Algunas funciones especiales

Daniel Campos Salas

(Material en construcción)

Contents

Vamos a introducir varias funciones relacionadas con números enteros y vamos a estudiar sus propiedades.

1 Factorial

Dado un entero positivo n, la cantidad de maneras en que podemos ordenar (digamos en fila) n objetos distintos es igual a

$$n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1,$$

ya que hay n posibilidades para la primera posición, $(n-1)$ restantes para la segunda posición, y así sucesivamente hasta llegar a la última posición, para la cual solo hay 1 posibilidad. Definimos el producto anterior como el **factorial** de n, o n **factorial**, y lo denotamos por $n!$ (el signo de exclamación

es parte de la notación). Aunque resulte un poco extraño, definimos $0! = 1$. De esta manera, para $n \geq 1$ tenemos la **relación de recurrencia**[1]

$$n! = n \cdot (n-1)!.$$

Los primeros términos de la sucesión son

$$0! = 1, \quad 1! = 1, \quad 2! = 2, \quad 3! = 6, \quad 4! = 24, \quad 5! = 120, \quad 6! = 720, \quad 7! = 5040, \ldots.$$

Como vemos, esta sucesión crece muy rápidamente; de hecho, crece más rápido que polinomios e inclusive que funciones exponenciales.

Ejercicio 1. *Demuestre que si $n \geq 4$, entonces $n! \geq 2^n$.*

Ejercicio 2. *Use la desigualdad de las medias aritmética y geométrica para demostrar que para todo entero positivo n se cumple que $n! \leq [(n+1)/2]^n$.*

Ejercicio 3. *El número $e = 2,7182\ldots$ satisface que $e^x \geq 1 + x$ para todo $x \in \mathbb{R}$.*

1. *Use este resultado para demostrar que $[(n+1)/n]^n \leq e$.*
2. *Use el resultado anterior para demostrar que*

$$(n+1) \cdot \left(\frac{n}{e}\right)^n \geq \left(\frac{n+1}{e}\right)^{n+1}.$$

3. *Use inducción y el resultado anterior para demostrar que $n! \geq (n/e)^n$.*

1.1 Tópicos avanzados: la fórmula de Stirling

Los resultados de los ejercicios anteriores nos dicen que

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

Una forma precisa de determinar el crecimiento de $n!$ es conocida como la **fórmula de Stirling**, que establece que

$$\lim_{n \to +\infty} \frac{n!}{(\frac{n}{e})^n \sqrt{n}} = \sqrt{2\pi},$$

es decir, $n!$ se comporta como $(n/e)^n \sqrt{2\pi n}$ cuando n es grande. Una ventaja de conocer esta aproximación es que el cálculo de esta última expresión no es recurrente, en contraste con la definición original de $n!$.

Ejercicio 4. *Suponga que un caminante se encuentra sobre la recta real y camina sobre los números enteros. En cada momento, tira una moneda (justa) para decidir si se mueve al entero anterior o al entero siguiente. Suponga que el caminante empieza originalmente en 0.*

1. *Si N es impar, calcule la probabilidad de que el caminante se encuentre de nuevo en 0 después de exactamente N pasos.*
2. *Si N es par, calcule la probabilidad de que el caminante se encuentre de nuevo en 0 después de exactamente N pasos.*
3. *Use la fórmula de Stirling para obtener una aproximación de la probabilidad calculada anteriormente cuando N es grande.*

[1] Decimos que una definición es recurrente cuando ella se invoca a sí misma. Por ejemplo, para definir la sucesión de los factoriales, empezamos con $0! = 1$ y para $n \geq 1$ definimos $n!$ en términos de $(n-1)!$ mediante $n! = n \cdot (n-1)!$. Otro ejemplo de definición recurrente es la de la sucesión de Fibonacci.

2 Función parte entera y parte fraccionaria

La **parte entera** $\lfloor a \rfloor$ de un número real a es el mayor entero posible que es menor o igual que a. De esta forma, si m es el entero que satisface $m \leq a < m+1$, entonces $\lfloor a \rfloor = m$. Es decir, la parte entera satisface que

$$\lfloor a \rfloor \leq a < \lfloor a \rfloor + 1. \tag{1}$$

Ejemplo 1. *Como* $3 < \pi < 4$ *y* $-4 < -\pi < -3$*, entonces* $\lfloor \pi \rfloor = 3$ *y* $\lfloor -\pi \rfloor = -4$.

Una primera propiedad un poco obvia es que la parte entera es **creciente**: si $a \leq b$, entonces $\lfloor a \rfloor \leq \lfloor b \rfloor$. En efecto, si $n = \lfloor a \rfloor$, entonces $n \leq a \leq b$, lo que implica que $n \leq \lfloor b \rfloor$, es decir, $\lfloor a \rfloor \leq \lfloor b \rfloor$.

Una propiedad un poco más interesante es la siguiente. Contraria a la desigualdad sub-aditiva del valor absoluto, $|a+b| \leq |a| + |b|$, la parte entera satisface la propiedad de **super-aditividad**,

$$\lfloor a+b \rfloor \geq \lfloor a \rfloor + \lfloor b \rfloor. \tag{2}$$

Para demostrar esto consideramos $m = \lfloor a \rfloor$ y $n = \lfloor b \rfloor$, de manera que $m \leq a$ y $n \leq b$. Esto implica que $m + n \leq a + b$ y por lo tanto, $m + n \leq \lfloor a + b \rfloor$, lo que demuestra (2).

Ejercicio 5. *Dé ejemplos donde se alcance la igualdad en* (2)*. Dé ejemplos donde no haya igualdad.*

Ejercicio 6. *Demuestre que si* n *es entero, entonces* $\lfloor a + n \rfloor = \lfloor a \rfloor + n$.

Definimos la **parte fraccionaria** $\{a\}$ de un número real a como la diferencia $\{a\} := a - \lfloor a \rfloor$, de manera que (1) arriba implica que

$$0 \leq \{a\} < 1. \tag{3}$$

Ejercicio 7. *Demuestre que la parte fraccionaria es* ***sub-aditiva****, es decir, satisface que*

$$\{a+b\} \leq \{a\} + \{b\}.$$

Dé ejemplos donde se alcance la igualdad y donde no se alcance.

2.1 Potencia en factorización del factorial

Ejercicio 8. *¿Cuántos ceros tiene 2020! al final de su expansión?*

El ejercicio anterior nos conduce a buscar las potencias de 2 y 5 que dividen a 2020!. Es razonable esperar que la potencia de 2 sea mayor que la de 5, de manera que solo necesitamos calcular cuál es la potencia de 5 que divide a 2020!. Hacemos esto de la siguiente manera: cada múltiplo de 5 aporta por lo menos un factor, de manera que tenemos $2020/5 = 404$ contribuciones. Ahora, los números divisibles por 25 contribuyen una vez más (ya que les contamos un factor anteriormente): tendríamos $404/5 = 80,8$. Claramente, necesitamos tomar la parte entera de esto, es decir, $\lfloor 404/5 \rfloor = 80$. Repetimos con 125 y 625, pues no hay múltiplos de 3125 menores o iguales que 2020. Al final debemos sumar todas estas contribuciones:

$$404 + 80 + 16 + 3 = 503.$$

En general, tenemos que si p es un primo, entonces la máxima potencia de p que divide a $n!$, la cual denotamos por $\text{pot}(p, n!)$, es

$$\boxed{\text{pot}(p, n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots.}$$

Aunque la suma anterior parece infinita en realidad es finita, ya que existe un entero k para el cual $n < p^k$ y por lo tanto las partes enteras a partir de ese punto son iguales a 0.

Ejercicio 9. *Sea p un primo y n un entero positivo. Considere la representación de n en base p, es decir, $n = a_0 + a_1 p + a_2 p^2 + \ldots$. Determine las expresiones $\lfloor n/p^k \rfloor$ en términos de los coeficientes. Demuestre que*

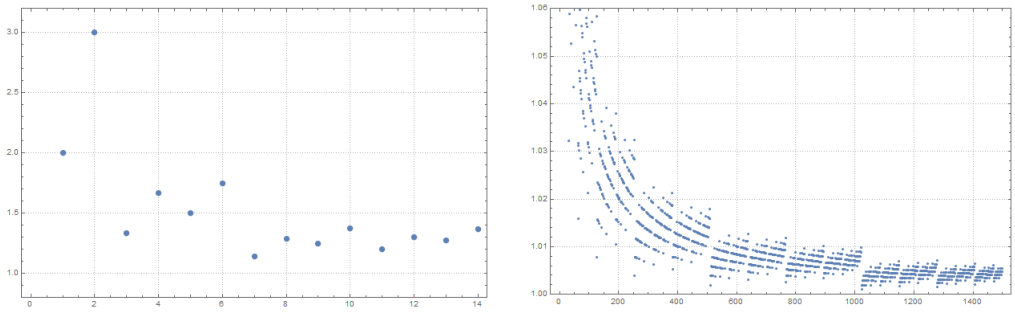
$$pot(p, n!) = \frac{n - (a_0 + a_1 + a_2 + \ldots)}{p - 1}.$$

Ejercicio 10. *Sea k un entero positivo. Calcule la máxima de potencia de p que divide a $(p^k)!$. Calcule el cociente de p^k entre el número anterior y calcule el límite de este cociente cuando $k \to +\infty$.*

Experimento. *En este experimento, ampliamos un poco los resultados del ejercicio anterior. Sea p su número primo favorito. Haga una lista de los exponentes de p en $n!$ para $1 \leq n \leq N$, para algún número grande N. Si escoge $p = 2, 3$ con $N = 100$ es suficiente, para $p = 5$ con $N = 150$ es suficiente. Calcule ahora los cocientes de n dividido por los exponentes de p en $n!$. ¿Qué observa para valores grandes de n? Repita este experimento para varios primos distintos y conjeture una respuesta. Ilustramos el cálculo con $p = 2$:*

n	1	2	3	4	5	6	7	8	9	10	11	12	13	...
$pot(2, n!)$	0	1	1	3	3	4	4	7	7	8	8	10	10	...
$n/pot(2, n!)$	$*$	2	3	1,33	1,66	1,5	1,75	1,14	1,29	1,25	1,38	1,2	1,3	...

En la siguiente imagen se muestran los cocientes $n/pot(2, n!)$ para $1 \leq n \leq 14$ y $1 \leq n \leq 1500$:



2.2 Teorema de Beatty

Una ilustración interesante y curiosa de los conceptos definidos es el siguiente resultado.

Teorema 2.1 (Beatty). *Si α y β son irracionales positivos tales que $1/\alpha + 1/\beta = 1$, entonces todo entero positivo pertenece exactamente a una de las sucesiones $\{\lfloor \alpha \rfloor, \lfloor 2\alpha \rfloor, \lfloor 3\alpha \rfloor, \ldots\}$ y $\{\lfloor \beta \rfloor, \lfloor 2\beta \rfloor, \lfloor 3\beta \rfloor, \ldots\}$.*

Prueba. Empezamos demostrando que ningún entero aparece dos veces en las sucesiones. Primero demostramos que no aparece dos veces en la misma sucesión: como tenemos que $1/\alpha < 1/\alpha + 1/\beta = 1$, entonces $\alpha > 1$. Esto implica que $(n+1)\alpha = n\alpha + \alpha > n\alpha + 1$. Por lo tanto,

$$\lfloor (n+1)\alpha \rfloor \geq \lfloor n\alpha + 1 \rfloor = \lfloor n\alpha \rfloor + 1,$$

lo cual previene que aparezcan términos repetidos en la misma sucesión. Demostramos ahora que no es posible que las diferentes sucesiones tengan términos en común. Supongamos por contradicción que $\lfloor m\alpha \rfloor = \lfloor n\beta \rfloor$. Esto quiere decir, que existe un entero (positivo) k tal que $k \leq m\alpha, n\beta < k + 1$. Como α y β son irracionales, entonces tenemos desigualdad estricta $k < m\alpha, n\beta$. Esto implica que

$$\frac{k}{\alpha} < m < \frac{k+1}{\alpha}, \qquad \frac{k}{\beta} < n < \frac{k+1}{\beta}.$$

Sumando estas dos desigualdades y usando la condición del problema obtenemos que $k < m+n < k+1$, lo cual no es posible porque $m+n$ es entero. Así concluimos entonces que todo entero positivo aparece a lo sumo una vez en la unión de las dos sucesiones.

Ahora demostramos que todo entero positivo pertenece a alguna de las sucesiones, y lo haremos, de nuevo, razonando por contradicción. Supongamos que el resultado es falso, es decir, existe un entero positivo k y enteros positivos m,n tales que

$$m\alpha, n\beta < k < k+1 < (m+1)\alpha, (n+1)\beta.$$

Procediendo como en la demostración anterior, tenemos que

$$m < \frac{k}{\alpha} < \frac{k+1}{\alpha} < m+1, \quad n < \frac{k}{\beta} < \frac{k+1}{\beta} < n+1.$$

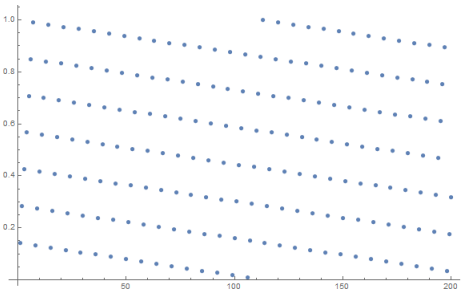
Sumando las desigualdades obtenemos que $m+n < k < k+1 < m+n+2$, lo cual no es posible, y así concluimos el resultado. □

2.3 Tópicos avanzados: los teoremas de Kronecker y Weyl

En la misma línea de las sucesiones aritméticas del teorema de Beatty, consideramos ahora la parte fraccionaria de una sucesión aritmética $\{\{\alpha\}, \{2\alpha\}, \{3\alpha\}, \ldots\}$. Esta sucesión no es interesante si α es racional, pues la sucesión es periódica. En efecto, si $\alpha = p/q$, entonces $\{(n+q)\alpha\} = \{n\alpha\}$, es decir, la sucesión tiene periodo q. La situación es más interesante cuando α es irracional.

Ejercicio 11. *Demuestre que si α es irracional, entonces $\{m\alpha\} \neq \{n\alpha\}$ para cualesquiera enteros distintos m, n.*

Ejemplo 2. *En el siguiente gráfico, se muestran los primeros 200 términos de la sucesión $\{\{\pi\}, \{2\pi\}, \{3\pi\}, \ldots\}$:*



Podemos notar en el ejemplo que los valores parecen distribuirse a lo largo de todo el intervalo $[0,1]$, es decir, no queda ningún "espacio vacío". Este resultado fue demostrado por Leopold Kronecker en 1884.

Teorema 2.2 (Teorema de densidad de Kronecker)**.** *Si α es irracional, entonces cualquier intervalo abierto de $[0,1]$ contiene términos de la sucesión $\{\{\alpha\}, \{2\alpha\}, \{3\alpha\}, \ldots\}$. Es decir, la sucesión es densa en el intervalo.*

Analizando con más cuidado el ejemplo de arriba, podríamos ver que 99 de los términos de la sucesión pertenecen a $[0, 1/2]$ y 101 términos a $[1/2, 1]$, es decir, la cantidad es casi proporcional a la longitud del intervalo. Este es un caso particular de lo observado por Hermann Weyl en 1909.

Teorema 2.3 (Teorema de equidistribución de Weyl)**.** *Si α es irracional y $(a,b) \subseteq [0,1]$, entonces la probabilidad de que los términos de la sucesión pertenezcan al intervalo (a,b) es $b-a$, es decir,*

$$\lim_{N\to+\infty} \frac{|\{\{n\alpha\} : 1 \leq n \leq N\} \cap (a,b)|}{N} = b - a.$$

En este caso decimos que la sucesión está equidistribuida en el intervalo.

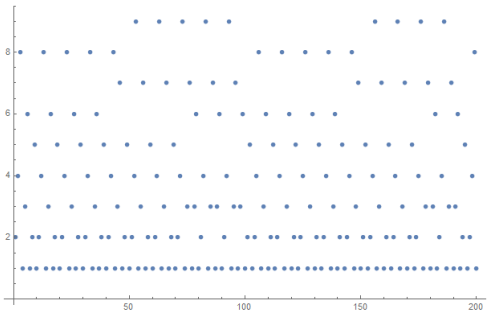
2.3.1 Ley de Benford

La ley de Benford es una observación empírica sobre la frecuencia con que aparecen los primeros dígitos en muchos conjuntos de datos de la vida cotidiana; para leer un poco más sobre la historia del origen de estas observaciones (primero con las tablas logarítmicas de Newcomb y posteriormente con las de Benford) puede ver [2]. En lo que resta, vamos a demostrar (rigurosamente) un caso particular de este fenómeno con la ayuda de los resultados presentados anteriormente.

Ejemplo 3. *Consideramos el conjunto de potencias de* 2 *y observamos sus primeros dígitos:*

n	1	2	3	4	5	6	7	8	9	10	11	12	13	...
2^n	1	2	4	16	32	64	128	256	512	1024	2048	4096	8192	...
primer dígito	1	2	4	1	3	6	1	2	5	1	2	4	8	...

Es curioso notar que el dígito 1 *es el que aparece con mayor frecuencia (*4 *de* 13 *veces). Con ayuda de una computadora podemos ver que para las primeras 200 potencias la distribución se ve así*



y la frecuencia es

Primer dígito	1	2	3	4	5	6	7	8	9
Frecuencia	60	36	24	20	16	13	11	11	9
Porcentaje	30%	18%	12%	10%	8%	6,5%	5,5%	5,5%	4,5%

Varios aspectos llaman la atención, entre ellos que el 1 *sigue siendo apareciendo con mayor frecuencia y también que las demás frecuencias son decrecientes.*

En general, podemos considerar la sucesión $\{a^n\}$, donde $a \geq 1$ es cualquier número real. Podemos escribir $a^n = 10^{n \log_{10} a}$, de manera que (1) implica que

$$10^{\lfloor n \log_{10} a \rfloor} \leq a^n < 10^{\lfloor n \log_{10} a \rfloor + 1},$$

de donde obtenemos que

$$1 \leq \frac{a^n}{10^{\lfloor n \log_{10} a \rfloor}} < 10.$$

Ahora bien, podemos reescribir

$$\frac{a^n}{10^{\lfloor n \log_{10} a \rfloor}} = \frac{10^{n \log_{10} a}}{10^{\lfloor n \log_{10} a \rfloor}} = 10^{n \log_{10} a - \lfloor n \log_{10} a \rfloor} = 10^{\{n \log_{10} a\}},$$

por lo que el primer dígito de a^n es igual a $\lfloor 10^{\{n \log_{10} a\}} \rfloor$. Ahora, el primer dígito de a^n es igual a d si y sólo si $\{n \log_{10} a\}$ pertenece al intervalo $[\log_{10} d, \log_{10}(d+1))$. El teorema de equidistribución de Weyl, Teorema 2.3, nos dice precisamente que la probabilidad de que esto suceda, en caso de que $\log_{10} a$ sea irracional [2] , es igual a

$$\log_{10}(d+1) - \log_{10} d = \log_{10}\left(\frac{d+1}{d}\right) = \log_{10}\left(1 + \frac{1}{d}\right).$$

[2]Por ejemplo, $\log_{10} a$ es irracional para cualquier entero positivo a que no sea una potencia de 10.

En la siguiente tabla mostramos las probabilidades calculadas y vemos como el ejemplo de arriba asemeja este comportamiento,

d	1	2	3	4	5	6	7	8	9
$\log_{10}(1+1/d)$	$0,3010$	$0,1761$	$0,1249$	$0,0969$	$0,0792$	$0,0669$	$0,580$	$0,0511$	$0,0458$
Porcentaje	$30,10\%$	$17,61\%$	$12,49\%$	$9,69\%$	$7,92\%$	$6,69\%$	$5,80\%$	$5,12\%$	$4,58\%$

3 Cantidad de divisores

Estudiamos ahora la cantidad de divisores $d(n)$ de un entero positivo n. Por ejemplo, para cualquier número primo p tenemos que $d(p) = 2$. Vemos que esta cantidad no depende de cuál primo sea, sino del hecho de que el número sea primo. Esto nos lleva a considerar la **factorización prima** de un número entero: si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, entonces cualquier divisor de n toma la forma $d = p_1^{\beta_1} \dots p_k^{\beta_k}$, con $0 \leq \beta_i \leq \alpha_i$. Para cada α_i obtenemos un total de $\alpha_i + 1$ posibles valores para β_i, de manera que la cantidad total de divisores de n está dada por

$$\boxed{d(n) = (\alpha_1 + 1) \dots (\alpha_k + 1).}$$

En comparación con la función exponencial p^α, la función lineal $\alpha + 1$ crece mucho más lento, por lo que $d(n)$ es una función mucho más lenta que n.

4 Suma de divisores

Dado un entero positivo n, denotamos por $\sigma(n)$ la suma de los divisores (positivos) de n. Empezamos calculando unos cuantos ejemplos:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	...
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28	14	24	...

Ejercicio 12. *Para p primo y k entero positivo, calcule $\sigma(p^k)$.*

4.1 Propiedad multiplicativa

Observamos que σ parece ser una función **multiplicativa**: esto quiere decir que $\sigma(m)\sigma(n) = \sigma(mn)$ cuando m y n son coprimos (es decir, que no comparten divisores comunes mayores a 1). Por ejemplo, $\sigma(12) = 28 = 4 \cdot 7 = \sigma(3)\sigma(4)$.

Comentario. *No es cierto que $\sigma(m)\sigma(n) = \sigma(mn)$ para todo m y n. Por ejemplo, $\sigma(2)\sigma(2) \neq \sigma(4)$.*

Parece un poco tautológico, pero es importante recalcar la siguiente propiedad de las funciones multiplicativas: para calcular el valor de la función en $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, es suficiente calcular la función en cada $p_i^{\alpha_i}$ y multiplicar los resultados. Por ejemplo, para calcular $\sigma(12)$ es suficiente factorizar $12 = 2^2 \cdot 3$ y así,

$$\sigma(12) = \sigma(2^2)\sigma(3) = \sigma(4)\sigma(3) = 7 \cdot 4 = 28.$$

Para demostrar que σ es multiplicativa, empezamos por analizar las expresiones

$$\sigma(m)\sigma(n) = \left(\sum_{a|m} a\right)\left(\sum_{b|n} b\right) = \sum_{a|m, b|n} ab, \qquad \sigma(mn) = \sum_{d|mn} d,$$

donde la expresión $\sum_{d|n} f(d)$ denota la suma de los valores $f(d)$ sobre todos los divisores d de n. Claramente, si $a|m$ y $b|n$, entonces $ab|mn$; es decir, todo término en la expansión de $\sigma(m)\sigma(n)$ aparece en la expansión de $\sigma(mn)$. En particular, esto implica que $\sigma(m)\sigma(n) \geq \sigma(mn)$ para cualesquiera m, n.

Sin embargo, no es siempre cierto es que todo término en la expansión de $\sigma(mn)$ proviene de un único término en la expansión de $\sigma(m)\sigma(n)$. Si tal fuera el caso, entonces tendríamos la igualdad $\sigma(m)\sigma(n) = \sigma(mn)$. Como mencionamos arriba, esto parece ser el caso cuando m y n son coprimos. En el siguiente resultado demostramos esta biyección entre los términos de ambas expresiones.

Proposición 4.1. *Si $(m,n)=1$, entonces todo divisor d de mn se puede expresar de manera única como $d=ab$ con $a|m$ y $b|n$.*

Comentario. *Es en este punto donde es crucial que m y n sean coprimos, pues el resultado es falso cuando m y n no son coprimos. Por ejemplo, 2 es divisor de $4=2\cdot 2$ y se puede expresar como $1\cdot 2$ o $2\cdot 1$. Esta es la razón por la que $\sigma(4)\neq\sigma(2)\sigma(2)$, pues*

$$\sigma(2)\sigma(2)=(1+2)(1+2)=1\cdot 1+\mathbf{1\cdot 2}+\mathbf{2\cdot 1}+2\cdot 2=(1+2+4)+\mathbf{2}=\sigma(4)+\mathbf{2}.$$

Prueba. Sea d un divisor de mn. Tenemos que demostrar dos resultados: que se puede lograr la descomposición $d=ab$ y que esta descomposición es única.

Empecemos con la unicidad: supongamos que $d=a_1b_1=a_2b_2$ con $a_i|m$ y $b_i|n$. Como $a_1|m$, $b_2|n$ y $(m,n)=1$, entonces $(a_1,b_2)=1$. Además, como $a_1|a_2b_2$, pues $d=a_1b_1=a_2b_2$, entonces lo anterior implica que $a_1|a_2$. Similarmente, $a_2|a_1$, y así $a_1=a_2$; esto implica también que $b_1=b_2$, lo que demuestra la unicidad de la representación.

Demostramos ahora la existencia de la descomposición. Podemos tomar $a:=(d,m)$, de manera que $a|d$ y $a|m$. Definimos $b:=d/a$, de manera que $d=ab$. Entonces solo falta demostrar que $b|n$. Por definición, tenemos que $(b,m/a)=(d/a,m/a)=1$ y además $b=d/a$ divide a $mn/a=(m/a)n$ (pues $d|mn$). Como $(b,m/a)=1$, entonces concluimos que $b|n$, como queríamos probar. □

Como dijimos anteriormente, el resultado que acabamos de demostrar demuestra que σ es multiplicativa. Esto nos permite obtener una fórmula explícita para $\sigma(n)$: si $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$, entonces

$$\sigma(n)=\sigma(p_1^{\alpha_1})\dots\sigma(p_k^{\alpha_k})=(1+p_1+\ldots+p_1^{\alpha_1})\dots(1+p_k+\ldots+p_k^{\alpha_k})=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\ldots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1}.$$

Ejercicio 13. *Demuestre que si 2^n-1 es primo, entonces n es primo. En tal caso decimos que 2^n-1 es un **primo de Mersenne**. Encuentre algunos primos de Mersenne.*

Ejercicio 14. *Sea p un número primo y suponga que 2^p-1 es primo. Calcule $\sigma(2^{p-1}(2^p-1))$.*

4.2 Números perfectos

Decimos que un número es **perfecto** si la suma de los divisores (positivos) menores que el número es igual a sí mismo; es decir, $\sigma(n)=2n$. En Ejercicio 14 vimos que una forma de generar números perfectos es mediante los primos de Mersenne 2^p-1; esto había sido notado por Euclides desde el siglo IV a.C. Algunos ejemplos de números perfectos son

$$6=2(2^2-1)=1+2+3,\quad 28=2^2(2^3-1)=1+2+4+7+14,$$

$$496=2^4(2^5-1)=1+2+4+8+16+31+62+124+248.$$

A continuación aplicamos los resultados obtenidos en la sección anterior, para demostrar que los números perfectos pares corresponden a los descritos en Ejercicio 14.

Teorema 4.2 (Euclides-Euler)**.** *Si n es un número perfecto par, entonces $n=2^{p-1}(2^p-1)$, con 2^p-1 un primo de Mersenne.*

Prueba. Sea $n=2^km$, con m impar, de manera que $\sigma(n)=\sigma(2^k)\sigma(m)=(2^{k+1}-1)\sigma(m)$. Dado que $\sigma(n)=2n=2^{k+1}m$, lo anterior implica que $2^{k+1}-1$ divide a m y además

$$\sigma(m)=\frac{2^{k+1}m}{2^{k+1}-1}=m+\frac{m}{2^{k+1}-1}.$$

Dado que m y $m/(2^{k+1}-1)$ son divisores de m, esta igualdad implica que estos deben ser los únicos divisores de m, de donde concluimos que m es primo y $m=2^{k+1}-1$. Por Ejercicio 13 esto implica que $k+1=p$ es primo y 2^p-1 es un primo de Mersenne, como queríamos probar. □

Sorprendentemente, a la fecha sigue siendo un **problema abierto** si existen números perfectos impares.

5 Función φ de Euler

La función φ de Euler cuenta todos los enteros positivos menores o iguales que un entero que son coprimos con él. Por ejemplo,

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	...
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	...

Al igual que con la función de suma de divisores, $\sigma(n)$, observamos en los casos anteriores la propiedad **multiplicativa**; es decir, $\varphi(mn) = \varphi(m)\varphi(n)$ si m y n son coprimos. La demostración de este hecho no es completamente trivial y necesitaremos un poco de trabajo. Sin embargo, los siguientes ejercicios y secciones ayudan a motivar el desarrollo posterior que haremos.

Ejercicio 15. *Para p primo y k entero positivo, determine $\varphi(p^k)$.*

Ejercicio 16. *Para p, q son primos distintos, determine $\varphi(pq)$.*

Ejercicio 17. *Para p, q son primos distintos y k, l enteros positivos, determine $\varphi(p^k q^l)$.*

Ejercicio 18. *Demuestre que si n es impar, entonces $\varphi(2n) = \varphi(n)$.*

5.1 Identidad básica

Un primer ejemplo donde la función aparece de manera natural es la siguiente. Consideramos ahora las fracciones

$$\frac{1}{n},\ \frac{2}{n}, \ldots,\ \frac{n}{n}$$

y las simplificamos completamente. Las nuevas fracciones tienen denominadores d que dividen a n y los numeradores respectivos son coprimos con d. Como en todas estas fracciones los numeradores son positivos y menores iguales que los denominadores, entonces la cantidad de fracciones con denominador d es exactamente $\varphi(d)$. Contando la cantidad total de fracciones, es decir n, obtenemos el siguiente resultado.

Proposición 5.1. *Si n es un entero positivo, entonces*

$$\sum_{d|n} \varphi(d) = n.$$

Ejercicio 19. *Lleve a cabo explícitamente el proceso anterior. Es decir, escoja su entero positivo favorito n, escriba las fracciones como antes, simplifíquelas y observe el resultado.*

Ejercicio 20. *Use el resultado anterior para calcular de manera alternativa $\varphi(p^k)$, $\varphi(pq)$ y $\varphi(p^k q^l)$.*

5.2 Pares de coprimos y rectas por el origen

Otra situación en la que la función φ aparece es el siguiente problema:

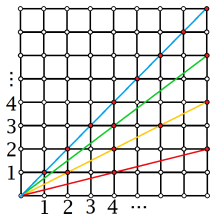
¿Cuál es la probabilidad de que dos enteros positivos sean coprimos?

El conjunto de pares de enteros positivos $\{(a, b) : a, b \in \mathbb{Z}^+\}$ es un conjunto infinito por lo que tratar con él puede ser un poco difícil si queremos hablar de probabilidades. Una manera de resolver esto, es aproximar el conjunto sucesivamente por los cuadrados de lados con N puntos $\{(a, b) : 1 \leq a, b \leq N\}$, estudiar el problema en este dominio y después hacer $N \to +\infty$. Es decir, hay que estudiar

$$\lim_{N \to +\infty} \frac{|\{(a, b) : 1 \leq a, b \leq N,\ a, b \text{ coprimos}\}|}{N^2}.$$

Este problema es equivalente a contar la cantidad de rectas distintas que hay entre puntos del conjunto $\{(a, b) : 1 \leq a, b \leq N\}$ y el origen. Esto se debe a que cada recta se puede poner en correspondencia

con un par de puntos coprimos (a, b); de hecho una pareja de enteros positivos (a, b) son coprimos si y sólo no hay otros puntos con coordenadas enteras en el segmento que une a (a, b) con el origen. Es decir, el punto con coordenadas coprimas es el "primer" punto con coordenadas enteras en esa recta.



Ejemplo 4. *Vemos que los pares* $(1,1)$, $(2,2)$, $(3,3)$, ... *pertenecen a la misma recta, pero solo* $(1,1)$ *es una pareja de enteros coprimos; es decir, esta recta la pondríamos en correspondencia con* $(1,1)$. *De igual forma, los pares* $(2,1)$, $(4,2)$, $(6,3)$, ... *pertenecen a la misma recta, pero solo* $(2,1)$ *son coprimos, por lo que identificaríamos esta recta con* $(2,1)$.

Como el problema es simétrico con respecto a a y b, y $a = b$ son coprimos si y sólo si $a = b = 1$, entonces podemos restringirnos al caso en que $1 \leq b < a \leq N$. Por lo tanto a puede variar entre 2 y N. Para cada uno de estos valores, si a y b son coprimos, entonces b puede tomar exactamente $\varphi(a)$ valores. Por lo tanto, la cantidad de puntos con $1 \leq b < a \leq N$ donde a y b son coprimos es igual a

$$\varphi(2) + \varphi(3) + \ldots + \varphi(N).$$

La cantidad total de pares en este caso es igual a $1 + 2 + \ldots + (N-1) = N(N-1)/2$, por lo que la probabilidad que buscamos es igual a

$$\lim_{N\to+\infty} \frac{\varphi(2) + \varphi(3) + \ldots + \varphi(N)}{N(N-1)/2} = 2 \lim_{N\to+\infty} \frac{\varphi(2) + \varphi(3) + \ldots + \varphi(N)}{N^2}.$$

Es curioso e interesante que este límite existe y es igual a $3/\pi^2$; es decir, que la probabilidad de que dos enteros positivos sean coprimos es igual a $6/\pi^2$, ver [3].

5.3 Fórmula explícita via principio de inclusión-exclusión

Retomamos los ejemplos de los ejercicios anteriores: calcular $\varphi(p^k)$ y $\varphi(p^k q^l)$. En el primer caso un número es coprimo con p^k si no es divisible entre p, pues p es el único factor primo. La cantidad de enteros positivos divisibles por p menores o iguales a p^k es igual a $p^k/p = p^{k-1}$, por lo que

$$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right).$$

De igual forma, los enteros positivos que son coprimos con $p^k q^l$ no pueden tener divisores en común con p ni con q. De nuevo, excluyendo los múltiplos de p y de q podríamos pensar que la cantidad de coprimos con $p^k q^l$ sería igual a

$$p^k q^l - \frac{p^k q^l}{p} - \frac{p^k q^l}{q}.$$

Sin embargo, hay enteros que estamos excluyendo **dos veces**, una cuando es un múltiplo de p y otra cuando es un múltiplo de q. Esto es el caso de los múltiplos de pq. Estos elementos hay que reincorporarlos a la cuenta, de manera que

$$\varphi(p^k q^l) = p^k q^l - \frac{p^k q^l}{p} - \frac{p^k q^l}{q} + \frac{p^k q^l}{pq} = p^k q^l\left(1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}\right) = p^k q^l\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right).$$

Ejercicio 21. *Demuestre el siguiente resultado que usamos en el argumento anterior: si* A_1 *y* A_2 *son conjuntos finitos, entonces*

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|,$$

donde $A_1 \cup A_2$ *y* $A_1 \cap A_2$ *son la unión e intersección, respectivamente, de los conjuntos* A_1 *y* A_2, *y* $|A|$ *denota la cantidad de elementos del conjunto* A.

Ejercicio 22. *Use el resultado anterior para demostrar que si A_1, A_2, A_3 son conjuntos finitos, entonces que*

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

El siguiente resultado básico de conteo es una formulación más general de la esencia capturada en los dos ejercicios anteriores.

Proposición 5.2 (Principio de inclusión-exclusión)**.** *Sean $A_1, A_2, \ldots, A_n$ conjuntos con un número finito de elementos. Para todo subconjunto no vacío $S \subseteq \{1, 2, \ldots, n\}$, denotamos por A_S a la intersección de los A_i con $i \in S$. Entonces*

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{\substack{S \subseteq \{1,\ldots,n\} \\ S \neq \emptyset}} (-1)^{|S|-1} |A_S|.$$

Comentario. *La notación usada en el enunciado puede parecer intimidante, pero no lo es. Por ejemplo, si tenemos A_1, A_2, A_3, entonces los subconjuntos no vacíos de $\{1, 2, 3\}$ son*

$$\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\},$$

y así los subconjuntos A_S, con $S \subseteq \{1, 2, 3\}$, $S \neq \emptyset$, son

$$A_{\{1\}} = A_1, \quad A_{\{2\}} = A_2, \quad A_{\{3\}} = A_3, \quad A_{\{1,2\}} = A_1 \cap A_2, \quad A_{\{1,3\}} = A_1 \cap A_3, \quad A_{\{2,3\}} = A_2 \cap A_3,$$

$$A_{\{1,2,3\}} = A_1 \cap A_2 \cap A_3.$$

Por lo tanto, la suma en el principio de inclusión-exclusión es igual a

$$\begin{aligned}(-1)^{1-1}(A_{\{1\}} + A_{\{2\}} + A_{\{3\}}) + (-1)^{2-1}(A_{\{1,2\}} + A_{\{1,3\}} + A_{\{2,3\}}) + (-1)^{3-1} A_{\{1,2,3\}} \\ = (|A_1| + |A_2| + |A_3|) - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + |A_1 \cap A_2 \cap A_3|.\end{aligned}$$

Esta expresión coincide justamente con la de ejercicio Ejercicio 22.

Ya estamos en posición de poder determinar explícitamente la fórmula para $\varphi(n)$. Considere la factorización prima $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Los números menores o iguales que n que **no** son coprimos con n tienen que ser divisibles por alguno de los primos p_j. Sea A_j el conjunto de enteros positivos menores o iguales que n divisible por p_j. Entonces tenemos que

$$\varphi(n) = n - |A_1 \cup A_2 \cup \ldots \cup A_k|.$$

Usamos Proposición 5.2 para escribir

$$\varphi(n) = n - \sum_{\substack{S \subseteq \{1,\ldots,k\} \\ S \neq \emptyset}} (-1)^{|S|-1} |A_S|.$$

Ahora, A_S contiene todos los enteros que son divisibles por p_j para todo $j \in S$. Por lo tanto, la cantidad de elementos en A_S es igual a n dividido entre el producto de estos primos, es decir,

$$|A_S| = \frac{n}{\prod_{j \in S} p_j} = n \prod_{j \in S} \frac{1}{p_j}.$$

De esta manera, obtenemos que

$$\varphi(n) = n\left(1 - \sum_{\substack{S \subseteq \{1,\ldots,k\} \\ S \neq \emptyset}} (-1)^{|S|-1} \prod_{j \in S} \frac{1}{p_j}\right).$$

Finalmente, observamos que

$$1 - \sum_{\substack{S\subseteq\{1,\ldots,k\}\\ S\neq\emptyset}} (-1)^{|S|-1} \prod_{j\in S} \frac{1}{p_j} = 1 + \sum_{\substack{S\subseteq\{1,\ldots,k\}\\ S\neq\emptyset}} \prod_{j\in S} \left(\frac{-1}{p_j}\right) = \left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_k}\right),$$

con lo que concluimos que

$$\boxed{\varphi(n) = n\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_k}\right).}$$

En particular, esto implica la propiedad multiplicativa que observamos al inicio de la discusión.

5.4 Propiedad multiplicativa via congruencias

En esta sección vamos a dar una demostración alternativa de la fórmula para $\varphi(n)$, demostrando primero la propiedad multiplicativa.

5.4.1 Congruencias

5.4.2 Teorema chino del residuo

5.4.3 Residuos invertibles

5.5 Teorema de Euler-Fermat

5.6 Problemas abiertos

Lehmer y Carmichael.

6 Fórmula de inversión de Möbius

Comentario.

$$d(n) = \sum_{d|n} 1.$$

7 Problemas

Puede consultar la sección 5.2 de [5] o el documento [6] (especialmente capítulos 10 y 12) para más problemas.

Problema 1. *Demuestre que si $n \geq 6$ es compuesto, entonces n divide a $(n-1)!$.*

Problema 2. *Halle todos los enteros positivos n, tales que $\lfloor\sqrt{n}\rfloor$ divide a n.*

Problema 3. *Determine todos los enteros positivos n para los que 2^{n-1} divide a $n!$.*

Problema 4. *Encuentre una función $f(n)$ tal que el n-ésimo término de la sucesión*

$$1,\ 2,\ 2,\ 3,\ 3,\ 3,\ 4,\ 4,\ 4,\ 4,\ldots$$

sea igual a $\lfloor f(n)\rfloor$.

Problema 5. *Demuestre el converso del teorema de Beatty: si todo entero positivo pertenece exactamente a una de las sucesiones $\{\lfloor\alpha\rfloor, \lfloor 2\alpha\rfloor, \lfloor 3\alpha\rfloor, \ldots\}$ y $\{\lfloor\beta\rfloor, \lfloor 2\beta\rfloor, \lfloor 3\beta\rfloor, \ldots\}$, entonces α y β son irracionales positivos tales que $1/\alpha + 1/\beta = 1$.*

Problema 6. *Sea $\alpha \geq 1$ un número real tal que $\log_{10}\alpha$ no es racional. Sean $d_1, d_2, \ldots, d_n$ dígitos, $d_1 \neq 0$, y considere el número de n dígitos $d = \overline{d_1 d_2 \ldots d_n}$. Demuestre que la probabilidad de que los primeros dígitos de un número en la sucesión de potencias $\{\alpha, \alpha^2, \alpha^3, \ldots\}$ sea igual al número d es igual a $\log_{10}(1 + 1/d)$.*

Problema 7 (Irlanda 1998)**.** *Halle todos los enteros positivos n con exactamente 16 divisores positivos, $1 = d_1 < d_2 < \ldots < d_{16} = n$, tales que $d_6 = 18$ y $d_9 - d_8 = 17$.*

Problema 8 (Singapur 1997)**.** *Determine todos los enteros positivos n con exactamente 6 divisores positivos, $1 < d_2 < d_3 < d_4 < d_5 < n$, tales que $n + 1 = 5(d_2 + d_3 + d_4 + d_5)$.*

Problema 9. *Suponga que $n > 6$ es un número perfecto y sea $p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ su factorización prima, con $p_1 < \ldots < p_k$. Demuestre que α_1 es par.*

Problema 10. *Demuestre que*

$$\sum_{k=1}^{n} \sigma(k) = \frac{1}{2} \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \left(\left\lfloor \frac{n}{k} \right\rfloor + 1 \right).$$

Problema 11. *Demuestre que en un conjunto de 10 enteros positivos consecutivos, hay al menos uno de ellos que es coprimo con todos los demás.*

Problema 12. *Demuestre que si $a|b$, entonces $\varphi(a)|\varphi(b)$.*

Problema 13. *Sean m, n enteros positivos y sea $d = (m, n)$. Demuestre que*

$$\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}.$$

Problema 14. *Demuestre que si a, n son enteros positivos, entonces $\varphi(a^n) = a^{n-1}\varphi(a)$.*

Problema 15. *Encuentre todos los enteros positivos n tales que $\varphi(n) = d(n)$.*

Problema 16. *Encuentre todos los enteros positivos n tales que $\varphi(n)$ divide a n.*

Problema 17. *Este problema descarta unos casos particulares en la conjetura de Lehmer. Demuestre que si $\varphi(n)$ divide a $n-1$, entonces n no puede tener exactamente dos o tres divisores primos distintos.*

Problema 18. *Demuestre que si $n > 1$, entonces*

$$\sum_{\substack{1 \leq d \leq n \\ (d,n)=1}} d = \frac{n\varphi(n)}{2}$$

Problema 19. *Demuestre que $\varphi(n)d(n) \geq n$ para todo entero positivo n.*

Problema 20. *Demuestre que $\varphi(n) \geq \sqrt{n}$ para $n > 6$.*

Problema 21 (D. Campos)**.** *Para un entero positivo n, sea $s(n)$ la suma de los dígitos de n (en base 10). Demuestre que la cantidad de enteros positivos que satisface la ecuación $\varphi(n) = [s(n)]^3$ es finita. (El número 2008 satisface $\varphi(2008) = 1000 = 10^3 = [s(2008)]^3$.)*

Problema 22 (OMCC 2006)**.** *Para cada número natural n, se define $f(n) = \lfloor n + \sqrt{n} + 1/2 \rfloor$. Pruebe que para cada $k \geq 1$, la ecuación*

$$f(f(n)) - f(n) = k$$

tiene exactamente $2k - 1$ soluciones.

Problema 23 (IMOLL 1985)**.** *Halle el menor entero positivo n tal que n tiene 144 divisores positivos y existen diez enteros positivos consecutivos que dividen a n.*

Problema 24 (IMOLL 1986). *Determine cuatro enteros positivos, tales que sean menores o iguales a* 70000 *y cada uno tenga más de* 100 *divisores.*

Problema 25 (IMOLL 1987). *Determine el menor entero positivo n tal que $n!$ termina exactamente en* 1987 *ceros.*

Problema 26 (IMOSL 2000). *Para un entero positivo n, sea $d(n)$ el número de divisores positivos de n. Hallar todos los enteros positivos n tales que $d^3(n) = 4n$.*

Problema 27 (IMOSL 2001). *Demuestre que no existe un entero positivo n, tal que para todo $k = 1, 2, \ldots, 9$, el primer dígito de $(n+k)!$ sea k.*

Problema 28 (IMOSL 2002). *Sean $p_1, p_2, \ldots, p_n$ primos distintos mayores a* 3. *Demuestre que $2^{p_1 p_2 \cdots p_n} + 1$ tiene por lo menos 4^n divisores.*

Problema 29 (G. Chicas, IMO 2019). *Encuentre todos los pares (k, n) de enteros positivos tales que*

$$k! = (2^n - 1)(2^n - 2)(2^n - 4) \ldots (2^n - 2^{n-1}).$$

Problema 30 (Putnam 1995). *Para cada real positivo α, defina el conjunto*

$$S(\alpha) := \{\lfloor \alpha \rfloor, \lfloor 2\alpha \rfloor, \lfloor 3\alpha \rfloor, \ldots\}.$$

Demuestre que no existen tres reales α, β, γ, tales que $\mathbb{Z}^+$ se puede expresar como una unión disjunta de $S(\alpha)$, $S(\beta)$ y $S(\gamma)$.

References

[1] J. Voight, *Perfect numbers: an elementary introduction*, `math.dartmouth.edu/~jvoight/notes/perfelem.pdf`.

[2] Colaboradores de Wikipedia, *Ley de Benford*, `es.wikipedia.org/wiki/Ley_de_Benford`.

[3] Colaboradores de Wikipedia, *Coprime integers*, `en.wikipedia.org/wiki/Coprime_integers`.

[4] Colaboradores de Wikipedia, *Euler's totient function*, `en.wikipedia.org/wiki/Euler%27s_totient_function`.

[5] F.E. Brochero, C.G. Moreira, N.C. Saldanha, E. Tengan, *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*, `livrariavirtual.impa.br`.

[6] P. Vandendriessche, H. Lee, *Problems in Elementary Number Theory*, `dropbox.com/s/s6a4594y773bbq0/20120716PEN.pdf`.