Capítulo 2

Funciones aritméticas

En el capítulo anterior hemos podido apreciar algunos aspectos de la Teoría de los Números y el tipo de problemas que pretende resolver. No debe extrañar que las funciones definidas sobre los naturales tengan una importancia capital. Estas funciones, reales o complejas, son las funciones aritméticas.

2.0.1. Propiedades generales

Dentro de todas las funciones aritméticas hay unas que merecen especial atención porque engloban a una gran parte de las funciones aritméticas más interesantes: son las funciones multiplicativas.

Definicion 2.0.1. *Diremos que una función aritmética f es multiplicativa si $f(nm) = f(n)f(m)$ para cualesquiera enteros positivos n, m con $(n, m) = 1$.*

Definicion 2.0.2. *Diremos que una función aritmética f es completamente multiplicativa si $f(nm) = f(n)f(m)$ para cualesquiera enteros positivos n, m.*

Observemos que si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ y f es una función multiplicativa entonces

$$f(n) = \prod_i f(p_i^{\alpha_i}).$$

Proposición 2.0.3. *Si $f(n)$ es una función multiplicativa entonces $g(n) = \sum_{d|n} f(d)$ también lo es.*

Demostración. Observemos que si $(m, n) = 1$, todo divisor d de mn ha de ser de la forma $d = d_1 d_2$ donde d_1 y d_2 han de ser divisores de m y n respectivamente. De igual manera, cada pareja de divisores de m y n nos da un divisor de mn. Entonces tenemos

$$\begin{aligned} g(mn) &= \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) \\ &= \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) = g(m) g(n). \end{aligned}$$

□

Ahora centraremos nuestra atención sobre las funciones aritméticas más interesantes, empezando con la función divisor.

2.0.2. La función divisor

La función divisor $\tau(n)$ se define como el número de divisores de n:

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

Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, los divisores de n son de la forma $d = p_1^{\beta_1} \cdots p_r^{\beta_r},\ 0 \leq \beta_i \leq \alpha_i,\ i = 1, \ldots, r$.

Proposición 2.0.4. *La función $\tau(n)$ es multiplicativa y si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ entonces $\tau(n) = \prod_i (1 + \alpha_i)$.*

Demostración. La proposición 2.0.3 implica, trivialmente, que la función divisor es multipicativa. Debido a eso se tiene que $\tau(n) = \prod_i \tau(p_i^{\alpha_i}) = \prod_i (1 + \alpha_i)$. □

2.0.3. La función σ, los números perfectos y los primos de Mersenne

La función σ se define de la forma

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

Como la función $f(n) = n$ es multiplicativa, el siguiente resultado se sigue también de la proposición 2.0.3.

Proposición 2.0.5. *La función σ es multiplicativa y si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, entonces*

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Demostración. De nuevo la Proposición 2.0.3 implica que σ es una función multiplicativa. Es por tanto suficiete demostrar que $\sigma(p_i^{\alpha_i}) = \frac{p_1^{\alpha_i+1}-1}{p_i-1}$.

$$\sigma(p_i^{\alpha_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

□

Con la función σ está relacionado el clásico problema de los números perfectos.

Decimos que un entero positivo n es perfecto si la suma de sus divisores menores que n coincide con n. Es decir, si $\sigma(n) = 2n$. El primer número perfecto es el 6 cuyos divisores son $1, 2, 3$ y 6. El siguiente es $28 = 1 + 2 + 4 + 7 + 14$.

El siguiente teorema caracteriza los números pares perfectos.

Teorema 2.0.6. *Un número par es perfecto si y sólo si $n = 2^{m-1}(2^m - 1)$ con $2^m - 1$ primo.*

Demostración. Si $2^m - 1$ es primo entonces $\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1) = (2^m - 1)2^m = 2n$ y n es un número perfecto.

Por otro lado, si n es par, n se puede escribir de la forma $n = 2^{m-1}s$ con s impar y $m \geq 2$. Por ser n un número perfecto tenemos que

$$2^m s = 2n = \sigma(n) = \sigma(2^{m-1})\sigma(s) = (2^m - 1)\sigma(s).$$

Entonces $\sigma(s) = s + \frac{s}{2^m-1}$. Como $\sigma(s)$ es un entero, $2^m - 1$ tiene que ser un divisor de s y por lo tanto $\frac{s}{2^m-1}$ también.

Ya que $\sigma(s)$ es la suma de todos los divisores de s, entonces s y $\frac{s}{2^m-1}$ han de ser los únicos divisores de s. Es decir $\frac{s}{2^m-1} = 1$ y además s tiene que ser primo. □

Aunque en este teorema han quedado perfectamente caracterizados los números perfectos pares, es un problema abierto responder a la pregunta de si existen infinitos números pares perfectos, que es lo mismo que responder sobre la existencia de infinitos primos de la forma $2^m - 1$, los llamados primos de Mersenne.

También se desconoce la existencia de números perfectos impares. No se ha encontrado ninguno pero no se ha demostrado que no existan.

2.0.4. La función de Moebius

Una de las funciones aritméticas más importantes en la teoría analítica de los números es la función de Moebius. Aunque la primera definición de la función pueda resultar algo articial en un principio, aparece de manera natural cuando, por ejemplo, se trata de contar el número de primos menores que una cantidad dada. Esto lo veremos posteriormente.

La función de Moebius $\mu(n)$ se define de la siguiente manera:

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n \text{ es el producto de } k \text{ primos distintos} \\ 0 & \text{si } n \text{ tiene algún divisor cuadrado mayor que 1.} \end{cases}$$

Proposición 2.0.7. *La función $\mu(n)$ es multiplicativa.*

Demostración. Si $(m, n) = 1$ entonces $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ y $n = q_1^{\beta_1} \cdots q_s^{\beta_s}$ con los p_i distintos de los q_j.

Si alguno de los α_i o de los β_j es mayor que 1, entonces m o n tienen algún divisor cuadrado que también lo será de mn. En este caso $\mu(mn) = \mu(m)\mu(n) = 0$.

Si $\alpha_1 = \cdots = \alpha_r = \beta_1 = \cdots = \beta_s = 1$ entonces $\mu(m) = \mu(p_1 \cdots p_r) = (-1)^r$, $\mu(n) = \mu(q_1 \cdots q_s) = (-1)^s$ y $\mu(p_1 \cdots p_r q_1 \cdots q_s) = (-1)^{r+s}$. □

Proposición 2.0.8.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & si\ n = 1 \\ 0, & si\ n > 1 \end{cases} .$$

Demostración. Al ser $\mu(n)$ multiplicativa, la función $g(n) = \sum_{d|n} \mu(d)$ también lo es. En ese caso, si $n = \prod_i q_i^{\alpha_i}$ entonces $g(n) = \prod_i g(q_i^{\alpha_i})$. Pero si q_i es primo, $g(q_i^{\alpha_i}) = \sum_{d|q_i^{\alpha_i}} \mu(d) = \mu(1) + \mu(q_i) + \mu(q_i^2) + \cdots + \mu(q_i^{\alpha_i}) = 1 - 1 + 0 + \cdots + 0 = 0$. □

Proposición 2.0.9. *i) Sea $f : \mathbb{Z}^+ \to \mathbb{C}$ y definamos $F : \mathbb{Z}^+ \to \mathbb{C}$ de la forma*

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

Entonces

$$f(n) = \sum_{d|n} \mu(d) F(n/d).$$

ii) Sea $f : \mathbb{R}^+ \to \mathbb{C}$ y definamos $F : \mathbb{R}^+ \to \mathbb{C}$ de la forma

$$F(x) = \sum_{n \leq x} f(x/n).$$

Entonces
$$f(x) = \sum_{n\leq x} \mu(n)F(x/n).$$

Demostración. i)
$$\begin{aligned} f(n) &= \sum_{c|n} \left(\sum_{d|(n/c)} \mu(d) \right) f(c) = \sum_{\substack{c,d \\ cd|n}} \mu(d) f(c) \\ &= \sum_{d|n} \mu(d) \sum_{c|(n/d)} f(c) = \sum_{d|n} \mu(d) F(n/d). \end{aligned}$$

ii)
$$\begin{aligned} f(x) &= \sum_{n\leq x} \left(\sum_{k|n} \mu(k) \right) f(x/n) = \sum_{\substack{k,l \\ kl\leq x}} \mu(k) f(x/(kl)) \\ &= \sum_{k\leq x} \mu(k) \left(\sum_{l\leq x/k} f(x/(lk)) \right) = \sum_{k|x} \mu(k) F(x/k). \end{aligned}$$

□

2.0.5. La función de Euler

La función $\phi(n)$ se define como el número de enteros positivos primos con n y menores o iguales que n.

Proposición 2.0.10. *La función $\phi(n)$ es multiplicativa.*

Demostración. Por la proposición 2.0.8, la función $\phi(n)$ también se puede escribir como
$$\phi(n) = \sum_{k\leq n} \sum_{d|(k,n)} \mu(d).$$

Reordenando las sumas tenemos
$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}.$$

La demostración se termina con la observación de que al ser $\mu(d)$ multiplicativa, también lo es $\frac{\mu(d)}{d}$. Entonces la función $\frac{\phi(n)}{n}$, y por tanto la función $\phi(n)$, es multiplicativa. □

Corolario 2.0.11.

$$\phi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

Demostración. Solamente hay que observar que $\frac{\phi(n)}{n}$ es multiplicativa y que $\frac{\phi(p^\alpha)}{p^\alpha} = \frac{p^\alpha - p^{\alpha-1}}{p^\alpha} = 1-\frac{1}{p}$. □

Proposición 2.0.12.

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

Demostración. La función $g(n) = \sum_{d|n}\phi(d)$ es multiplicativa. Por lo tanto sólo hay que demostrar que $g(p^m) = p^m$ para todo primo p y para todo entero positivo m, Esto es,

$$\begin{aligned} g(p^m) = \sum_{d|p^m}\phi(d) &= \phi(1)+\phi(p)+\phi(p^2)+\cdots+\phi(p^m) = \\ &= 1+(p-1)+(p^2-p)+\cdots+(p^m-p^{m-1}) = p^m. \end{aligned}$$

□

2.0.6. El número de divisores primos de un entero

Dado un entero positivo n se define $\omega(n)$ como el número de divisores primos distintos de n y $\Omega(n)$ como el número de divisores primos de n contando la multiplicidad. Más formalmente, si $n = q_1^{\alpha_1}\cdots q_k^{\alpha_k}$, donde los q_i son primos distintos, se define $\omega(n) = k$ y $\Omega(n) = \alpha_1+\cdots+\alpha_k$. Algunas veces es conveniente utilizar las siguientes expresiones alternativas:

$$\omega(n) = \sum_{p|n}1, \qquad \Omega(n) = \sum_{p^m|n}1.$$

Proposición 2.0.13. *Existen constantes positivas c_1, c_2 tales que para todo $n \geq 3$ se tiene que*

i) $\Omega(n) \leq c_1 \log n$

ii) $\omega(n) \leq c_2 \log n/(\log\log n)$.

Demostración. Si $n = q_1^{\alpha_1}\cdots q_k^{\alpha_k}$ es claro que $n \geq 2^{\alpha_1+\cdots+\alpha_k} = 2^{\Omega(n)}$. Tomando logaritmos se obtiene i).

La parte ii) se pide en el ejercicio 2.2.23 □

2.1. Promedio de funciones aritméticas

En general, las funciones aritméticas se comportan de un modo bastante irregular. Los valores $\tau(n)$, $\phi(n)$, $\mu(n)$ no dependen tanto de la magnitud de n como de su factorización en números primos.

Tiene por tanto mayor sentido preguntarse por el comportamiento de dichas funciones en media. Veremos por ejemplo que

$$D(x) = \sum_{n \le x} \tau(n) \sim x \log x$$

y que

$$\Phi(x) = \sum_{n \le x} \phi(n) \sim \frac{\pi^2}{6} x^2.$$

El siguiente teorema va a ser una herramienta importante para estimar sumas por medio de integrales.

Teorema 2.1.1 (Identidad de Abel)**.** *Para toda función aritmética $a(n)$, sea $A(x) = \sum_{n \le x} a(n)$ y sea f una función con derivada continua en $[1, \infty)$. Entonces tenemos*

$$\sum_{n \le x} a(n) f(n) = A(x) f(x) - \int_1^x A(t) f'(t) dt.$$

Demostración. Utilizaremos el hecho de que $a(n) = A(n) - A(n-1)$ y que $f(n) - f(n-1) = \int_{n-1}^n f'(t) dt$. Definimos también $a(0) = 0$ y $k = \lfloor x \rfloor$.

$$\begin{aligned}
\sum_{1 \le n \le k} a(n) f(n) &= \sum_{1 \le n \le k} \left(A(n) - A(n-1) \right) f(n) \\
&= \sum_{1 \le n \le k} A(n) f(n) - \sum_{0 \le n \le k-1} A(n) f(n+1) \\
&= \sum_{1 \le n \le k-1} A(n) \left(f(n) - f(n-1) \right) + A(k) f(k) \\
&= -\sum_{1 \le n \le k-1} A(n) \int_n^{n+1} f'(t) dt + A(k) f(k) \\
&= -\int_1^k A(t) f'(t) dt + A(x) f(x) - \int_k^x A(t) f'(t) dt \\
&= A(x) f(x) - \int_1^x A(t) f'(t) dt.
\end{aligned}$$

□

En los cálculos posteriores nos va a interesar el orden de magnitud de algunas funciones más que su valor exacto. Para ello introducimos la siguiente notación:

Notación:

a) $f(x) = O(g(x))$ cuando $x \to \infty$ si existe una constante positiva C tal que $|f(x)| \leq C|g(x)|$ para x suficientemente grande.

b) $f(x) = o(g(x))$, cuando $x \to \infty$ si $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

Análogamente se definen $f(x) = O(g(x))$ y $f(x) = o(g(x))$ cuando $x \to x_0$.

También usaremos la notación $f(x) \ll g(x)$ y la notación $f(x) \gg g(x)$ para indicar que existe una constante positiva C tal que $f(x) \leq Cg(x)$ y $f(x) \geq Cg(x)$ respectivamente.

2.1.1. La constante de Euler

Proposición 2.1.2.

$$\sum_{k=1}^{n} \frac{1}{k} = \log n + \gamma + O(1/n),$$

donde γ es la constante de Euler.

Demostración. Aplicaremos la identidad de Abel a la función aritmética más sencilla de todas, $a(n) = 1$, y a la función $f(x) = \frac{1}{x}$ para estimar las sumas parciales de la serie armónica.

Dichas funciones cumplen las condiciones de la identidad de Abel con $A(x) = \lfloor x \rfloor$ y $f'(x) = -\frac{1}{x^2}$. Tenemos entonces que

$$\begin{aligned} \sum_{k=1}^{n} \frac{1}{k} &= \frac{A(n)}{n} + \int_1^n \frac{A(t)}{t^2} dt = 1 + \int_1^n \frac{t - \{t\}}{t^2} dt \\ &= 1 + \log n - \int_1^\infty \frac{\{t\}}{t^2} dt + \int_n^\infty \frac{\{t\}}{t^2} dt. \end{aligned}$$

Observemos que la última integral es $O\left(\frac{1}{n}\right)$. Entonces

$$\lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \log n \right) = 1 - \int_1^\infty \frac{\{t\}}{t^2} dt.$$

Esta constante es la llamada de Euler:

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

□

La constante de Euler es una de las constantes, como π y como e, que aparecen de una manera natural en las matemáticas. Sin embargo se desconoce si γ es un número racional o irracional.

2.1.2. Fórmulas de Mertens

Teorema 2.1.3.

$$a) \qquad \sum_{p\le x} \frac{\log p}{p} = \log x + O(1), \qquad x \to \infty$$

$$b) \qquad \sum_{p\le x} \frac{1}{p} = \log\log x + B + O\left(\frac{1}{\log x}\right), \qquad x \to \infty$$

Demostración. En la prueba de estas leyes asintóticas vamos a utilizar la fórmula

$$\log(m!) = m\log m - m + O(\log m),$$

que la podemos deducir comparando $\log(m!)$ con la integral $\int_1^m \log t dt = m \log m - m$, ya que la diferencia

$$\begin{aligned}\left|\sum_{k=1}^{m} \log k - \int_1^m \log t dt\right| &\le \sum_{k=1}^{m} \left|\log k - \int_{k-1}^{k} \log t dt\right| \\ \le \sum_{k=2}^{m} |\log k - \log(k-1)| &\le \sum_{k=1}^{m} O(1/k) = O(\log m)\end{aligned}$$

a) Por el lema 1.2.4 sabemos que $m! = \prod_{p\le m} p^{\alpha_p}$, donde $\alpha_p = \lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots$. Tomando logaritmos obtenemos la relación:

$$\begin{aligned}\log(m!) &= \sum_{p\le m} \left\lfloor \frac{m}{p} \right\rfloor \log p + \sum_{p\le m} \left(\sum_{k\ge 2} \left\lfloor \frac{m}{p^k} \right\rfloor \log p \right) \\ &= m \sum_{p\le m} \frac{\log p}{p} + \sum_{p\le m} \left(\left\lfloor \frac{m}{p} \right\rfloor - \frac{m}{p} \right) \log p + O(m) \\ &= m \sum_{p\le m} \frac{\log p}{p} + O\left(\sum_{p\le m} \log p \right) + O(m).\end{aligned}$$

Teniendo en cuenta que $\log(m!) = m\log m + O(m)$ y que $\sum_{p\leq m}\log p \leq (\log m)\pi(m) = O(m)$, resulta que:

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

Es decir,

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

b) La segunda suma la escribimos de la forma

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

donde $a(n) = \frac{\log p}{p}$ si n es primo y $a(n) = 0$ en caso contrario.

Estamos en condiciones de aplicar el lema de sumación de Abel:

$$\sum_{p\leq x}\frac{1}{p} = \frac{1}{\log x}A(x) + \int_2^x \frac{A(t)}{t(\log t)^2}dt,$$

donde

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

por el resultado anterior.

Tenemos que:

$$\int_2^x \frac{A(t)}{t(\log t)^2}dt = \int_2^x \frac{dt}{t\log t} + \int_2^x \frac{A(t)-\log t}{t(\log t)^2}dt = I_1 + I_2.$$

$$\begin{aligned}
I_1 &= \int_2^x \frac{dt}{t\log t} = \log\log x - \log\log 2.\\
I_2 &= \int_2^\infty \frac{A(t)-\log t}{t(\log t)^2}dt - \int_x^\infty \frac{O(1)}{t(\log t)^2}dt\\
&= \int_2^\infty \frac{A(t)-\log t}{t(\log t)^2}dt + O\left(\frac{1}{\log x}\right).
\end{aligned}$$

Por lo tanto,

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

donde

$$B = 1 - \log\log 2 + \int_2^\infty \frac{A(t) - \log t}{t(\log t)^2} dt.$$

□

Observación 2.1.4. *Puede demostrarse que la constante B tiene la forma siguiente:*

$$B = \gamma + \sum_p \left\{ \log\left(1 - \frac{1}{p}\right) + \frac{1}{p} \right\},$$

donde γ es la constante de Euler.

2.1.3. La función $r(n)$. Puntos de coordenadas enteras sobre circunferencias

Dado un entero positivo n, se define $r(n)$ como el número de sus representaciones como suma de dos cuadrados.

$$r(n) = \#\{n = t^2 + s^2 : \; s, t \in \mathbb{Z}\}.$$

Por ejemplo $1 = (\pm 1)^2 + 0^2 = 0^2 + (\pm 1)^2$ y, por tanto $r(1) = 4$. De igual manera tenemos $r(2) = 4$, $r(3) = 0$, $r(4) = 4$, $r(5) = 8$, $r(6) = 0$, $r(7) = 0$, $r(8) = 4$, etc..

Basta echar una ojeada a una tabla de valores de $r(n)$ para percibir su carácter irregular. Por ello es razonable definir la función

$$R(n) = \sum_{k=1}^{n} r(k)$$

de tal manera que $\frac{R(n)}{n}$ sea un promedio de $r(k)$ y esperar que esta nueva función tenga una distribución de valores más regular.

Ambas funciones tienen una representación muy sencilla en trminos del retículo fundamental:

$r(n)$ = número de puntos del retículo $\mathbb{Z}^2$(de coordenadas enteras) que están situados sobre la circunferencia de radio $\sqrt{n}$ y centro el origen.

$R(n)$ = número de puntos de coordenadas enteras situados en el círculo de centro el origen y radio $\sqrt{n}$.

El siguiente resultado, debido a Gauss, nos da el orden de magnitud de la función $R(n)$ para valores grandes del entero n.

Teorema 2.1.5.

$$R(n) = \pi n + O(\sqrt{n}).$$

Demostración. A cada punto ν de coordenadas enteras le asociamos el cuadrado de área uno, Q_ν, que le tiene como vértice suroeste. El número $R(n)$ es igual al área de la región F del plano formada por la unión de los cuadrados Q_ν tales que ν está dentro del círculo $x^2 + y^2 \leq n$.

Este área no es exactamente igual al área del círculo de radio $\sqrt{n}$, pues algunos de los cuadrados escogidos tienen parte fuera del círculo, mientras que quedan porciones dl círculo sin recubrir.

Sin embargo podemos trazar dos círculos C_1 y C_2 centrados en el origen y de radios respectivos $\sqrt{n} - \sqrt{2}$ y $\sqrt{n} + \sqrt{2}$ tales que

$$C_1 \subset F \subset C_2.$$

Por lo tanto, $\pi(\sqrt{n} - \sqrt{2})^2 \leq R(n) \leq \pi(\sqrt{n} + \sqrt{2})^2$, lo cual implica que $R(n) = \pi n + O(\sqrt{n})$. $\square$

Este resultado fue obtenido por Gauss a principios del siglo pasado. En torno al año 1906, W. Sierpinski demostró que el error $E(n) = |R(n) - \pi n|$ era $O(n^{1/3})$. El mejor resultado hasta la fecha se debe a Iwaniec: $E(n) = O(n^{\frac{7}{22}+\epsilon})$ para todo $\epsilon > 0$.

En el otro sentido Hardy y Landau probaron que la relación $E(n) = O(n^{1/4})$ es falsa. Es un famoso problema de la teoría de los números encontrar el orden de magnitud exacto del error $E(n)$. ¿Es cierto que $E(n) = O(n^{1/4+\epsilon})$ para todo $\epsilon > 0$?

2.1.4. Promedio de la función divisor

La función $\tau(n)$ ha sido estudiada en el capítulo anterior. Análogamente al caso anterior, consideramos,

$$D(n) = \sum_{k=1}^{n} \tau(k).$$

EL cociente $\frac{D(n)}{n}$ mide el número de divisores que, en promedio, tiene un número comprendido entre 1 y n.

Veamos la interpretación geométrica: $\tau(n)$ es el número de puntos de coordenadas enteras del primer cuadrante que están sobre la hipérbola $xy = n$ y $D(n)$ es el número de puntos que se encuentran en la región R comprendida entre la hipérbola $xy = n$ y las rectas $x = 1$, $y = 1$.

Teorema 2.1.6.
$$D(n) = n \log n + (2\gamma - 1)n + O(\sqrt{n})$$
donde γ es la constante de Euler.

Demostración.

$$\begin{aligned}
D(n) &= \sum_{k \leq n} \tau(k) = \sum_{k \leq n} \sum_{ab=k} 1 = \sum_{ab \leq n} 1 \\
&= \sum_{\substack{ab \leq n \\ a \leq \sqrt{n}}} 1 + \sum_{\substack{ab \leq n \\ b \leq \sqrt{n}}} 1 - \sum_{\substack{ab \leq n \\ a,b \leq \sqrt{n}}} 1 = 2 \sum_{\substack{ab \leq n \\ a \leq \sqrt{n}}} -[\sqrt{n}]^2 \\
&= 2 \sum_{a \leq \sqrt{n}} \left\lfloor \frac{n}{a} \right\rfloor - n + O(\sqrt{n}) = 2 \sum_{a \leq \sqrt{n}} \frac{n}{a} - n + O(\sqrt{n}) \\
&= 2n \log(\sqrt{n}) + 2n\gamma - n + O(\sqrt{n}).
\end{aligned}$$

□

2.1.5. Puntos visibles desde el origen

Un punto de coordenadas enteras es visible desde el origen si el segmento rectilíneo que une dicho punto con el origen no contiene a ningún otro.

Es fácil observar que el punto de coordenadas enteras (a, b) es visible desde el origen si y sólo si $(a, b) = 1$.

Consideremos la región cuadrada del plano $1 \leq x \leq r,\ 1 \leq y \leq r$.

Sea $N(r)$ el número de puntos de coordenadas enteras en este cuadrado y sea $N'(r)$ el número de ellos que son visibles desde el origen.

El cociente $\frac{N'(r)}{N(r)}$ mide la proporción de puntos del cuadrado que son visibles desde el origen.

Teorema 2.1.7. *El conjunto de coordenadas enteras visibles desde el origen tiene densidad $\frac{6}{\pi^2}$.*

Demostración. Por simetría tenemos que

$$N'(r) = -1 + 2 \sum_{1 \leq n \leq r} \sum_{\substack{1 \leq m \leq n \\ (m,n)=1}} 1 = -1 + 2 \sum_{1 \leq n \leq r} \phi(r)$$

donde ϕ es la función de Euler.

Recordando que $\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$ y reordenando las sumas tenemos

$$\begin{aligned}
\sum_{n\le r}\phi(n) &= \sum_{n\le r}\sum_{d|n}\mu(d)\frac{n}{d} = \sum_{n\le r}\sum_{\substack{q,d\\ qd=r}}\mu(d)q \\
&= \sum_{\substack{q,d\\ qd\le r}}\mu(d)q = \sum_{d\le r}\mu(d)\sum_{q\le[r/d]} q = \sum_{d\le r}\mu(d)\left\{\frac{[r/d]([r/d]+1)}{2}\right\} \\
&= \sum_{d\le r}\mu(d)\left\{\frac{r^2}{d^2}+O(\frac{r}{d})\right\} = \frac{r^2}{2}\sum_{d\le r}\frac{\mu(d)}{d^2}+O\left(r\sum_{d\le r}\frac{1}{d}\right) \\
&= \frac{r^2}{2}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}-\frac{r^2}{2}\sum_{d>r}\frac{\mu(d)}{d^2}+O\left(r\sum_{d\le r}\frac{1}{d}\right) = \frac{r^2}{2}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O(r\log r).
\end{aligned}$$

Para calcular la constante $\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}$ volvamos a la identidad de Euler comentada en el capítulo 1.

Si $s>1$ teníamos que $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_p\left(1-\frac{1}{p^s}\right)^{-1}$. Entonces

$$\frac{1}{\zeta(s)} = \prod_p\left(1-\frac{1}{p^s}\right) = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}.$$

Es bien conocido que $\zeta(2)=\frac{\pi^2}{6}$. Asumiendo este hecho, tenemos que

$$\sum_{n\le r}\phi(n) = \frac{3}{\pi^2}r^2+O(r\log r).$$

Obviamente $N(r) = r^2+O(r)$. Luego

$$\frac{N'(r)}{N(r)} = \frac{\frac{6}{\pi^2}r^2+O(r\log r)}{r^2+O(r)} = \frac{\frac{6}{\pi^2}+O\left(\frac{\log r}{r}\right)}{1+O\left(\frac{1}{r}\right)}.$$

Haciendo tender r a infinito obtenemos el teorema. □

2.1.6. El número típico de divisores primos de un entero y el problema de la tabla de multiplicar de Erdős

Empezamos estimando el valor medio de la función $\omega(n)$.

Proposición 2.1.8.

$$\sum_{n\le x}\omega(n) = x\log\log x+O(x).$$

Demostración.

$$
\begin{aligned}
\sum_{n\le x}\omega(n) &= \sum_{n\le x}\sum_{p|n}1=\sum_{p\le x}\sum_{\substack{n\le x\\ p|n}}1=\sum_{p\le x}\left\lfloor\frac{x}{p}\right\rfloor\\
&= \sum_{p\le x}\left(\frac{x}{p}-\left\{\frac{x}{p}\right\}\right)=x\sum_{p\le x}\frac{1}{p}+O(\pi(x))\\
&= x(\log\log x+O(1))+O(x/\log x)\\
&= x\log\log+O(x).
\end{aligned}
$$

□

Es decir, el valor medio de $\omega(n)$ para los $n\le x$ es $\log\log x+O(1)$. Pero vamos a demostrar algo más fuerte. Vamos a ver que $\omega(n)\sim\log\log x$ para casi todos los $n\le x$. Eso será consecuencia del siguiente teorema probado por Hardy y Ramanujan en 1917.

Teorema 2.1.9.

$$\sum_{n\le x}(\omega(n)-\log\log x)^2=O(x\log\log x).$$

Demostración. Utilizando la Proposición 2.1.8 tenemos que

$$
\begin{aligned}
\sum_{n\le x}(\omega(n)-\log\log x)^2 &= \sum_{n\le x}\omega^2(n)-2\log\log x\sum_{n\le x}\omega(n)+x(\log\log x)^2\\
&= \sum_{n\le x}\omega^2(n)-x(\log\log x)^2+O(x\log\log x).
\end{aligned}
$$

Así que tenemos que demostrar que

$$\sum_{n\le x}\omega^2(n)=x(\log\log x)^2+O(x\log\log x).$$

Claramente tenemos que

$$
\begin{aligned}
\sum_{n\le x}\omega^2(n) &= \sum_{n\le x}\left(\sum_{p\le n}1\right)^2=\sum_{n\le x}\left(\sum_{p|n}1+2\sum_{\substack{pq|n\\ p<q}}1\right)\\
&= \sum_{n\le x}\omega(n)+2\sum_{p<q\le x}\sum_{\substack{n\le x\\ pq|n}}1=2\sum_{\substack{p<q\\ pq\le x}}\left\lfloor\frac{x}{pq}\right\rfloor+O(x\log\log x)\\
&= 2\sum_{p<q\le\sqrt{x}}\left\lfloor\frac{x}{pq}\right\rfloor+2\sum_{\sqrt{x}<q\le x}\sum_{p\le x/q}\left\lfloor\frac{x}{pq}\right\rfloor+O(x\log\log x)
\end{aligned}
$$

Observar que

$$\begin{aligned}
\sum_{\sqrt{x}<q\le x}\sum_{p\le x/q}\left\lfloor \frac{x}{pq}\right\rfloor &\le x\sum_{\sqrt{x}<q\le x}\frac{1}{q}\sum_{p\le x}\frac{1}{p}\\
&\le x\left(\log\log x+O(1)\right)\sum_{\sqrt{x}<q\le x}\frac{1}{q}\\
&\le x\left(\log\log x+O(1)\right)\left(\log\log x-\log\log\sqrt{x}+O(1)\right)\\
&= O(x\log\log x).
\end{aligned}$$

Por otra parte,

$$\begin{aligned}
2\sum_{p<q\le\sqrt{x}}\left\lfloor \frac{x}{pq}\right\rfloor &= 2\sum_{p<q\le\sqrt{x}}\left(\frac{x}{pq}+O(1)\right)\\
&= 2x\sum_{q\le\sqrt{x}}\frac{1}{q}\sum_{p<q}\frac{1}{p}+O\left(\sum_{q\le\sqrt{x}}\pi(q)\right)\\
&= 2x\sum_{q\le\sqrt{x}}\frac{1}{q}(\log\log q+O(1))+O(x)\\
&= 2x\sum_{q\le\sqrt{x}}\frac{\log\log q}{q}+O(x\log\log x).
\end{aligned}$$

Utilizando (ver Ejercicio 2.2.24) que $\sum_{q\le\sqrt{x}}\frac{\log\log q}{q}=\frac{(\log\log x)^2}{2}+O(\log\log x)$ llegamos a

$$2\sum_{p<q\le\sqrt{x}}\left\lfloor \frac{x}{pq}\right\rfloor = x(\log\log x)^2+O(x\log\log x).$$

□

Consideremos la tabla de multiplicar $n\times n$ que todos hemos visto en la escuela, normalmente para $n=10$. Las n^2 entradas de la tabla no son todas diferentes. Es claro que hay una simetría respecto la diagonal. Llamemos $M(n)$ al número de entradas diferentes en la tabla de multiplicar $n\times n$. Obviamente se tiene que $M(n)\le n^2$ y si tenemos en cuenta la simetría podemos decir algo más: $M(n)\le\frac{n(n+1)}{2}$.

Erdős demostró que $M(n)=o(n^2)$ y cuya demostración dejamos como ejercicio avanzado.

Teorema 2.1.10 (Erdős)**.**

$$\lim_{n\to\infty}\frac{M(n)}{n^2}=0.$$

Hace unos pocos años Kevin Ford halló el verdadero orden de magnitud de $M(n)$:

$$M(n) \asymp \frac{n^2}{(\log n)^{1-\frac{1+\log\log 2}{\log 2}}(\log\log n)^{3/2}}.$$

2.2. Ejercicios del capítulo 2

2.2.1. *El conserje de un hotel cierra todas las puertas el primer día, el segundo abre las pares, el tercer día vuelve (si estaba abierta la cierra y viceversa) las múltiplos de* 3*, el cuarto día las múltiplos de* 4*, etcétera.*

¿Qué puertas quedarán cerradas al final del proceso?

2.2.2. *Demostrar que* $\sum_{m|n} \tau(m^2) = \tau^2(n)$.

2.2.3. *Demostrar que*

$$\sum_{n=1}^{\infty} \frac{\tau(n)}{n^2} = \frac{\pi^4}{36}.$$

2.2.4. *Demostrar que, dado* $k \geq 1$*, la suma de los inversos de los enteros positivos con exactamente* k *divisores es convergente si y sólo si* k *es impar.*

2.2.5. *Demostrar las identidades*

$$\prod_{d|n} d = n^{\tau(n)/2}, \qquad \sum_{m|n} \tau^3(m) = \left(\sum_{m|n} \tau(m)\right)^2.$$

2.2.6. *Demostrar que un número perfecto impar no puede ser de la forma* $p^\alpha q^\beta$, p, q *primos.*

2.2.7. *Demostrar que para todo* $\epsilon > 0$ *se tiene* $\tau(n) = O(n^\epsilon)$*. Demostrar también que la estimación* $\tau(n) = O\left((\log n)^r\right)$ *no es cierta para ningún* r.

2.2.8. *Demostrar que*

$$\sum_{\substack{m\leq n\\(m,n)=1}} m = \frac{n\phi(n)}{2}.$$

2.2.9. *Calcular* $\limsup_{n\to\infty} \frac{\phi(n)}{n}$ *y* $\liminf_{n\to\infty} \frac{\phi(n)}{n}$.

2.2.10. *Demostrar que el conjunto* $\left\{\frac{\phi(n)}{n},\ n \geq 1\right\}$ *es denso en el intervalo* $[0, 1]$.

2.2.11. *Demostrar que* $\sigma(n) = O(n \log n)$.

2.2.12. *Demostrar que*

$$\frac{1}{2} < \frac{\sigma(n)\phi(n)}{n^2} \leq 1.$$

2.2.13. *Usar los dos ejercicios anteriores para concluir que* $\phi(n) \gg n/\log n$.

2.2.14. *Buscar todos los enteros tales que a)* $\phi(n) = \frac{n}{2}$, *b)* $\phi(n) = \phi(2n)$, *c)* $\phi(n) = 12$.

2.2.15. *Demostrar que* $\sum_{d^2|n} \mu(d) = |\mu(n)|$.

2.2.16. *La función de Mandgoldt se define de la siguiente manera:*

$$\Lambda(n) = \begin{cases} \log p, & \text{si } n \text{ es una potencia de un primo } p \\ 0 & \text{en otro caso.} \end{cases}$$

Demostrar que $\sum_{d|n} \Lambda(d) = \log n$ *y que* $\sum_{d|n} \mu(d) \log d = -\Lambda(n)$. *Demostrar también que si* $Re(s) > 1$ *entonces,*

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

2.2.17. *Demostrar que para cada* $0 \leq \alpha < 1$ *se tiene el desarrollo asintótico*

$$\sum_{n \leq x} \frac{1}{n^\alpha} = \frac{x^{1-\alpha}}{1-\alpha} + c_\alpha + O(x^{-\alpha})$$

para una constante c_α.

2.2.18. *Estimar el número de fracciones irreducibles en el intervalo* $[0, 1]$ *con denominador menor o igual que* N.

2.2.19. *Sea* $r_3(n) = \#\{n = x^2 + y^2 + z^2 : x, y, z \in \mathbb{Z}\}$. *Hallar una fórmula asintótica para* $R_3(x) = \sum_{n \leq x} r_3(n)$.

2.2.20. *Se dice que un entero positivo es libre de cuadrados si no es divisible por ningún cuadrado mayor que* 1. *Estimar el número de enteros positivos menores que* x *que son libres de cuadrados.*

2.2.21. *Hallar una fórmula asintótica para* $\sum_{n \leq x} \sigma(n)$ *donde* $\sigma(n) = \sum_{d|n} d$.

2.2.22. *Hallar el error en esta demostración del teorema del número primo.*

Teorema del número primo: $\pi(x) \sim \frac{x}{\log x}$.

Demostración: *Por el teorema de Chebychev sabemos que* $\frac{x}{4\log x} \leq \pi(x) \leq \frac{4x}{\log x}$. *Supongamos que* $\pi(x) \sim \alpha\frac{x}{\log x}$ *y queda por denostrar que* $\alpha = 1$. *En lo que sigue utilizaremos la fórmula de Mertens,* $\sum_{p\leq x}\frac{1}{p} \sim \log\log x$, *y la fórmula de sumación de Abel:*

$$\sum_{p\leq x}\frac{1}{p} = \frac{\pi(x)}{x} + \int_2^x \frac{\pi(t)}{t^2}dt \sim \alpha\frac{1}{\log x} + \alpha\int_2^x \frac{1}{t\log t}dt \sim \alpha\log\log x.$$

Por lo tanto $\alpha = 1$ *y* $\pi(x) \sim \frac{x}{\log x}$.

2.2.23. *Demostrar que existe una constante positiva c tal que* $\omega(n) > c\log n/(\log\log n)$.

2.2.24. *Demostrar que*

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

2.2.25. *Demostrar que* $\sum_{n\leq x}(\Omega(n) - \omega(n))^2 = O(x)$.

2.2.26. *Utilizar el problema anterior y el Teorema 2.1.9 para demostrar*

$$\sum_{n\leq x}(\Omega(n) - \log\log x)^2 = O(x\log\log x).$$

2.2.27. *Demostrar que para todo* $\epsilon > 0$ *se tiene que*

$$|\{n \leq x :\ |\Omega(n) - \log\log x| > (\log\log x)^{1/2+\epsilon/2}\}| = O\left(\frac{x}{(\log\log x)^{\epsilon}}\right).$$

2.2.28. *Demostrar el Teorema 2.1.10.*