Universidad Nacional
Autónoma de México

Facultad de Ciencias

Teoría de los números I - Tarea III

Alumnos:
Semenov Flores Dimitri
Gladín García Ángel Iván

Profesor:
Alejandro De Las Peñas Castaño

Ayudante:
Aurora Guadalupe Borges Sánchez

12 de Abril de 2019

1. Función zeta de Rieman

Sea $\zeta(s) := \sum_{n\geq 1} n^{-s}$ la función zeta de Riemann. Por demostrar las siguientes identidades

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

  Demostración. Por definición de la función zeta de Riemann:

  $$\begin{aligned}\frac{1}{\zeta(s)} &= \prod_{p\ primo} (1-p^s) \\ &= (1-\frac{1}{2^s})(1-\frac{1}{3^s})(1-\frac{1}{5^s})(1-\frac{1}{7^s})\cdots\end{aligned}$$

  Donde la expasión de este producto sería:

  $$\begin{aligned}&= 1 + \sum_{n\ primo} (\frac{-1}{n^s}) + \sum_{n=p_1p_2} (\frac{-1}{p_1^s}\frac{-1}{p_2^s}) \sum_{n=p_1p_2p_3} (\frac{-1}{p_1^s}\frac{-1}{p_2^s}\frac{-1}{p_3^s}) + \cdots \\ &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\end{aligned}$$

  □

- $\zeta(s)^2 = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$

  Demostración.

  $$\begin{aligned}\zeta(s)^2 &= (\sum_{n=1}^{\infty} \frac{1}{n^s})(\sum_{n=1}^{\infty} \frac{1}{n^s}) \\ &= (1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\cdots) + (1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\cdots)\end{aligned}$$

  Expandiendo el producto

  $$\begin{aligned}&= 1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\cdots \\ &\quad +\frac{1}{2^s}+\frac{1}{4^s}+\frac{1}{6^s}+\frac{1}{8^s}+\frac{1}{10^s}+\cdots \\ &\quad +\frac{1}{3^s}+\frac{1}{6^s}+\frac{1}{9^s}+\frac{1}{12^s}+\frac{1}{15^s}+\cdots \\ &\quad +\frac{1}{4^s}+\frac{1}{8^s}+\frac{1}{12^s}+\frac{1}{16^s}+\frac{1}{20^s}+\cdots \\ &\quad +\frac{1}{5^s}+\frac{1}{10^s}+\frac{1}{15^s}+\frac{1}{20^s}+\frac{1}{25^s}+\cdots \\ &\quad \vdots \\ &= 1+\frac{2}{2^s}+\frac{2}{3^s}+\frac{3}{4^s}+\frac{2}{5^s}+\cdots\end{aligned}$$

Pero se observa que en cada término $\frac{1}{n^s}$ en la suma va a ocurrir tantas veces como n pueda representarse como producto. Pero además, en cada numerador del término, representa el número de divisores de n, lo que es la función aritmética τ.
Ergo, la suma queda expresada como $\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$. □

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

  Demostración.

$$\begin{aligned}\zeta(s)\zeta(s-1) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{n=1}^{\infty} \frac{n}{n^s} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d|n}^{\infty} d \\ &= \sum_{n=1}^{\infty} \frac{1}{n^s} \sigma(n) \\ &= \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}\end{aligned}$$

  □

- Usa ls irracionalidad de $\zeta(2) = \frac{\pi^2}{6}$ para probar que hay una infinidad de números primos.
- Usa ls irracionalidad de $\zeta(2) = \frac{\pi^2}{6}$ para probar que hay una infinidad de números primos.

  Demostración. Por contradicción. Suponer que $\zeta(2) = \frac{\pi^2}{6}$ en un número racional suponiendo que hay un número finito de números primos.
  El producto dobre todos los primos, ósea $\prod_p (1-p^{-2})^{-1}$ es un número racional si y solo sí el número de todos los número primos fuera finito, esto es $\zeta(2)$ racional. Pero $\frac{\pi^2}{6}$ es irracional. Lo cual es una contracción. □

2. Funciones multiplicativas

1. Por demostrar que $f : \mathbb{Z} \longrightarrow \mathbb{R}$ es multiplicativa si y solamente si $f(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = f(p_1^{\alpha_1}) \cdots f(p_s^{\alpha_s})$ para cualesquiera p_i primos y $\alpha_i \geq 0$

   Demostración. Demostramos ambas implicaciones

- f es multiplicativa $\implies f(p_1^{\alpha_1}\cdots p_s^{\alpha_s}) = f(p_1^{\alpha_1})\cdots f(p_s^{\alpha_s})$
  Como f es multiplicativa tenemos que abre el producto de números que son primos relativos y como $p_1, p_2, \ldots, p_s$ son primos distintos tenemos que todos son primos relativos entre todos y esto implica que $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$ también son primos relativos entre todos.
  Dado lo anterior tenemos que

$$f(p_1^{\alpha_1}\cdots p_s^{\alpha_s}) = f(p_1^{\alpha_1})\cdots f(p_s^{\alpha_s})$$

  (todos los primos tienen que ser distintos)
- Si $f(p_1^{\alpha_1}\cdots p_s^{\alpha_s}) = f(p_1^{\alpha_1})\cdots f(p_s^{\alpha_s}) \implies f$ es multiplicativa
  Sean $a, b \in \mathbb{Z}$ tales que $(a, b) = 1$ y cuya descomposición en primos de cada uno es:

$$a = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_s^{\alpha_s}$$
$$b = q_1^{\beta_1}\cdot q_2^{\beta_2}\cdots q_r^{\beta_r}$$

  Dado que $(a, b) = 1$ tenemos que $p_i \neq q_i$ para todo p_i y para todo q_i por lo que cada primo es distinto y por lo tanto cada uno de las potencias de primos es primo relativo con los demás, aplicando f al producto ab y sustituyendo a y b por su descomposición en primos tenemos lo siguiente:

$$\begin{aligned} f(ab) &= f((p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_s^{\alpha_s})(q_1^{\beta_1}\cdot q_2^{\beta_2}\cdots q_r^{\beta_r})) \\ &= f(p_1^{\alpha_1})\cdot f(p_2^{\alpha_2})\cdots f(p_s^{\alpha_s}) f(q_1^{\beta_1})\cdot f(q_2^{\beta_2})\cdots f(q_r^{\beta_r}) \\ &= (f(p_1^{\alpha_1})\cdot f(p_2^{\alpha_2})\cdots f(p_s^{\alpha_s}))(f(q_1^{\beta_1})\cdot f(q_2^{\beta_2})\cdots f(q_r^{\beta_r})) \\ &= f(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_s^{\alpha_s}) f(q_1^{\beta_1}\cdot q_2^{\beta_2}\cdots q_r^{\beta_r}) \\ &= f(a)f(b) \end{aligned}$$

  Por lo tanto f es multiplicativa

Dado lo anterior concluimos que f es multiplicativa si y solamente si $f(p_1^{\alpha_1}\cdot\cdots p_s^{\alpha_s}) = f(p_1^{\alpha_1})\cdots f(p_s^{\alpha_s})$ para cualesquiera p_i primos y $\alpha_i \geq 0$

□

2. Sea f y g funciones multiplicativas, por demostrar que $f = g$ si y solamente si $f(p^\alpha) = g(p^\alpha)$ para todo primo p y para toda $\alpha > 0$. Esto quiere decir que las funciones multiplicativas estan completamente determinadas por sus valores en las potencias de los primos.

   Demostración. Demostramos ambas implicaciones

   - Si $f = g \implies f(p^\alpha) = g(p^\alpha)$
     Sea p un número primo y $\alpha \geq 0$, como $f = g$ tenemos que $f(p^\alpha) = g(p^\alpha)$

- Si $f(p^\alpha) = g(p^\alpha)$ para todo primo p y para toda $\alpha \geq 0 \implies f = g$

  Tenemos que $f = g$ si y solo si $f(x) = g(x)$ para todo x en el dominio de la función, en este caso $\mathbb{Z}$

  Sea $x \in \mathbb{Z}$ cuya descomposición en primos es $x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ donde tenemos que $\alpha_i > 0$

  Como cada uno los primos en la descomposición de x son distintos tenemos que todos son primos relativos con todos y por lo tanto sus potencias también son primos relativos con todo. Dado lo anterior al aplicar f a x tenemos lo siguiente

$$\begin{aligned} f(x) &= f(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}) \\ &= f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \cdots f(p_s^{\alpha_s}) \\ &= g(p_1^{\alpha_1}) \cdot g(p_2^{\alpha_2}) \cdots g(p_s^{\alpha_s}) \\ &= g(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}) \\ &= g(x) \end{aligned}$$

  Por lo tanto $f = g$

Por lo anterior concluimos que $f = g$ si y solamente si $f(p^\alpha) = g(p^\alpha)$ para todo primo p y para toda $\alpha > 0$ con f y g funciones multiplicativas

□

3. Si f y g son funciones multiplicativas, por demostrar que $fg(n) := f(n)g(n)$ y $\frac{1}{f}(n) := \frac{1}{f(n)}$ son multiplicativas. ¿Será $f \circ g$ una función multiplicativa?

   - Por demostrar que fg es multiplicativa

     Demostración. Sean $a, b \in \mathbb{Z}$ tales que $(a, b) = 1$ aplicamos fg a ab

$$\begin{aligned} fg(ab) &= f(ab)g(ab) \\ &= f(a)f(b)g(a)g(b) \\ &= (f(a)g(a))(f(b)g(b)) \\ &= fg(a)fg(b) \end{aligned}$$

     Por lo tanto fg es multiplicativa

     □

   - Por demostrar que $\frac{1}{f}$ es multiplicativa

     Demostración. Sean $a, b \in \mathbb{Z}$ tales que $(a, b) = 1$ aplicamos $\frac{1}{f}$ a ab

$$\begin{aligned}\frac{1}{f}(ab) &= \frac{1}{f(ab)} \\ &= \frac{1}{f(a)f(b)} \\ &= \frac{1}{f(a)} \cdot \frac{1}{f(b)} \\ &= \frac{1}{f}(a) \cdot \frac{1}{f}(b)\end{aligned}$$

Por lo tanto $\frac{1}{f}$ es multiplicativa

□

Afirmamos que $f \circ g$ no necesariamente es una función multiplicativa, ya que no necesariamente la imagen de f o g de dos primos relativos también son dos primos relativos, por ejemplo:

$$\begin{aligned}\tau(4) &== 3 \\ \tau(9) &= 3 \\ \sigma(9) &= 13 \\ \sigma(\tau(4(9)) &= \sigma(\tau(4)\tau(9)) \\ &= \sigma(3 * 3) \\ &= \sigma(9) = 13 \\ \sigma(\tau(4)) * \sigma(\tau(9)) &= \sigma(3)\sigma(3) \\ &= 4 * 4 \\ &= 16\end{aligned}$$

4. Si f es una función multiplicativa, por demostrar que

$$g(n) := \sum_{d|n} f(d)$$

también es multiplicativa

Demostración. Sean $a, b \in \mathbb{Z}$ tales que $(a, b) = 1$, como a y b son primos relativos tenemos que no comparten primos en su factorización única en primos por lo que para cada divisor d de ab tomamos la factorización única en primos, sea n el producto de los primos en la factorizacion de d que dividen a a y m el producto de los primos en la factorización de d que dividen a b

Dado esto tenemos que

$$\begin{aligned} g(ab) &= \sum_{d|ab} f(d) \\ &= \sum_{m|b} \sum_{n|a} f(nm) \\ &= \sum_{m|b} \sum_{n|a} f(n)f(m) \\ &= \sum_{m|b} f(m) \sum_{n|a} f(n) \\ &= g(a)g(b) \end{aligned}$$

Por lo tanto g también es multiplicativa

□

3. Función contadora de divisores

1. Prueba que $\tau(n) \neq \mathcal{O}\big((\log n)^k\big)$ para toda k y que $\tau(n) = \mathcal{O}(\sqrt{n})$.

   Demostración. □

2. Demuestra que $\tau(n)$ es impar $\iff$ n es un cuadrado.

   Demostración. Antes de proceder con la demostración, se dará la definición de la función τ, un número cuadrado y unos resultado que serán usados.

   (a) Sea n un entero positivo, entonces se denota a $\tau(n)$ como el número factores positivos de n, que es $\tau(n) = \sum_{d|n} 1$.

   (b) El n-ésimo número cuadrado se denota $s_n = n^2, n \geq 1$.

   (c) El producto de números impares es **impar**.

   (d) Sea $n = p^e$, entonces $\tau(n) = \tau(n^e) = (e+1)$.

   (e) Sea n un entero positivo con descomposición canónica $n = p_1^{e_1} \cdots p_k^{e_k}$.

   $$\begin{aligned} \tau(n) &= \tau(p_1^{e_1} \cdots p_k^{e_k}) \\ &= \tau(p_1^{e_1}) \cdots \tau(p_k^{e_k}) && \text{Por ser multiplicativa} \\ &= (e_1+1) \cdots (e_k+1) && \text{Por } (d) \end{aligned}$$

   $\Longrightarrow$) Por demostrar: n es cuadrado
   Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, entonces por lo enunciado anteriormente se sigue que, $\tau(n) = (\alpha_1+1) \cdots (\alpha_k+1)$, como por hipótesis se tiene que $\tau(n)$ es impar, entonces, en particular (por lo dicho anteriormente), (α_i+1) es impar para $1 \leq i \leq k$, entonces se debe tener que α_i es par para $1 \leq i \leq k$, como α_i es

par, entonces se puede reescribir de la forma $\alpha = 2\beta$.
Entonces $n = p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_k^{2\beta_k} = (p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k})^2$, ergo n es cuadrado.

$\Longleftarrow$) Por demostrar: $\tau(n)$ es impar
Como por hipótesis n es cuadrado de la forma $n = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_k^{2\alpha_k}$, entonces se tiene que $\tau(n) = (2\alpha_1+1)(2\alpha_2+1)\cdots(2\alpha_k+1)$, como $(2\alpha_i+1)$ para $1 \geq i \geq k$ es par, entonces $(2\alpha_1+1)(2\alpha_2+1)\cdots(2\alpha_k+1)$ también es impar.
Ergo $\tau(n)$ es impar. □

3.
$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$$

Demostración. Sea $n^{\tau(n)} = \prod_{d|n} n$. Entonces

$$n^{\tau(n)} = \prod_{d|n} n = \prod_{d|n} d(\frac{n}{d}) = \prod_{d|n} d \prod_{d|n} \frac{n}{d}$$

Por otro lado, tenemos que se da la siguiente igualdad: $\prod_{d|n} d = \prod_{d|n} \frac{n}{d}$

$$= \prod_{d|n} d \prod_{d|n} d = \prod_{d|n} d^2 = (\prod_{d|n} d)^2$$

Después de haber hecho el análisis previo podemos concluir que

$$(\prod_{d|n} d)^2 = n^{\tau(n)}$$

Sacando raiz cuadrada de ambos lados, se tienes entonces

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$$

□

4. Prueba que para toda $k > 1$, existen $n, m \in \mathbb{Z}$ tales que $\tau(n) + \tau(m) = k$.

Demostración. Recordemos que $\tau(p^j) = j + 1$

Dado el hecho anterior sea $k > 2$ entonces consideremos $n = p^{k-2}$ y $m = 1$ con p primo

Con lo anterior tenemos que

$$\begin{aligned} \tau(p^{k-2}) + \tau(1) &= (k-2) + 1 + 1 \\ &= (k-2) + 2 \\ &= k \end{aligned}$$

Por lo tanto para toda $k > 1$ existen $n, m \in \mathbb{Z}$ tales que $\tau(n) + \tau(m) = k$.

□

4. La función ϕ de Euler

1. Por demostrar que $\phi(n)$ es par para toda $n > 2$

   Demostración. Separamos para el caso cuando n es par y cuando n es impar

   - n es par
     Como n es par entonces $n = 2k$ para alguna $k \geq 2 \implies \phi(n) = n\prod_{p|n}(1 - \frac{1}{p}) = 2k\prod_{p|n}(1 - \frac{1}{p})$ por lo que $\phi(n)$ es par
   - n es impar
     Sea $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ la factorización en primos de n, donde como n es impar entonces todos los p_i son impares
     Sea $p_2^{\alpha_2} \cdots p_r^{\alpha_r} = m$ entonces $n = p_1^{\alpha_1} \cdot m$ y además $(p_1^{\alpha_1}, m) = 1$
     Calculamos $\phi(n)$

     $$\begin{aligned}\phi(n) &= \phi(p_1^{\alpha_1})\phi(m)\\ &= p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\phi(m)\\ &= p_1^{\alpha_1 - 1}(p_1 - 1)\phi(m)\end{aligned}$$

     Pero como p_1 es impar entonces $p_1 - 1$ es par, por lo que $(p_1 - 1)p_1^{\alpha_1 - 1}\phi(m)$ es par

   Por lo tanto $\phi(n)$ es par para $n > 2$

   □

2. Por demostrar que :

   $$\sum_{k=1}^{n} k = \frac{n}{2}\phi(n) \tag{1}$$

   con $(k, n) = 1$, $k < n$ y $n > 1$

   Demostración. Primero demostramos que $(k, n) = 1 \iff (n - k, n) = 1$

   Demostración. $\implies$) Supongmos que $(k, n) = 1$ y sea $(n - k, n) = d$, por definición de m.c.d tenemos que $d \mid n$ y $d \mid n - k \implies d \mid k$.

   Lo anterior implica que d es divisor común de n y k por lo que $d \mid 1 \implies d = 1$

   $\impliedby$) Supongamos que $(n - k, n) = 1$ y sea $(n, k) = d$, por definición de m.c.d tenemos que $d \mid n$ y $d \mid k \implies d \mid n - k$

   Lo anterior implica que d es divisor común de n y $n - k$ por lo que $d \mid 1 \implies d = 1$

   Por lo tanto $(k, n) = 1 \iff (n - k, n) = 1$

   □

Si $n = 2$ entonces $\frac{n}{2}\phi(n) = \frac{2}{2}1 = 1$ y $\sum_{k=1}^{n} k$ con $(k, 2) = 1$ y $k < 2$ es igual a 1. Por lo anterior la identidad se cumple para $n = 2$

Suponemos que $n > 2$

Tenemos que la suma $\sum_{k=1}^{n} k$ tiene $\phi(n)$ terminos, pero notemos que por cada j tal que $(j, n) = 1$ que aparece en la suma tenemos por el resultado anterior que en la suma también aparece $n - j$ ya que $(n - j, n) = 1$ y al sumar ambos obtenemos n

Dado lo anterior como $\phi(n)$ es par tomamos los primeros $\frac{\phi(n)}{2}$ primos relativos que llamamos $r_1, r_2, \ldots, r_{\frac{\phi(n)}{2}}$ y por el resultado anterior tenemos que los otros $\frac{\phi(n)}{2}$ primos relativos con n son $n - r_1, n - r_2, \ldots, n - r_{\frac{\phi(n)}{2}}$ y por lo tanto la suma de las $k < n$ tales que $(k, n) = 1$ es de la siguiente forma:

$$\begin{aligned}
\sum_{k=1}^{n} k &= r_1 + r_2 + \cdots + r_{\frac{\phi(n)}{2}} + n - r_1 + n - r_2 + \cdots + n - r_{\frac{\phi(n)}{2}} \\
&= (r_1 + n - r_1) + (r_2 + n - r_2) + \cdots + (r_{\frac{\phi(n)}{2}} + n - r_{\frac{\phi(n)}{2}}) \\
&= (n + r_1 - r_1) + (n + r_2 - r_2) + \cdots + (n + r_{\frac{\phi(n)}{2}} - r_{\frac{\phi(n)}{2}}) \\
&= n(\frac{\phi(n)}{2}) \\
&= \frac{n}{2}\phi(n)
\end{aligned}$$

□

3. Por demostar que $\phi(n)\phi(m) = \phi((n, m))\phi([n, m])$ para toda $n, m > 0$

Demostración. Recordemos por lo visto en la tarea 1 que $mn = (m, n)[m, n]$ y notamos dos casos:

- $(n, m) = 1$
  Como ϕ es una función multiplicativa tenemos que $\phi(n)\phi(m) = \phi(nm) = \phi((m, n)[m, n]) = \phi((1)[m, n]) = \phi(1)\phi([m, n])$
- $(n, m) = d > 1$
  Desarrollamos la expresion $\phi(n)\phi(m)$ considerando $(n, m) = d$ y $[n, m] = c$:

$$\begin{aligned}
\phi(n)\phi(m) &= n\prod_{p|n}(1 - \frac{1}{p}) \cdot m\prod_{q|m}(1 - \frac{1}{q}) \\
&= (nm)\prod_{p|n}(1 - \frac{1}{p})\prod_{q|m}(1 - \frac{1}{q}) \\
&= (dc)\prod_{p|n}(1 - \frac{1}{p})\prod_{q|m}(1 - \frac{1}{q})
\end{aligned}$$

Notemos que los primos que dividen a c son todos los primos que dividen a m y todos los primos que dividen a n, lo anterior pasa porque $dc = mn \implies c = \frac{mn}{d}$

Tambíen vemos que los primos que dividen a d tienen que dividir a m y a n ya que d es un divisor común de m y n, por lo que los primos que dividen a d son los primos que tienen en común n y m

Notemos que como $d > 1$ entonces hay algunos primos que aparecen en $\prod_{p|n}(1 - \frac{1}{p})$ y en $\prod_{q|m}(1 - \frac{1}{q})$

Sean $t_0, t_1, \ldots, t_h$ los primos que aparecen en ambos productos, $e_0, e_1, \ldots e_l$ los primos que solo dividen n y $u_1, u_2, \ldots, u_w$ los primos que solo dividen a m. Dado lo anterior reescribimos el producto que teniamos considerando $A = (m \prod_{(t|m)(t|n)}(1 - \frac{1}{t}) \prod_{e|n}(1 - \frac{1}{e}) \prod_{u|m}(1 - \frac{1}{u}))$

$$\begin{aligned}
(dc)\prod_{p|n}(1-\frac{1}{p})\prod_{q|m}(1-\frac{1}{q}) &= (dc)\prod_{e|n}(1-\frac{1}{e})\prod_{u|m}(1-\frac{1}{u})\prod_{(t|m)(t|n)}(1-\frac{1}{t})^2 \\
&= (d\prod_{(t|m)(t|n)}(1-\frac{1}{t}))A \\
&= \phi(d)(m\prod_{(t|m)(t|n)}(1-\frac{1}{t})\prod_{e|n}(1-\frac{1}{e})\prod_{u|m}(1-\frac{1}{u})) \\
&= \phi(d)\phi(c) \\
&= \phi((n,m))\phi([m,n])
\end{aligned}$$

Por lo tanto $\phi(n)\phi(m) = \phi((n,m))\phi([n,m])$ para toda $n, m > 0$

□

Curiosamente tenemos que el resultado anterior se cumple para cualquier f multiplicativa

Demostración. Sean $n, m > 0$

Dividimos en dos casos

- $(n, m) = 1$
  Es análogo a la prueba para la ϕ de Euler, pero reemplazamos ϕ for f
- $(n, m) = d > 1$
  Como n y m no son primos relativos tenemos que tienen primos en común en su factorización en primos
  Sean $p_1, p_2, \ldots, p_s$ los primos en común de n y m, $q_1, q_2, \ldots, q_k$ los primos que unicamente aparecen en la factorización de n y $r_1, r_2, \ldots, r_t$ los primos que unicamente aparecen en la factorización de m
  Como f es multiplicativa tenemos que
  $f(n) = f(p_1^{\alpha_1}), f(p_2^{\alpha_2}), \ldots, f(p_s^{\alpha_s}) f(q_1^{j_1}) f(q_2^{j_2}) \ldots f(q_k^{j_p})$

$f(m) = f(p_1^{\beta_1}), f(p_2^{\beta_2}), \ldots, f(p_s^{\beta_s}) f(r_1^{h_1}) f(r_2^{h_2}) \ldots f(r_k^{h_i})$
Y por otro lado la factorización única en primos de (m, n) son los primos $p_1, p_2, \ldots, p_s$, mientras que la factorización única en primos de $[m, n]$ son los primos $p_1, p_2, \ldots, p_s, r_1, r_2, \ldots, r_t, q_1, q_2, \ldots, q_k$
Recordemos de la tarea 2 que $ord_p([m, n]) = max\{ord_p(m), ord_p(n)\}$ y $ord_p((m, n)) = min\{ord_p(m), ord_p(n)\}$, por lo que dado que f es multiplicativa y tomando las factorizaciones de (n, m) y $[n, m]$ en primos tenemos lo siguiente

$$f((n, m)) = f(p_1^{\alpha_1}), f(p_2^{\alpha_2}), \ldots, f(p_s^{\alpha_s})$$
$$f([n, m]) = f(p_1^{\beta_1}), f(p_2^{\beta_2}), \ldots, f(p_s^{\beta_s}) f(r_1^{h_1}) f(r_2^{h_2}) \ldots f(r_k^{h_i}) f(q_1^{j_1}) f(q_2^{j_2}) \ldots f(q_k^{j_p})$$

Donde suponemos sin perdidad de generalidad y para simplificar que $min_{p_i}\{(ord_{p_i}(n), ord_{p_i}(m)\} = ord_{p_i}(n)$ y que $max_{p_i}\{(ord_{p_i}(n), ord_{p_i}(m)\} = ord_{p_i}(m)$
Por lo anterior concluimos que $f(n)f(m) = f((n, m))f([n, m])$ para cualquier f función multiplicativa

□

5. La función φ de Euler y la infinidad de números primos

Para toda $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ se cumple que

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$

Usa esta fórmula para probar que hay una infinidad de números primos.

Demostración. Se tiene que $\varphi(n)$ es la función que cuenta cuantos primos relativos se tiene del intervalo $S = [1, n]$. Suponiendo que que hay un número m tal que $1 < m \leq n$ que no es primo relativo con n, entonces solo hay un número primo relativo con n que sería el 1. Entonces $\varphi(m) = 1$. □

6. Números perfectos

1. Un entero $n > 0$ es perfecto si $\sigma(n) = 2n$. Por demostrar que n es perfecto si y solo si:

$$\sum_{d|n} \frac{1}{d} = 2 \tag{2}$$

Demostración. Demostarmos ambas implicaciones

Primero notemos que si d es un divisor de n entonces existe un entero q tal que $dq = n$ y adempas tenemos que $q = \frac{n}{d}$, lo anterior nos dice que q también es un divisor de n y $\frac{n}{q} = d$.

Dado el hecho anterior tenemos que el hecho de que d o q aparezca en la suma $\sum_{r|n} r$ implica que el otro termino también aparece la suma y por lo tanto $\sum_{d|n} \frac{n}{d} = \sum_{d|n} d$

- Por demostar que si $n > 0$ es un número entero perfecto, entonces

$$\sum_{d|n} \frac{1}{d} = 2$$

Demostración. Como n es un número entero perfecto tenemos que $\sigma(n) = \sum_{d|n} d = 2n$, dividiendo por n obtenemos lo siguiente:

$$\begin{aligned} 2 &= \frac{1}{n} \sum_{d|n} d \\ &= \sum_{d|n} \frac{d}{n} \\ &= \sum_{d|n} \frac{1}{\frac{n}{d}} \\ &= \sum_{q|n} \frac{1}{q} \end{aligned}$$

Y por lo tanto si $\sigma(n) = 2n$ entonces $\sum_{d|n} \frac{1}{d} = 2$

□

- Por demostrar que si $\sum_{d|n} \frac{1}{d} = 2$ entonces n es un número entero perfecto
  Dado que $\sum_{d|n} \frac{1}{d} = 2$ multiplicamos la expresion por n y obtenemos lo siguiente:

$$\begin{aligned} 2 &= \sum_{d|n} \frac{1}{d} \\ 2n &= n \cdot \sum_{d|n} \frac{1}{d} \\ &= \sum_{d|n} n \cdot \frac{1}{d} \\ &= \sum_{d|n} \frac{n}{d} \end{aligned}$$

Recordemos que si $d \mid n$ entonces existe una q tal que $dq = n$ y además $q = \frac{n}{d}$ y $\frac{n}{q} = d$, por lo que $\sum_{d|n} \frac{n}{d} = \sum_{d|n} d$
Por lo tanto $\sum_{d|n} d = 2n \implies \sigma(n) = 2n$, por lo cual n es un número entero perfecto

□

2. Por demostrar que si n es un número perfecto y par, entonces es una suma cosecutiva de potencias de 2

   Demostración. Recordemos que la suma de las primeras $m-1$ potencias de un número s es $\frac{s^m-1}{s-1}$

   Sea n un número perfecto y par, por el enunciado 6.3 tenemos que $n = 2^{p-1}(2^p-1)$ con p primo y (2^p-1) número primo.

   Notemos que la suma de las primeras $p-1$ potencias de 2 es $\frac{2^p-1}{2-1} = \frac{2^p-1}{1} = 2^p - 1$

   Dado lo anterior tenemos lo siguiente:

$$\begin{aligned} n &= 2^{p-1}(2^p-1) \\ &= 2^{p-1} \cdot \sum_{i=0}^{p-1} 2^i \\ &= \sum_{i=0}^{p-1} 2^{p-1} \cdot 2^i \\ &= \sum_{i=0}^{p-1} 2^{p-1+i} \end{aligned}$$

   La cual es una suma consecutiva de potencias de 2

   Por lo tanto si n es un número perfecto y par, entonces n es una suma consecutiva de potencias de 2

   □

3. Por demostrar que si $2^p - 1$ es primo, entonces $2^{p-1}(2^p-1)$ es perfecto. Conversamente, por demostrar que si n es un número perfecto y par, entonces $n = 2^{p-1}(2^p-1)$ con p primo y (2^p-1) primo

   - Por demostrar que si 2^p-1 es primo, entonces $2^{p-1}(2^p-1) = n$ es perfecto

     Demostración. Notemos que $(2^{p-1}, 2^p-1) = 1$ debido a que 2^{p-1} es par y $2^p - 1$ es impar

Calculamos $\sigma(2^{p-1}(2^p-1)) = \sigma(2^{p-1})\sigma((2^p-1))$ (ya que $\sigma(x)$ es multiplicativa)

$$\begin{aligned}\sigma(2^{p-1}(2^p-1)) &= \sigma(2^{p-1})\sigma(2^p-1)\\ &= \frac{2^p-1}{2-1}\cdot(2^p-1+1)\\ &= (2^p-1)\cdot 2^p\\ &= 2((2^p-1)2^{p-1})\\ &= 2n\end{aligned}$$

Por lo tanto si 2^p-1 es primo, entonces $2^{p-1}(2^p-1) = n$ es perfecto

□

- Por demostrar que si n es un número perfecto y par, entonces $n = 2^{p-1}(2^p-1)$ con p primo y (2^p-1) primo

Demostración. Sea $n = 2^k m$ con m impar y $ord_2(n) = k$ es decir $(2^k, m) = 1$
Como n es perfecto tenemos que $2n = \sigma(n) = \sigma(2^k m) = \sigma(2^k)\sigma(m)$
Y tenemos que $\sigma(2^k m) = (2^{k+1}-1)\sigma(m)$ y dado esto tenemos la igualdad $2n = 2^{k+1}m = (2^{k+1}-1)\sigma(m)$
De lo anterior tenemos que $2^{k+1}-1 \mid 2^{k+1}m \implies 2^{k+1}-1 \mid m$ (Lema de Euclides)
Por lo anterior tenemos que existe $r \in \mathbb{Z}$ tal que $(2^{k+1}-1)r = m$
$\implies (2^{k+1})\frac{m}{(2^{k+1}-1)} = \sigma(m) = m + r + \ldots$
Y de esto tenemos que

$$(2^{k+1})r = m + r + \ldots \tag{3}$$

Y notemos que $m + r = m + \frac{m}{(2^{k+1}-1)} = \frac{(2^{k+1}-1)m+m}{(2^{k+1}-1)} = \frac{2^{k+1}m}{(2^{k+1}-1)}$
Sustituimos en la ecuacion 3

$$\begin{aligned}2^{k+1}r &= \frac{2^{k+1}m}{(2^{k+1}-1)} + \cdots(\text{demás divisores})\\ r &= \frac{m}{(2^{k+1}-1)} + \ldots\frac{(\text{demás divisores})}{2^{k+1}}\\ r &= r + (\frac{\text{demás divisores})}{2^{k+1}})\end{aligned}$$

Lo anterior nos indica que el conjunto de los demás divisores tiene que ser vacío
$D_m - \{m, r\} = \varnothing$ y por lo tanto m es primo y $r = 1$
Y por lo tanto $m = 2^{p+1}-1$ es primo y $n = 2^p m = 2^p 2^{p+1} - 1$ □

A pesar de los resultados expuestos por lo visto en clase tenemos que la pregunta ¿Hay números perfectos impares? es una pregunta que no ha podido ser resuelta, aunque si se han encontrado algunos propiedades que tendria que cumplir el número si es que existe

7. Suma de divisores

1. Demuestra que $\sigma(n)$ es impar si y solamente si $n = m^2$ ó $n = 2m^2$ para alguna $m \in \mathbb{Z}$.

   Demostración. Recordando las siguientes propiedades de la función aritmética σ.

   - Sea $n = p^r$, entonces $\sigma(n) = \frac{p^{r+1}-1}{p-1}$.
   - Sea $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{e_r}$, entonces $\sigma(n) = \prod_{1\leq i\leq r}\frac{p_i^{k_i+1}-1}{p_i-1} = \prod_{1\leq i\leq r}(1 + p_i + p_i^2 + \ldots p_i^{k_i})$.

   Sea n la descomposición canónica en primos $n = p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$, como por hipótesis $\sigma(n)$ es impar entonces cada término del producto también son impares. Para $(1 + p_i + p_i^2 + \ldots p_i^{k_i})$ siendo impar, las siguientes condiciones se deben cumplir.
   p_i es par, esto es porque todos los términos de $1 + p_i + p_i^2 + \ldots p_i^{k_i}$ son pares a excepción del 1.
   k_i es par, porque $1 + p_i + p_i^2 + \ldots + p_i^{k_i}$ tiene un número impar de términos impares.
   En el primer caso, significa que $p_i^{k_i}$ es potencia de dos. En el segundo caso, significa que $p_i^{k_i}$ es un cuadrado.
   El argumento se vale de regreso, teniendo así la doble implicación. □

2. Prueba que $\sigma(1) + \sigma(2) + \cdots + \sigma(n) \leq n^2$ para toda $n > 1$.

   Demostración. Sea $n > 1$ notemos lo siguiente:

   Tenemos por al algoritmo de la división que para todo $1 \leq m_i \leq n$ existen $q_i, r_i \in \mathbb{Z}$ tales que:

   $$m_i q_i + r_i = n \tag{4}$$

   Dado lo anterior tenemos que para cada m_i el número de veces que aparece en la suma $\sigma(1) + \sigma(2) + \cdots + \sigma(n)$ tiene que ser q_i, ya que m_i divide a $m_i(1), m_i(2), \ldots, m_i(q_i)$ y cada uno de esos terminos aparece en la suma $\sigma(1) + \sigma(2) + \cdots + \sigma(n)$ por lo que m_i aparece en $\sigma(m_i(1)), \sigma(m_i(2)), \ldots, \sigma(m_i(q_i))$

   Por lo anterior podemos reescribir lo suma de la siguiente forma:

$$\sigma(1)+\sigma(2)+\cdots+\sigma(n)=1(\frac{n}{1})+2(\frac{n}{2})+3(\frac{n}{3})+\cdots+n(\frac{n}{n}) \tag{5}$$

Donde $\frac{n}{m_i}=q_i$

Notemos que si en cada termino en lugar de solo multiplicar por q_i también sumamos el residuo r_i la expresion toma la forma

$(1(\frac{n}{1})+r_1)+(2(\frac{n}{2})+r_2)+(3(\frac{n}{3})+r_3)+\cdots+(n(\frac{n}{n})+r_n)=n+n+n+\cdots+n(\text{n veces})=n^2$

Pero notemos que si algun m_i no divide a n entonces $m_i(\frac{n}{m_i})=m_iq_i\leq m_iq_i+r_i=n$

Por lo tanto $\sigma(1)+\sigma(2)+\cdots+\sigma(n)\leq n^2$ para toda $n>1$.

□

3. (1) Prueba que
$$\frac{\sigma(n)}{n}=\sum_{d|n}\frac{1}{d}.$$

Demostración. Consideremos la siguiente igualdad

$$n\sum_{d|n}\frac{1}{d}=\sum_{d|n}\frac{n}{d}$$

Recordando la definición de la función σ, la cual es $\sigma(n)=\sum_{d|n}d$ entonces podemos ver que la suma de los divisores de un número n es $\sum_{d|n}d=\sum_{d|n}\frac{n}{d}$. Con el análisis previo hecho, damos la siguiente igualdad:

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

Entonces $n\sum_{d|n}\frac{1}{d}=\sigma(n)$.
Ergo $\sum_{d|n}\frac{1}{d}=\frac{\sigma(n)}{n}$ □

4. (2) Concluye que
$$\frac{\sigma(1)}{1}+\frac{\sigma(2)}{2}+\cdots+\frac{\sigma(n)}{n}\leq 2n$$
(Hint: $\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}\cdots=\frac{\pi^2}{6}<2$)

Demostración. Sea $n>1$ recordando el argumento usado en la pregunta 7.2:

Tenemos por al algoritmo de la división que para todo $1\leq m_i\leq n$ existen $q_i,r_i\in\mathbb{Z}$ tales que:

$$m_iq_i+r_i=n \tag{6}$$

Dado lo anterior tenemos que para cada $\frac{1}{m_i}$ el número de veces que aparece en la suma $\frac{\sigma(1)}{1} + \frac{\sigma(2)}{2} + \cdots + \frac{\sigma(n)}{n}$ tiene que ser q_i, ya que m_i divide a $m_i(1), m_i(2), \ldots, m_i(q_i)$ y cada uno de esos terminos se le aplica la sigma en la suma $\frac{\sigma(1)}{1}+\frac{\sigma(2)}{2}+\cdots+\frac{\sigma(n)}{n}$ por lo que m_i aparece en $\frac{\sigma(m_i(1))}{m_i(1)}+\frac{\sigma(m_i 2)}{m_i 2}+\cdots+\frac{\sigma(m_i q_i)}{m_i q_i}$
Por lo anterior podemos reescribir lo suma de la siguiente forma:

$$\frac{\sigma(1)}{1} + \frac{\sigma(2)}{2} + \cdots + \frac{\sigma(n)}{n} = \frac{\frac{n}{1}}{1} + \frac{\frac{n}{2}}{2} + \cdots + \frac{\frac{n}{n}}{n}$$

Donde $\frac{n}{m_i} = q_i$
Desarrollando

$$\begin{aligned}\frac{\frac{n}{1}}{1} + \frac{\frac{n}{2}}{2} + \cdots + \frac{\frac{n}{n}}{n} &= \frac{n}{1^2} + \frac{n}{2^2} + \cdots + \frac{n}{n^2} \\ &= n(\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2})\end{aligned}$$

Y por el **hint** tenemos que

$$n(\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2}) < 2n$$

Por lo tanto $\frac{\sigma(1)}{1} + \frac{\sigma(2)}{2} + \cdots + \frac{\sigma(n)}{n} \leq 2n$

□