left(\frac{\sqrt{k}+\sqrt{hP}}{\sqrt{k}}\right)^k \end{aligned}$$

y además

$$\sqrt{k}+\sqrt{hP} \leq \sqrt{2}\,(k+hP),$$

entonces

$$\begin{aligned} M_k(q;h) &\ll 3^k \left(\sqrt{2}(C+1)\right)^k k^k q^k \left(\frac{k+hP}{\sqrt{k}}\right)^k \\ &\ll C^k q k^{k/2} (k+hP)^{k/2}, \end{aligned}$$

para una redefinición de la constante absoluta C, probando el teorema principal. □

Capítulo 5

Un resultado de análisis combinatorio

En este último capítulo mostramos la prueba del teorema 4.0.8, que usamos para probar la proposición 4.0.9. ¿En qué radica la diferencia con el estudio de una variable aleatoria $Y = \sum_{i\in I} Y_i$, o lo que es lo mismo, qué hace diferente el problema de acotar $M_k(q;h)$ de acotar $\mu_k(h,P)$? La respuesta evidente está en la gran diferencia entre las variables X_i y sus análogas Y_i: la independencia. Si calculamos el análogo de los términos $F_I^*(I)/q = \mathbb{E}_{\text{obs}}\left[y^{\operatorname{card} I}\right]$, la esperanza de un producto $\prod_{i\in I} Y_i$ tenemos

$$\mathbb{E}\left[\prod_{i\in I} Y_i\right] = \prod_{i\in I} \mathbb{E}[Y_i] = P^{\operatorname{card} I} = \left(\frac{\varphi(q)}{q}\right)^{\operatorname{card} I}.$$

Si usamos la igualdad

$$\varphi(q) = q\prod_{p|q}\left(1-\frac{1}{q}\right)$$

tenemos

$$\mathbb{E}\left[\prod_{i\in I} Y_i\right] = \prod_{p|q}\left(1-\frac{1}{p}\right)^{\operatorname{card} I},$$

mientras que

$$\mathbb{E}\left[\prod_{i\in I} X_i\right] = \prod_{p|q}\left(1-\frac{\operatorname{card} I}{p}\right).$$

Si observamos desde otro punto de vista este hecho, vemos que mientras las covarianzas

$$\mathbb{E}\left[\prod_{i\in I}(Y_i - P)\right]$$

son nulas, tenemos que (ver la prueba de la proposición 4.0.9)

$$\begin{aligned}\mathbb{E}\left[\prod_{i\in I}(X_i - P)\right] &= \mathbb{E}_{\text{obs}}\left[(y-P)^{\operatorname{card} I}\right] \\ &= P^{\operatorname{card} I}\sum_{s=0}^{\operatorname{card} I}(-1)^{\operatorname{card} I - s}\binom{\operatorname{card} I}{s}\prod_{p|q}\frac{1-s/p}{(1-1/p)^s}.\end{aligned}$$

Esto implica a priori la necesidad de encontrar una herramienta para acotar dichos términos, objetivo que nos proponemos en este capítulo.

5.1. Estimaciones sobre una forma general

Nuestra intención en la presente sección es el preparar el camino para la acotación de la expresión

$$\sum_{s\geq 0}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}\frac{1-sx_i}{(1-x_i)^s},$$

que es la generalización natural de la ecuación (5.1). El primer paso es expresarla como un polinomio en las variables $X_i = x_i/(1-x_i)$.

Lema 5.1.1. *Sea $x \in \mathbb{C} - \{1\}$. Entonces*

$$\frac{1-sx}{(1-x)^s} = 1 - X^2\sum_{r\geq 0}(r+1)\binom{s}{r+2}X^r,$$

donde $X = x/(1-x)$.

Demostración. Observemos que

$$\begin{aligned}\frac{1-sx}{(1-x)^s} &= \frac{(1-x+x)^{s-1}\,(1-x-(s-1)x)}{(1-x)^{s-1}(1-x)} \\ &= \left(1+\frac{x}{1-x}\right)^{s-1}\left(1-(s-1)\frac{x}{1-x}\right) \\ &= \sum_{r\geq 0}\binom{s-1}{r}\left(\frac{x}{1-x}\right)^r\left(1-(s-1)\frac{x}{1-x}\right) \\ &= \sum_{r\geq 0}\binom{s-1}{r}\left(\frac{x}{1-x}\right)^r - \sum_{r\geq 0}(s-1)\binom{s-1}{r-1}\left(\frac{x}{1-x}\right)^r \\ &= \sum_{r\geq 0}\left[\binom{s-1}{r} - (s-1)\binom{s-1}{r-1}\right]\left(\frac{x}{1-x}\right)^r \qquad (5.1)\end{aligned}$$

puesto que $\binom{s-1}{-1} = 0$. Ahora, usando el lema 1.1.1 tenemos que

$$\begin{aligned}(r-1)\binom{s}{r} &= r\binom{s}{r} - \binom{s}{r} = s\binom{s-1}{r-1} - \left[\binom{s-1}{r} + \binom{s-1}{r-1}\right] \\ &= (s-1)\binom{s-1}{r-1} - \binom{s-1}{r},\end{aligned}$$

y reemplazando esto en (5.1) obtenemos

$$\begin{aligned}\frac{1-sx}{(1-x)^s} &= -\sum_{r\geq 0}(r-1)\binom{s}{r}\left(\frac{x}{1-x}\right)^r \\ &= 1-\sum_{r\geq 2}(r-1)\binom{s}{r}\left(\frac{x}{1-x}\right)^r \\ &= 1-\left(\frac{x}{1-x}\right)^2\sum_{r\geq 0}(r+1)\binom{s}{r+2}\left(\frac{x}{1-x}\right)^r,\end{aligned}$$

como se quiere probar. □

En adelante, para un vector $\bar{x}=(x_i)_{1\leq i\leq m}\in(\mathbb{C}\backslash\{1\})^m$, denotaremos

$$X_i=\frac{x_i}{1-x_i},\qquad X=\left(\frac{x_i}{1-x_i}\right)_{1\leq i\leq m}\in\mathbb{C}^m,$$

y si $J\subset[\![1,m]\!]$ (ordenado en forma creciente), entonces

$$X_J=\left(\frac{x_i}{1-x_i}\right)_{i\in J}\in\mathbb{C}^{|J|}.$$

El lema anterior nos permite expresar el término $(1-sx)/(1-x)^s$ como un polinomio en la variable X.

Lema 5.1.2. *Para $a_{i,j}\in\mathbb{C}$, $0\leq r_j\leq k$, $1\leq j\leq m$ se tenemos*

$$\prod_{j=1}^{m}\left(1-\sum_{rj=0}^{k}a_{r_j,j}\right)=\sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\sum_{\substack{r_j\geq 0\\(j\in J)}}\prod_{j\in J}a_{r_j,j}.$$

Demostración. La prueba se sigue usando el lema 2.3.1: denotemos

$$b_j=\sum_{r_j\in[\![0,k]\!]}a_{r_j,j}.$$

Entonces del lema 2.3.1,

$$\begin{aligned}\prod_{j=1}^{m}(1-b_j) &= \sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\prod_{j\in J}b_j, \\ &= \sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\prod_{j\in J}\sum_{r_j\in[\![0,k]\!]}a_{r_j,j},\end{aligned}\tag{5.2}$$

y notando que

$$\prod_{j\in J}\sum_{0\leq r_j\leq m}a_{r_j,j}=\sum_{\substack{r_j\geq 0\\(j\in J)}}\prod_{j\in J}a_{r_j,j}$$

tenemos el resultado. □

Denotamos, para $\vec{r} = (r_1, \ldots, r_k) \in \mathbb{Z}^k$

$$\omega(\vec{r}, t) := \frac{\prod_{j=1}^{k} r_j!}{t!} \sum_{s=0}^{t} (-1)^{t-s} \binom{t}{s} \prod_{j=1}^{k} \binom{s}{r_j} \tag{5.3}$$

Como una consecuencia de los lemas 5.1.1, 2.3.1 y 5.1.2 tenemos la siguiente identidad, que expresa la suma $\sum_{s\geq 0}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}\frac{1-sx_i}{(1-x_i)^s}$ como un polinomio en las variables X_i, $1 \leq i \leq m$.

Proposición 5.1.3. *Sean $x = (x_1, \ldots, x_m) \in (\mathbb{C}\backslash\{1\})^m$ y $t \in \mathbb{Z}^+$. Tenemos que*

$$\sum_{s\geq 0}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}\frac{1-sx_i}{(1-x_i)^s} = \sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\prod_{j\in J}X_j^2\, t!\sum_{\substack{r_j\geq 0\\(j\in J)}}\omega(\vec{r}_J+2,t)\prod_{j\in J}\binom{s}{r_j+2}X_j^{r_j}.$$

Demostración. Para simplificar la notación, denotemos

$$A_i = 1 - X_i^2 \sum_{r_i\geq 0}(r_i+1)\binom{s}{r_i+2}X_i^{r_i},$$

y del lema 5.1.1 entonces

$$\prod_i A_i = \prod_{i=1}^{m}\frac{a-sx_i}{(1-x_i)^s} = \prod_{i=1}^{m}\left(1 - X_i^2\sum_{r_i\geq 0}(r_i+1)\binom{s}{r_i+2}X_i^{r_i}\right).$$

Luego, del lema 5.1.2

$$\begin{aligned}\prod_{i=1}^{m} A_i &= \prod_{i=1}^{m}\left(1 - X_i^2\sum_{r_i\geq 0}(r+1)\binom{s}{r_i+2}X_i^{r_i}\right),\\ &= \sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\left(\prod_{j\in J}X_j\right)^2\sum_{\substack{r_j\geq 0\\(j\in J)}}\prod_{j\in J}(r_j+1)\binom{s}{r_j+2}X_j^{r_j},\end{aligned}$$

y por tanto

$$\begin{aligned}&\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}A_i\\ =\ &\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\left(\prod_{j\in J}X_j\right)^2\sum_{\substack{r_j\geq 0\\(j\in J)}}\prod_{j\in J}(r_j+1)\binom{s}{r_j+2}X_j^{r_j}\\ =\ &\sum_{J\subset[\![1,m]\!]}\left(\prod_{j\in J}X_j\right)^2\sum_{\substack{r_j\geq 0\\(j\in J)}}\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{j\in J}(r_j+1)\binom{s}{r_j+2}X_j^{r_j}. \qquad (5.4)\end{aligned}$$

Recordando que de la definición (5.3)

$$\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{j\in J}\binom{s}{r_j+2}=\frac{t!}{\prod_{j\in J}(r_j+2)!}\omega(\vec{r}_J+2,t),$$

donde $\vec{r}_J=(r_j)_{j\in J}$ y $\vec{r}_J+2=(r_j+2)_{j\in J}$, reemplazamos en (5.4) y obtenemos

$$\begin{aligned}&\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}A_i\\ =\ &\sum_{J\in[\![1,m]\!]}(-1)^{|J|}\left(\prod_{j\in J}X_j\right)^2 t!\sum_{\substack{r_j\geq 0\\(j\in J)}}\omega(\vec{r}_J+2,t)\prod_{j\in J}\frac{r_j+1}{(r_j+2)!}X_j^{r_j},\end{aligned}$$

que es lo que queríamos probar. □

Mayorar los coeficientes $\omega(\vec{r}_J+2,t)$ será una parte importante de nuestro trabajo. A continuación hacemos un estudio de los coeficientes $\omega(\vec{r},t)$ interpretándolos como soluciones a un problema de enumeración de conjuntos. Para tal fin, recordamos un famoso resultado de análisis combinatorio, conocido como *principio de inclusión-exclusión.*

Lema 5.1.4 (Principio de inclusión-exclusión)**.** *Sea Ω un conjunto finito no vacío. Consideremos los subconjuntos $A_1,\ldots,A_k$ de Ω. Entonces*

$$\operatorname{card}\bigcup_{i=1}^{k}A_i\ =\ \sum_{\substack{J\subset[\![1,k]\!]\\J\neq\emptyset}}(-1)^{|J|+1}\operatorname{card}\bigcap_{j\in J}A_j$$

Demostración. Podemos suponer sin pérdida de generalidad que $\Omega=\bigcup A_i$. Consideremos los indicadores 1_{A_i}, $1\leq i\leq k$. Luego,

$$0=1_{(\bigcup A_i)^c}=1_{\bigcap A_i^c}=\prod_{i=1}^{k}\left(1-1_{A_i}\right).$$

Usando el lema 2.3.1 nos da

$$\begin{aligned}0\ &=\ \sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\prod_{j\in J}1_{A_j}\\ &=\ 1+\sum_{\substack{J\subset[\![1,m]\!]\\J\neq\emptyset}}(-1)^{|J|}\prod_{j\in J}1_{A_j},\end{aligned}$$

de donde

$$1=\sum_{\substack{J\subset[\![1,m]\!]\\J\neq\emptyset}}(-1)^{|J|+1}\prod_{j\in J}1_{A_j}(\omega),$$

para todo $\omega\in\Omega$. Sumando sobre todos los elementos $\omega\in\Omega=\bigcup A_i$ obtenemos el resultado deseado. □

El principio de inclusión exclusión puede ser planteado desde un punto de vista ligeramente distinto: suponiendo que tenemos un conjunto finito A y un conjunto de propiedades P, aplicables a los elementos del conjunto A. Si denotamos, para $p \in P$, por

$$A_p = \{x \in A;\ x \text{ tiene la propiedad } p\},$$

y para $B \subset P$

$$A_B = \bigcap_{p \in B} A_p,$$

(con $A_\emptyset = A$) el conjunto de los elementos en A que poseen todas las propiedades $p \in B$, entonces la cantidad de elementos $x \in A$ que poseen por lo menos alguna propiedad $p \in P$ es

$$\operatorname{card}\left(\bigcup_{p \in P}\right) = \sum_{\substack{B \subset P \\ P \neq \emptyset}} (-1)^{\operatorname{card} B + 1} \operatorname{card} A_B.$$

Luego, el número de los elementos en A que no cumplen ninguna de las propiedades $p \in P$ es

$$\sum_{B \subset P} (-1)^{\operatorname{card} B} \operatorname{card} A_B.$$

Proposición 5.1.5. *Sea $r = (r_1, \ldots, r_k) \in \mathbb{N}^k$. El número de formas de escoger k subconjuntos $A_1, \ldots, A_k$ de $[\![1, t]\!]$ tales que*

i) $\operatorname{card} A_j = r_j$, *para todo* $j = 1, \ldots, k$.

ii) $\bigcup_{j=1}^{k} A_j = [\![1, t]\!]$.

es exactamente

$$\frac{t!}{\prod_{j=1}^{k} r_j!} \omega(\vec{r}, t).$$

Demostración. Empecemos la prueba con una observación. Dado un subconjunto $B \subset [\![1, t]\!]$ con cardinal s, el número de maneras de obtener k-uplas $(A_1, \ldots, A_k)$ tales que $A_i \subset B$ para todo i es exactamente

$$\prod_{i=1}^{k} \binom{s}{r_i}.$$

Luego,el número de formas de escoger una k-upla $(A_1, \ldots, A_k)$ de subcojuntos de $[\![1, t]\!]$ tales que su $\operatorname{card} A_i = r_i$ para cada i es exactamente

$$\prod_{i=1}^{k} \binom{t}{r_i}. \tag{5.5}$$

A este número, le debemos restar la cantidad de k-uplas tales que su unión no es $[\![1,k]\!]$. Definiendo

$$B_i = [\![1,t]\!] \backslash \{i\},$$

para $i = 1, \ldots, t$, tales k-uplas $(A_1, \ldots A_k)$ son tales que

$$A_i \subset B_j,$$

para todo $i = 1, \ldots, k$, para algún $j \in \{1, \ldots, t\}$. Dado un subconjunto $B \subset [\![1,t]\!]$ definamos

$$T_B = \{(A_1, \ldots, A_k\} : \, A_i \subset B, \, \operatorname{card} A_i = r_i, \, \forall i \in \{1, \ldots, k\}\}\,.$$

De este modo, el número de maneras de escoger $(A_1, \ldots, A_k)$ tales que $A_i \subset B$ para todo i es exactamente

$$\operatorname{card} T_B = \prod_{i=1}^{k} \binom{\operatorname{card} B}{r_i}.$$

Luego, el número de k-uplas tales que su unión es un subconjunto propio de $[\![1,t]\!]$ es, por el principio de inclusión-exclusión

$$\operatorname{card} \bigcup_{i=1}^{t} T_{B_i} = \sum_{i=1}^{t} (-1)^{i-1} \sum_{\substack{J \subset [\![1,t]\!] \\ |J|=i}} \operatorname{card} \bigcap_{j \in J} T_{B_j}. \tag{5.6}$$

Ahora bien, notemos que

$$\begin{aligned}
\sum_{\substack{J \subset [\![1,t]\!] \\ |J|=i}} \operatorname{card} \bigcap_{j \in J} T_{B_j} &= \sum_{\substack{B \subset [\![1,t]\!] \\ \operatorname{card} B = t-i}} \operatorname{card} T_B \\
&= \sum_{\substack{B \subset [\![1,t]\!] \\ \operatorname{card} B = t-i}} \prod_{j=1}^{k} \binom{t}{t-i} \prod_{j=1} \binom{t-i}{r_j} \\
&= \binom{t}{t-i} \prod_{j=1}^{k} \binom{t}{t-i} \prod_{j=1} \binom{t-i}{r_j},
\end{aligned}$$

puesto que ambas cantidades suman, sobre cada $B \subset [\![1,t]\!]$ con cardinal $t-i$ por separado, el número de elementos de T_B. Luego, reemplazando en (5.6) tenemos que el número buscado (digamos x) es, por (5.5),

$$\begin{aligned}
x &= \prod_{j=1}^{k} \binom{t}{r_j} - \left(\sum_{i=1}^{t} (-1)^{i-1} \binom{t}{t-i} \prod_{j=1} \binom{t-i}{r_j} \right) \\
&= \sum_{s=0}^{t} (-1)^{t-s} \binom{t}{s} \prod_{j=1}^{k} \binom{s}{r_j}
\end{aligned}$$

que es

$$\frac{t!}{\prod_{j=1}^{k} r_j!}\omega(\vec{r},t).$$

por la definicion de $\omega(\vec{r},t)$. □

Lema 5.1.6. *Sea $t \in \mathbb{Z}^+$ y $\{R_j\}_{1\le j\le k}$ una partición del conjunto $[\![1,r]\!]$ (observemos que $r = \sum \operatorname{card} R_i$). Sea $\vec{r} = (\operatorname{card} R_1, \ldots, \operatorname{card} R_k) \in \mathbb{N}^k$. Entonces existen exactamente $\omega(\vec{r},t)$ particiones $\{B_i\}_{1\le i\le t}$ de $[\![1,r]\!]$ tales que*

$$\operatorname{card} R_j \cap B_i \le 1$$

para todo $1 \le j \le k$ y $1 \le i \le t$.

Demostración. Consideremos una partición B de $[\![1,t]\!]$ con la enumeración $B = \{B_i,\ 1 \le i \le t\}$. Dado $x \in [\![1,r]\!]$ existe un único $i \in \{1,\ldots,t\}$ tal que $x \in B_i$. Definamos la aplicación $\tau_B : [\![1,r]\!] \to [\![1,t]\!]$ por

$$\tau_B(x) = i, \qquad \text{para } x \in B_i.$$

Observemos que τ_B es sobreyectiva. Además, la condición $|R_j \cap B_i| \le 1$ para todo i,j es equivalente a afirmar que para cada $j \in \{1,\ldots,k\}$: $\tau_{B,j} := \tau_B|_{R_j}$ es inyectiva. En efecto, fijado un j, afirmar que $\tau_{B,j}$ no es inyectiva equivale a afirmar que existen dos elementos (o más) en R_j tales que tienen la misma imagen, digamos i, que equivale a decir que esos dos elementos están en el mismo B_i por definición de τ. Esto prueba lo observado. Ahora, τ_B depende de la enumeración de B, por lo que deducimos que para cada partición B tal que $|R_j \cap B_i| \le 1$, para todo i,j, existen exactamente $t!$ aplicaciones $\tau_B : [\![1,r]\!] \to [\![1,t]\!]$ sobreyectivas tales que $\tau_{B,j}$ es inyectiva para todo $j \in [\![1,k]\!]$. De hecho, toda aplicación τ con éstas características se puede expresar como τ_B para alguna partición B de $[\![1,r]\!]$. Definiendo

$$T = \left\{\tau : [\![1,r]\!] \to [\![1,t]\!] / \tau \text{ es sobreectiva, } \tau_j = \tau|_{R_j} \text{ es inyectiva, para todo } j \in [\![1,k]\!]\right\}$$

tenemos que por cada $t!$ elementos de T, existe una partición B con las características deseadas.

Ahora, calculemos el número de aplicaciones $\tau \in T$.

Fijemos una colección enumerada $\{A_i,\ i \in [\![1,k]\!]\}$ de subconjuntos de $[\![1,t]\!]$ tal que $\operatorname{card} A_i = r_i$ y

$$[\![1,t]\!] = \bigcup_{j=1}^{k} A_j.$$

Observemos que hay $\prod_{j=1}^{k} r_i!$ formas de definir aplicaciones $\tau \in T$ de modo que $\tau(R_j) = A_j$ para todo $j \in [\![1,k]\!]$. Además, por el lema 5.1.5, el número de k-uplas $(A_1,\ldots,A_k)$ es

$$\frac{t!}{\prod_{j=1}^{k} r_j!},$$

por lo que el número de elementos τ de T es

$$\prod_{j=1}^{k} r_j! \frac{t!}{\prod_{j=1}^{k} r_j!}\omega(\vec{r},t) = t!\omega(\vec{r},t),$$

con lo que se prueba la proposición. □

Corolario 5.1.7. *Sea $t \in \mathbb{N}$ y $\vec{r} = (r_1,\ldots,r_k) \in \mathbb{N}^n$. Entonces*

$$0 \leq \omega(\vec{r},t) \leq \left\{ \begin{matrix} \sum_{j=1}^{k} r_j \\ t \end{matrix} \right\}.$$

Demostración. Es una consecuencia inmediata del hecho que $\left\{ \begin{matrix} \sum r_i \\ t \end{matrix} \right\}$ mide el número de particiones de $[\![1, \sum r_i]\!]$ en t subconjuntos. □

5.2. Mayoración del sumando que involucra $\omega(\vec{r}_J + 2, t)$

Esta sección está dedicada a la mayoración del término

$$\sum_{\substack{r_j \geq 0 \\ j \in J}} \omega(\vec{r}_J + 2, t) \prod_{j \in J} \binom{s}{r_j + 2}$$

que aparece en la proposición 5.1.3, donde $\vec{r}_J = (r_j)_{j\in J} \subset \mathbb{N}^{|J|}$ con $J \subset [\![1,m]\!]$. Para un vector

$$X = (X_1,\ldots,X_m) \in \mathbb{C}^m$$

denotaremos como antes con $X_J = (X_j)_{j\in J}$ y con $\|.\|_\infty$ y $\|.\|$ a las normas del máximo y euclideana en $\mathbb{C}^m$, definidas por

$$\|X\|_\infty = \max_{1\leq i\leq k} |X_i|$$

y

$$\|X\| = \sqrt{\sum_{i=1}^{k} |X_i|^2}$$

respectivamente.

Lema 5.2.1. *Suponiendo que $t\|X\|_\infty \leq K$, entonces*

$$\left|\sum_{\substack{r_j\geq 0\\(j\in J)}} \omega(\vec{r}_J+2,t)\prod_{j\in J}\frac{r_j+1}{(r_j+2)!}X_j^{r_j}\right| \leq \frac{t^{2|J|}}{t!}\left(\frac{e^K-1}{K}\right)^{|J|},$$

Demostración. Para simplificar la notación denotemos con

$$E=\left|\sum_{r_j\geq 0} \omega(\vec{r}_J+2,t)\prod_{j\in J}\frac{r_j+1}{(r_j+2)!}X_j^{r_j}\right|.$$

Como $|X_j|\leq\|X\|_\infty$, $\frac{r_j+1}{(r_j+2)!}=\frac{1}{(r_j+2)r_j!}\leq\frac{1}{(r_j+1)!}$ y por el corolario 5.1.7

$$\omega(\vec{r}_J+2,t)\leq\left\{\begin{matrix}\sum_{j\in J}(r_j+2)\\ t\end{matrix}\right\}=\left\{\begin{matrix}\sum_{j\in J}r_j+2|J|\\ t\end{matrix}\right\},$$

entonces

$$\left|\sum_{r_j\geq 0} \omega(\vec{r}_J+2,t)\prod_{j\in J}\frac{r_j+1}{(r_j+2)!}X_j^{r_j}\right| \leq \sum_{\substack{r_j\geq 0\\(j\in J)}}\left\{\begin{matrix}\sum_{j\in J}r_j+2|J|\\ t\end{matrix}\right\}\frac{\|X\|_\infty^{\sum_{j\in J}r_j}}{\prod_{j\in J}(r_j+1)!}.$$

Denotemos con $\lambda=\sum_{j\in J}r_j$; agrupando los multi-índices $\vec{r}$ que tienen la misma suma de componentes obtenemos

$$\begin{aligned}E &\leq \sum_{\lambda\geq 0}\left\{\begin{matrix}\lambda+2|J|\\ t\end{matrix}\right\}\|X\|_\infty^\lambda \sum_{\substack{r_j\geq 0\\(j\in J)\\ \sum r_j=\lambda}}\frac{1}{\prod_{j\in J}(r_j+1)!}\\ &= \sum_{\lambda\geq 0}\left\{\begin{matrix}\lambda+2|J|\\ t\end{matrix}\right\}\frac{\|X\|_\infty^\lambda}{(\lambda+|J|)!}\sum_{\substack{r_j\geq 0\\(j\in J)\\ \sum r_j=\lambda}}\frac{(\lambda+1)!}{\prod_{j\in J}(r_j+1)!},\end{aligned}$$

y haciendo el cambio de variable $\vec{\mu}=\vec{r}+1$ en la suma interior

$$E\leq\sum_{\lambda\geq 0}\left\{\begin{matrix}\lambda+2|J|\\ t\end{matrix}\right\}\frac{\|X\|_\infty^\lambda}{(\lambda+|J|)!}\sum_{\substack{\mu_j\geq 1\\(j\in J)\\ \sum\mu_j=\lambda+|J|}}\frac{(\lambda+|J|)!}{\prod_{j\in J}(\mu_j!)!}.$$

Usando la proposición 1.1.5 en la suma interior obtenemos

$$E\leq\sum_{\lambda\geq 0}\frac{|J|!}{(\lambda+|J|)!}\left\{\begin{matrix}\lambda+2|J|\\ t\end{matrix}\right\}\left\{\begin{matrix}\lambda+|J|\\ |J|\end{matrix}\right\}\|X\|_\infty^\lambda.$$

Haciendo uso de la acotación de la proposición 1.1.6 tenemos que $\left\{\begin{matrix}\lambda+2|J|\\ t\end{matrix}\right\}\leq t^{\lambda+2|J|}/t!$, de donde

$$E\leq\frac{t^{2|J|}}{t!}\sum_{\lambda\geq 0}\frac{|J|!}{(\lambda+|J|)!}\left\{\begin{matrix}\lambda+|J|\\ |J|\end{matrix}\right\}(t\|X\|_\infty)^\lambda.$$

Haciendo el cambio de variable $s = \lambda + |J|$ obtenemos

$$\begin{aligned} E &\leq \frac{t^{2|J|}}{t!} \sum_{s \geq |J|} \frac{|J|!}{s!} \left\{ \begin{matrix} s \\ |J| \end{matrix} \right\} (t\|X\|_\infty)^{s-|J|} \\ &= (t\|X\|_\infty)^{-|J|} \frac{t^{2|J|}}{t!} \sum_{s \geq 0} \frac{|J|!}{s!} \left\{ \begin{matrix} s \\ |J| \end{matrix} \right\} (t\|X\|_\infty)^{s} \end{aligned}$$

pues $\left\{ \begin{matrix} s \\ |J| \end{matrix} \right\} = 0$ para $0 \leq s < |J|$. Luego, usando la identidad (1.3)

$$\begin{aligned} E &\leq \frac{t^{2|J|}}{t!} \left(\frac{e^{t\|X\|_\infty} - 1}{t\|X\|_\infty} \right)^{|J|} = \frac{t^{2|J|}}{t!} \left(\frac{e^{t\|X\|_\infty} - e^0}{t\|X\|_\infty - 0} \right)^{|J|} \\ &\leq \frac{t^{2|J|}}{t!} \left(\frac{e^K - 1}{K} \right)^{|J|}, \end{aligned}$$

siendo la última desigualdad una consecuencia de la convexidad de la función exponencial y la hipótesis $t\|X\|_\infty \leq K$, con lo cual concluímos la prueba. □

En el caso que $t \geq 2|J|$ podemos hacer una acotación algo más fina.

Lema 5.2.2. *Si $t\|X\|_\infty \leq K$ y $t \geq 2|J|$ entonces*

$$\left| \sum_{\substack{r_j \geq 0 \\ (j \in J)}} \omega(\vec{r}_J + 2, t) \prod_{j \in J} \frac{r_j + 1}{(r_j + 2)!} X_j^{r_j} \right| \leq \frac{\sqrt{(2|J|)!}|J|^{t/2}}{t!} \left(2\frac{e^{K/\sqrt{2}} - 1}{K} \right)^t \|X_J\|^{t-2|J|}.$$

Demostración. Observemos que

$$\begin{aligned} \left| \sum_{\substack{r_j \geq 0 \\ (j \in J)}} \omega(\vec{r}_J + 2, t) \prod_{j \in J} \frac{r_j + 1}{(r_j + 2)!} X_j^{r_j} \right| &\leq \sum_{\substack{r_j \geq 0 \\ (j \in J)}} \omega(\vec{r}_J + 2, t) \prod_{j \in J} \frac{r_j + 1}{(r_j + 2)!} |X_j|^{r_j} \\ &= \sum_{r \geq 0} \sum_{\substack{\vec{r}_J \geq 0 \\ \sum r_j = r}} \omega(\vec{r} + 2, t) \prod_{j \in J} \frac{r_j + 1}{(r_j + 2)!} |X_j|^{r_j}. \end{aligned}$$

Denotemos con S a la suma que se desea mayorar para simplificar la notación. Así, como

$$\prod_{j \in J} \frac{r_j + 1}{(r_j + 2)!} = \prod_{j \in J} \frac{1}{(r_j + 2)! r_j!}$$

entonces

$$S \leq \sum_{r \geq 0} \sum_{\substack{\vec{r}_J \geq 0 \\ \sum r_j = r}} \frac{\omega(\vec{+}2, t)}{\left(\prod_{j \in J} r_j! \right)^{1/2} (r_j + 2)} \prod_{j \in J} \frac{|X_j|^{r_j}}{\left(\prod_{j \in J} r_j! \right)^{1/2}},$$

y usando la desigualdad de Cauchy-Schwartz tenemos

$$\begin{aligned} S &\leq \sum_{r\geq 0}\left(\sum_{\substack{\vec{r}_J\geq 0\\ \sum_j r_j=r}} \frac{\omega(\vec{r}_J+2)^2}{\prod_{j\in J} r_j!(r_j+2)^2}\right)^{1/2}\left(\sum_{\substack{\vec{r}_j\geq 0\\ \sum_j r_j=r}}\prod_{j\in J}\frac{|X_j|^{2r_j}}{r_j!}\right)^{1/2} \\ &\leq \sum_{r\geq 0}\left(\sum_{\substack{\vec{r}_J\geq 0\\ \sum_j r_j=r}} \frac{\omega(\vec{r}_J+2)^2}{\prod_{j\in J}(r_j+2)!}\right)^{1/2}\left(\sum_{\substack{\vec{r}_j\geq 0\\ \sum_j r_j=r}}\prod_{j\in J}\frac{|X_j|^{2r_j}}{r_j!}\right)^{1/2}. \end{aligned}$$

Usamos la proposición 5.1.7, de donde $\omega(\vec{r}_J+2,t)\leq \left\{{r+2|J|\atop t}\right\}$, y así

$$\begin{aligned} S &\leq \sum_{r\geq 0}\left\{{r+2|J|\atop t}\right\}\left(\sum_{\substack{\vec{r}_J\geq 0\\ \sum_j r_j=r}} \frac{1}{\prod_{j\in J}(r_j+2)!}\right)^{1/2}\left(\sum_{\substack{\vec{r}_J\geq 0\\ \sum_j r_j=r}}\frac{1}{\prod_{j\in J}}\prod_{j\in J}|X_j|^{2r_j}\right)^{1/2} \\ &= \sum_{r\geq 0}\frac{\left\{{r+2|J|\atop t}\right\}}{((r+2|J|)!r!)^{1/2}}\left(\sum_{\substack{\vec{r}_J\geq 0\\ \sum_j r_j=r}} \frac{(r+2|J|)!}{\prod_{j\in J}(r_j+2)!}\right)^{1/2}\left(\sum_{\substack{\vec{r}_J\geq 0\\ \sum_j r_j=r}}\frac{r!}{\prod_{j\in J} r_j!}\prod_{j\in J}|X_j|^{2r_j}\right)^{1/2} \\ &= \sum_{r\geq 0}\frac{\left\{{r+2|J|\atop t}\right\}}{((r+2|J|)!r!)^{1/2}}\left(\sum_{\substack{\vec{r}_J\geq 0\\ \sum_j r_j=r}} \binom{r+2|J|}{\vec{r}+2}\right)^{1/2}\left(\sum_{\substack{\vec{r}_J\geq 0\\ \sum_j r_j=r}}\binom{r}{\vec{r}}\prod_{j\in J}|X_j|^{2r_j}\right)^{1/2}. \end{aligned}$$

Usando el corolario 1.1.3 y la proposición 1.1.2 en cada uno de los paréntesis respectivamente obtenemos

$$\begin{aligned} S &\leq \sum_{r\geq 0}\frac{\left\{{r+2|J|\atop t}\right\}}{((r+2|J|)!r!)^{1/2}}\left(|J|^{r+2|J|}\right)^{1/2}\left(\sum_{j\in J}|X_j|^2\right)^{r/2} \\ &= \sum_{r\geq 0}\left(\frac{1}{(r+2|J|)!r!}\right)^{1/2}\left\{{r+2|J|\atop t}\right\}\left(|J|^{r+2|J|}\right)^{1/2}\|X_J\|^r. \end{aligned}$$

Observando que

$$\frac{1}{r!}=\frac{(r+2|J|)!}{(2|J|!)(r+2|J|-2|J|)!}\frac{(2|J|)!}{(r+2|J|)!}=\frac{(2|J|)!}{(r+2|J|)!}\binom{r+2|J|}{2|J|}\leq\frac{(2|J|)!}{(r+2|J|)!}2^{r+2|J}$$

obtenemos

$$S \leq ((2|J|)!)^{1/2}\sum_{r\geq 0}\frac{(2|J|)^{(r+2|J|)/2}}{(r+2|J|)!}\left\{{r+2|J|\atop t}\right\}\|X_J\|^r,$$

y haciendo en cambio de variable $\mu = r + 2|J|$ se tiene

$$S \leq \frac{((2|J|)!)^{1/2}}{\|X_J\|^{2|J|}} \sum_{\mu \geq 2|J|} \frac{(2|J|)^{\mu/2}}{\mu!} \left\{ {\mu \atop t} \right\} \|X_J\|^{\mu} = \frac{((2|J|)!)^{1/2}}{\|X_J\|^{2|J|}} \sum_{\mu \geq 0} \left\{ {\mu \atop t} \right\} \frac{\left(\sqrt{2|J|}\|X_J\|\right)^{\mu}}{\mu!},$$

puesto que para $\mu < 2|J| \leq t$ tenemos $\left\{ {\mu \atop t} \right\} = 0$. Luego, en virtud de la proposición 1.3,

$$S \leq \frac{((2|J|)!)^{1/2}}{\|X_J\|^{2|J|}} \frac{\left(e^{\sqrt{2|J|}\|X_J\|} - 1\right)^t}{t!} = \frac{\sqrt{(2|J|)!}}{t!} \sqrt{2|J|}^t \left(\frac{e^{\sqrt{2|J|}\|X_J\|} - 1}{\sqrt{2|J|}\|X_J\|} \right)^t \|X_J\|^{t-2|J|}. \tag{5.7}$$

Como $\|X_J\| \leq |J|^{1/2}\|X\|_\infty$ y, por hipótesis, $t\|X\|_\infty \leq K$ entonces $\sqrt{2|J|}\|X_J\| \leq K/\sqrt{2}$, y usando la convexidad de la función exponencial resulta

$$\frac{e^{\sqrt{2|J|}\|X_J\|} - 1}{\sqrt{2|J|}\|X_J\|} \leq \frac{e^{K/\sqrt{2}} - 1}{K/\sqrt{2}}.$$

Reemplazando esto en (5.7) obtenemos el resultado deseado. □

Lema 5.2.3. *Para $k \in \mathbb{N}$ tenemos*

$$\sum_{\substack{J \subset [\![1,m]\!] \\ |J|=k}} \left| \prod_{j \in J} X_j \right|^2 \leq \frac{\|X\|^{2k}}{k!}$$

Demostración. Observemos en primer lugar que para $a_i > 0$, $i \in [\![1, m]\!]$, tenemos

$$\left(\sum_{i=1}^m a_i \right)^k = \sum_{\substack{i_j \in [\![1,m]\!] \\ (j \in [\![1,k]\!])}} \prod_{j=1}^k a_{i_j}.$$

Dado un $J = \{i_1 < i_2 < \ldots < i_k\} \subset [\![1, m]\!]$ ($|J| = k$), el producto $\prod_{j=1}^k a_{i_j}$ aparece almenos $k!$ veces en la suma de la derecha, por lo que tenemos

$$\left(\sum_{i=1}^m a_i \right)^k \geq k! \sum_{\substack{J \subset [\![1,m]\!] \\ |J|=k}} \prod_{j \in J} a_{i_j}.$$

En el caso en que $a_i = |X_i|^2$ obtenemos la desigualdad deseada. □

Lema 5.2.4. *Para $\lambda > 0$ se tiene*

$$\sum_{J \subset [\![1,m]\!]} \lambda^{|J|} \left| \prod_{j \in J} X_j \right|^2 \leq e^{\lambda \|X\|^2}.$$

Demostración. Usando el lema 5.2.3 tenemos

$$\begin{aligned}\sum_{J\subset[\![1,m]\!]}\lambda^{|J|}\left|\prod_{j\in J}X_j\right|^2 &= \sum_{k=1}\sum_{\substack{J\subset[\![1,m]\!]\\|J|=k}}\left|\prod_{j\in J}\lambda^{1/2}X_j\right|^2\\ &\leq \sum_{k=1}^{m}\frac{\left\|\lambda^{1/2}X\right\|^{2k}}{k!}\\ &\leq e^{\left\|\lambda^{1/2}X\right\|^2}=e^{\lambda\|X\|^2},\end{aligned}$$

que es lo que se quiere probar. □

Lema 5.2.5. *Sean $\lambda\in\mathbb{R}$ y $k\in\mathbb{N}$. Entonces*

$$\sum_{\substack{J\subset[\![1,m]\!]\\|J|\geq k}}\lambda^{|J|}\left|\prod_{j\in J}X_j\right|^2\leq\lambda^k e^{\lambda\|X\|^2}\frac{\|X\|^{2k}}{k!}.$$

Demostración. En primer lugar notemos que

$$\sum_{n\geq k}\frac{x^n}{n!}=\frac{x^k}{k!}\sum_{n\geq k}\frac{x^{n-k}}{n(n-1)\dots(n-k+1)}\leq\frac{x^k}{k!}\sum_{i\geq 0}\frac{x^i}{i!}=\frac{x^k}{k!}e^x.$$

Luego, usando el lema 5.2.3 tenemos

$$\begin{aligned}\sum_{\substack{J\subset[\![1,m]\!]\\|J|\geq k}}\left|\prod_{j\in J}\right|^2 &= \sum_{n\geq k}\sum_{\substack{J\subset[\![1,m]\!]\\|J|=n}}\left|\prod_{j\in J}\lambda^{1/2}X_j\right|^2\\ &\leq \sum_{n\geq k}\frac{\left(\lambda\|X\|^2\right)^n}{n!}\\ &\leq \frac{\left(\lambda\|X\|^2\right)^k}{k!}e^{\lambda\|X\|^2}\frac{\|X\|^{2k}}{k!}.\end{aligned}$$

□

Dado un vector $x\in(\mathbb{C}\backslash\{1\})^m$ denotaremos a fin de simlificar la notación por

$$X=(X_i)_{1\leq i\leq m}=\left(\frac{x_1}{1-x_1},\dots,\frac{x_m}{1-x_m}\right)\in(\mathbb{C}\backslash\{1\})^m.$$

Proposición 5.2.6. *Sean K, $K'>0$ en $\mathbb{R}$, $t\in\mathbb{N}$ y $x\in(\mathbb{R}\backslash\{1\})^m$. Si $t\|X\|_\infty\leq K$ y $t\|X\|^2\leq K'$ entonces*

$$\left|\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}\frac{1-sx_i}{(1-sx_i)^s}\right|\leq 2C_1^t\left(t\|X\|^2\right)^{t/2}+C_2C_3^t\left(t\|X\|^2\right)^{(t+1)/2},$$

donde

$$C_1 = 2\left(e^{K/\sqrt{2}} - 1\right),\ C_2 = 2\frac{e^K - 1}{K}\,\text{máx}\left(1, \sqrt{K'}\right)\ \text{y}\ C_3 = e^{K'(e^K-1)/K}\sqrt{2e\frac{e^K-1}{K}}.$$

Por consiguiente,

$$\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}\frac{1-sx_i}{(1-sx_i)^s} \ll_{K,K'} \left(Ct\|X\|^2\right)^{t/2}.$$

Demostración. Para simplificar la notación, denotemos con

$$\mathbb{S} = \sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}\frac{1-sx_i}{(1-sx_i)^s}.$$

De la proposición 5.1.3 tenemos

$$\mathbb{S} = \sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\left(\prod_{j\in J}X_j\right)^2 t!\sum_{\substack{r_j\geq 0\\(j\in J)}}\omega(\vec{r}_J+2,t)\prod_{j\in J}\frac{r_j+1}{(r_j+2)!}X_j^{r_j},$$

y separando la suma para $|J| \leq t/2$ y $|J| > t/2$ tenemos que

$$\mathbb{S} = \mathbb{S}_1 + \mathbb{S}_2,$$

donde

$$\mathbb{S}_1 = \left|\sum_{\substack{J\subset[\![1,m]\!]\\|J|\leq t/2}}(-1)^{|J|}\left(\prod_{j\in J}X_j\right)^2 t!\sum_{\substack{r_j\geq 0\\(j\in J)}}\omega(\vec{r}_J+2,t)\prod_{j\in J}\frac{r_j+1}{(r_j+2)!}X_j^{r_j}\right|$$

y

$$\mathbb{S}_2 = \left|\sum_{\substack{J\subset[\![1,m]\!]\\|J|> t/2}}(-1)^{|J|}\left(\prod_{j\in J}X_j\right)^2 t!\sum_{\substack{r_j\geq 0\\(j\in J)}}\omega(\vec{r}_J+2,t)\prod_{j\in J}\frac{r_j+1}{(r_j+2)!}X_j^{r_j}\right|.$$

Denotemos con $C_1 = 2\left(e^{K/\sqrt{2}} - 1\right)/K$. Empezamos acotando $\mathbb{S}_1$. Del lema 5.2.2 y el hecho que $\|X_J\| \leq \|X\|$ tenemos

$$\begin{aligned}
\mathbb{S}_1 &\leq \sum_{\substack{J\subset[\![1,m]\!]\\|J|\leq t/2}}\left|\prod_{j\in J}X_j\right|\sqrt{(2|J|)!}|J|^{t/2}\left(2\frac{e^{K/\sqrt{2}}-1}{K}\right)^t\|X_J\|^{t-2|J|}\\
&= \sum_{\substack{J\subset[\![1,m]\!]\\|J|\leq \lfloor t/2\rfloor}}\left|\prod_{j\in J}X_j\right|\sqrt{(2|J|)!}|J|^{t/2}C_1^t\|X\|^{t-2|J|}\\
&= \sum_{k=0}^{\lfloor t/2\rfloor}\|X\|^{t-2k}\sqrt{(2k)!}k^{t/2}C_1^t\sum_{\substack{J\subset[\![1,m]\!]\\|J|=k}}\left|\prod_{j\in J}X_j\right|.
\end{aligned}$$

Usando el lema 5.2.3 obtenemos

$$\begin{aligned}\mathbb{S}_1 &\leq C_1^t \sum_{k=0}^{\lfloor t/2 \rfloor} k^{t/2} \frac{\sqrt{(2k)!}}{k!} \|X\|^{2k} \|X\|^{t-2k} \\ &= C_1^t \sum_{k=0}^{\lfloor t/2 \rfloor} k^{t/2} \binom{2k}{k}^{1/2} \|X\|^t \\ &\leq C_1^t \|X\|^t \left(\frac{t}{2}\right)^{t/2} \sum_{k=0}^{\lfloor t/2 \rfloor} \sqrt{2^{2k}},\end{aligned}$$

y como

$$\sum_{k=0}^{\lfloor t/2 \rfloor} 2^k = 2^{\lfloor t/2 \rfloor + 1} - 1 \leq 2^{t/2+1}$$

entonces

$$\mathbb{S}_1 \leq 2C_1^t \left(t\|X\|^2\right)^{t/2}. \tag{5.8}$$

Ahora acotemos $\mathbb{S}_2$. Denotemos con $C_2 = \left(e^K - 1\right)/K$. Del lema 5.2.1 tenemos

$$\begin{aligned}\mathbb{S}_2 &\leq \sum_{\substack{J \subset [\![1,m]\!] \\ |J| > t/2}} \left| \prod_{j \in J} X_j \right| t^{2|J|} \left(\frac{e^K - 1}{K}\right)^{|J|} \\ &= \sum_{\substack{J \subset [\![1,m]\!] \\ |J| \geq \lfloor t/2 \rfloor + 1}} \left(C_2 t^2\right)^{|J|} \left| \prod_{j \in J} X_j \right|^2,\end{aligned}$$

y usando el lema 5.2.5 tenemos

$$\mathbb{S}_2 \leq \left(c_2 t^2\right)^{\lfloor t/2 \rfloor + 1} e^{C_2 t^2 \|X\|^2} \frac{\|X\|^{2\lfloor t/2 \rfloor + 2}}{(\lfloor t/2 \rfloor + 1)!}.$$

Sabemos que $n! \geq (n/e)^n e$, de donde

$$\begin{aligned}\mathbb{S}_2 &\leq \left(C_2 t^2\right)^{\lfloor t/2 \rfloor + 1} e^{C_2 t^2 \|X\|^2} \frac{\|X\|^{2\lfloor t/2 \rfloor + 2}}{\left(\frac{\lfloor t/2 \rfloor + 1}{e}\right)^{\lfloor t/2 \rfloor + 1} e} \\ &= e^{-1} \left(C_2 e \frac{t^2}{\lfloor t/2 \rfloor + 1} \|X\|^2\right)^{\lfloor t/2 \rfloor + 1} e^{C_2 t^2 \|X\|^2},\end{aligned}$$

y como $t^2/(\lfloor t/2 \rfloor + 1) \leq t^2/(t/2) = 2t$ y $\lfloor t/2 \rfloor + 1 \leq t/2 + 1$ entonces

$$\begin{aligned}\mathbb{S}_2 &\leq e^{-1} \left(2C_2 e\right)^{t/2+1} \left(e^{2C_2 t \|X\|^2}\right)^{t/2} \left(t\|X\|^2\right)^{\lfloor t/2 \rfloor + 1} \\ &= 2C_2 \left(2C_2 e^{2C_2 t \|X\|^2 + 1}\right)^{t/2} \left(t\|X\|^2\right)^{\lfloor t/2 \rfloor + 1}.\end{aligned}$$

Luego, como por hipótesis $t\|X\|^2 \leq K'$ entonces

$$\mathbb{S}_2 \leq 2C_2 \left(2C_2 e^{2C_2 K' + 1}\right)^{t/2} \left(t\|X\|^2\right)^{\lfloor t/2 \rfloor + 1}.$$

Observemos que como $t\|X\|^2 \leq K'$ entonces

$$\left(t\|X\|^2\right)^{\lfloor t/2\rfloor+1} = \left(t\|X\|^2\right)^{(t+1)/2}$$

si t es impar, y

$$\left(t\|X\|^2\right)^{\lfloor t/2\rfloor+1} = \left(t\|X\|^2\right)^{t/2+1} \leq \sqrt{K'}\left(t\|X\|^2\right)^{(t+1)/2}$$

si es par. Luego,

$$\mathbb{S}_2 \leq 2C_2 \,\text{máx}\left(1, \sqrt{K'}\right)\left(2C_2 e^{2C_2K'+1}\right)^{t/2}\left(t\|X\|^2\right)^{(t+1)/2,}$$

lo que junto con (5.8) prueba el resultado. □

Capítulo 6

Conclusiones

A modo de epílogo del presente trabajo presentamos algunas consideraciones finales (las referencias precisas a las fuentes de los resultados que iremos mencionando pueden ser encontradas en [5]) para el teorema 4.0.12 probado en la sección anterior, el cual puede ser considerado como una aproximación a la siguiente acotación uniforme:

Conjetura 6.0.7. *Para una constante absoluta $c > 0$ tenemos*

$$M_k(q;h) \ll q\,(ck)^{k/2}\left(k + h\frac{\varphi(q)}{q}\right)^{k/2}$$

uniformemente en $k \geq 0$, $h \geq 0$ y $q \in \mathbb{N}$.

Este resultado, conjeturable a la vista del teorema 4.0.12, está intrínsicamente ligado a la prueba de una conjetura presentada por P. Erdös, que asegura la existencia de un número real $x > 0$ tal que, para todo $q \in \mathbb{N} - \{0\}$,

$$\sum_{i=1}^{\varphi(q)} e^{x(a_{i+1}-a_i)\varphi(q)/q} \ll \varphi(q), \tag{6.1}$$

donde $1 = a_1 < a_2 < \cdots$ es la sucesión de enteros coprimos con q. Observando que

$$g(q) = \max_{i\in\mathbb{N}} a_{i+1} - a_i,$$

se sigue directamente que

$$g(q) \ll \frac{q}{\varphi(q)}\log q,$$

donde g es la función de Jhacobstal definida en la introducción del trabajo. Ésta acotación es por lo general la acotación más fuerte admitida para la función g. De hecho, Erdös muestra que la expresión

$$(1 + o(1))\omega(q)\frac{q}{\varphi(q)}$$

es un orden normal y minorante para $g(q)$, mientras que la mejor acotación conocida, obtenida por H. Iwaniec está dada por la expresión

$$g(q) \ll \frac{q}{\varphi(q)}\omega(q)^2 \log 2\omega(q).$$

Del mismo modo, la conjetura 6.0.7 permitiría probar la siguiente acotación de la diferencia entre dos primos consecutivos

$$p_{n+1} - p_n \ll p_n^{1/2} \log p_n,$$

acotación ya probada por Cramér bajo la asumpción hipótesis de Riemann.
Por otro lado, recordemos el famoso teorema de Linnik, el cual asegura la existencia de una constante $L > 0$ (llamada comunmente constante de Linnik) tal que el primer primo $p_{a,d}$ en una sucesión de aritmética $(a + nd)_{n\in\mathbb{N}}$, con $(a, d) = 1$ puede ser acotado en la forma

$$p_{a,d} \ll d^L.$$

Algunos trabajos sobre el menor valor de L admisible conjeturan que $L = 2$. En este contexto, la conjetura 6.0.7 permite probar la acotación

$$p_{a,d} \ll d^2(\log d)^2,$$

y de este modo $p_{a,d} \ll d^{2+\varepsilon}$, para todo $\varepsilon > 0$.

Bibliografía

[1] T. Apostol, *Introducction to Analytic Number Theory*, Springer-Verlag, New York (1976)

[2] T. Apostol, *Mathematical Analysis*, Addison-Wesley Publishing, London (1974).

[3] P. Billingsley, *Convergence of Probability Measures* 2da Edición, John Wiley and Sons (1999).

[4] A. Chadozeau, *Sur la répartition des entiers premiers à un entier sans petit facteur premier*, Journal of Number Theory 128 (2008) 2282–2317.

[5] A. Chadozeau, *Sur la répartition des entiers premiers à un entier donné*, Tesis doctoral, Université Bordeaux I (2006).

[6] K.L. Chung, *A Course in Probability Theory*, 3ra Edición, Academic Press, London (2001).

[7] H. Cramér, *On the Order of Magnitude of the Difference between Consecutive Prime Numbers*, Acta Arith. 2 (1936), 23–46.

[8] J.M. Desohuillers, *Probability and Number Theory: some examples of conenctions*, University of Bordeaux (1997).

[9] R. Durret, *Probability: Theory and Examples* 4ta Edición, Cambridge University Press (2010).

[10] H. Halberstam, K.F. Roth, *Sequences*, Springer Verlag, New-York (1983).

[11] P.R Halmos, *Measure Theory*, Van Nostrand, New York (1950).

[12] G.H. Hardy y E. M. Wright, *An Introduction to the Theory of Numbers* 4ta Edición, Oxford University Press (1960).

[13] G.H. Hardy, S.Ramanujan, *The Normal Number of Prime Factors of a Number n*, Quarterly Journal of Mathematics, XLVIII, 1917, 76-92.

[14] H.L. Montgomery, K. Soundararajan, *Primes in short intervals*, Comm. Math. Phys. 252 (1–3) (2004), 589-–617.

[15] H.L. Montgomery, R.C. Vaughan, *On the distribution of reduced residues*, Ann. of Math. 123 (1986) 311–333.

[16] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press (1995).

[17] E. Artin, *The Gamma Function*, Holt, Rinehart and Wiston (1964).

[18] V. Romanovsky, *Note on the moments of a binomial* $(p + q)^n$ *about its mean*, Biometrika 15 (1910), 410.

[19] W. Rudin, *Real and Complex Analysis*, McGraw-Hill (1970).

[20] L. Comtei, *Analyse combinatoire, tome 2*, Coll. Le mathématicien, vol. 5, Presses Universitaires de France, París (1970).