FORMATO 2 (Anexo No.3)

FORMULARIO DE LA DESCRIPCIÓN DE LA TESIS DOCTORAL O DEL TRABAJO DE GRADO

TÍTULO COMPLETO DE LA TESIS DOCTORAL O TRABAJO DE GRADO: Funciones Aritméticas y Temas Selectos de Teoría de Números.

SUBTÍTULO, SI LO TIENE: _____

_____

AUTOR O AUTORES

Apellidos Completos	Nombres Completos
Torres Chaves	Juan Camilo

DIRECTOR (ES) TESIS DOCTORAL O DEL TRABAJO DE GRADO

Apellidos Completos	Nombres Completos
Castro Chadid	Iván

ASESOR (ES) O CODIRECTOR

Apellidos Completos	Nombres Completos

TRABAJO PARA OPTAR AL TÍTULO DE: Matemático

FACULTAD: Ciencias

PROGRAMA: Carrera X Licenciatura ___ Especialización ____ Maestría ____ Doctorado ____

NOMBRE DEL PROGRAMA: Matemáticas

NOMBRES Y APELLIDOS DEL DIRECTOR DEL PROGRAMA: Patricia Hernández Romero

CIUDAD: BOGOTÁ **AÑO DE PRESENTACIÓN DEL TRABAJO DE GRADO**: 2009

NÚMERO DE PÁGINAS 136

TIPO DE ILUSTRACIONES: Ninguna

SOFTWARE requerido y/o especializado para la lectura del documento Adobe Reader (u otro programa que lea documentos en archivos PDF).

MATERIAL ANEXO (Vídeo, audio, multimedia o producción electrónica): Ninguno

Duración del audiovisual: _____ minutos.

Número de casetes de vídeo: _____ Formato: VHS ___ Beta Max ___ ¾ ___ Beta Cam ____ Mini DV ____ DV Cam ____ DVC Pro ____ Vídeo 8 ____ Hi 8 ____

Otro. Cual? _____

Sistema: Americano NTSC _____ Europeo PAL _____ SECAM _____

Número de casetes de audio: _____

Número de archivos dentro del CD (En caso de incluirse un CD-ROM diferente al trabajo de grado): Cinco (incluyendo el trabajo de grado, los anexos y las firmas)

PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o tener una mención especial)*:

_____

DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS: Son los términos que definen los temas que identifican el contenido.

ESPAÑOL	INGLÉS
Funciones Aritméticas	Arithmetical Functions
Teoría de Números	Number Theory
Parte Entera	Floor Function
Números perfectos	Perfect Numbers
Números de Fermat	Fermat Numbers

RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS: (Máximo 250 palabras - 1530 caracteres):

La presente tesis tiene como objetivo el estudio metódico de las funciones aritméticas y algunos temas relacionados con ellas como lo son la función parte entera, los Teoremas de Euler, Fermat y Wilson; los números perfectos y los números de Fermat.

This thesis has the aim of present a methodic study of the arithmetical functions and some topics related to them, like the floor integer, the theorems of Euler, Fermat and Wilson; the perfect numbers and the Fermat numbers.

FUNCIONES ARITMÉTICAS Y TEMAS SELECTOS DE TEORÍA DE NÚMEROS

JUAN CAMILO TORRES CHAVES

TRABAJO DE GRADO

Presentado como requisito parcial

para optar al título de

Matemático

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE CIENCIAS

CARRERA DE MATEMÁTICAS

Bogotá, D.C.

Julio de 2009

NOTA DE ADVERTENCIA

Artículo 23 de la Resolución N° 13 de Julio de 1946

"La Universidad no se hace responsable por los conceptos emitidos por sus alumnos en sus trabajos de tesis. Solo velará por que no se publique nada contrario al dogma y a la moral católica y por que las tesis no contengan ataques personales contra persona alguna, antes bien se vea en ellas el anhelo de buscar la verdad y la justicia".

FUNCIONES ARITMÉTICAS Y TEMAS SELECTOS DE TEORÍA DE NÚMEROS

JUAN CAMILO TORRES CHAVES

APROBADO

Iván Castro Chadid
Director

Gustavo Nieto Clavijo, M.Sc.
Jurado

Héctor Linares González, M.Sc.
Jurado

FUNCIONES ARITMÉTICAS Y TEMAS SELECTOS DE TEORÍA DE NÚMEROS

JUAN CAMILO TORRES CHAVES

APROBADO

Ingrid Schuler, Ph.D Decana Académica	Patricia Hernández Romero, M.Sc. Directora Carrera

Índice general

Resumen

La presente tesis tiene como objetivo el estudio metódico de las funciones aritméticas y algunos temas relacionados con ellas como lo son la función parte entera; los Teoremas de Euler, Fermat y Wilson; y los números perfectos, pseudoprimos, de Carmichael, de Fermat y los de Mersenne.

Introducción

> *La Matemática es la reina de las ciencias y la Teoría de Números la reina de las Matemáticas.* Carl Friedrich Gauss

La Teoría de Números es posiblemente el área más rica de las Matemáticas; en ella confluyen las demás y de ella nacen muchas otras, es por esto que Gauss la llegó a considerar como la reina de las Matemáticas. Estudiar la Teoría de Números es estudiar la obra de grandes genios que se dedicaron a ella y es una excelente forma de adquirir lo que se conoce como «madurez matemática»; es así como nace el interés de presentar como trabajo de grado una monografía de ciertos temas de la Teoría de Números a los cuales se les dedica menos de un capítulo en la mayoría de los libros de texto.

El tema principal de la monografía es el estudio de las funciones aritméticas y algunos temas relacionados con ella, pero que también tiene un interés por sí mismos, como es el caso de la función parte entera; el Teorema de Euler, el Pequeño Teorema de Fermat, el Teorema de Wilson y las consecuencias de estos teoremas; el estudio de ciertos números especiales como son los números perfectos y su relación con los números de Mersenne, los pseudoprimos, los números de Carmichael y los números de Fermat.

Es así como esta monografía pretende ser de gran ayuda para aquéllos que deseen incursionar de una forma más profunda en estos bellos temas de la Teoría de Números. Se presupone que el lector ya haya visto un curso en Teoría de Números, pues el objetivo principal es el de utilizar esta monografía como complemento de los textos guías tradicionales de Teoría de Números.

Para llevar a cabo la presente monografía se realizó un estudio minucioso de la actual bibliografía sobre funciones aritméticas. Se recopilaron los teoremas más importantes y se buscaron los ejercicios más interesantes sobre el tema. Muchos de estos ejercicios son tomados de competencias o de revistas matemáticas. Otros son problemas que se dejan a cargo del lector en los tradicionales textos de Teoría de Números. Algunos nuevos ejercicios surgían cundo se cambiaban pequeños detalles a los enunciados de anteriores ejercicios ya planteados. Dado la gran cantidad de problemas de la presente monografía, muchos de los métodos utilizados para resolver determinados problemas

fueron aplicados para resolver otro tipo de problemas que inicialmente habían sido resueltos utilizando diferentes métodos, es así como algunos teoremas y ejercicios poseen más de una demostración, este hecho permite al lector elegir aquella demostración que le es más natural a él.

Por último es importantes aclarar el significado de algunas notaciones que se utilizan a lo largo del texto: Los símbolos (a, b) y $[a, b]$ se utilizan respectivamente para indicar el máximo común divisor y el mínimo común múltiplo de a y b. El símbolo $\langle a, b\rangle$ se utiliza para indicar la pareja ordenada cuya primera componente es a y la segunda es b. Para un conjunto finito A, el símbolo $\#A$ significará el cardinal de A. El símbolo $\sum_{d|n}$ indica que la suma se hace sobre todos los divisores positivos de n y el símbolo $\prod_{p|n}$ indica que el producto se hace sobre todos los primos que dividen a n. La expresión $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, para $n \geq 2$, quiere expresar la factorización única de n como productos de primos donde los p_i son primos con $p_1 < p_2 < \cdots < p_m$ y los α_i enteros positivos.

Formulación del Problema y Justificación

Constantemente se están produciendo resultados diversos sobre distintos temas de las Matemáticas y en particular de la Teoría de Números. Éstos al no estar organizados y estructurados secuencialmente en un texto pierden la posibilidad de convertirse en teorías que contribuyan a enriquecer el acervo cultural tan necesario para la formación de especialistas en las distintas áreas de las Matemáticas, es por eso que se hace necesario ir reciclando toda esa valiosa producción para que pueda allanar el camino que permita que quienes ingresan por primera vez a este tipo de conocimiento puedan acceder más fácilmente a la formación requerida.

Como fruto de mi interés por la Teoría de Números me he propuesto tomar una de las áreas que más me apasionan como son las funciones aritméticas y efectuar un proceso de investigación, organización, síntesis y enriquecimiento desde mi propia perspectiva de esta área de la Teoría de Números.

Objetivos

Objetivo General

Hacer un estudio extenso, profundo y metódico de las funciones aritméticas y otros temas de Teoría de Números.

Objetivos Específicos

1) Mostrar las propiedades más importantes relacionadas con las funciones multiplicativas y la convolución de Dirichlet, incorporando recientes y novedosos resultados de estos temas que si bien es cierto que son frutos de investigaciones, no hacen parte de los textos tradicionales de esta área del conocimiento.

2) Investigar e incorporar propiedades relevantes y novedosas de las funciones multiplicativas $\varphi, \tau, \sigma, \sigma_k$ y μ; y de la función parte entera.

3) Presentar diferentes consecuencias del Teorema de Euler, el Pequeño Teorema de Fermat y el Teorema de Wilson.

4) Presentar un estudio sistemático de los números pseudoprimos, de Carmichael, perfectos y de Fermat.

Capítulo 1

Introducción a las Funciones Aritméticas

En el presente capítulo introduciremos el concepto de función aritmética y aún más importante el de función multiplicativa. Al mismo tiempo introduciremos la funciones multiplicativas más sobresalientes, las cuales se irán estudiando a lo largo de esta monografía. El propósito del presente capítulo es el de servir como base para los demás capítulos de forma tal que éstos se puedan leer independientemente.

1.1. Definición y ejemplos

Definición 1.1. *Una función cuyo dominio es el conjunto de los enteros positivos* ($\mathbb{Z}^+$) *y cuyo codominio el conjunto de los números complejos* ($\mathbb{C}$) *, se denomina una* ***función aritmética.***

Definición 1.2. *La función* φ *definida* $\forall n \in \mathbb{Z}^+$*, mediante*
$\varphi(n) =$ *número de enteros positivos menores o iguales que* n *y primos relativos con* n*,*
se denomina ***función*** φ ***de Euler.***

Ejemplo. Dado que los únicos enteros postivos menores o iguales que 12, primos relativos con 12 son 1, 5, 7 y 11 entonces $\varphi(12) = 4$. Dado que los únicos enteros postivos menores o iguales que 9, primos relativos con 9 son 1, 2, 4, 5, 7 y 8 entonces $\varphi(9) = 6$.

Como se observó en el ejemplo anterior, no es muy eficiente determinar el valor de $\varphi(n)$ verificando cada uno de los enteros positivos menores o iguales que n. Más adelante en este cápitulo se expresará $\varphi(n)$ en términos de la factorización de n como producto de primos, la cual nos dará una forma más rápida para determinar su valor.

Apartir de la definición de φ es fácil deducir que:

Corolario 1.3. *Sea n un entero positivo. $\varphi(n) = n - 1$ sii n es primo.*

Definición 1.4. *Definimos la función τ, $\forall n \in \mathbb{Z}^+$, mediante*
$\tau(n) =$ número de divisores positivos que tiene n.

Ejemplo. Dado que hay 4 ($\{1, 2, 4, 8\}$) divisores positivos de 8 entonces $\tau(8) = 4$. Dado que 9 tiene sólo 3 divisores positivos ($\{1, 3, 9\}$) entonces $\tau(9) = 3$.

Teorema 1.5. *Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ entonces*

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1).$$

Demostración. Dado que los divisores de n son de la forma $n = p_1^{c_1} p_2^{c_2} \cdots p_m^{c_m}$ con $0 \leq c_i \leq \alpha_i$, $\forall i = 1, ..., m$, es claro que hay tantos divisores de n como m-plas $(c_1, c_2, ..., c_m)$ donde $0 \leq c_i \leq \alpha_i$, $\forall i = 1, ..., m$. La cantidad de estas m-plas es $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1)$. □

Definición 1.6. *Definimos la función σ, $\forall n \in \mathbb{Z}^+$, mediante*
$\sigma(n) =$ suma de los divisores positivos de n.
En general definimos la función σ_λ, $\forall n \in \mathbb{Z}^+$, mediante $\sigma_\lambda(n) = \sum_{d|n} d^\lambda$ donde $\lambda \in \mathbb{Z}^+$.

Observación. Observe que $\sigma_1 = \sigma$ y que $\sigma_0 = \tau$.

Ejemplo. Vemos que $\sigma(8) = 1 + 2 + 4 + 8 = 15$ y que $\sigma_2(9) = 1^2 + 3^2 + 9^2 = 91$.

Apartir de la definición de σ es fácil deducir que:

Corolario 1.7. *Sea n un entero positivo. $\sigma(n) = n + 1$ sii n es primo.*

1.2. Funciones multiplicativas

Definición 1.8. *Sea f una función aritmética no nula, diremos que f es:*

a) ***Multiplicativa*** *si siempre que $(m, n) = 1$ se tiene que $f(mn) = f(m)f(n)$.*

b) ***Completamente Multiplicativa*** *si $\forall\, n, m \in \mathbb{Z}^+$ se tiene que $f(mn) = f(m)f(n)$.*

Observación. Toda función completamente multiplicativa es multiplicativa.

Ejemplo. La función $f(n) = n^z$ donde $z \in \mathbb{C}$, la función $id(n) = n$ y la función constante $u(n) = 1$ son ejemplos de funciones completamente multiplicativas.

Lema 1.9. *Si f es una función multiplicativa entonces $f(1) = 1$.*

Demostración. Como f es no nula, existe $n \in \mathbb{N}$ tal que $f(n) \neq 0$. Dado que $f(n) = f(n \cdot 1) = f(n)f(1)$, pues $(n, m) = 1$, cancelando $f(n)$ a ambos lados de la ecuación se tiene que $f(1) = 1$. □

Lema 1.10. *Sean f y g funciones multiplicativas entonces fg es también una función multiplicativa. Si además $g(n) \neq 0, \forall n$, entonces f/g también es una función multiplicativa.*

Demostración. Es claro que $fg(1) = 1$. Sean $(m, n) = 1$, utilizando las propiedad de la funciones multiplicativas y la conmutatividad en los complejos tenemos que

$$\begin{aligned} fg(mn) &= f(mn)g(mn) \\ &= f(m)f(n)g(m)g(n) \\ &= f(m)g(m)f(n)g(n) \\ &= fg(mn)fg(mn). \end{aligned}$$

Demostrar que f/g es multiplicativa, con $g(n) \neq 0, \forall n$, queda a cargo del lector. □

En general mediante inducción se llega a que el producto de funciones multiplicativas es multiplicativa.

Lema 1.11. *Sea f una función con $f(1) = 1$, se tiene que:*

a) f es multiplicativa sii $f\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}\right) = f\left(p_1^{\alpha_1}\right) f\left(p_2^{\alpha_2}\right) \cdots f\left(p_m^{\alpha_m}\right)$ para todo $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$.

b) Si f es multiplicativa, entonces f es completamente multiplicativa sii $f(p^\alpha) = f(p)^\alpha$ para todo primo p y para todo entero positivo α.

Demostración. Evidente, se deja a cargo del lector. □

Teorema 1.12. *Sea f una función multiplicativa (completamente multiplicativa) y k un entero positivo, entonces la función F definida para todo $n \in \mathbb{Z}^+$ como $F(n) = f\left(n^k\right)$ es también multiplicativa (completamente multiplicativa).*

Demostración.

i) $F(1) = f\left(1^k\right) = f(1) = 1$.

ii) Sea $(m, n) = 1$, entonces $F(mn) = f\left((mn)^k\right) = f\left(m^k n^k\right)$. Pero $f\left(m^k n^k\right) = f\left(m^k\right) f\left(n^k\right)$ pues f es multiplicativa y $\left(m^k, n^k\right) = 1$, luego $F(mn) = f\left(m^k\right) f\left(n^k\right) = F(m)F(n)$.

El caso en el que se desea probar que si f es completamente multiplicativa entonces también lo es F, se demuestra de forma similar. □

Teorema 1.13. *Sean f y g funciones multiplicativas, entonces la función F definida como*

$$F(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right), \qquad \forall n \in \mathbb{Z}^+,$$

es una función multiplicativa.

Demostración. Sean $n, m \in \mathbb{Z}^+$ con $(n, m) = 1$, luego $d|nm$ sii d es de la forma $d = uv$ con $u|n$ y $v|m$. Además $(u, v) = \left(\frac{n}{u}, \frac{m}{v}\right) = 1$, por lo tanto

$$\begin{aligned} F(nm) &= \sum_{d|nm} f(d) g\left(\frac{nm}{d}\right) \\ &= \sum_{u|n} \sum_{v|m} f(uv) g\left(\frac{nm}{uv}\right) \\ &= \sum_{u|n} \sum_{v|m} f(u) f(v) g\left(\frac{n}{u}\right) g\left(\frac{m}{v}\right) \\ &= \left(\sum_{u|n} f(u) g\left(\frac{n}{u}\right)\right) \left(\sum_{v|m} f(v) g\left(\frac{m}{v}\right)\right) \\ &= F(n) F(m). \end{aligned}$$

□

Tomando la función constante $g(n) = 1$ y aplicando el teorema anterior obtenemos el siguiente resultado.

Corolario 1.14. *Sea f una función multiplicativa, la función F definida como*

$$F(n) = \sum_{d|n} f(d), \qquad \forall n \in \mathbb{Z}^+,$$

es multiplicativa.

Lema 1.15. *Sea f una función multiplicativa, y $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ se tiene que*

$$\sum_{d|n} f(d) = \prod_{i=1}^{m} \left(1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i})\right).$$

Demostración 1. Sabemos por el corolario anterior que $F(n) = \sum_{d|n} f(d)$ es multiplicativa, luego

$$\begin{aligned} F(n) &= \prod_{i=1}^{m} F(p_i^{\alpha_i}) \\ &= \prod_{i=1}^{m} \left(1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i})\right). \end{aligned}$$

□

Demostración 2. Tomando el producto de la derecha de la ecuación y expandiendolo obtenemos una suma de términos de la forma $f(p_1^{c_1}) f(p_2^{c_2}) \cdots f(p_m^{c_m}) = f(p_1^{c_1} p_2^{c_2} \cdots p_m^{c_m})$ donde los c_i varian entre 0 y α_i, $\forall i = 1, ..., m$. Esta suma de términos no es otra cosa que $\sum_{d|n} f(d)$. □

Teorema 1.16. *Para* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ *se tiene que*

$$\sigma_\lambda(n) = \prod_{i=1}^{m} \frac{p_i^{\lambda(\alpha_i+1)} - 1}{p_i - 1}.$$

En especial se tiene que

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

y

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1).$$

Demostración. Es fácil observar que la función $f(n) = n^\lambda$ es una función completamente multiplicativa. Luego podemos aplicar el lema 1.15.
De allí obtenemos que

$$\sum_{d|n} d^\lambda = \prod_{i=1}^{m} \left(1 + p^\lambda + (p^\lambda)^2 + \cdots + (p^\lambda)^{\alpha_i}\right). \tag{1}$$

Si $\lambda = 0$ entonces es claro que

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1).$$

Si $\lambda \neq 0$, y dandonos cuenta que el lado derecho de (1) es una serie geométrica finita tenemos que

$$\sigma_\lambda(n) = \sum_{d|n} d^\lambda = \prod_{i=1}^{m} \frac{p_i^{\lambda(\alpha_i+1)} - 1}{p_i - 1}.$$

Haciendo $\lambda = 1$ tenemos la correspondiente expresión para $\sigma(n)$. □

A partir del teorema anterior, para el lector no le debe ser difícil deducir el siguiente resultado.

Corolario 1.17. *La función* σ_λ *es multiplicativa.*

Observación. En el corolario 1.14 vimos que si f es multiplicativa entonces $F(n) = \sum_{d|n} f(d)$ es multiplicativa, pero no necesariamente es cierto que si f es completamente multiplicativa, F lo sea. Por ejemplo tomemos $f(n) = n$, la cual es completamente multiplicativa y $F(n) = \sigma(n)$, la cual no es completamente multiplicativa.

A continuación presentaremos un resultado interesante que se obtiene utilizando el concepto de función multiplicativa y el lema 1.15, pero que cuyo enunciado nada tiene que ver con funciones aritméticas. Para ello también necesitamos antes el siguiente lema:

Lema 1.18. *Sean n y m enteros positivos. Entonces:*

a) Si $n \equiv m \equiv 1 \mod 4$ entonces $nm \equiv 1 \mod 4$.

b) Si $n \equiv m \equiv 3 \mod 4$ entonces $nm \equiv 1 \mod 4$.

c) Si $n \equiv 1 \mod 4$ entonces $\forall s \in \mathbb{Z}^+$ se tiene que $n^s \equiv 1 \mod 4$.

d) Si $n \equiv 3 \mod 4$ entonces para s par se tiene que $n^s \equiv 1 \mod 4$ y para s impar se tiene que $n^s \equiv 3 \mod 4$.

e) La función f tal que

$$f(n) = \begin{cases} 0, & \text{si } n \text{ es par} \\ 1, & \text{si } n \equiv 1 \mod 4 \\ -1, & \text{si } n \equiv 3 \mod 4 \end{cases}$$

es una función completamente multiplicativa.

Demostración. a), b), c) y *d)* son triviales. Demostraremos *e).*

Es claro que $f(1) = 1$. Sean n y m enteros postivos.

i) Si n es par entonces nm es par y $f(nm) = 0$, además se tiene que $f(n)f(m) = 0 \cdot f(m) = 0$. (Si m es par es análogo)

ii) Si $n \equiv m \equiv 1 \mod 4$ entonces $f(n)f(m) = 1 \cdot 1 = 1$ y $nm \equiv 1 \mod 4$, de donde $f(nm) = 1$.

iii) Si $n \equiv m \equiv 3 \mod 4$ entonces $f(n)f(m) = (-1)(-1) = 1$ y $nm \equiv 1 \mod 4$, de donde $f(nm) = 1$.

iv) Si $n \equiv 1 \mod 4$ y $m \equiv 3 \mod 4$ entonces $f(n)f(m) = 1(-1) = -1$ y $nm \equiv 3 \mod 4$, de donde $f(nm) = -1$. (Si $n \equiv 3 \mod 4$ y $m \equiv 1 \mod 4$ es análogo)

□

Teorema 1.19. *Dado un entero positivo n, el número de sus divisores de la forma $4k+1$ es mayor o igual al número de sus divisores de la forma $4k+3$.*

Demostración. Tomando la función $f(n)$ del lema anterior, basta con demostrar que $\sum_{d|n} f(d) \geq 0$. Como f es multiplicativa por el lema 1.15 tenemos que para $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$,

$$\sum_{d|n} f(d) = \prod_{i=1}^{m} \left(1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i})\right).$$

i) Si $2|n$ entonces 2 no le aporta nada al producto anterior.

ii) Si $p|n$ con p primo de la forma $4k+1$ entonces $1+f(p)+\cdots+f(p^\alpha)$ es positivo, pues por el lema anterior, parte *c)*, se tiene que cualquier potencia de p también es de la forma $4k+1$.

iii) Si $p|n$ con p primo de la forma $4k+3$. Para α par se tiene que

$$1+f(p)+\cdots+f(p^\alpha)=1-1+1-1+\cdots+1=1$$

Para α impar se tiene que

$$1+f(p)+\cdots+f(p^\alpha)=1-1+1-1+\cdots+1-1=0$$

De *i), ii)* y *iii)* nos convencemos de que $\sum_{d|n} f(d)\geq 0$. □

A partir de la anterior demostración es fácil deducir el siguiente corolario.

Corolario 1.20. *Sea $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}$, n tiene tantos divisores de la forma $4k+1$ como de la forma $4k+3$ sii existe α_i impar.*

1.3. Función μ de Möbius

Definición 1.21. *Diremos que n es un entero libre de cuadrados sii es falso que exista p primo tal que $p^2|n$.*

Lema 1.22. *Sea $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}$. El número de divisores de n que son libres de cuadrados es 2^m.*

Demostración. Es claro que el número de divisores de n libres de cuadrados es igual al números de divisores de $m=p_1p_2\cdots p_m$, es decir igual a $\tau(m)=(1+1)(1+1)\cdots(1+1)=2^m$. □

Definición 1.23. *La función μ definida $\forall n\in\mathbb{Z}^+$, mediante*

$$\mu(n)=\begin{cases}1 & \text{si } n=1\\ 0 & \text{si existe } p \text{ primo tal que } p^2|n\\ (-1)^m & \text{si } n \text{ es el producto de } m \text{ primos diferentes.}\end{cases}$$

se denomina ***función μ de Möbius****.*

Es claro entonces que un entero n es libre de cuadrados sii $|\mu(n)|=1$. A partir de este hecho y el lema 1.22 se obtiene el siguiente resultado.

Corolario 1.24. *Si* $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$ *entonces*

$$\sum_{d|n} |\mu(d)| = 2^m.$$

Ejemplo. Se tiene que $\mu(3) = (-1)^1 = -1$.Dado que $24 = 2^3 \cdot 3$ se tiene que $\mu(24) = 0$. Dado que $42 = 2 \cdot 3 \cdot 7$ se tiene que $\mu(42) = (-1)^3 = -1$.

Lema 1.25. *La función de Möbius es multiplicativa pero no completamente multiplicativa.*

Demostración. Veamos que μ es multiplicativa, para ello tomemos $n, m \in \mathbb{Z}^+$ con $(n, m) = 1$.

i) Si $n = 1$ entonces

$$\begin{aligned} \mu(nm) &= \mu(m) \\ &= 1\mu(m) \\ &= \mu(1)\mu(m) \\ &= \mu(n)\mu(m). \end{aligned}$$

Si $m = 1$, idéntico.

ii) Si existe p primo tal que $p^2|n$, entonces $p^2|nm$.

$$\begin{aligned} \mu(nm) &= 0 \\ &= 0\mu(m) \\ &= \mu(n)\mu(m). \end{aligned}$$

Si existe p primo tal que $p^2|m$, idéntico.

iii) Si n y m son libres de cuadrados, es decir $n = p_1 \cdots p_s$ y $m = q_1 \cdots q_r$ donde $p_1, \ldots, p_s, q_1 \ldots, q_r$ son todos primos diferentes pues $(n, m) = 1$. Se tiene que

$$\begin{aligned} \mu(nm) &= (-1)^{s+r} \\ &= (-1)^s(-1)^r \\ &= \mu(n)\mu(m). \end{aligned}$$

Para ver que μ no es completamente multiplicativa, basta con tomar p primo y observar que

$$\mu(p^2) = 0$$

pero

$$\mu(p)\mu(p) = (-1)(-1) = 1.$$

□

Ejercicio 1.26. Probar que $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0, \forall n \geq 1$.

Desarrollo. Por el algoritmo de la división, existen enteros $q, r \in \mathbb{Z}^+$ tales que

$$n = 4q + r \text{ con } 0 \leq r < 4.$$

i) Si $r = 0$, entonces $4|n$, de donde $\mu(n) = 0$.

ii) Si $r = 1$, entonces $4|n+3$, de donde $\mu(n+3) = 0$.

iii) Si $r = 2$, entonces $4|n+2$, de donde $\mu(n+2) = 0$.

iv) Si $r = 3$, entonces $4|n+1$, de donde $\mu(n+1) = 0$.

□

Teorema 1.27. *Sea f una función multiplicativa y $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ entonces*

$$\sum_{d|n} \mu(d) f(d) = \prod_{i=1}^{m} (1 - f(p_i))$$

Demostración. Al ser μf multiplicativa entonces $F(n) = \sum_{d|n} (\mu f)(d) = \sum_{d|n} \mu(d) f(d)$ también lo es.

Luego

$$\begin{aligned} F(n) &= \prod_{i=1}^{m} F(p_i^{\alpha_i}) \\ &= \prod_{i=1}^{m} \left(\sum_{j=0}^{\alpha_i} \mu(p_i^j) f(p_i^j) \right) \\ &= \prod_{i=1}^{m} (f(1) - f(p_i)) \\ &= \prod_{i=1}^{m} (1 - f(p_i)). \end{aligned}$$

□

Utilizando el teorema anterior primero con $f(n) = 1$ y luego con $f(n) = 1/n$ obtenemos respectivamente los siguientes corolarios.

Corolario 1.28.

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

Corolario 1.29.

$$\sum_{d|n} \frac{\mu(d)}{d} = \begin{cases} 1 & si\ n = 1 \\ \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) & si\ n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}. \end{cases}$$

Una leve variación en la demostración del teorema 1.27 nos lleva al siguiente lema:

Lema 1.30. *Para $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ y f función multiplicativa se tiene que*

$$\sum_{d|n} |\mu(d)| f(d) = \sum_{d|n} \mu^2(d) f(d) = \prod_{i=1}^{m} (1 + f(p_i)).$$

Ejercicio 1.31. Demostar el corolario 1.24 utilizando el lema anterior.

Demostración. Tomando $f(n) = 1$, $\forall n \in \mathbb{Z}^+$, se tiene que

$$\sum_{d|n} |\mu(d)| = \prod_{i=1}^{m} (1 + 1) = 2^m.$$

□

Ejercicio 1.32. Demostrar que

$$\sum_{d|n} |\mu(d)| \varphi(d) = \begin{cases} 1 & \text{si } n = 1 \\ \prod_{p|n} p & \text{si } n > 1 \end{cases}$$

Demostración. Para $n = 1$ es claro que se tiene, para $n > 1$ se ve que

$$\begin{aligned} \sum_{d|n} |\mu(d)| \varphi(d) &= \prod_{p|n} (1 + \varphi(p)) \\ &= \prod_{p|n} (1 + (p - 1)) \\ &= \prod_{p|n} p. \end{aligned}$$

□

Teorema 1.33. *Sean las parejas $\langle n_1, a_1 \rangle, \langle n_2, a_2, \rangle \ldots, \langle n_k, a_k \rangle$ en $\mathbb{Z}^+ \times \mathbb{C}$. Definimos $T = \{i : n_i = 1\}$ y $S = \sum_{i \in T} a_i$. Además para $d \in \mathbb{Z}^+$ definimos*

$$T_d = \{i : d | n_i\}$$

y

$$S_d = \begin{cases} \sum_{i \in T_d} a_i & si\ T_d \neq \emptyset \\ 0 & si\ T_d = \emptyset \end{cases}$$

Entonces

$$S = \sum_{d \in \mathbb{Z}^+} \mu(d) S_d.$$

Demostración. Sabemos, por el corolario 1.28, que

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

por lo tanto

$$S = \sum_{i=1}^{k} a_i \left(\sum_{d|n_i} \mu(d) \right).$$

Sean $d_1, d_2, \ldots, d_r$ los enteros positivos que dividen algún n_i $(1 \leq i \leq k)$, se tiene que

$$\begin{aligned} S &= \sum_{j=1}^{r} \mu(d_j) \left(\sum_{i \in T_{d_j}} a_i \right) \\ &= \sum_{j=1}^{r} \mu(d_j) S_{d_j} \\ &= \sum_{d \in \mathbb{Z}^+} \mu(d) S_d. \end{aligned}$$

□

Definición 1.34. *Para $x \in \mathbb{R}$, definimos la **parte entera** de x como el único entero n tal que $n \leq x < n+1$. A ese único entero n lo denotaremos como $\lfloor x \rfloor$.*

Corolario 1.35. *Para n entero positivo se tiene que*

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

Demostración 1. Utilizando las definiciones y notaciones del teorema anterior hacemos $n_k = (k, n)$ y $a_k = 1, \forall k = 1, \ldots, n-1$. Se observa que $S = \varphi(n)$, además S_d es igual a la cantidad de n_i's $(n_i = (i, n))$ que son divisibles por d. Como (i, n) es divisible por d sii $d|n$, se tiene que $S_d = 0$ si $d \nmid n$. Si $d|n$ entonces S_d será igual al la

cantidad de múltiplos de d que son menores que n, es decir $\frac{n}{d}$. Luego por el teorema anterior se tiene que

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

Es decir

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

□

Demostración 2. Es claro ver que

$$\varphi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(n,k)} \right\rfloor \qquad \text{y que} \qquad \sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor.$$

En especial vemos que

$$\sum_{d|(n,k)} \mu(d) = \left\lfloor \frac{1}{(n,k)} \right\rfloor,$$

luego

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d) = \sum_{d|n} \sum_{\substack{k=\alpha d \\ 1\le k\le n}} \mu(d) = \sum_{d|n} \mu(d) \sum_{\substack{k=\alpha d \\ 1\le k\le n}} 1.$$

Dado que $k = \alpha d$ con $1 \le k \le n$ sii $1 \le \alpha \le n/d$, entonces

$$\varphi(n) = \sum_{d|n} \mu(d) \sum_{\alpha=1}^{n/d} 1 = \sum_{d|n} \mu(d)\frac{n}{d}.$$

□

Teorema 1.36. *Para $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ se tiene que*

$$\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{m} \frac{p_i - 1}{p_i}$$

Demostración 1. Consecuencia inmendiata del corolario 1.29 y el corolario anterior.

□

Demostración 2.

$$\begin{aligned}
\prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) &= 1 - \sum_{i=1}^{m} \frac{1}{p_i} + \sum_{1\le i<j\le m} \frac{1}{p_i p_j} - \sum_{1\le i<j<k\le m} \frac{1}{p_i p_j p_k} + \cdots + \frac{(-1)^m}{p_1 p_2 \cdots p_m} \\
&= \sum_{d|n} \frac{\mu(d)}{d} \\
&= \varphi(n).
\end{aligned}$$

□

Ejemplo. Calculemos los valores de $\varphi(12)$ y de $\varphi(9)$. En el primer caso se tiene que $12 = 2^2 \cdot 3$, por lo tanto

$$\varphi(12) = 12\left(\frac{2-1}{2}\right)\left(\frac{3-1}{3}\right) = 4.$$

En el segundo caso se tiene que $9 = 3^2$, por lo tanto

$$\varphi(9) = 9\left(\frac{3-1}{3}\right) = 6.$$

A partir del teorema anterior, para el lector no le debe ser difícil deducir el siguiente resultado.

Corolario 1.37. *La funcion φ es multiplicativa.*

Corolario 1.38. *Existen infinitos números primos.*

Demostración. Supongamos que existen solo un número finito de primos. Sean estos $p_1, p_2, \ldots, p_m$. Sea $a = p_1 p_2, \cdots p_m$. Sabemos que

$$\varphi(a) = a\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right) = (p_1 - 1)(p_2 - 1)\cdots(p_m - 1) \geq (2-1)(3-1) = 2$$

es decir $\varphi(a) \geq 2$. Pero a solo tiene como primo relativo a 1 pues para cualquier otro $n > 1$ se tiene que existe p_i tal que $p_i | n$, luego $\varphi(a) = 1$, lo cual es una contradicción. □

Ejercicio 1.39. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Demostrar que:

a) $\sum_{d|n} \mu(d)\varphi(d) = \prod_{i=1}^{m}(2 - p_i)$

b) $\sum_{d|n} \mu(d)\sigma_\lambda(d) = (-1)^m (p_1 \cdots p_m)^\lambda$

Desarrollo. Utilizando el teorema 1.27 y el hecho de que $\varphi(p) = p-1$ y $\sigma_\lambda(p) = 1+p^\lambda$ para p primo tenemos que:

a) $\sum_{d|n} \mu(d)\varphi(d) = \prod_{i=1}^{m}(1 - (p_i - 1)) = \prod_{i=1}^{m}(2 - p_i)$.

b) $\sum_{d|n} \mu(d)\sigma_\lambda(d) = \prod_{i=1}^{m}(1 - (1 + p_i^\lambda)) = (-1)^m (p_1 \cdots p_m)^\lambda$.
En especial se tiene que

$$\sum_{d|n} \mu(d)\sigma(d) = (-1)^m p_1 \cdots p_m$$

y que

$$\sum_{d|n} \mu(d)\tau(d) = (-1)^m$$

□

Ejercicio 1.40. Si n es un número par, probar que $\sum_{d|n} \mu(d)\varphi(d) = 0$.

Desarrollo. Consecuencia inmediata del ejercicio anterior, parte a). □

El anterior resultado se puede deducir del siguiente corolario:

Corolario 1.41. *Sea f una función multiplicativa tal que $f(2) = 1$. Entonces para todo n entero positivo par, se tiene que*

$$\sum_{d|n} \mu(d)f(d) = 0.$$

Demostración.

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n} (1 - f(p)) = (1 - f(2)) \prod_{\substack{p|n \\ p>2}} (1 - f(p)) = 0.$$

□

Ejercicio 1.42. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Demostrar que:

$$\sum_{d|n} d\mu(d) = \prod_{i=1}^{m} (1 - p_i) = \frac{(-1)^m}{n} p_1 p_2 \cdots p_m \varphi(n).$$

Demostración. Tomando la función definida como $f(n) = n$, $\forall n \in \mathbb{Z}^+$ y aplicando el teorema 1.27 tenemos que

$$\sum_{d|n} d\mu(d) = \prod_{i=1}^{m} (1 - p_i).$$

Por otro lado sabemos que

$$\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{m} \left(\frac{1 - p_i}{-p_i}\right) = \frac{n(-1)^m}{p_1 \cdots p_m} \prod_{i=1}^{m} (1 - p_i).$$

Se ve entonces que

$$\prod_{i=1}^{m} (1 - p_i) = \frac{(-1)^m}{n} p_1 p_2 \cdots p_m \varphi(n)$$

Obteniendose el resultado deseado. □

Ejercicio 1.43. Probar que

$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}, \qquad \forall n \in \mathbb{Z}^+.$$

Demostración. Es claro que para $n = 1$ se tiene. Sea $\theta(n) = \frac{\mu(n)}{\varphi(n)}, \forall n \in \mathbb{Z}^+$. Se tiene que θ es multiplicativa, luego para $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ se tiene que

$$\begin{aligned}
\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} &= \sum_{d|n} \mu(d)\theta(d) \\
&= \prod_{i=1}^{m} (1 - \theta(p_i)) \\
&= \prod_{i=1}^{m} \left(1 + \frac{1}{p_i - 1}\right) \\
&= \frac{1}{\prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)} \\
&= \frac{n}{\varphi(n)}.
\end{aligned}$$

□

1.4. Fórmula de inversión de Möbius

Teorema 1.44 (Fórmula de inversión de Möbius). *Sean f y F funciones aritméticas, entonces*

$$F(n) = \sum_{d|n} f(d), \qquad \forall n \in \mathbb{Z}^+$$

sii

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right), \qquad \forall n \in \mathbb{Z}^+.$$

Demostración. Definimos (sólo para esta demostración) $h(n) = 1, \forall n \in \mathbb{Z}^+$.

$\Rightarrow$)

$$\begin{aligned}
\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \left(\sum_{c|\frac{n}{d}} f(c)\right) \\
&= \sum_{d|n} \sum_{c|\frac{n}{d}} \mu(d) f(c) h\left(\frac{n}{dc}\right) \\
&= \sum_{\alpha\beta\gamma=n} \mu(\alpha) f(\beta) h(\gamma) \\
&= \sum_{\beta|n} f(\beta) \left(\sum_{\alpha|\frac{n}{\beta}} \mu(\alpha)\right).
\end{aligned}$$

Utilizando el corolario 1.28 vemos que

$$\sum_{\alpha|\frac{n}{\beta}} \mu(\alpha) = \begin{cases} 1 & \text{si } \beta = n \\ 0 & \text{en los otros casos.} \end{cases}$$

Luego

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = f(n).$$

$\Leftarrow$)

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d|n} \sum_{c|d} \mu(c) F\left(\frac{d}{c}\right) \\ &= \sum_{d|n} \sum_{c|d} \mu(c) F\left(\frac{d}{c}\right) h\left(\frac{d}{c}\right) \\ &= \sum_{\alpha\beta\gamma=n} \mu(\alpha) F(\beta) h(\gamma) \\ &= \sum_{\beta|n} F(\beta) \left(\sum_{\alpha|\frac{n}{\beta}} \mu(\alpha) \right) \\ &= F(n). \end{aligned}$$

□

Teorema 1.45. *$\forall n \in \mathbb{Z}^+$, se tiene que*

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

Demostración 1. Por el corolario 1.35 tenemos que

$$\varphi(n) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right).$$

Luego utilizando la fórmula de inversión de Möbius obtenemos el resultado buscado. □

Demostración 2. Sea d un divisor positivo de n. Definimos $H_d = \{k \in I_n \mid (k, n) = d\}$. Es claro que

$$H_d = \{k \in I_n \mid (k, n) = d\} = \left\{ j \in I_{\frac{n}{d}} \mid \left(j, \frac{n}{d}\right) = 1 \right\},$$

de donde se tiene que $\#H_d = \varphi\left(\frac{n}{d}\right)$. Por otra parte se tiene que

$$\bigcup_{d|n} H_d = I_n.$$

Luego

$$\sum_{d|n} \#H_d = n,$$

de donde se tiene que

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

□

Observación. Observe que la primera demostración se basa en el corolario 1.35 y luego el uso de la fórmula de inversión de Möbius. Se puede invertir el orden con la demostración 2 para demostrar primero este teorema y luego aplicar la fórmula de inversión de Möbius para obtener el corolario 1.35.

Ejercicio 1.46. Demostrar que

$$n = \sum_{d|n} \mu(d)\sigma\left(\frac{n}{d}\right).$$

Demostración. Dado que

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

utilizando la fórmula de inversión de Möbius obtenemos que

$$n = \sum_{d|n} \mu(d)\sigma\left(\frac{n}{d}\right).$$

□

1.5. Funciones aditivas

Definición 1.47. *Sea f una función aritmética tal que $f(1) = 0$. Diremos que f es* ***aditiva*** *si $f(nm) = f(n) + f(m)$ siempre que $(n, m) = 1$ y diremos que es* ***completamente aditiva*** *si $f(nm) = f(n) + f(m)$, $\forall n, m \in \mathbb{Z}$.*

Ejemplo. La función $s\log(n)$ es completamente aditiva para todo $s \in \mathbb{C}$.

Definición 1.48.

a) Definimos la función ω mediante $\omega(1) = 0$ y $\omega(n) = m$ para $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$.

b) Definimos la función Ω mediante $\Omega(1) = 0$ y $\Omega(n) = \alpha_1 + \alpha_2 + \cdots + \alpha_m$ para $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$.

Corolario 1.49. *La función ω es aditiva y la función Ω es completamente aditiva.*

Demostración. Evidente a partir de la definición anterior. □

Teorema 1.50 (Paul Erdős). *Sea f una función completamente aditiva de valor real y monótona no decreciente (es decir si $n \leq m$ entonces $f(n) \leq f(m)$), entonces existe $c \in \mathbb{R}^+$ tal que $f(n) = c \log n$, $\forall n \in \mathbb{Z}^+$.*

Demostración. Sean n y m enteros positivos con $m \geq 2$ y sean $\alpha_1, \alpha_2, \ldots$ una sucesión estrictamente creciente de enteros positivos. Es claro que existe una sucesión $k_1, k_2, \ldots$ de números naturales tales que

$$m^{k_i} \leq n^{\alpha_i} < m^{k_i+1}, \qquad \forall i \in \mathbb{Z}^+. \tag{1}$$

Es decir $k_i \log m \leq \alpha_i \log n < (k_i + 1) \log m$, $\forall i \in \mathbb{Z}^+$. Dividiendo por $\alpha_i \log m$ obtenemos que

$$\frac{k_i}{\alpha_i} \leq \frac{\log n}{\log m} < \frac{k_i}{\alpha_i} + \frac{1}{\alpha_i}.$$

De donde es claro que $\lim_{i\to\infty} \frac{k_i}{\alpha_i} = \frac{\log n}{\log m}$.

Por otro lado, dado que f es completamente aditiva y monótona no decreciente, de (1) vemos que

$$k_i f(m) \leq \alpha_i f(n) \leq (k_i + 1) f(m), \qquad \forall i \in \mathbb{Z}^+.$$

Dividiendo por $\alpha_i f(m)$, obtenemos que

$$\frac{k_i}{\alpha_i} \leq \frac{f(n)}{f(m)} \leq \frac{k_i}{\alpha_i} + \frac{1}{\alpha_i},$$

de donde vemos que $\lim_{i\to\infty} \frac{k_i}{\alpha_i} = \frac{f(n)}{f(m)}$.

Se tiene entonces que $\frac{f(n)}{f(m)} = \frac{\log n}{\log m}$, o lo que es lo mismo, $f(n) = \frac{f(m)}{\log m} \log n$. Tomando $c = \frac{f(m)}{\log m}$, obtenemos el resultado deseado. □

1.6. La Función de Von Mangoldt y la Función de Liouville

Definición 1.51. *Definimos la **función Von Mangoldt** como*

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^\alpha \text{ donde } p \text{ es primo y } \alpha \in \mathbb{Z}^+ \\ 0 & \text{en otro caso.} \end{cases}$$

Teorema 1.52. *Se tiene que:*

a) $\sum_{d|n} \Lambda(d) = \log n$

b) $\Lambda(n) = -\sum_{d|n} \mu(d) \log d$

Demostración. a) Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, luego

$$\begin{aligned}\sum_{d|n} \Lambda(d) &= \sum_{j=1}^{\alpha_1} \Lambda(p_1^j) + \cdots + \sum_{j=1}^{\alpha_m} \Lambda(p_m^j) \\ &= \alpha_1 \log p_1 + \cdots \alpha_m \log p_m \\ &= \log p_1^{\alpha_1} + \cdots + \log p_m^{\alpha_m} \\ &= \log n\end{aligned}$$

b) Por la fórmula de inversión de Möbius se tiene que

$$\begin{aligned}\Lambda(n) &= \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d) \log n - \sum_{d|n} \mu(d) \log d.\end{aligned}$$

Como $\sum_{d|n} \mu(d) = 0$ si $n > 1$ y $\log n = 0$ si $n = 1$ entonces

$$\sum_{d|n} \mu(d) \log n = 0, \qquad \forall n \in \mathbb{Z}^+$$

Luego

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d.$$

□

Definición 1.53. *Definimos la función de Liouville* λ *como* $\lambda(1) = 1$ *y* $\lambda(n) = (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_m}$ *si* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$.

Lema 1.54. λ *es completamente multiplicativa.*

Demostración. Evidente. □

Teorema 1.55. *Para todo* $n \in \mathbb{Z}^+$ *se tiene que*

$$\sum_{d|n} \lambda(n) = \begin{cases} 1, & \textit{si } n \textit{ es un cuadrado perfecto} \\ 0, & \textit{en otro caso.} \end{cases}$$

Demostración. Sea $F(n) = \sum_{d|n} \lambda(n)$. Como λ es multiplicativa entonces también los es F. Para $n = p^\alpha$ con p primo y $\alpha \in \mathbb{Z}^+$ se ve que

$$F\left(p^\alpha\right) = \sum_{d|p^\alpha} \lambda(d) = 1 + \lambda(p) + \lambda\left(p^2\right) + \cdots + \lambda\left(p^\alpha\right) = 1 - 1 + 1 - \cdots + (-1)^\alpha.$$

Apartir de lo anterior es claro que $F\left(p^\alpha\right) = 1$ si α es par y $F\left(p^\alpha\right) = 0$ si α es impar. Dado que F es multiplicativa es claro que

$$\sum_{d|n} \lambda(n) = \begin{cases} 1, & \text{si } n \text{ es un cuadrado perfecto} \\ 0, & \text{en otro caso.} \end{cases}$$

□

1.7. La Convolución de Dirichlet

Definición 1.56. *Sean f y g dos funciones aritméticas y F definida como*

$$F(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a) g(b).$$

Llamaremos a F la convolución de Dirichlet entre f y g y la denotaremos como $f * g$.

Lema 1.57. *Sean f, g y h funciones aritméticas, entonces se cumple que:*

a) $f * g = g * f$. (Ley conmutativa)

b) $f * (g * h) = (f * g) * h$. (Ley asociativa)

Demostración.

a) Evidente.

b) Vemos que

$$\begin{aligned} [f * (g * h)](n) &= \sum_{ad=n} \left(f(a) \sum_{bc=d} g(b) h(c) \right) \\ &= \sum_{ad=n} \sum_{bc=d} f(a) g(b) h(c) \\ &= \sum_{abc=n} f(a) g(b) h(c). \end{aligned}$$

Análogamente se puede demostrar que

$$[(f * g) * h](n) = \sum_{abc=n} f(a) g(b) h(c).$$

□

Definición 1.58. *Definimos las funciones e y u como $e(n) = \left\lfloor \frac{1}{n} \right\rfloor$ y $u(n) = 1$ para todo n en los enteros positivos, respectivamente.*

Observación. Observe que

$$e(n) = \left\lfloor \frac{1}{n} \right\rfloor = \mu * u(n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1. \end{cases}$$

Lema 1.59. *Sea f una función aritmética, entonces se cumple $f * e = e * f = f$.*

Demostración.

$$e * f(n) = \sum_{d|n} \left\lfloor \frac{1}{d} \right\rfloor f\left(\frac{n}{d}\right) = f(n),$$

pues $\left\lfloor \frac{1}{d} \right\rfloor = 0$ si $d > 1$. □

Lema 1.60. *Sea f una función aritmética tal que $f(1) \neq 0$, entonces existe una única función f^{-1}, llamada la inversa de Dirichlet de f, tal que $f * f^{-1} = f^{-1} * f = e$. Además f^{-1} viene dada por las sigiuentes fórmulas de recurrencia:*

$$f^{-1}(1) = \frac{1}{f(1)} \qquad y \qquad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \text{ para } n > 1.$$

Demostración. Para $n = 1$ vemos que

$$\left(f * f^{-1}\right)(1) = e(1) \iff f(1)f^{-1}(1) = 1 \iff f^{-1}(1) = \frac{1}{f(1)}.$$

Supongamos que para todo $m < n$ se tiene determinado el valor único de $f^{-1}(m)$. Luego para $n > 1$ vemos que

$$\begin{aligned} \left(f * f^{-1}\right)(n) = e(n) &\iff f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0 \\ &\iff f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d). \end{aligned}$$

□

Ejercicio 1.61. Probar la fórmula de inversión de Möbius (teorema 1.44) utilizando el hecho de que la inversa de Dirichlet de μ es u.

Demostración. Por el corolario 1.28 vemos que $\mu^{-1} = u$, luego:

$$F = f * u \iff F * \mu = f * (u * \mu) \iff F * \mu = f.$$

□

Teorema 1.62. *Si f y g son funciones multiplicativas entonces $f * g$ es una función multiplicativa.*

Demostración. Es el mismo teorema 1.13. □

Lema 1.63. *Sean f y g funciones aritméticas. Si g y $f*g$ son funciones multiplicativas entonces f también lo es.*

Demostración. Supongamos que f no es multiplicativa entonces existen dos opciones: $f(1) = 0$ o $f(1) = 1$ pero existen m y n tales que $(m, n) = 1$ y $f(mn) \neq f(m)f(n)$. En el primer caso se llega a la contradicción de que $(f * g)(1) = 0$, contradiciendo que $f * g$ es multiplicativa. Para el segundo caso elegimos m y n tales que el producto mn sea lo menor posible. Si $mn = 1$ $(m = n = 1)$ entonces $f(1) \neq f(1)f(1)$ y por lo tanto $f(1) \neq 1$ lo cual contradice que $f(1) = 1$. Luego $mn > 1$, de donde para todo a y todo b con $(a, b) = 1$ y $ab < mn$ se tiene que $f(ab) = f(a)f(b)$. Vemos entonces que

$$\begin{aligned}
(f * g)(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) \\
&= \sum_{\substack{a|m \\ b|n}} f(ab)g\left(\frac{mn}{ab}\right) \\
&= \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(ab)g\left(\frac{mn}{ab}\right) + f(mn)g(1) \\
&= \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) + f(mn) \\
&= \sum_{a|m} f(a)g\left(\frac{m}{a}\right) \sum_{b|n} f(b)g\left(\frac{n}{b}\right) - f(m)f(n) + f(mn) \\
&= (f * g)(m)(f * g)(n) - f(m)f(n) + f(mn).
\end{aligned}$$

Como $f(mn) - f(m)f(n) \neq 0$ entonces $(f*g)(mn) - (f*g)(m)(f*g)(n) \neq 0$, es decir $(f*g)(mn) \neq (f*g)(m)(f*g)(n)$. Por lo tanto $f*g$ no es una función multiplicativa, lo cual es una contradicción. □

Corolario 1.64. *Si f es multiplicativa, también lo es f^{-1}.*

Demostración. Como $e = f * f^{-1}$ y e y f son multiplicativas, entonces por el lema anterior f^{-1} es multiplicativa. □

Teorema 1.65. *Sea f una función multiplicativa. Entonces f es completamente multiplicativa sii $f^{-1}(n) = \mu(n)f(n)$, $\forall n \in \mathbb{Z}^+$.*

Demostración.

$\Rightarrow$) Como f es completamente multiplicativa entonces

$$\mu f * f(n) = \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = f(n)\sum_{d|n}\mu(d) = f(n)e(n) = e(n),$$

ya que $f(1)e(1) = 1$ y $f(n)e(n) = f(n)0 = 0$ para $n > 1$.

$\Leftarrow$) Como f es multiplicativa, basta con probar que $f\left(p^\alpha\right) = f(p)^\alpha$ para p primo y $\alpha \in \mathbb{Z}^+$. Como $f^{-1}(n) = \mu(n)f(n)$, $\forall n \in \mathbb{Z}^+$, entonces

$$\sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = 0 \qquad \text{para todo } n > 1.$$

Luego para $n = p^\alpha$ tenemos que $\mu(1)f(1)f\left(p^\alpha\right) + \mu(p)f(p)f\left(p^{\alpha-1}\right) = 0$, de donde

$$f\left(p^\alpha\right) = f(p)f\left(p^{\alpha-1}\right). \tag{1}$$

Probaremos que $f\left(p^\alpha\right) = f(p)^\alpha$ por inducción sobre α. Para $\alpha = 1$ se cumple pues $f(p^1) = f(p)^1$. Supongamos que se cumple para α y probemos que se tiene para $\alpha+1$. Utlizando (1) y la hipótesis de inducción vemos que

$$f\left(p^{\alpha+1}\right) = f(p)f\left(p^\alpha\right) = f(p)f(p)^\alpha = f(p)^{\alpha+1}.$$

□

Corolario 1.66. *Se tiene que:*

a) $\varphi^{-1}(n) = \sum_{d|n} d\mu(d) = \prod_{p|n}(1-p)$, *es decir* $\varphi^{-1} = \mu N * u$.

b) $\sigma_k^{-1}(n) = \sum_{d|n} d^k\mu(d)\mu\left(\frac{n}{d}\right)$, *es decir* $\sigma_k^{-1} = \mu N_k * \mu$.

c) $\lambda^{-1}(n) = \mu^2(n) = |\mu(n)|$.

Demostración.

a) Por el corolario 1.35 sabemos que $\varphi = \mu * N$. Como N es completamente multiplicativa entonces $N^{-1} = \mu N$ por el teorema anterior. Luego $\varphi^{-1} = \mu^{-1} * N^{-1} = u * \mu N$. La identidad

$$\sum_{d|n} d\mu(d) = \prod_{p|n} (1-p)$$

es el ejercicio 1.42.

b) Sabemos que $\sigma_k = N_k * u$, además como N_k es completamente multiplicativa entonces $N_k^{-1} = \mu N_k$. Luego $\sigma_k^{-1} = N_k^{-1} * u^{-1} = \mu N_k * \mu$.

c) Como λ es completamente multiplicativa entonces $\lambda^{-1} = \mu\lambda$.

   i) Si $n = 1$, vemos que $\mu(1)\lambda(1) = 1$ y que $\mu^2(1) = |\mu(1)| = 1$.

   ii) Si n es el producto de m primos diferentes, tenemos que $\mu(n)\lambda(n) = (-1)^m(-1)^m = (-1)^{2m} = 1$ y que $\mu^2(n) = |\mu(n)| = 1$.

   iii) Si n no es libre de cuadrados entonces $\mu(n)\lambda(n) = 0\lambda(n) = 0$ y $\mu^2(n) = |\mu(n)| = 0$.

   De i), ii) y iii) vemos que $\lambda^{-1} = \mu\lambda = \mu^2 = |\mu|$.

□

Capítulo 2

La Función φ de Euler

El presente capítulo tiene como proposito mostrar las principales propiedades que posee la función φ de Euler.

2.1. Identidades

Lema 2.1. *Si $m, n \in \mathbb{Z}^+$ y $(m, n) = d$, entonces*

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

Demostración. Si $d = 1$ es claro que se tiene el resultado. Si m y n no son primos relativos, entonces tienen factores primos comunes. Sean estos $p_1, p_2, \cdots, p_s$. Entonces $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} r$ y $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s} t$ con $(r, t) = 1$. Vemos que

$$\varphi(mn) = mn \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) \prod_{p|r} \left(1 - \frac{1}{p}\right) \prod_{p|t} \left(1 - \frac{1}{p}\right)$$

.

$$\varphi(m) = m \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) \prod_{p|r} \left(1 - \frac{1}{p}\right)$$

$$\varphi(n) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) \prod_{p|t} \left(1 - \frac{1}{p}\right)$$

de donde se tiene que

$$\varphi(m)\varphi(n) = \varphi(mn) \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) = \varphi(mn)\frac{\varphi(d)}{d}.$$

□

Ejercicio 2.2. Sea $n, k \in \mathbb{Z}^+$, demostrar que $\varphi\left(n^k\right) = n^{k-1}\varphi(n)$.

Demostración 1.

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

□

Demostración 2. Por inducción sobre k. Es claro que se tiene para $k = 1$. Supongamos que se cumple para k y probemos para $k+1$. Vemos que, como $\left(n^k, n\right) = n$,

$$\frac{\varphi(n)}{n}\varphi\left(n^k n\right) = \varphi\left(n^k\right)\varphi(n).$$

Cancelando $\varphi(n)$, obtenemos que $\varphi\left(n^{k+1}\right) = n\varphi(n^k)$. Por hipótesis de inducción $\varphi(n^k) = n^{k-1}\varphi(n)$, luego $\varphi\left(n^{k+1}\right) = n^k\varphi(n)$. □

Teorema 2.3. *Sean n y j enteros con $n \geq 2$ y $j \geq 0$, entonces el número de enteros positivos entre jn y $(j+1)n$ primos relativos con n es $\varphi(n)$.*

Demostración. Sea x un entero tal que $jn < x < (j+1)n$, entonces existe un único $y \in \mathbb{Z}$ con $1 \leq y < n$ tal que $x = jn + y$. Si $(x, n) = 1$, se tiene que $(jn + y, n) = 1$. Luego $(y, n) = 1$.

Por otra parte, sea $y \in \mathbb{Z}$ tal que $1 \leq y < n$ y $(y, n) = 1$, entonces $jn < jn + y < (j+1)n$ y $(jn + y, n) = 1$.

De lo anterior se desprende que el número de enteros entre jn y $(j+1)n$ primos relativos con n es igual al número de enteros entre 0 y n primos relativos con n, es decir $\varphi(n)$. □

Corolario 2.4. *Si $n, k \in \mathbb{Z}^+$, entonces el número de enteros positivos menores o iguales a kn que son primos relativos con n es $k\varphi(n)$.*

Demostración. Si $n = 1$ es claro que se tiene, luego supongamos que $n > 1$. Utilizando el teorema anterior, variando j entre 0 y $k-1$, obtenemos el resultado deseado. □

Ejercicio 2.5. Demostrar que si $n \geq 2$, entonces la suma de todos los enteros positivos menores que n y primos relativos con n es $n\frac{\varphi(n)}{2}$.

Demostración. Si $n = 2$ es claro que se tiene el resultado. Si $n \geq 3$, sea $1 \leq d < n$ tal que $(d, n) = 1$, entonces $(n - d, n) = 1$. Luego si aparece el sumando d, también aparece el sumando $n - d$ y estos son diferentes (de lo contrario se llegaría a una contradicción). Como $d + (n - d) = n$, entonces

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

□

Teorema 2.6 (American Mathematical Monthly, Problema E1217, [11]). *Para todo entero positivo n, se tiene que*

$$\prod_{d|n} d^{\varphi(d)+\varphi(\frac{n}{d})} = n^n.$$

Demostración.

$$\begin{aligned}\prod_{d|n} d^{\varphi(d)+\varphi(\frac{n}{d})} &= \prod_{d|n} d^{\varphi(d)} \prod_{d|n} d^{\varphi(\frac{n}{d})} \\ &= \prod_{d|n} d^{\varphi(d)} \prod_{d|n} \left(\frac{n}{d}\right)^{\varphi(\frac{n}{d})} \\ &= \prod_{d|n} n^{\varphi(d)} \\ &= n^{\sum_{d|n}\varphi(d)} \\ &= n^n.\end{aligned}$$

□

Observación. Siguiendo las mismas líneas de la demostración anterior se puede demostrar que

$$\prod_{d|n} d^{d+\frac{n}{d}} = n^{\sigma(n)}.$$

Lema 2.7. *Sean $n, k \in \mathbb{Z}^+$, se tiene que*

$$\left\lfloor \frac{n+1}{k} \right\rfloor - \left\lfloor \frac{n}{k} \right\rfloor = \begin{cases} 1 & \text{si } k|n+1 \\ 0 & \text{en otro caso.} \end{cases}$$

Demostración 1. i) Si $k|n+1$, existe $q \in \mathbb{Z}^+$ tal que $n+1 = qk$ de donde

$$\frac{n+1}{k} = q$$

y por lo tanto

$$\left\lfloor \frac{n+1}{k} \right\rfloor = q.$$

Además $n = qk - 1$ de donde

$$\frac{n}{q} = q - \frac{1}{k}$$

y por lo tanto

$$\left\lfloor \frac{n}{k} \right\rfloor = q - 1.$$

ii) Si $k \nmid n+1$, existen $q, r \in \mathbb{N}$ tales que $n+1 = qk + r$ con $0 < r < k$, de donde

$$\frac{n+1}{k} = q + \frac{r}{k}$$

luego

$$\left\lfloor \frac{n+1}{k} \right\rfloor = q.$$

Además $n = qk + r - 1$, de donde

$$\frac{n}{k} = q + \frac{r-1}{k}$$

luego

$$\left\lfloor \frac{n}{k} \right\rfloor = q.$$

De i) y ii) se obtiene el resultado buscado. □

Demostración 2. i) Si $k \nmid n+1$ entonces hay tantos multiplos de k entre 1 y n que entre 1 y $n+1$, es decir

$$\left\lfloor \frac{n}{k} \right\rfloor = \left\lfloor \frac{n+1}{k} \right\rfloor$$

ii) Si $k|n+1$ entonces hay un múltiplo más de k entre 1 y $n+1$ que entre 1 y n, es decir

$$\left\lfloor \frac{n}{k} \right\rfloor + 1 = \left\lfloor \frac{n+1}{k} \right\rfloor$$

De i) y ii) se obtiene el resultado buscado. □

Ejercicio 2.8. Demostrar que

$$\sum_{d=1}^{n} \varphi(d) \left\lfloor \frac{n}{d} \right\rfloor = \frac{n(n+1)}{2}$$

Demostración 1. Sabemos que

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

y que

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

Luego

$$\sum_{k=1}^{n} \sum_{d|k} \varphi(d) = \frac{n(n+1)}{2}$$

Consideremos la suma

$$\sum_{k=1}^{n}\sum_{d|k}\varphi(d)$$

si la expandimos, para un d fijo entre 1 y n, $\varphi(n)$ va a aparecer tantas veces como múltiplos de d entre 1 y n haya, es decir $\left\lfloor \frac{n}{d} \right\rfloor$. Luego

$$\sum_{d=1}^{n}\varphi(d)\left\lfloor\frac{n}{d}\right\rfloor = \sum_{k=1}^{n}\sum_{d|k}\varphi(d)$$
$$\frac{n(n+1)}{2}$$

□

Demostración 2. Por inducción sobre n. Para $n = 1$ es claro que se cumple, supongamos que se cumple para n y probemos que se cumple para $n+1$.

Se tiene que

$$\begin{aligned}\sum_{k=1}^{n+1}\varphi(k)\left\lfloor\frac{n+1}{k}\right\rfloor &= \sum_{k=1}^{n+1}\varphi(k)\left\lfloor\frac{n}{k}\right\rfloor + \sum_{k=1}^{n+1}\varphi(k)\left(\left\lfloor\frac{n+1}{k}\right\rfloor - \left\lfloor\frac{n}{k}\right\rfloor\right)\\ &= \sum_{k=1}^{n}\varphi(k)\left\lfloor\frac{n}{k}\right\rfloor + \sum_{k=1}^{n+1}\varphi(k)\left(\left\lfloor\frac{n+1}{k}\right\rfloor - \left\lfloor\frac{n}{k}\right\rfloor\right)\end{aligned}$$

Utilizando la hipótesis de inducción y el lema anterior, tenemos que

$$\begin{aligned}\sum_{k=1}^{n+1}\varphi(k)\left\lfloor\frac{n+1}{k}\right\rfloor &= \frac{n(n+1)}{2} + \sum_{k|n+1}\varphi(k)\\ &= \frac{n(n+1)}{2} + n + 1\\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

□

Ejercicio 2.9. Demostrar que

$$\sum_{d|n}(-1)^{n/d}\varphi(d) = \begin{cases}0 & \text{si } n \text{ es par}\\ -n & \text{si } n \text{ es impar.}\end{cases}$$

Demostración.

i) Si n es impar entonces

$$\sum_{d|n}(-1)^{n/d}\varphi(d) = \sum_{d|n}(-1)\varphi(d) = -\sum_{d|n}\varphi(d) = -n.$$

ii) Si n es par, entonces podemos expresarlo de la forma $n = 2^\alpha m$ con $\alpha \geq 1$ y m impar. Vemos entonces que

$$\begin{aligned}
\sum_{d|n}(-1)^{n/d}\varphi(d) + n &= \sum_{d|n}(-1)^{n/d}\varphi(d) + \sum_{d|n}\varphi(d) \\
&= \sum_{d|n}\left[(-1)^{n/d}+1\right]\varphi(d) \\
&= \sum_{d|2^{\alpha-1}m}\left[(-1)^{n/d}+1\right]\varphi(d) + \sum_{d|m}\left[(-1)^{n/2^\alpha d}+1\right]\varphi(2^\alpha d) \\
&= 2\sum_{d|2^{\alpha-1}m}\varphi(d) + 0 \\
&= 2\left(2^{\alpha-1}m\right) \\
&= 2^\alpha m \\
&= n.
\end{aligned}$$

Luego

$$\sum_{d|n}(-1)^{n/d}\varphi(d) = 0.$$

□

Ejercicio 2.10. Sea $n \in \mathbb{Z}^+$, sabemos que siempre podemos expresarlo de la forma $n = 2^\alpha m$ con $\alpha \in \mathbb{N}$ y m impar. Demostrar que

$$\sum_{d|n}(-1)^d\varphi(d) = (2^\alpha - 2)\, m.$$

Demostración.

$$\begin{aligned}
\sum_{d|n}(-1)^d\varphi(d) &= \sum_{d|2^\alpha m}(-1)^d\varphi(d)\\
&= \sum_{d|m}(-1)^d\varphi(d) + \sum_{k=1}^{\alpha}\sum_{d|m}(-1)^{2^k d}\varphi\left(2^k d\right)\\
&= -\sum_{d|m}\varphi(d) + \sum_{k=1}^{\alpha}\varphi\left(2^k\right)\sum_{d|m}\varphi(d)\\
&= -m + m\left(\sum_{d|2^\alpha}\varphi(d) - 1\right)\\
&= -m + m\left(2^\alpha - 1\right)\\
&= \left(2^\alpha - 2\right)m.
\end{aligned}$$

□

Teorema 2.11 (The American Mathematical Monthly, Problema 5337, [46]). *Sean m, n enteros positivos y $g = (m, n)$, entonces*

$$\frac{\sum\limits_{\substack{d|n\\(d,m)\neq 1}}\varphi\left(\frac{n}{d}\right)}{\sum\limits_{\substack{d|n\\(d,m)=1}}\varphi\left(\frac{n}{d}\right)} = \frac{g-\varphi(g)}{\varphi(g)}.$$

Demostración. Para $n = 1$ se tiene que ambos lados de la expresión dan cero. Veamos para $n \geq 2$ con $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$. Sean $n_1 = \prod\limits_{p_i\nmid m} p_i^{\alpha_i}$ y $n_2 = \prod\limits_{p_i|m} p_i^{\alpha_i}$. Se tiene que

$$\sum_{\substack{d|n\\(d,m)=1}}\varphi\left(\frac{n}{d}\right) = \sum_{d|n_1}\varphi\left(\frac{n_1 n_2}{d}\right) = \varphi(n_2)\sum_{d|n_1}\varphi\left(\frac{n_1}{d}\right) = n_1\varphi(n_2).$$

Luego

$$\frac{\sum\limits_{\substack{d|n\\(d,m)\neq 1}} \varphi\left(\frac{n}{d}\right)}{\sum\limits_{\substack{d|n\\(d,m)=1}} \varphi\left(\frac{n}{d}\right)} = \frac{n - \sum\limits_{\substack{d|n\\(d,m)=1}} \varphi\left(\frac{n}{d}\right)}{\sum\limits_{\substack{d|n\\(d,m)=1}} \varphi\left(\frac{n}{d}\right)}$$
$$= \frac{n_1 n_2 - n_1\varphi(n_2)}{n_1\varphi(n_2)}$$
$$= \frac{n_2 - \varphi(n_2)}{\varphi(n_2)}$$
$$= \frac{g - \varphi(g)}{\varphi(g)}.$$

□

2.2. Divisibilidad

Teorema 2.12. *$\varphi(n)$ es par sii $n \geq 3$.*

Demostración 1.

$\Rightarrow$) Evidente, pues $\varphi(1) = \varphi(2) = 1$ son impares.

$\Leftarrow$) Sea $n \geq 3$.

i) Si $n = 2^\alpha$, con $\alpha \geq 2$, entonces $\varphi\left(2^\alpha\right) = 2^\alpha - 2^{\alpha-1}$, el cual es claramente par.

ii) Si $n = 2^\alpha p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_m^{\alpha_m}$, con $\alpha \geq 0$, $\alpha_2, \alpha_3, \ldots, \alpha_m \geq 1$ y los p_i's impares entonces es claro que $\varphi(n) = \varphi\left(2^\alpha\right)\varphi\left(p_2^{\alpha_2}\right)\varphi\left(p_3^{\alpha_3}\right)\cdots\varphi\left(p_m^{\alpha_m}\right)$ y por lo tanto $\varphi\left(p_2^{\alpha_2}\right)|\varphi(n)$. Como $\varphi\left(p_2^{\alpha_2}\right) = p_2^{\alpha_2-1}(p_2 - 1)$ es par, también lo es $\varphi(n)$.

□

Demostración 2. Si $n = 1$ o $n = 2$ entonces $\varphi(n)$ es impar. Si $n \geq 3$ y d un entero tal que $1 \leq d < n$ y $(d, n) = 1$ entonces $(n - d, n) = 1$. Es claro que nunca se tiene que $d = n - d$, pues si se tuviera se tendría entonces que $2d = n$ y como $(d, n) = 1$, entonces $d = 1$ y por lo tanto $n = 2$, contradiciendo el hecho de que $n \geq 3$. Luego se puede agrupar los primos relativos positivos de n, menores que n en parejas, cuyos elementos son diferentes y petenencen a una sola pareja. De donde se sigue que $\varphi(n)$ es par. □

Lema 2.13. *Sean $n, m \in \mathbb{Z}^+$ tales que $n|m$, entonces $\varphi(n)|\varphi(m)$.*

Demostración 1. Si $n = 1$ es claro que $\varphi(n)|\varphi(m)$. Si $m = 1$, dado que $n|m$, entonces $n = 1$ y se tiene el caso anterior. Si $n, m > 1$, con $m = nk$ para algún $k \in \mathbb{Z}^+$, entonces en el caso en el que todos los divisores primos de m también son todos los divisores primos de n se tiene que

$$\varphi(m) = m\prod_{p|m}\left(1-\frac{1}{p}\right) = nk\prod_{p|n}\left(1-\frac{1}{p}\right) = k\varphi(n),$$

y en el caso en el que existe algún divisor primo de m que no sea divisor de n se tiene que

$$\varphi(m) = m\prod_{p|m}\left(1-\frac{1}{p}\right) = nk\prod_{p|n}\left(1-\frac{1}{p}\right)\prod_{\substack{p|m\\ p\nmid n}}\left(1-\frac{1}{p}\right) = \alpha\varphi(n),$$

donde

$$\alpha = k\prod_{\substack{p|m\\ p\nmid n}}\left(1-\frac{1}{p}\right) = k\prod_{\substack{p|m\\ p\nmid n}}\left(\frac{p-1}{p}\right)$$

claramente es un entero pues los divisores primos de m que no son divisores primos de n, tienen que ser divisores primos de k.

En ambos casos llegamos a que $\varphi(n)|\varphi(m)$. □

Demostración 2. Por inducción sobre m. Si $m = 1$, entonces $n = 1$ y por lo tanto $\varphi(n)|\varphi(m)$. Supongamos que para todo entero postivo k menor que m, $(m > 1)$ se tiene que siempre que $c|k$ $(c \in \mathbb{Z}^+)$, entonces $\varphi(c)|\varphi(k)$

Sea $n \in \mathbb{Z}^+$ tal que $n|m$. Existe $a \in \mathbb{Z}^+$ tal que $na = m$. Si $(n, a) = d$ entonces

$$\varphi(n)\varphi(a)\frac{d}{\varphi(d)} = \varphi(na) = \varphi(m). \tag{1}$$

Si $a = m$ entonces $n = 1$ y es claro que $\varphi(n)|\varphi(m)$. Si $a \neq m$ entonces $a < m$ pero como $d|a$, entoces por hipótesis de inducción tenemos que $\varphi(d)|\varphi(a)$. Luego

$$\frac{\varphi(a)}{\varphi(d)} \in \mathbb{Z}^+.$$

En (1) vemos que $\varphi(n)|\varphi(m)$. □

Observación. Observe que el recíproco no se tiene, por ejemplo $\varphi(3) = \varphi(4) = 2$ y por lo tanto $\varphi(3)|\varphi(4)$, pero $3 \nmid 4$.

Teorema 2.14. *Sean $a, b \in \mathbb{Z}^+$, entonces $a|b$ sii $\varphi(ab) = a\varphi(b)$.*

Demostración.

$\Rightarrow$) Sean $a, b \in \mathbb{Z}^+$ tales que $a|b$. Si a o b es igual a 1, la igualdad es evidente. Si $a > 1$ y $b > 1$ y tendiendo en cuenta que los primos que dividen a a también dividen a b, entonces

$$\varphi(ab) = ab\prod_{p|ab}\left(1-\frac{1}{p}\right) = ab\prod_{p|b}\left(1-\frac{1}{p}\right) = a\varphi(b).$$

$\Leftarrow$) Sean $a, b \in \mathbb{Z}^+$ tales que

$$\varphi(ab) = a\varphi(b). \tag{1}$$

Si $a = 1$ es claro que $a|b$. Si $b = 1$ entonces (1) queda reducido a $\varphi(a) = a$ el cual solo se cumple si $a = 1$ y tenemos entonces el caso anterior. Si $a, b > 1$, entonces (1) se transforma en

$$ab\prod_{p|ab}\left(1-\frac{1}{p}\right) = ab\prod_{p|b}\left(1-\frac{1}{p}\right),$$

es decir

$$\prod_{p|ab}\left(1-\frac{1}{p}\right) = \prod_{p|b}\left(1-\frac{1}{p}\right). \tag{2}$$

Si $a \nmid b$ es porque existen primos que dividen a pero no a b y por lo tanto

$$\prod_{p|ab}\left(1-\frac{1}{p}\right) = \prod_{p|b}\left(1-\frac{1}{p}\right)\prod_{\substack{p|a\\ p\nmid b}}\left(1-\frac{1}{p}\right).$$

A partir de lo anterior, (2) queda reducido a

$$\prod_{\substack{p|a\\ p\nmid b}}\left(1-\frac{1}{p}\right) = 1.$$

Lo cual es una contradicción pues el producto de números menores que 1 no puede ser 1. De donde $a|b$. □

Corolario 2.15. *Sean $a, b, k \in \mathbb{Z}^+$, entonces $a|b$ sii $\varphi(a^k b) = a^k\varphi(b)$.*

Demostración.

$\Rightarrow$) Por inducción sobre k. Para $k = 1$ se reduce al teorema anterior. Supongamos que se cumple para k y probemos que se tiene para $k+1$. Como $a|b$ entonces $a|a^k b$, luego utilizando el teorema anterior tenemos que

$$\varphi(a^{k+1}b) = \varphi(aa^k b) = a\varphi(a^k b). \tag{1}$$

Por hipótesis de inducción tenemos que $\varphi(a^k b) = a^k \varphi(b)$. Luego reemplazando en (1), vemos que $\varphi(a^{k+1}b) = aa^k\varphi(b) = a^{k+1}\varphi(b)$.

$\Leftarrow$) Supongamos que $\varphi(a^k b) = a^k\varphi(b)$. Luego por el teorema anterior tenemos que $a^k|b$, de donde se tiene que $a|b$. □

Corolario 2.16. *Sea $m \geq 2$ entonces $n|\varphi(n^m)$.*

Demostración. Consecuencia inmediata del teorema 2.14. □

Ejercicio 2.17 (The American Mathematical Monthly, Problema E1483, [30]). Para cada pareja $\langle a, b\rangle$ de enteros positivos, demostrar que existen infinitas parejas $\langle A, B\rangle$ de enteros positivos tales que $\varphi(A) \equiv 0 \mod a$, $\varphi(B) \equiv 0 \mod b$ y $\varphi(A + B + AB) \equiv 0 \mod a + b$.

Demostración. Sea $A = pa^2(a+b)^2$ y $B = qb^2(a+b)^2$, donde p y q son enteros positivos arbitrarios. Se tiene que $a|\varphi(a^2)$ y que $\varphi(a^2)|\varphi(A)$ por el corolario anterior y el lema 2.13. Luego $a|\varphi(A)$ y por lo tanto $\varphi(A) \equiv 0 \mod a$. Análogamente se tiene que $\varphi(B) \equiv 0 \mod b$. Además $A + B + AB = (a+b)^2\left[pa^2 + qb^2 + pqa^2b^2(a+b)^2\right]$ de donde $a + b|\varphi\left((a+b)^2\right)$ y $\varphi\left((a+b)^2\right)|\varphi(A + B + AB)$. Luego $a + b|\varphi(A + B + AB)$ y por lo tanto $\varphi(A + B + AB) \equiv 0 \mod a + b$. □

Ejercicio 2.18. Si n tiene m factores primos impares diferentes, demostrar que $2^m|\varphi(n)$.

Demostración. Sea $n = 2^\alpha p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ en donde los p_i's son primos impares distintos, $\alpha_i \geq 1\ \forall i \in \{1, \ldots, m\}$ y $\alpha \in \mathbb{N}$. Entonces

$$\varphi(n) = \varphi\left(2^\alpha\right) \prod_{i=1}^{m} p_i^{\alpha_i - 1}(p_i - 1).$$

Como los p_i's son impares, entonces $2|p_i - 1$, $\forall i \in \{1, \ldots, m\}$. Luego $2^m|\varphi(n)$. □

Ejercicio 2.19 (The American Mathematical Monthly, E3037, [14]). Encontrar los enteros positivos n tales que $\varphi(n)|n$.

Demostración. Es claro que para $n = 1$ se tiene que $\varphi(1)|1$. Sea $n \geq 2$ con $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Si $\varphi(n)|n$ entonces $\exists x \in \mathbb{Z}^+$ tal que

$$n = x\varphi(n) = xn \prod_{i=1}^{m} \frac{p_i - 1}{p_i},$$

luego $p_1 p_2 \cdots p_m = x(p_1 - 1)(p_2 - 1)\cdots(p_m - 1)$. Es claro que si todos los primos fueran impares el lado izquierdo de la igualdad sería impar y el derecho par, lo que es una contradicción. Luego uno de los primos tiene que ser 2, sea $p_1 = 2$. Tenemos entonces que $2p_2 \cdots p_m = x(p_2 - 1)\cdots(p_m - 1)$. Es claro que no puede haber

más de dos primos impares pues si los hubiera, el lado derecho sería divisible por 4, lo que no sucede con el lado izquierdo. Así que como máximo solo hay un primo impar.

Para el caso en el que existe un primo impar, $2p_2 = x(p_2 - 1)$ donde p_2 es impar. Luego existe $y \in \mathbb{Z}^+$ tal que $p_2 - 1 = 2y$ y la igualdad queda reducida a $p_2 = xy$ con $x \neq 1$ pues si $x = 1$ entonces $\varphi(n) = n$ lo cual es una contradicción pues $\varphi(n) < n$ para $n \geq 2$. Luego $y = 1$ y $x = p_2$, de donde se tiene que $p_2 - 1 = 2$ y por lo tanto $p_2 = 3$.

Luego si $\varphi(n)|n$ para $n \geq 2$ entonces $n = 2^{\alpha_1}3^{\alpha_2}$, con $\alpha_1 \geq 1$ y $\alpha_2 \geq 0$. Por el contrario si $n = 2^{\alpha_1}3^{\alpha_2}$ con $\alpha_1 \geq 1$ y $\alpha_2 \geq 0$ se tiene que $\varphi(n) = 2^{\alpha_1 - 1}$ si $\alpha_2 = 0$ y $\varphi(n) = 2^{\alpha_1}3^{\alpha_2}\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 2^{\alpha_1}3^{\alpha_2 - 1}$ si $\alpha_2 \geq 1$. En ambos casos se tiene que $\varphi(n)|n$. □

2.3. Desigualdades

Ejercicio 2.20. Demostrar que si los enteros positivos m y n no son primos relativos entonces $\varphi(m)\varphi(n) < \varphi(mn)$.

Demostración. Consecuencia inmediata del lema 2.1. □

Ejercicio 2.21. Sean $n, m \in \mathbb{Z}^+$ con $n > 1$. Demostrar que: $\varphi(nm) = \varphi(m)$ sii $n = 2$ y m es impar.

Demostración.
⇒)

i) Si $(n, m) \neq 1$, entonces por el ejercicio 2.20 se tiene que $\varphi(n)\varphi(m) \leq \varphi(nm) = \varphi(m)$, de donde se tiene que $\varphi(n) < 1$, lo cual claramente es una contradicción. Luego $(n, m) = 1$, es decir $\varphi(nm) = \varphi(n)\varphi(m)$. Como $\varphi(nm) = \varphi(m)$, entonces $\varphi(n)\varphi(m) = \varphi(m)$ y por lo tanto $\varphi(n) = 1$. Luego, como $n > 1$, $n = 2$.

ii) Supongamos que m es par, es decir existen $\alpha, r \in \mathbb{Z}^+$ tales que $m = 2^{\alpha}r$. Es claro entonces que
$$\varphi(2m) = 2^{\alpha}\varphi(r) > 2^{\alpha - 1}\varphi(r) = \varphi(m),$$
lo cual es una contradicción. Por lo tanto m debe ser impar.

⇐) Si $n = 2$ y m es impar, entonces
$$\varphi(nm) = \varphi(2m) = \varphi(2)\varphi(m) = 1\varphi(m) = \varphi(m).$$

□

Ejercicio 2.22. Sea $n \in \mathbb{Z}^+$, demostrar que
$$\varphi(2n) = \begin{cases} \varphi(n), & \text{si } n \text{ es par} \\ 2\varphi(n), & \text{si } n \text{ es impar.} \end{cases}$$

Demostración. El caso para n par se deduce del ejercicio anterior. Para n impar utilizar la misma idea que se utilizó en ii) en la demostración del ejercicio anterior. □

Lema 2.23. *Sean $a, b \in \mathbb{Z}^+$, entonces $\varphi(ab) \leq a\varphi(b)$.*

Demostración. Si a o b es igual a 1, la desigualdad es evidente (de hecho se tiene la igualdad). Si $a > 1$ y $b > 1$, entonces

$$\varphi(ab) = ab \prod_{p|ab} \left(1 - \frac{1}{p}\right) \leq ab \prod_{p|a} \left(1 - \frac{1}{p}\right) = a\varphi(b).$$

□

Ejercicio 2.24. Demostrar que si $d|n$ y $1 \leq d < n$, entonces $n - \varphi(n) > d - \varphi(d)$.

Demostración. Vemos que

$$\begin{aligned} n &= \sum_{a|n} \varphi(a) \\ &= \sum_{\substack{a|d \\ 1 \leq d < n}} \varphi(a) + \varphi(d) + \cdots + \varphi(n) \\ &= (d - \varphi(d)) + \varphi(d) + \cdots + \varphi(n) \\ &> (d - \varphi(d)) + \varphi(n). \end{aligned}$$

Por lo tanto $n - \varphi(n) > d - \varphi(d)$. □

Ejercicio 2.25. Demostrar que $\varphi(n^a) > n^{a-1}$ para $n > 2$ y a entero positivo.

Demostración. La desigualdad buscada $\varphi(n^a) > n^{a-1}$ es equivalente a las siguientes desigualdades:

$$\begin{aligned} n^a \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) > n^{a-1} &\iff n \prod_{i=1}^{m} \left(\frac{p_i - 1}{p_i}\right) > 1 \\ &\iff \frac{\prod_{i=1}^{m}(p_i - 1)}{p_1 p_2 \cdots p_m} > \frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}} \end{aligned}$$

donde $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ es la factorización de n como producto de primos. Es claro que esta última desigualdad se tiene para $n > 2$. □

Lema 2.26. *Sea n un entero con $n \geq 2$ y p_1 el menor primo que divide a n. Se tiene entonces que $p_1 \leq n^{1/\omega(n)}$, donde la igualdad solo se tiene si n es primo ($n = p_1$).*

Demostración. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ $(\omega(n) = m)$. Vemos que

$$p_1^{\omega(n)} = \underbrace{p_1 p_1 \cdots p_1}_{m\text{veces}} \leq p_1 p_2 \cdots p_m \leq p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} = n,$$

donde es claro que ambas igualdades se tienen al mismo tiempo solo cuando $n = p_1$. □

Ejercicio 2.27. Sea n un entero con $n \geq 2$. Demostrar que $\varphi(n) \leq n - n^{1-\frac{1}{\omega(n)}}$, donde la igualdad solo ocurre si n es primo.

Demostración. Sea p_1 el menor primo que divide a n. Luego

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \leq n \left(1 - \frac{1}{p_1}\right) = n - \frac{n}{p_1} \leq n - \frac{n}{n^{1/\omega(n)}},$$

donde la última desigualdad se debe al lema 2.26. Es claro además que las igualdades solo se tiene si n es primo. □

Ejercicio 2.28. Demostrar que si n es un número compuesto, entonces $\varphi(n) \leq n - \sqrt{n}$. Donde la igualdad solo se tiene si $n = p^2$ para algún primo p.

Demostración. Sea p_1 el menor primo que divide a n. Si $\omega(n) = 1$ entonces $n = p_1^{\alpha}$ con $\alpha \geq 2$, y por lo tanto $p_1 \leq n^{1/\alpha} \leq \sqrt{n}$. Si $\omega(n) \geq 2$ entonces, por el lema 2.26, tenemos que $p_1 \leq n^{1/\omega(n)} \leq \sqrt{n}$. En ambos casos llegamos a que $\frac{1}{p_1} \geq \frac{1}{\sqrt{n}}$. Vemos entonces que

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

Es claro además que la igualdad solo se tiene si $n = p_1^2$. □

Ejercicio 2.29. Demostrar que para n entero positivo, se tiene que $\varphi(n) \geq \frac{n}{2^{\omega(n)}}$. Donde la igualdad solo se tiene para $n = 2^{\alpha}$ con $\alpha \geq 0$.

Demostración. Si $n = 1$ es claro que se tiene la igualdad. Para $n \geq 2$ vemos que

$$\frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right) \geq \prod_{p|n} \left(1 - \frac{1}{2}\right) = \prod_{p|n} \left(\frac{1}{2}\right) = \frac{1}{2^{\omega(n)}}.$$

Se ve claramente que la igualdad solo se tiene si $n = 2^{\alpha}$ con $\alpha \geq 0$. □

Lema 2.30. *Sea $f : \mathbb{N} \longrightarrow \mathbb{R}^+$ y $F(n) = \sum_{d|n} f(d)$. Demostrar que para todo entero positivo n,*

$$\prod_{d|n} f(d) \leq \left(\frac{F(n)}{\tau(n)}\right)^{\tau(n)}.$$

Demostración. Utilizando la desigualdad entre media geométrica y media aritmética, tenemos que

$$\left(\prod_{d|n} f(d)\right)^{1/\tau(n)} \leq \frac{1}{\tau(n)} \sum_{d|n} f(d).$$

De donde es claro que se tiene el teorema. □

Ejercicio 2.31. Demostrar que para todo entero positivo n, se tiene que

$$\prod_{d|n} \varphi(d) \leq \left(\frac{n}{\tau(n)}\right)^{\tau(n)}.$$

Demostración. Utilizar el lema anterior con $f = \varphi$. □

2.4. Solución de Ecuaciones

Ejercicio 2.32. Demostrar que hay infinitos números pares k tales que la ecuación $\varphi(n) = k$ no tiene solución.

Demostración. Demostraremos que si $k = 2 \cdot 7^r$ con $r \in \mathbb{Z}^+$ entonces $\varphi(n) = k$ no tiene solución. Supongamos que existe n tal que $\varphi(n) = 2 \cdot 7^r$. Es claro que $n = 1$ no puede ser, luego $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, de donde se tiene que

$$2 \cdot 7^r = \varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_m^{\alpha_m - 1} = (p_1 - 1)(p_2 - 1) \cdots (p_m - 1) \qquad (1)$$

En (1) se observa que si de $p_1, p_2, \ldots, p_m$ hay al menos dos primos impares, entonces el lado derecho sería divisible por 4 y el lado izquierdo no. Luego n es de la forma $n = 2^\alpha$, $n = 2^\alpha p^\beta$ o $n = p^\beta$ con p primo impar. Es claro que no se puede tener $n = 2$ o $n = 2^2$ pues $\varphi(2) = 1$ y $\varphi(4) = 2$. Si $n = 2^\alpha$ o $n = 2^\alpha p^\beta$ con $\alpha \geq 3$ entonces otra vez en (1) se observa que el lado derecho es divisible por 4 y el izquierdo no.

Si $n = p$ entonces $\varphi(n) = p - 1 = 2 \cdot 7^r$, de donde $p = 2 \cdot 7^r + 1$. Pero $2 \cdot 7^r + 1$ es divisible por 3 pues $2 \cdot 7^r \equiv 2 \cdot 1^r \equiv 2 \equiv -1 \bmod 3$ de donde se llega a una contradicción. Si $n = p^\beta$ con $\beta > 1$ entonces $\varphi(n) = p^{\beta-1}(p-1) = 2 \cdot 7^r$, luego $p = 7$. Es claro entonces que se llega a una contradicción pues $7^{\beta-1} \cdot 6 \neq 2 \cdot 7^r$.

Los unicos casos que faltan son $n = 2^\alpha p^\beta$ con $\alpha = 1$ o $\alpha = 2$ y $\beta \geq 1$. En estos casos se tiene que $\varphi(n) = 2^{\alpha-1} p^{\beta-1}(p-1) = 2 \cdot 7^r$, luego $p = 7$ de donde $2^{\alpha-1} 7^{\beta-1} 6 = 2 \cdot 7^r$, lo cual es una contradicción. □

Ejercicio 2.33 (The American Mathematical Monthly, Problema E2317, [29]). Encontrar todas las parejas de enteros positivos m, n tales que $\varphi(mn) = \varphi(m) + \varphi(n)$.

Solución. Sea $\varphi(mn) = \varphi(m) + \varphi(n)$. Sea $(m, n) = d$, sabemos que

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

de donde se tiene que

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

Sean $a = \frac{\varphi(m)}{\varphi(d)}$ y $b = \frac{\varphi(n)}{\varphi(d)}$ (a y b son enteros positivos debido al lema 2.13), luego

$$\frac{1}{a} + \frac{1}{b} = \frac{\varphi(d)}{\varphi(m)} + \frac{\varphi(d)}{\varphi(n)} = \frac{\varphi(d)\left[\varphi(m) + \varphi(n)\right]}{\varphi(m)\varphi(n)} = \frac{\varphi(d)\varphi(mn)}{\varphi(m)\varphi(n)} = d.$$

Como $a, b, d \in \mathbb{Z}^+$, entonces la ecuación $\frac{1}{a} + \frac{1}{b} = d$ solo tiene solución si $a = b = 1$ y $d = 2$ o cuando $a = b = 2$ y $d = 1$. En el primer caso se tiene que $\varphi(m) = \varphi(n) = 1$, de donde $m = n = 2$. En el segundo caso se tiene que $\varphi(m) = \varphi(n) = 2$, de donde $m = 3$ y $n = 4$ o $m = 4$ y $n = 3$. Es decir $\langle m, n\rangle = \langle 2, 2\rangle, \langle 3, 4\rangle$ o $\langle 4, 3\rangle$. Por otro lado verificando estos valores comprobamos que todos cumplen que $\varphi(mn) = \varphi(m)+\varphi(n)$. *Respuesta:* $\langle 2, 2\rangle, \langle 3, 4\rangle, \langle 4, 3\rangle$. □

Lema 2.34. *Sean $n \geq 2$, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ su factorización como producto de primos y*

$$x = \frac{n^2}{\varphi(n)} = \prod_{i=1}^{m} \frac{p_i^{\alpha_i+1}}{p_i - 1},$$

entonces x es un entero con exactamente los mismos divisores primos que n sii $\prod_{i=1}^{m}(p_i - 1)|n$.

Demostración.

$\Rightarrow$) Sea

$$x = \prod_{i=1}^{m} \frac{p_i^{\alpha_i+1}}{p_i - 1} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m} \qquad \beta_i \geq 1, \forall i.$$

Es claro que $n = p_1^{\beta_1-1} p_2^{\beta_2-1} \cdots p_m^{\beta_m-1} \prod_{i=1}^{m}(p_i - 1)$, de donde se tiene que $\prod_{i=1}^{m}(p_i - 1)|n$.

$\Leftarrow$) Si $\prod_{i=1}^{m}(p_i - 1)|n$ entonces $\prod_{i=1}^{m} \frac{p_i^{\alpha_i}}{p_i-1}$, es un entero de la forma $p_1^{c_1} p_2^{c_2} \cdots p_m^{c_m}$ con $c_i \geq 0$, $\forall i$. Es claro entonces que x es un entero con exactamente los mismos divisores primos que n. □

Lema 2.35. *Sea $n \geq 2$ con $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ y x un entero positivo con exactamente los mismos divisores primos que n, entonces $\varphi(x) = n$ sii*

$$x = \frac{n^2}{\varphi(n)} = \prod_{i=1}^{m} \frac{p_i^{\alpha_i+1}}{p_i - 1}.$$

Demostración.

$\Rightarrow$) Si $\varphi(x) = n$, como x tiene los mismos divisores primos que n entonces

$$\varphi(x) = x \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right),$$

de donde se tiene que $\frac{\varphi(x)}{x} = \frac{\varphi(n)}{n}$ y por lo tanto $x = \frac{n^2}{\varphi(n)}$.

$\Leftarrow$) Si $x = \frac{n^2}{\varphi(n)}$, como x tiene los mismos divisores primos que n entonces

$$\begin{aligned}
\varphi(x) &= x \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) \\
&= \prod_{i=1}^{m} \left(\frac{p_i^{\alpha_i+1}}{p_i - 1}\right) \prod_{i=1}^{m} \left(\frac{p_i - 1}{p_i}\right) \\
&= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \\
&= n.
\end{aligned}$$

□

Ejercicio 2.36 (The American Mathematical Monthly, Problema 4221, [18]). Demostrar que para todo $k \in \mathbb{Z}^+$, la ecuación $\varphi(x) = k!$ es soluble.

Demostración. Para $k = 1$ es claro que se tiene. Para $k > 1$ hacemos $n = k! = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Es claro $\prod_{i=1}^{m}(p_i - 1) | k! = n$. Por el lema 2.34 obtenemos que $x = \frac{n^2}{\varphi(n)}$ es un entero con exactamente los mismos divisores primos que n, y por el lema 2.35 obtenemos que $\varphi(x) = n = k!$.

Observación. Utilizando la misma idea se tiene que para $k, s \in \mathbb{Z}^+$, la ecuación $\varphi(x) = (k!)^s$ es soluble.

□

Lema 2.37. *Para m entero postivo, se tiene que $m \leq 2^{m-1}$, donde la igualdad solo se tiene para $m = 1$ y $m = 2$.*

Demostración. Demostraremos por inducción que $m \leq 2^{m-1}$ para $m > 2$. Es claro que se tiene para $m = 3$. Supongamos que se cumple para m (> 2) y probemos que se tiene para $m + 1$. Por hipótesis de inducción tenemos que $m < 2^{m-1}$, además es claro que $1 < 2^{m-1}$, luego $m + 1 < 2^{m-1} + 2^{m-1} = 2\left(2^{m-1}\right) = 2^m = 2^{(m+1)-1}$. □

Corolario 2.38. *Para n y m enteros positivos con $n > 2$, se tiene que $n^{m-1} > m$.*

Ejercicio 2.39 (The American Mathematical Monthly, E1576, [22]). Encontrar todas las parejas de enteros positivos $\langle n, s \rangle$ tales que $n^{\varphi(s)} = s$.

Solución. Supongamos que se cumple $n^{\varphi(s)} = s$ para alguna pareja $\langle n, s\rangle$ con $n > 2$. Sea $\varphi(s) = m$, se tiene entonces, por el ejercicio 2.25, que $m = \varphi\left(n^{\varphi(s)}\right) > n^{\varphi(s)-1} = n^{m-1}$, contradiciendo el anterior corolario. Luego solo debemos verificar para enteros positivos $n \leq 2$. Para $n = 1$ es claro que solo se tiene para $\langle n, s\rangle = \langle 1, 1\rangle$. Para $n = 2$ es claro que si $2^{\varphi(s)} = s$, entonces $\varphi\left(2^{\varphi(s)}\right) = \varphi(s)$ y por lo tanto $\varphi(s) = 2^{\varphi(s)-1}$, de donde se tiene que $\varphi(s) = 1$ o $\varphi(s) = 2$, es decir $s = 1, 2, 3$ o 5. Comprobando los casos se ve que solo se tiene para $\langle n, s\rangle = \langle 2, 2\rangle$ y $\langle 2, 4\rangle$. □

2.5. Ejercicios Adicionales

Teorema 2.40. *Para $b \in \mathbb{Z}^+$ (fijo) se tiene que el número de fracciones irreducibles $\frac{a}{b}$ ($(a, b) = 1$) con $0 < \frac{a}{b} \leq 1$, es $\varphi(b)$.*

Demostración. Dado que la condición $0 < \frac{a}{b} \leq 1$ es equivalente a la condición $1 < a \leq b$, se tiene que

$$\#\left\{a \mid 0 < \frac{a}{b} \leq 1, (a, b) = 1\right\} = \#\left\{a \mid 1 < a \leq b, (a, b) = 1\right\} = \varphi(b).$$

□

Ejercicio 2.41. Demostrar que hay infinitos enteros positivos n tales que $\varphi^2(n) + n^2$ es un cuadrado perfecto.

Demostración. Sean $\alpha, \beta \geq 1$, sabemos que

$$\begin{aligned}\varphi\left(3^\alpha 5^\beta\right) &= \varphi(3^\alpha)\varphi(5^\beta)\\ &= \left[3^{\alpha-1}(3-1)\right]\left[5^{\beta-1}(5-1)\right]\\ &= 8 \cdot 3^{\alpha-1}5^{\beta-1}.\end{aligned}$$

De donde tenemos que para $n = 3^\alpha 5^\beta$ con $\alpha, \beta \geq 1$

$$\begin{aligned}\varphi^2(n) + n^2 &= \left(8 \cdot 3^{\alpha-1}5^{\beta-1}\right)^2 + \left(3^\alpha 5^\beta\right)^2\\ &= \left(3^{\alpha-1}5^{\beta-1}\right)^2\left(8^2 + 15^2\right)\\ &= \left(3^{\alpha-1}5^{\beta-1}\right)^2\left(17^2\right)\\ &= \left(17 \cdot 3^{\alpha-1}5^{\beta-1}\right)^2.\end{aligned}$$

□

Ejercicio 2.42 (The American Mathematical Monthly, Problema 3122, [4]). Para $n > 1$ entero, sea $\frac{P(n)}{Q(n)}$ la fracción reducida a su mínima expresión que representa el menor valor de $\frac{\varphi(m)}{m}$ para $0 < m < n$. Es decir

$$\frac{P(n)}{Q(n)} = \min\left\{\frac{\varphi(m)}{m} : 0 < m < n\right\}, \text{donde } (P(n), Q(n)) = 1.$$

Demostrar que $P(n)$ es de la forma $2^a 3^b$ $(a, b \geq 0)$ para $1 < n < 2 \cdot 10^{11}$.

Demostración. Es claro que $m = 1$ no puede ser el menor valor que tome $\frac{\varphi(m)}{m}$, de hecho para $m = 1$ es el máximo valor que se tiene.

Para $m > 1$ se tiene que

$$\frac{\varphi(m)}{m} = \prod_{p|m} \left(1 - \frac{1}{p}\right),$$

luego si $m' = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ y $m'' = p_1 p_2 \cdots p_k$ entonces $\frac{\varphi(m')}{m'} = \frac{\varphi(m'')}{m''}$, de donde podemos restringir la busqueda a aquellos valores de m que son libres de cuadrados.

Sea $m = 2 \cdot 3 \cdot 5 \cdots p$, el producto de los primos $\leq p$ donde p también es primo. Si omitimos en la factorización de m algunos de los primos $\leq p$, es claro que obtenemos un mayor valor de $\frac{\varphi(m)}{m}$, del mismo modo obtenemos un valor mayor para $\frac{\varphi(m)}{m}$ si reemplazamos m como el producto de un solo primo $\bar{p}$ mayor que p ($m = \bar{p}$). Luego es claro que debemos reducir nuestra búsqueda solamanete a los números que sean de la forma $m = 2 \cdot 3 \cdot 5 \cdots p$ con p primo y por supuesto $0 < m < n$. Sean m_1 y m_2 dos enteros positivos menores que n que sean de la forma anteriormente mencionada, es decir, suponiendo $m_1 < m_2$,

$$\begin{aligned} m_1 &= 2 \cdot 3 \cdot 5 \cdots p_1 \\ m_2 &= 2 \cdot 3 \cdot 5 \cdots p_1 p_2 p_3 \cdots p_k. \end{aligned}$$

Se tiene entonces que

$$\frac{\varphi(m_2)}{m_2} = \frac{\varphi(m_1)}{m_1} \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) < \frac{\varphi(m_1)}{m_1}.$$

Luego es claro que el menor valor de $\frac{\varphi(m)}{m}$ se tiene cuando $m = 2 \cdot 3 \cdot 5 \cdots p$ donde p es el mayor primo para el que se sigue teniendo que $m < n$. Es claro que para ese valor de m se tiene que

$$\frac{\varphi(m)}{m} = \left(\frac{2-1}{2}\right)\left(\frac{3-1}{3}\right)\left(\frac{5-1}{5}\right) \cdots \left(\frac{p-1}{p}\right),$$

de donde $\varphi(m) = \prod_{q \leq p}(q-1) = 2 \cdot 4 \cdot 6 \cdot 10 \cdots (p-1)$, donde el producto se hace a través de todos los primos q menores que p. Factorizando $\varphi(m)$ como producto de primos, se observa que el primer primo que se repite diferente al 2 y al 3 es el 5 y ocurre cuando $p = 31$, luego es claro que $P(n) = 2^a 3^b$ siempre que $n \leq 2 \cdot 3 \cdot 5 \cdots 29 \cdot (31-1)$, donde este último producto es mayor que $2 \cdot 10^{11}$. □

Capítulo 3

Las Funciones σ_λ, σ y τ

El presente capítulo tiene como proposito mostrar las principales propiedades que posee la funciones σ_λ, σ y τ.

3.1. Identidades

Lema 3.1. *Para n entero positivo se tiene que*

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

Demostración. Si d recorre todos los divisores de n, entonces n/d también lo hace, luego

$$\begin{aligned} \frac{\sigma(n)}{n} &= \sum_{d|n} \frac{d}{n} \\ &= \sum_{d|n} \frac{1}{n/d} \\ &= \sum_{d|n} \frac{1}{d} \end{aligned}$$

□

Observación. Una leve modificación a la demostración anterior nos lleva a la siguiente identidad

$$\frac{\sigma_z(n)}{n^z} = \sum_{d|n} \frac{1}{d^z}, \qquad \forall z \in \mathbb{C}.$$

Lema 3.2. *La sucesión $\frac{\sigma(n)}{n}$ no está acotada.*

Demostración. Por el lema anterior sabemos que

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

Tomando la subsucesión $\frac{\sigma(n!)}{n!}$, vemos que

$$\begin{aligned} \frac{\sigma(n!)}{n!} &= \sum_{d|n!} \frac{1}{d} \\ &\geq \sum_{k=1}^{n} \frac{1}{k} \end{aligned}$$

Sabemos de los cursos de cálculo que $\sum_{k=1}^{n} \frac{1}{k}$ es una sucesión no acotada, luego la subsucesión $\frac{\sigma(n!)}{n!}$ no es acotada y por lo tanto $\frac{\sigma(n)}{n}$ tampoco lo es. □

En especial el lema 3.1 es un caso especial del siguiente teorema cuando se toma $a = 1$.

Teorema 3.3. *Sea $a \in \mathbb{R}$, entonces para todo $n \in \mathbb{Z}^+$ se tiene que*

$$\sigma_{-a}(n) = n^{-a}\sigma_a(n).$$

Demostración.

$$\sigma_{-a}(n) = \sum_{d|n} d^{-a} = n^{-a} \sum_{d|n} \left(\frac{n}{d}\right)^a = n^{-a} \sum_{d|n} d^a = n^{-a}\sigma_a(n).$$

□

Lema 3.4. *Para todo entero positivo n se tiene que*

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

Demostración.

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

Luego

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

□

Ejercicio 3.5. Demostrar que

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

Demostración.

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{1}{2^n - 1} &= \sum_{n=1}^{\infty} \left(\frac{1}{2^n} \cdot \frac{1}{1 - \left(\frac{1}{2}\right)^n} \right) \\
&= \sum_{n=1}^{\infty} \frac{1}{2^n} \left(1 + \frac{1}{2^n} + \frac{1}{2^{2n}} + \cdots \right) \\
&= \sum_{n=1}^{\infty} \left(\frac{1}{2^n} + \frac{1}{2^{2n}} + \frac{1}{2^{3n}} \cdots \right) \\
&= \sum_{d_1=1}^{\infty} \sum_{d_2=1}^{\infty} \frac{1}{2^{d_1 d_2}} \\
&= \sum_{n=1}^{\infty} \frac{1}{2^n} \left(\sum_{d_1 d_2 = n} 1 \right) \\
&= \sum_{n=1}^{\infty} \frac{\tau(n)}{2^n}.
\end{aligned}$$

□

Ejercicio 3.6. Sean $n \in \mathbb{Z}^+$ y α el mayor entero tal que $2^\alpha | n$. Demostrar que

$$\frac{\tau(2n)}{\tau(n)} = \frac{\alpha + 2}{\alpha + 1}.$$

Demostración. Sea $n = 2^\alpha m$ con m impar. Tenemos que

$$\tau(2n) = \tau\left(2^{\alpha+1} m\right) = \tau\left(2^{\alpha+1}\right) \tau(m) = (\alpha + 2)\tau(m) \tag{1}$$

y que

$$\tau(n) = \tau\left(2^\alpha m\right) = \tau\left(2^\alpha\right) \tau(m) = (\alpha + 1)\tau(m). \tag{2}$$

Dividiendo (1) y (2) obtenemos el resultado buscado. □

Observación. De forma análoga si n lo expresamos de la forma $n = 2^\alpha m$ con m impar y α entero no negativo, y si además α_1, α_2 son enteros no negativos, se tiene que

$$\frac{\tau\left(2^{\alpha_1} n\right)}{\tau\left(2^{\alpha_2} n\right)} = \frac{\alpha + \alpha_1 + 1}{\alpha + \alpha_2 + 1}.$$

Ejercicio 3.7. Demostrar que

$$\left(\sum_{d|n}\tau(d)\right)^2 = \sum_{d|n}\tau^3(d).$$

Demostración. Por el lema 1.10 y por el corolario 1.14, se tiene que ambos lados de la ecuación son funciones multiplicativas, luego es suficiente con probar la identidad para $n = p^\alpha$ con p primo y $\alpha \in \mathbb{Z}^+$.
Por un lado

$$\begin{aligned}\left(\sum_{d|n}\tau(d)\right)^2 &= \big(\tau(1)+\tau(p)+\tau(p^2)+\cdots+\tau(p^\alpha)\big)^2\\ &= (1+2+3+\cdots+(\alpha+1))^2\\ &= \left[\frac{(\alpha+1)(\alpha+2)}{2}\right]^2.\end{aligned}$$

Por el otro lado

$$\begin{aligned}\sum_{d|n}\tau^3(d) &= \tau^3(1)+\tau^3(p)+\tau^3(p^2)+\cdots+\tau^3(p^\alpha)\\ &= 1^3+2^3+3^3+\cdots+(\alpha+1)^3\\ &= \left[\frac{(\alpha+1)(\alpha+2)}{2}\right]^2.\end{aligned}$$

□

Ejercicio 3.8 (The American Mathematical Monthly, Problema E1850, [37]). Demostrar que

$$\sigma(n) = \sum_{m=1}^{n}\int_0^m \cos\left(\frac{2\pi n\,\lfloor x+1\rfloor}{m}\right)dx = \sum_{m=1}^{n}\sum_{k=1}^{m}\cos k\left(\frac{2\pi n}{m}\right).$$

Demostración. Tenemos que

$$\int_0^m \cos\left(\frac{2\pi n\,\lfloor x+1\rfloor}{m}\right)dx = \sum_{k=1}^{m}\int_{k-1}^{k}\cos k\left(\frac{2\pi n}{m}\right)dx = \sum_{k=1}^{m}\cos k\left(\frac{2\pi n}{m}\right).$$

Utilizando el hecho de que

$$\sum_{k=1}^{m}\cos kx = \frac{\cos\left(\frac{m+1}{2}x\right)\sin\left(\frac{mx}{2}\right)}{\sin\frac{x}{2}},$$

vemos que

$$\sum_{k=1}^{m} \cos k\left(\frac{2\pi n}{m}\right) = \frac{cos\left(\frac{\pi(m+1)n}{m}\right)\sin(\pi n)}{\sin\left(\frac{\pi n}{m}\right)}. \tag{1}$$

Si $m \nmid n$ se tiene que en (1) el numerador es 0 y el denominador diferente a 0. Luego

$$\sum_{k=1}^{m} \cos k\left(\frac{2\pi n}{m}\right) = 0.$$

Si $m|n$ tenemos entonces una expresión indeterminada. Utilizando L'Hopital obtenemos que

$$\begin{aligned}\sum_{k=1}^{m} \cos k\left(\frac{2\pi n}{m}\right) &= \frac{\frac{-\pi(m+1)}{m}\sin\left(\frac{\pi(m+1)n}{m}\right)\sin(\pi n) + \pi\cos\left(\frac{\pi(m+1)n}{m}\right)\cos(\pi n)}{\frac{\pi}{m}\cos\left(\frac{\pi n}{m}\right)} \\ &= \frac{m\cos\left(\frac{\pi(m+1)n}{m}\right)\cos(\pi n)}{\cos\left(\frac{\pi n}{m}\right)}.\end{aligned}$$

i) Si n es impar, entonces m es impar, luego $\cos(\pi n) = \cos\left(\frac{\pi n}{m}\right) = -1$ y $\cos\left(\frac{\pi(m+1)n}{m}\right) = 1$, de donde

$$\sum_{k=1}^{m} \cos k\left(\frac{2\pi n}{m}\right) = m.$$

ii) Si n es par y m impar entonces $\cos(\pi n) = \cos\left(\frac{\pi n}{m}\right) = \cos\left(\frac{\pi(m+1)n}{m}\right) = 1$, de donde

$$\sum_{k=1}^{m} \cos k\left(\frac{2\pi n}{m}\right) = m.$$

iii) Si n, m y $\frac{n}{m}$ son pares entonces $\cos(\pi n) = \cos\left(\frac{\pi n}{m}\right) = \cos\left(\frac{\pi(m+1)n}{m}\right) = 1$, de donde

$$\sum_{k=1}^{m} \cos k\left(\frac{2\pi n}{m}\right) = m.$$

iv) Si n y m son pares y $\frac{n}{m}$ es impar entonces $\cos(\pi n) = \cos\left(\frac{\pi n}{m}\right) = \cos\left(\frac{\pi(m+1)n}{m}\right) = -1$, de donde

$$\sum_{k=1}^{m} \cos k\left(\frac{2\pi n}{m}\right) = m.$$

Se tiene entonces que

$$\int_0^m \cos\left(\frac{2\pi n \lfloor x+1 \rfloor}{m}\right) dx = \begin{cases} m, & \text{si } m|n \\ 0, & \text{si } m \nmid n. \end{cases}$$

de donde se tiene que

$$\sigma(n) = \sum_{m=1}^{n} \int_0^m \cos\left(\frac{2\pi n \lfloor x+1 \rfloor}{m}\right) dx.$$

□

3.2. Divisibilidad

Teorema 3.9. *$\tau(n)$ es impar sii n es un cuadrado perfecto.*

Demostración 1. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, luego

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1).$$

Se tiene entonces que

$$\begin{aligned} \tau(n) \text{ es impar} &\iff \alpha_i + 1 \text{ es impar}, \forall i = 1, ..., m \\ &\iff \alpha_i \text{ es par}, \forall i = 1, ..., m \\ &\iff n \text{ es un cuadrado perfecto.} \end{aligned}$$

□

Demostración 2. Si n no es un cuadrado perfecto, se tiene que si d es un divisor de n, entonces n/d es un divisor diferente de n, pues si $d = n/d$ entonces $n = d^2$ sería un cuadrado perfecto. Luego los divisores se pueden agrupar en parejas, de donde se tiene que el número de estos tiene que ser par.

Si n es un cuadrado perfecto, entonces existe k entero y divisor de n tal que $n = k^2$, si d es un divisor de n diferente de k, entonces n/d es otro divisor de n diferente de d, asi que todos los divisores de n se pueden agrupar en parejas, a escepción de k, de donde se tiene que el número de estos divisores tiene que ser impar. □

Teorema 3.10. *Sea $n \in \mathbb{Z}^+$,*

1) Si $n = 1$ entonces $\sigma(n)$ es impar.

2) Si $n = 2^\alpha$ con $\alpha \in \mathbb{Z}^+$ entonces $\sigma(n)$ es impar.

3) Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ con α_i par para todos los i tales que p_i es impar entonces $\sigma(n)$ es impar.

4) Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ y $\exists i$ (entre 1 y m) con p_i y α_i impares entonces $\sigma(n)$ es par.

Demostración.

1) Evidente.

2) Sabemos que $\sigma(n) - 1 = 2 + 2^2 + \cdots + 2^\alpha$ es par, luego $\sigma(n)$ es impar.

3) Sea p un primo impar y α par, entonces $\sigma(p) - 1 = p + p^2 + \cdots + p^\alpha$ es par pues se están sumando un número par (α) de términos impares $(p, p^2, \ldots, p^\alpha)$, luego $\sigma(p)$ es impar.

   Si $p_1 = 2$ entonces $\sigma(n) = \sigma(2^{\alpha_1})\sigma(p_2^{\alpha_2}) \cdots \sigma(p_m^{\alpha_m})$, el cual es un producto de impares. Si $p_i \neq 2\ \forall i = 1, \cdots, m$ entonces $\sigma(n) = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2}) \cdots \sigma(p_m^{\alpha_m})$ el cual también es producto de impares.

4) Sea i ente 1 y m tal que p_i es impar y α_i par, entonces $\sigma(p_i) = 1 + p + p^2 + \cdots + p^{\alpha_i}$ es par, pues se están sumando un número par $(\alpha_i + 1)$ de términos impares $(1, p, p^2, \ldots, p^{\alpha_i})$. Como $\sigma(p_i) | \sigma(n)$ entonces $\sigma(n)$ es par.

□

Ejemplo.
$\sigma(2^8)$ es impar por 2).
$\sigma(3^2 7^2 11^4)$ es impar por 3).
$\sigma(2^7 5^4 13^{12})$ es impar por 3).
$\sigma(5^6 7^3 19^5)$ es impar por 4).

De hecho el teorema anterior sigue siendo cierto si σ se cambia por σ_k con $k \in \mathbb{Z}^+$, su demostración es idéntica. Es importante resaltar que k tiene que ser entero positivos pues para cualquier otro tipo de valor, el teorema no sigue siendo cierto. Podemos resumir esto con el siguiente corolario.

Corolario 3.11. *Sean $n = p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_m^{\alpha_m}$ y $k \in \mathbb{Z}^+$, entonces $\sigma_k(n)$ es par sii $\exists i$ (entre 1 y m) tal que p_i y α_i son impares.*

Otra forma de escribir el corolario anterior es la siguiente

Corolario 3.12. *Sean n y k enteros positivos, entonces $\sigma_k(n)$ es impar sii n es un cuadrado perfecto o dos veces un cuadrado perfecto.*

Teorema 3.13. *Sean $n \geq 2$, entonces $\sigma(n) = 2^k$ para algún $k \in \mathbb{Z}^+$ sii n es libre de cuadrados y sus factores primos son primos de Mersenne.*

Demostración. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, luego

$$\sigma(n) = \prod_{i=1}^{m} (1 + p_1 + \cdots + p_1^{\alpha_1}) \tag{1}$$

$\Rightarrow$) Como $\sigma(n) = 2^k$ para algún $k \in \mathbb{Z}^+$ entonces si p es un primo divisor de n entonces por (1) se tiene que $1 + p + ... + p^\alpha = 2^s$ para algún $s \in \mathbb{Z}^+$. Se tiene que α es impar pues de lo contrario $1 + p + ... + p^\alpha$ sería impar, sea $\alpha = 2q + 1$ con $q \in \mathbb{N}$.

Se tiene entonces que $(1 + p)(1 + p^2 + p^4 + \cdots + p^{2q}) = 2^s$ y por lo tanto

$$1 + p = 2^r \tag{2}$$

y

$$1 + p^2 + \cdots + (p^2)^q = 2^t \tag{3}$$

para algunos $r, t \in \mathbb{N}$.

Si $q > 0$ entonces $t > 0$ pues de lo contrario la igualdad en (3) no se tendría. Al ser $t > 0$, q tiene que ser impar, $q = 2v + 1$, pues de lo contrario $1 + p^2 + \cdots + (p^2)^q$ sería impar. Luego

$$(1 + p^2)\left[1 + (p^2)^2 + ... + (p^2)^v\right] = 2^t$$

de donde se tiene que $1+p^2 = 2^u$, para algún $u \in \mathbb{Z}^+$. Dado que $2^r = 1+p < 1+p^2 = 2^u$, se tiene que $2^r | 2^u$ es decir $1 + p | 1 + p^2$. Además $1 + p | 1 - p^2$ de donde se llega a que $1 + p | ((1 + p^2) + (1 - p^2)) = 2$.

Como $1 + p | 2$ entonces $1 + p \leq 2$ lo cual es una contradicción pues $1 + p \geq 1 + 2 = 3$. Se tiene entonces que $q = 0$ es decir n es libre de cuadrados. De (2) se tiene que todo factor primo de n es un primo de Mersenne.

$\Leftarrow$) Como n es libre de cuadrados y sus factores primos son primos de Mersenne entonces existen c_i's tales que $p_i = 2^{c_i} - 1$ y además $\alpha_i = 1$. De (1) se tiene que

$$\begin{aligned} \sigma(n) &= \prod_{i=1}^{m} 2^{c_i} \\ &= 2^k \end{aligned}$$

para algún $k \in \mathbb{Z}^+$. □

Ejercicio 3.14. Sea n un entero positivo tal que $\sigma(n)$ es primo. Demostrar que $\tau(n)$ también tiene que ser primo.

Demostración. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ tal que $\sigma(n)$ es primo. Sabemos que

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

de donde es claro que $m = 1$, pues si $m > 1$ entonces $\sigma(n)$ se puede escribir como el producto de m enteros diferentes de 1 y por lo tanto se contradice el hecho de que $\sigma(n)$ es primo. Luego n es de la forma $n = p^\alpha$ con p primo y $\alpha \in \mathbb{Z}^+$, por lo que basta demostrar nada más que $\tau\left(p^\alpha\right) = \alpha + 1$ es primo.

Supongamos que $\alpha + 1$ no es primo, es decir $\alpha + 1 = ab$ con $1 < a \leq b < \alpha + 1$. Observemos que

$$\begin{aligned}
\sigma(n) &= \sigma\left(p^\alpha\right) \\
&= \frac{p^{\alpha+1} - 1}{p - 1} \\
&= \frac{p^{ab} - 1}{p - 1} \\
&= \frac{p^a - 1}{p - 1}\left(p^{a(b-1)} + p^{a(b-2)} + \cdots + p^a + 1\right).
\end{aligned}$$

Es decir $\sigma(n)$ se puede expresar como el producto de dos enteros mayores que 1, obteniedose así una contradicción, pues $\sigma(n)$ es primo. Deducimos entonces que $\alpha+1$ es primo. □

Según la demostración del ejercicio anterior obtenemos el siguiente corolario.

Corolario 3.15. *Si $\sigma(n)$ es primo entonces $n = p^\alpha$ con p y $\alpha + 1$ primos.*

Ejercicio 3.16 (Putnam, 1969). Si $24|n + 1$ entonces $24|\sigma(n)$.

Demostración. Como $24|n + 1$, entonces $\exists k \in \mathbb{Z}^+$ tal que $n = 24k - 1$. Diremos que a y b son una pareja de divisores complementarios de n si $ab = n$. Con a y b pareja de divisores complementarios de n tenemos que

$$ab = n = 24k - 1 \tag{1}$$

De (1) se observa que ni a, ni b son divisibles por 2 ni por 3.
Sabemos que

$$\begin{aligned}
a(a + b) &= a^2 + ab \\
&= a^2 + 24k - 1 \\
&= (a - 1)(a + 1) + 24k.
\end{aligned} \tag{2}$$

Como a es impar, $a-1$ y $a+1$ son pares. Al ser dos pares consecutivos alguno tiene que ser divisible por 4. En general $(a-1)(a+1)$ es divisible por 8.

Como $a-1$, a y $a+1$ son enteros consecutivos alguno de estos debe ser divisible por 3. Sabemos que a no lo es, luego $3|(a-1)(a+1)$. Junto con el anterior resultado tenemos que $24|(a-1)(a+1)$ y en (2) se ve que $24|a(a+b)$. De (1) se observa también que a no es divisible por 24, luego $24|a+b$.

Veamos primero que n no puede ser un cuadrado perfecto. Si n es un cuadrado perfecto entonces $n = c^2$ para algún $c \in \mathbb{Z}^+$. Luego

$$\begin{aligned} c^2 &= 24k-1 \\ c^2-1 &= 24k-2 \\ (c-1)(c+1) &= 24k-2 \end{aligned}$$

Al ser $n+1$ par entonces n y por lo tanto c son impares. Por un argumento ya utilizado se puede llegar a que $(c-1)(c+1)$ es divisible por 8 lo cual es una contradicción pues $24k-2$ no es divisible por 8. Como n no puede ser un cuadrado perfecto, entonces $a \neq b$ para todas las parjas de divisores complementarios de n. Considerando a la pareja de divisores complementarios (a,b) igual que la pareja (b,a), es claro entonces que $\sigma(n) = \sum(a+b)$ donde (a,b) varía a través de todas las parejas de divisores complementarios de n. De donde es claro que $24|\sigma(n)$. □

3.3. Desigualdades

Ejercicio 3.17. Demostrar que para todo entero positivo n, se tiene que

$$2^{\omega(n)} \leq \tau(n) \leq 2^{\Omega(n)}.$$

Demostración. Para $n = 1$ es claro que se tiene. Para $n \geq 2$ vemos que como $2^{\omega(n)}, \tau(n)$ y $2^{\Omega(n)}$ son funciones multiplicativas, basta con demostrar la desigualdad para $n = p^\alpha$ con p primo y $\alpha \in \mathbb{Z}^+$. En este caso la desigualdad a demostrar queda reducida a $2 \leq \alpha+1 \leq 2^\alpha$, la cual es claramente cierta. □

Ejercicio 3.18. Demostrar que

$$\sigma(n) < n(1+\log n), \qquad \text{para } n \geq 2.$$

Demostración. Tenemos que

$$\begin{aligned} \frac{\sigma(n)}{n} &= \sum_{d|n} \frac{1}{d} \\ &\leq 1 + \frac{1}{2} + \cdots + \frac{1}{n} \\ &< 1 + \log n \end{aligned}$$

donde la última desigualdad se tiene para $n \geq 2$. Luego

$$\sigma(n) < n(1 + \log n), \qquad \text{para } n \geq 2.$$

□

Ejercicio 3.19 (The American Mathematical Monthly, Problema E1625, [7]). Demostrar que $\frac{\sigma(n)}{\tau(n)} \geq \sqrt{n}$.

Demostración. Para d divisor de n, tenemos que

$$\frac{d + \frac{n}{d}}{2} \geq \sqrt{d \cdot \frac{n}{d}} = \sqrt{n},$$

por la desigualdad entre media aritmética y media geométrica. Luego

$$\begin{aligned} \sum_{d|n} \left(\frac{d + \frac{n}{d}}{2} \right) &\geq \sum_{d|n} \sqrt{n} \\ \frac{\sigma(n) + \sigma(n)}{2} &\geq \tau(n)\sqrt{n} \\ \sigma(n) &\geq \tau(n)\sqrt{n} \\ \frac{\sigma(n)}{\tau(n)} &\geq \sqrt{n}. \end{aligned}$$

□

Ejercicio 3.20 (The American Mathematical Monthly, Problema E1749, [36]). Demostrar que $\frac{\sigma(n)}{\tau(n)} \leq \frac{2n}{3}$ para $n > 2$.

Demostración. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, vemos que

$$\frac{\sigma(n)}{n\tau(n)} = \frac{\prod_{i=1}^{m} (1 + p_i + \cdots + p_i^{\alpha_i})}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \prod_{i=1}^{m} (\alpha_i + 1)} = \prod_{i=1}^{m} \frac{1 + 1/p_i + \cdots + 1/p_i^{\alpha_i}}{\alpha_i + 1}.$$

Sabemos que $1 + 1/p_i + \cdots + 1/p_i^{\alpha_i} \leq \alpha_i + 1$, $\forall i = 1, ..., m$, de donde

$$\frac{1 + 1/p_i + \cdots + 1/p_i^{\alpha_i}}{\alpha_i + 1} \leq 1. \tag{1}$$

Como $n > 2$ entonces $p_i \geq 3$ $\forall i$ o $\exists \alpha_i$ tal que $\alpha_i \geq 2$ (pues de lo contrario $n \leq 2$). En el caso en que $\exists \alpha_i \geq 2$ se tiene por (1) que

$$\frac{\sigma(n)}{n\tau(n)} \leq \frac{1 + 1/2 + \cdots + 1/2^{\alpha_i}}{\alpha_i + 1} \leq \frac{\frac{1}{1-1/2}}{3} = \frac{2}{3}.$$

Solo basta probarlo para el caso en que $p_i \geq 3$ y $\alpha_i = 1$ $\forall i$. Para este caso, por (1), se tiene que

$$\frac{\sigma(n)}{n\tau(n)} \leq \frac{1 + 1/3}{2} = \frac{2}{3}.$$

□

Ejercicio 3.21.

a) Sea n un número compuesto, demostrar que $\sigma(n) > n + \sqrt{n}$.

b) Si p_n es el n-ésimo primo, demostrar que $\lim_{n\to\infty}(\sigma(p_n + 1) - \sigma(p_n)) = \infty$.

Demostración.

a) Sea d un divisor de n con $1 < d < n$, entonces $\frac{n}{d}$ también es un divisor de n y $1 < \frac{n}{d} < n$. Es claro que $d \geq \sqrt{n}$ o $\frac{n}{d} \geq \sqrt{n}$ pues si $d < \sqrt{n}$ y $\frac{n}{d} < \sqrt{n}$ entonces $n = d \cdot \frac{n}{d} < \sqrt{n}\sqrt{n} = n$, lo cual es una contradicción. Sin pérdida de generalidades podemos suponer que $d \geq \sqrt{n}$, luego

$$\sigma(n) \geq n + d + 1 \geq n + \sqrt{n} + 1 > n + \sqrt{n}.$$

b) Para $n \geq 2$ se tiene que

$$\sigma(p_n + 1) - \sigma(p_n) > (p_n + 1 + \sqrt{p_n + 1}) - (p_n + 1) = \sqrt{p_n + 1}.$$

Como $\lim_{n\to\infty} \sqrt{p_n + 1} = \infty$, entonces $\lim_{n\to\infty}(\sigma(p_n + 1) - \sigma(p_n)) = \infty$.

□

Lema 3.22. *Sean n y d enteros positivos, el número de múltiplos de d entre 1 y n es $\left\lfloor \frac{n}{d} \right\rfloor$ (O el número de enteros positivos menores o iguales que n, que son divisbles por d).*

Demostración. Un múltiplo de d entre 1 y n es de la forma $kd \leq n$ con k entero positivo. Es claro entonces que $k \leq \frac{n}{d}$, y como k es entero entonces $1 \leq k \leq \left\lfloor \frac{n}{d} \right\rfloor$. Así que la cantidad de múltiplos de d entre 1 y n es igual al número de enteros entre 1 y $\left\lfloor \frac{n}{d} \right\rfloor$, es decir igual a $\left\lfloor \frac{n}{d} \right\rfloor$. □

Ejercicio 3.23. Para n entero positivo, demostrar que

$$\sigma(1) + \sigma(2) + \cdots + \sigma(n) \leq n^2$$

Demostración. Consideremos la suma $\sigma(1) + \sigma(2) + \cdots + \sigma(n)$, es claro que en esta suma el 1 aparece $\left\lfloor \frac{n}{1} \right\rfloor$ veces, el 2 aparece $\left\lfloor \frac{n}{2} \right\rfloor$, ..., el n aparece $\left\lfloor \frac{n}{n} \right\rfloor$ veces, luego

$$\begin{aligned}\sigma(1) + \sigma(2) + \cdots + \sigma(n) &= 1\left\lfloor \frac{n}{1} \right\rfloor + 2\left\lfloor \frac{n}{2} \right\rfloor + \cdots + n\left\lfloor \frac{n}{n} \right\rfloor \\ &\leq 1 \cdot \frac{n}{1} + 2 \cdot \frac{n}{2} + \cdots + n \cdot \frac{n}{n} \\ &= n^2.\end{aligned}$$

□

Ejercicio 3.24 (Torneo de Matemáticas Harvard-MIT, 2004). Para n entero positivo, demostrar que

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

Demostración. Por el lema 3.1 sabemos que $\frac{\sigma(k)}{k}=\sum_{d|k}\frac{1}{d}$, luego la desigualdad a probar es equivalente a

$$\sum_{d|1}\frac{1}{d}+\sum_{d|2}\frac{1}{d}+\cdots+\sum_{d|n}\frac{1}{d}<2n.$$

En la suma, 1 aparece $\left\lfloor\frac{n}{1}\right\rfloor$ veces, $1/2$ aparece $\left\lfloor\frac{n}{2}\right\rfloor$ veces, ..., $1/n$ aparece $\left\lfloor\frac{n}{n}\right\rfloor$ veces, luego

$$\begin{aligned}\sum_{d|1}\frac{1}{d}+\sum_{d|2}\frac{1}{d}+\cdots+\sum_{d|n}\frac{1}{d}&=1\left\lfloor\frac{n}{1}\right\rfloor+\frac{1}{2}\left\lfloor\frac{n}{2}\right\rfloor+\cdots+\frac{1}{n}\left\lfloor\frac{n}{n}\right\rfloor\\&\leq\frac{1}{1}\cdot\frac{n}{1}+\frac{1}{2}\cdot\frac{n}{2}+\cdots+\frac{1}{n}\cdot\frac{n}{n}\\&=\frac{n}{1^2}+\frac{n}{2^2}+\cdots+\frac{n}{n^2}.\end{aligned}$$

Luego basta probar que

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

o lo que es equivalente

$$\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{n^2}<1. \tag{1}$$

Para ello observemos que

$$\begin{aligned}\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{n^2}&<\frac{1}{1\cdot2}+\frac{1}{2\cdot3}+\cdots+\frac{1}{(n-1)n}\\&=\left(1-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{3}\right)+\cdots+\left(\frac{1}{n-1}-\frac{1}{n}\right)\\&=1-\frac{1}{n}<1.\end{aligned}$$

Observe que la desigualdad (1) se obtiene fácilmente si apelamos al conocido resultado

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots=\frac{\pi^2}{6}<2.$$

□

Corolario 3.25. *Para todo entero positivo n se tiene que $\sigma_2(n)\geq n\tau(n)$.*

Demostración. Utilizando el lema 3.4 y la desigualdad entre media geométrica y media aritmética, se tiene que

$$n = \left(\prod_{d|n} d^2\right)^{1/\tau(n)} \leq \frac{1}{\tau(n)} \sum_{d|n} d^2 = \frac{\sigma_2(n)}{\tau(n)}.$$

□

Observación. Recordemos que la igualdad en la desigualdad entre media geométrica y media aritmética solo se tiene si los términos que se estan considerando son todos iguales. En este caso específico, cuando todos los divisores de n son iguales. Esto ocurre cuando $n = 1$, luego si $n \geq 2$ se tiene que $\sigma_2(n) > n\tau(n)$.

Teorema 3.26. *Para todo $n \in \mathbb{Z}^+$ y para todo d divisor propio de n, se tiene que*

$$\frac{\sigma(n)}{n} > \frac{\sigma(d)}{d}.$$

Demostración. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ y $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$ con $0 \leq \beta_i \leq \alpha_i$, $\forall i \in \{1, \ldots, m\}$ y al menos un $j \in \{1, \ldots, m\}$ tal que $\beta_j \neq \alpha_j$. Es claro entonces que

$$\frac{\sigma(n)}{n} = \prod_{i=1}^{m} \left(1 + \frac{1}{p_i} + \cdots + \frac{1}{p_i^{\alpha_i}}\right) > \prod_{i=1}^{m} \left(1 + \frac{1}{p_i} + \cdots + \frac{1}{p_i^{\beta_i}}\right) = \frac{\sigma(d)}{d}.$$

□

3.4. Ejercicios Adicionales

Lema 3.27. *Sean $n \in \mathbb{Z}^+$ y $S = \{\langle a, b\rangle \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid ab = n \text{ y } (a, b) = 1\}$, entonces $\#S = 2^{\omega(n)}$.*

Demostración. Si $n = 1$ entonces los únicos valores posibles son $a = 1$ y $b = 1$, y es claro que se tiene el lema para este caso. Sean $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ ($\omega(n) = m$) y $\langle a, b\rangle \in S$. Es claro que para p_i ($1 \leq i \leq m$) se tiene que $p_i | a$ o $p_i | b$, pero no ambos casos. Luego $p_i^{\alpha_i} | a$ o $p_i^{\alpha_i} | b$, pero no ambos casos. Es así como el problema se puede reducir simplemente a encontrar el número de formas en las que se pueden distribuir los $p_i^{\alpha_i}$ en dos grupos (los que dividen a a y los que dividen a b) y es claro que este número es 2^m. □

Ejercicio 3.28.

a) Sean d y n enteros positivos tales que $d^2 | n$. Demostrar que el número de parejas de enteros positivos $\langle a, b\rangle$ tales que $(a, b) = d$ y $ab = n$ es $2^{\omega(n/d^2)}$.

b) Demostrar que

$$\tau(n) = \sum_{d^2|n} 2^{\omega(n/d^2)}.$$

Demostración.

a) Sean $A = \frac{a}{d}$ y $B = \frac{b}{d}$. Es claro entonces que $(a,b) = d$ y $ab = n$ sii $(A,B) = 1$ y $AB = \frac{n}{d^2}$, luego el número de parejas que estamos buscando es igual al número de parejas de enteros positivos $\langle A, B\rangle$ tales que $(A,B) = 1$ y $AB = \frac{n}{d^2}$. Por el lema anterior sabemos que es $2^{\omega(n/d^2)}$.

b) Sea $(a,b) = d$ con $ab = d$. Como $(a,b) = d$ entonces $a = dx_1$ y $b = dx_2$ con $x_1, x_2 \in \mathbb{Z}^+$, luego es claro que $d^2|n$. Sea $H_d = \{\langle a,b\rangle \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid (a,b) = d \text{ y } ab = n\}$. Si $d^2 \nmid n$ entonces $\#H_d = 0$, luego

$$\sum_{d|n} \#H_d = \sum_{d^2|n} \#H_d,$$

pero es claro que

$$\tau(n) = \sum_{d|n} \#H_d,$$

de donde se tiene que

$$\tau(n) = \sum_{d^2|n} \#H_d = \sum_{d^2|n} 2^{\omega(n/d^2)}.$$

□

Ejemplo. Si n es $36 = 2^2 3^2$ entonces se tiene que el conjunto de los d tales que $d^2|n$ esta integrado por los números 1,2,3 y 6. Luego

$$\sum_{d^2|36} 2^{\omega(n/d^2)} = 2^{\omega(36)} + 2^{\omega(9)} + 2^{\omega(4)} + 2^{\omega(1)} = 2^2 + 2^1 + 2^1 + 2^0 = 9.$$

Por otro lado tenemos que $\tau(36) = 9$.

Ejercicio 3.29. Sea $n \in \mathbb{Z}^+$, demostrar que el número de parejas $\langle a,b\rangle$ de enteros positivos tales que $[a,b] = n$ es $\tau(n^2)$.

Demostración. Definimos f para todo $n \in \mathbb{Z}^+$ como

$$f(n) = \#\left\{\langle a,b\rangle \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid [a,b] = n\right\}.$$

Veamos que f es multiplicativa. Es claro que $f(1) = 1 = \tau(1^2)$. Sean $(m,n) = 1$ y a, b enteros positivos tales que $[a,b] = mn$. Es claro que a se puede escribir de forma única

como $a = a_1a_2$ con $a_1|m$ y $a_2|n$. Del mismo modo b se puede escribir de forma única como $b = b_1b_2$ con $b_1|m$ y $b_2|n$. De aquí es claro que $[a_1, b_1] = m$ y $[a_2, b_2] = n$. Es decir de cada pareja $\langle a, b\rangle$ con $[a, b] = mn$ se obtienen unas únicas parejas $\langle a_1, b_1\rangle$ y $\langle a_2, b_2\rangle$ tales que $[a_1, b_1] = m$ y $[a_2, b_2] = n$. Del mismo modo por cada par de parejas $\langle a_1, b_1\rangle$ y $\langle a_2, b_2\rangle$ con $[a_1, b_1] = m$ y $[a_2, b_2] = n$, se obtiene una única pareja $\langle a, b\rangle$ ($a = a_1a_2$ y $b = b_1b_2$) con $[a, b] = mn$. Demostrando así que f es multiplicativa.

Veamos que $f(n) = \tau(n^2)$. Como $\tau(n^2)$ también es multiplicativa por el teorema 1.12, basta con demostrar que para p primo y $\alpha \in \mathbb{Z}^+$ se tiene que $f(p^\alpha) = \tau(p^{2\alpha})$. Para este caso ($n = p^\alpha$) se tiene que $a = p_1^{\alpha_1}$ y $b = p^{\alpha_2}$ donde $\alpha = \max\{\alpha_1, \alpha_2\}$. Si $\alpha = \alpha_1$ entonces α_2 puede ser $0, 1, \ldots, \alpha$ ($\alpha + 1$ posibilidades). Si $\alpha = \alpha_2$ entonces α_1 puede ser $0, 1, \ldots, \alpha$ ($\alpha + 1$ posibilidades). Entonces el número de posibilidades de elegir α_1 y α_2, que es lo mismo que el número de posibilidades de elegir a y b, es $(\alpha + 1) + (\alpha + 1) - 1$ (recuerde que $\alpha = \alpha_1 = \alpha_2$ se contó dos veces), es decir $2\alpha + 1 = \tau(p^{2\alpha})$. □

Ejercicio 3.30. Sea $k \in \mathbb{R}$, definimos para todo entero positivo n la función σ_k^* como

$$\sigma_k^*(n) = \sum_{\substack{d|n \\ d \text{ impar}}} d^k,$$

es decir la suma de las potencias k-ésimas de los divisores positivos impares de n (Es claro que si n no tiene divisores impares, es decir si n es una potencia de 2, $\sigma_k^*(n) = 0$). Demostrar que $\sigma_k^*(n)$ es multiplicativa.

Demostración. Sea $(m, n) = 1$.

i) Si m y n son impares entonces

$$\sigma_k^*(mn) = \sigma_k(mn) = \sigma_k(m)\sigma_k(n) = \sigma_k^*(m)\sigma_k^*(n).$$

ii) Si m es par y n impar entonces $m = 2^\alpha r$ con r impar y se tiene que $(r, n) = 1$ de donde vemos que

$$\begin{aligned}\sigma_k^*(mn) = \sigma_k^*(2^\alpha rn) = \sigma_k^*(rn) = \sigma_k(rn) = \sigma_k(r)\sigma_k(n)\\ = \sigma_k^*(r)\sigma_k^*(n) = \sigma_k^*(2^\alpha r)\sigma_k^*(n) = \sigma_k^*(m)\sigma_k^*(n).\end{aligned}$$

iii) Si m es impar y n par, el procedimiento es análogo a ii).

iv) El caso en que m y n sean ambos pares no se puede dar pues $(m, n) = 1$.

□

Observación. En especial la funciones $\tau^*(n)$ y $\sigma^*(n)$, definidas respectivamente como el número de divisores positivos impares de n y la suma de los divisores positivos impares de n, son funciones multiplicativas. Por otro lado si definimos $\sigma_k^{**}(n)$ como

$$\sigma_k^{**}(n) = \sum_{\substack{d|n \\ d \text{ par}}} d^k,$$

(obviamente con $\sigma_k^{**}(n) = 0$ si n es impar) obtenemos que esta función no es multiplicativa pues si tomamos m y n primos relativos con m par y n impar obtenemos que mn es par y por lo tanto $\sigma_k^{**}(nm) \neq 0$ pero $\sigma_k^{**}(m)\sigma_k^{**}(n) = \sigma_k^{**}(m) \cdot 0 = 0$.

Ejercicio 3.31 (The American Mathematical Monthly, Problema 4493, [17]). Demostrar que $\sum_{n=1}^{\infty} \frac{\sigma(n)}{n!}$ es irracional.

Demostración. Supongamos que $\sum_{n=1}^{\infty} \frac{\sigma(n)}{n!} = \frac{r}{s}$ con $r, s \in \mathbb{Z}^+$ y $(r, s) = 1$.

Elegimos p primo tal que $p > s$ y $p > 6$.

$$\sum_{n=1}^{\infty} \frac{\sigma(n)}{n!} = \sum_{n=1}^{p-1} \frac{\sigma(n)}{n!} + \sum_{n=p}^{\infty} \frac{\sigma(n)}{n!}$$

$$(p-1)! \sum_{n=1}^{\infty} \frac{\sigma(n)}{n!} = (p-1)! \sum_{n=1}^{p-1} \frac{\sigma(n)}{n!} + (p-1)! \sum_{n=p}^{\infty} \frac{\sigma(n)}{n!}.$$

Cambiando el índice de la última sumatoria por $c = n - p$ obtenemos que

$$(p-1)! \sum_{n=1}^{\infty} \frac{\sigma(n)}{n!} = (p-1)! \sum_{n=1}^{p-1} \frac{\sigma(n)}{n!} + (p-1)! \sum_{c=0}^{\infty} \frac{\sigma(p+c)}{(p+c)!}$$

$$(p-1)! \sum_{n=1}^{\infty} \frac{\sigma(n)}{n!} = (p-1)! \sum_{n=1}^{p-1} \frac{\sigma(n)}{n!} + \sum_{c=0}^{\infty} \frac{\sigma(p+c)}{p(p+1)\cdots(p+c)}.$$

$(p-1)! \sum_{n=1}^{\infty} \frac{\sigma(n)}{n!}$ es un entero, pues recordando que $s \leq p-1$, tenemos que

$$(p-1)! \sum_{n=1}^{\infty} \frac{\sigma(n)}{n!} = (p-1)! \frac{r}{s} = 1 \cdot 2 \cdot 3 \cdots (s-1)(s+1) \cdots (p-1)r \in \mathbb{Z}^+.$$

También se tiene que

$$(p-1)! \sum_{n=1}^{\infty} \frac{\sigma(n)}{n!} = \sum_{n=1}^{p-1} (n+1)(n+2) \cdots (p-1)\sigma(n) \in \mathbb{Z}^+.$$

Luego si demostraramos que $k = \sum_{c=0}^{\infty} \frac{\sigma(p+c)}{p(p+1)\cdots(p+c)}$ no es un entero, obtendríamos una contradicción.

Sabemos que $\sigma(p) = 1+p$ y que $\sigma(p+c) < 1+2+3+\cdots+(p+c) = \frac{1}{2}(p+c)(p+c+1)$, luego

$$\sum_{c=1}^{\infty} \frac{\sigma(p+c)}{p(p+1)\cdots(p+c)} < \sum_{c=1}^{\infty} \frac{p+c+1}{2p(p+1)\cdots(p+c-1)}. \tag{1}$$

Veamos que si $c \geq 1$ entonces $\frac{p+c+1}{2p(p+1)\cdots(p+c-1)} < \frac{p+c}{2p^c}$, lo que es lo mismo que

$$\begin{aligned} &\frac{p+c+1}{p+2} < \frac{(p+1)\cdots(p+c-1)}{p^{c-1}} \\ \iff &\frac{p+2+(c-1)}{p+2} < \left(\frac{p+1}{p}\right)\left(\frac{p+2}{p}\right)\cdots\left(\frac{p+c-1}{p}\right) \\ \iff &1+\frac{c-1}{p+2} < \left(1+\frac{1}{p}\right)\left(1+\frac{2}{p}\right)\cdots\left(1+\frac{c-1}{p}\right). \end{aligned}$$

Es claro que esta última desigualdad se cumple pues

$$1+\frac{c-1}{p+2} < 1+\frac{c-1}{p} < \left(1+\frac{1}{p}\right)\left(1+\frac{2}{p}\right)\cdots\left(1+\frac{c-1}{p}\right). \tag{2}$$

Luego por (1) y (2) se tiene que

$$\begin{aligned} \sum_{c=1}^{\infty} \frac{\sigma(p+c)}{p(p+1)\cdots(p+c)} &< \sum_{c=1}^{\infty} \frac{p+2}{2p^c} \\ &= \frac{p+2}{2} \sum_{c=1}^{\infty} \left(\frac{1}{p}\right)^c \\ &= \frac{p+2}{2}\left(\frac{1}{1-\frac{1}{p}} - 1\right) \\ &= \frac{p+2}{2(p-1)} \end{aligned} \tag{3}$$

Veamos que si $p > 6$, entonces $\frac{p+2}{2(p-1)} < \frac{p-1}{p}$, lo que es lo mismo que

$$\begin{aligned} &p(p+2) < 2(p-1)^2 \\ \iff &p^2+2p < 2p^2-4p+2 \\ \iff &0 < p^2-6p+2. \end{aligned}$$

Esta última desigualdad es cierta para $p > 6$ ya que $p^2-6p+2 > p^2-p\cdot p+2 = 2 > 0$.

Sabemos que

$$k = \frac{\sigma(p)}{p} + \sum_{c=1}^{\infty} \frac{\sigma(p+c)}{p(p+1)\cdots(p+c)}.$$

Como $\sigma(p) = p+1$, entonces $\frac{\sigma(p)}{p} = 1 + \frac{1}{p}$ y por lo tanto

$$k = 1 + \frac{1}{p} + \sum_{c=1}^{\infty} \frac{\sigma(p+c)}{p(p+1)\cdots(p+c)}. \tag{4}$$

De (3) y (4) se tiene que

$$1 < k < 1 + \frac{1}{p} + \frac{p+2}{2(p-1)} = 1 + \frac{p+1}{p(p-1)} < 2.$$

Es decir k no es un entero. □

Ejercicio 3.32 (The American Mathematical Monthly, Problema 4518, [16]). Demostrar que $\sum_{n=1}^{\infty} \frac{\sigma_2(n)}{n!}$ es irracional.

Demostración. Supongamos que $\sum_{n=1}^{\infty} \frac{\sigma_2(n)}{n!} = \frac{a}{b}$ para a y b enteros positivos. Eligiendo p primo tal que $p > b$ y $p > 20$, vemos que

$$(p-1)!\frac{a}{b} = (p-1)!\sum_{n=1}^{\infty} \frac{\sigma_2(n)}{n!} = (p-1)!\sum_{n=1}^{p-1} \frac{\sigma_2(n)}{n!} + \frac{\sigma_2(p)}{p} + \frac{\sigma_2(p+1)}{p(p+1)} + \sum_{n=p+2}^{\infty} \frac{\sigma_2(n)}{p(p+1)\cdots n}$$

es entero. Como $(p-1)!\sum_{n=1}^{\infty} \frac{\sigma_2(n)}{n!}$ es entero, entonces

$$S = \frac{\sigma_2(p)}{p} + \frac{\sigma_2(p+1)}{p(p+1)} + \sum_{n=p+2}^{\infty} \frac{\sigma_2(n)}{p(p+1)\cdots n}$$

es entero.

Además se tiene que

$$n^2 < \sigma_2(n) < n^2 \sum_{k=1}^{n} \frac{1}{k^2} < n^2 \frac{\pi^2}{6}.$$

Para $n > 20$ vemos que $n^2\frac{\pi^2}{6} < \frac{7}{4}n(n-1)$. Observamos que esta desigualdad es equivalente a $21 < n\,(21 - 2\pi^2)$. Sabemos que $\pi < 3{,}15$ y por lo tanto $\pi^2 < 9{,}9225 < 10$. Se tiene entonces que para $n > 20$, $21 < 21(21-20) < n(21-2\pi^2)$. Luego para $n > 20$ se tiene que $n^2 < \sigma_2(n) < \frac{7}{4}n(n-1)$, de donde para $n > 20$, $\sigma_2(n) = n(n-1)(1+\alpha_n)$ con $0 < \alpha_n < \frac{3}{4}$.

Sabemos que S es entero, luego la siguiente expresión también es un entero:

$$\begin{aligned} S-p-1 &= \frac{\sigma_2(p)}{p} + \frac{\sigma_2(p+1)}{p(p+1)} + \sum_{n=p+2}^{\infty} \frac{\sigma_2(n)}{p(p+1)\cdots n} - p - 1 \\ &= \frac{1+p^2}{p} + \frac{(p+1)p(1+\alpha_{p+1})}{p(p+1)} + \sum_{p+2}^{\infty} \frac{n(n-1)(1+\alpha_n)}{p(p+1)\cdots n} - p - 1 \\ &= \frac{1}{p} + \alpha_{p+1} + \sum_{p+2}^{\infty} \frac{1+\alpha_n}{p(p+1)\cdots(n-2)}. \end{aligned}$$

Pero

$$\begin{aligned} 0 < S-p-1 &< \frac{1}{p} + \frac{3}{4} + 2\left(\frac{1}{p} + \frac{1}{p(p+1)} + \cdots\right) \\ &< \frac{1}{p} + \frac{3}{4} + 2\left(\frac{1}{p} + \frac{1}{p^2} + \cdots\right) \\ &= \frac{1}{p} + \frac{3}{4} + 2\left(\frac{1}{1-\frac{1}{p}} - 1\right) \\ &= \frac{1}{p} + \frac{3}{4} + \frac{2}{p-1} \\ &< \frac{1}{20} + \frac{3}{4} + \frac{2}{19} < 1. \end{aligned}$$

Lo que es una contradicción. □

Capítulo 4

Otros temas sobre Funciones Aritméticas

4.1. Más sobre la Función de Möbius

Ejercicio 4.1. Sea n un entero positivo mayor que 1, libre de cuadrados con $\omega(n)$ par. Demostrar que

$$\sum_{\substack{d|n \\ 0<d<\sqrt{n}}} \mu(d) = 0.$$

Demostración. Si d es un divisor de n tal que $0 < d < \sqrt{n}$, entonces existe d' divisor de n tal que $d' > \sqrt{n}$ y $dd' = n$. Es claro que $(d, d') = 1$, luego $\mu(n) = \mu(dd') = \mu(d)\mu(d')$, pero $\mu(n) = (-1)^{\omega(n)} = 1$ por ser $\omega(n)$ par, de donde $\mu(d) = \mu(d')$. Luego

$$\begin{aligned} 2 \sum_{\substack{d|n \\ 0<d<\sqrt{n}}} \mu(d) &= \sum_{\substack{d|n \\ 0<d<\sqrt{n}}} \mu(d) + \sum_{\substack{d'|n \\ d'>\sqrt{n}}} \mu(d') \\ &= \sum_{d|n} \mu(d) \\ &= 0. \end{aligned}$$

De donde se tiene que

$$\sum_{\substack{d|n \\ 0<d<\sqrt{n}}} \mu(d) = 0.$$

□

Ejercicio 4.2. Sea m un entero positivo. Demostrar que

$$\sum_{\varphi(n)=m} \mu(n) = 0,$$

donde la suma se realiza sobre todos los enteros positivos n tales que $\varphi(n) = m$.

Demostración. Es claro que solo se deben considerar los n libres de cuadrados. Si n es un entero libre de cuadrados e impar tal que $\varphi(n) = m$, entonces $n' = 2n$ también es libre de cuadrados y cumple también que $\varphi(n') = m$ (y viceversa). Además $\mu(n) + \mu(n') = (-1)^{\omega(n)} + (-1)^{\omega(n)+1} = 0$, luego

$$\sum_{\varphi(n)=m} \mu(n) = 0.$$

□

Ejercicio 4.3. Demostrar que

$$\sum_{\substack{d|n \\ |\mu(d)|=1}} \mu\left(\frac{n}{d}\right) = \begin{cases} (-1)^m, & \text{si } n = p_1^2 p_2^2 \cdots p_m^2 \ (p_1 < p_2 < \cdots < p_m \text{ primos}) \\ 0, & \text{en otro caso.} \end{cases}$$

Demostración.

i) Supongamos que existe p primo tal que $p^3|n$. Dado que la suma

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

simboliza la suma a través de todos los divisores d de n libres de cuadrados, entonces $\frac{n}{d}$ seguirá siendo un número que no es libre de cuadrados y por lo tanto

$$\sum_{\substack{d|n \\ |\mu(d)|=1}} \mu\left(\frac{n}{d}\right) = 0.$$

ii) Si no existe p primo tal que $p^3|n$ entonces n es de la forma $n = p_1^2 p_2^2 \cdots p_m^2 r$ donde los p_i's son primos diferentes, r es libre de cuadrados y $(p_1^2 p_2^2 \cdots p_m^2, r) = 1$. Hagamos $s = p_1^2 p_2^2 \cdots p_m^2$. Vemos que

$$\sum_{\substack{d|n \\ |\mu(d)|=1}} \mu\left(\frac{n}{d}\right) = \sum_{\substack{d|sr \\ |\mu(d)|=1}} \mu\left(\frac{sr}{d}\right) = \sum_{\substack{d_1|s \\ |\mu(d_1)|=1}} \sum_{\substack{d_2|r \\ |\mu(d_2)|=1}} \mu\left(\frac{s}{d_1}\right) \mu\left(\frac{r}{d_2}\right).$$

Es claro que

$$\mu\left(\frac{s}{d_1}\right) = \begin{cases} (-1)^m, & \text{si } n = p_1 p_2 \cdots p_m \\ 0, & \text{en otro caso.} \end{cases}$$

Luego

$$\sum_{\substack{d|n \\ |\mu(d)|=1}} \mu\left(\frac{n}{d}\right) = (-1)^m \sum_{\substack{d_2|r \\ |\mu(d_2)|=1}} \mu\left(\frac{r}{d_2}\right) = (-1)^m \sum_{d_2|r} \mu\left(\frac{r}{d_2}\right) = \begin{cases} (-1)^m, & \text{si } r = 1 \\ 0, & \text{si } r \geq 1 \end{cases}$$

(la última igualdad es debida al corolario 1.28). Observe que el caso en que $r = 1$ es cuando $n = p_1^2 p_2^2 \cdots p_m^2$.

□

Lema 4.4. *Para todo entero $k > 1$ se tiene que*

$$\sum_{j=1}^{k} \binom{k}{j} j = k \cdot 2^{k-1}.$$

Demostración.

$$\sum_{j=1}^{k} \binom{k}{j} j = \sum_{j=1}^{k} \frac{k!j}{j!(k-j)!} = \sum_{j=1}^{k} \frac{k(k-1)!}{(j-1)!((k-1)-(j-1))!} = k \sum_{j=1}^{k} \binom{k-1}{j-1} = k \cdot 2^{k-1}.$$

□

Ejercicio 4.5. Demsotrar que para $n \in \mathbb{Z}^+$, se tiene que

$$\prod_{d|n} \mu(d) = \begin{cases} 1, & \text{si } n = 1 \\ -1, & \text{si } n \text{ es primo} \\ 0, & \text{si existe } p \text{ primo tal que } p^2|n \\ 1, & \text{si } n \text{ es compuesto y libre de cuadrados.} \end{cases}$$

Demostración. Se demostrará para el caso en el que n sea compuesto y libre de cuadrados, los demás casos son evidentes. Sea $n = p_1 p_2 \cdots p_k$ con $k > 1$ (los p_i's son primos diferentes). Como el número de divisores d de n con j divisores primos diferentes es $\binom{k}{j}$ y como para esos divisores $\mu(d) = (-1)^j$, se tiene que $\prod_{d|n} \mu(d) = (-1)^a$, donde $a = \sum_{j=1}^{k} \binom{k}{j} j$. Como a es par debido al lema anterior, obtenemos entonces el resultado deseado. □

4.2. Más sobre Funciones Multiplicativas

Teorema 4.6. *Sea f una función aritmética con $f(1) = 1$, entonces f es multiplicativa sii*
$f((m,n))\, f([m,n]) = f(m)f(n)\ \forall m, n \in \mathbb{Z}^+$.

Demostración.

$\Rightarrow$) Sea f una función multiplicativa, $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ y $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ con $\alpha_i, \beta_i \in \mathbb{N}$, $\forall i$. Es claro que para $i \in \{1, 2, \ldots, r\}$ se tiene que

$$f\left(p_i^{\min\{\alpha_i,\beta_i\}}\right) f\left(p_i^{\max\{\alpha_i,\beta_i\}}\right) = f\left(p_i^{\alpha_i}\right) f\left(p_i^{\beta_i}\right),$$

luego vemos que

$$\begin{aligned} f((m,n))\, f([m,n]) &= f\left(\prod_{i=1}^{r} p_i^{\min\{\alpha_i,\beta_i\}}\right) f\left(\prod_{i=1}^{r} p_i^{\max\{\alpha_i,\beta_i\}}\right) \\ &= \prod_{i=1}^{r} f\left(p_i^{\min\{\alpha_i,\beta_i\}}\right) \prod_{i=1}^{r} f\left(p_i^{\max\{\alpha_i,\beta_i\}}\right) \\ &= \prod_{i=1}^{r} f\left(p_i^{\min\{\alpha_i,\beta_i\}}\right) f\left(p_i^{\max\{\alpha_i,\beta_i\}}\right) \\ &= \prod_{i=1}^{r} f\left(p_i^{\alpha_i}\right) f\left(p_i^{\beta_i}\right) \\ &= \prod_{i=1}^{r} f\left(p_i^{\alpha_i}\right) \prod_{i=1}^{r} f\left(p_i^{\beta_i}\right) \\ &= f(m)f(n). \end{aligned}$$

$\Leftarrow$) Sea f tal que $f((m,n))\, f([m,n]) = f(m)f(n)$. Para $(m,n) = 1$, y por lo tanto $[m,n] = mn$, la igualdad se reduce a $f(1)f(mn) = f(m)f(n)$, es decir $f(mn) = f(m)f(n)$. □

Observación. Tomando la función $f(n) = n\ \forall n \in \mathbb{Z}^+$ obtenemos el ya conocido resultado $(a,b)\,[a,b] = ab$.

Ejercicio 4.7. Sean f y g funciones multiplicativas y definimos

$$h(n) = \sum_{\substack{dr=n \\ (d,r)=1}} f(d)g(r), \qquad \forall n \in \mathbb{Z}^+.$$

Demostrar que h es multiplicativa.

Demostración.

i) $h(1) = f(1)g(1) = 1$.

ii) Sean $(n,m) = 1$ y $(d,r) = 1$ con $dr = nm$. Es claro que se pueden encontrar factorizaciones únicas de d y r, $d = d_1d_2$ y $r = r_1r_2$ tales que $n = d_1r_1$ y $m = d_2r_2$, y obviamente con $(d_1,r_1) = (d_2,r_2) = 1$. Más aún, es claro que $(d,r) = 1$ sii $(d_1,r_1) = (d_2,r_2) = 1$. Por lo tanto

$$\begin{aligned} f(d)f(r) &= f(d_1d_2)g(r_1r_2) \\ &= f(d_1)f(d_2)g(r_1)g(r_2) \\ &= [f(d_1)g(r_1)]\,[f(d_2)g(r_2)]\,, \end{aligned}$$

y dado que a cada valor de d y r corresponden únicos valores d_1, d_2, r_1, r_2 y viceversa, entonces

$$\sum_{\substack{dr=nm\\(d,r)=1}} f(d)g(r) = \sum_{\substack{d_1r_1=n\\(d_1,r_1)=1}} f(d_1)g(r_1) \sum_{\substack{d_2r_2=m\\(d_2,r_2)=1}} f(d_2)g(r_2)$$
$$h(nm) = h(n)h(m).$$

□

Ejercicio 4.8. Sean f y g funciones multiplicativas y definimos

$$h(n) = \sum_{[d,r]=n} f(d)g(r), \qquad \forall n \in \mathbb{Z}^+.$$

Demostrar que h es multiplicativa.

Demostración.

i) $h(1) = f(1)g(1) = 1$.

ii) Sean $(n, m) = 1$ y $[d, r] = mn$. Luego d y r se pueden factorizar de forma única, $d = d_1d_2$ y $r = r_1r_2$ de tal forma que $[d_1, r_1] = m$ y $[d_2, r_2] = n$ (recordemos que $(m, n) = 1$), además es claro que si $[d_1, r_1] = m$ y $[d_2, r_2] = n$ entonces $[d, r] = mn$ donde $d = d_1d_2$ y $r = r_1r_2$. Además para cada d los valores d_1 y d_2 son únicos y viceversa. Luego

$$\begin{aligned} h(mn) &= \sum_{[d,r]=mn} f(d)g(r) \\ &= \sum_{\substack{[d_1,r_1]=m\\[d_2,r_2]=n}} f(d_1)f(d_2)g(r_1)g(r_2) \\ &= \sum_{[d_1,r_1]=m} f(d_1)g(r_1) \sum_{[d_2,r_2]=n} f(d_2)g(r_2) \\ &= h(m)h(n). \end{aligned}$$

□

Ejercicio 4.9. Demostrar que para $n \geq 2$, se tiene que

$$\sum_{[d,r]=n} \varphi(d)\varphi(r) = n^2 \prod_{p|n} \left(1 - \frac{1}{p^2}\right).$$

Demostración. Por el ejercicio anterior sabemos que

$$\sum_{[d,r]=n} \varphi(d)\varphi(r)$$

es multiplicativa. Luego basta probar la identidad para $n = p^\alpha$ con p primo y $\alpha \in \mathbb{Z}^+$. Vemos que, $[d, r] = p^\alpha$ sii $d = p^a$ y $r = p^b$ con $\max\{a, b\} = \alpha$, luego

$$\begin{aligned} f\left(p^\alpha\right) &= \sum_{\substack{a=\alpha \\ b<\alpha}} \varphi\left(p^a\right)\varphi\left(p^b\right) + \sum_{\substack{a\leq\alpha \\ b=\alpha}} \varphi\left(p^a\right)\varphi\left(p^b\right) \\ &= \varphi\left(p^\alpha\right) \sum_{d|p^{\alpha-1}} \varphi(d) + \varphi\left(p^\alpha\right) \sum_{d|p^\alpha} \varphi(d) \\ &= \varphi\left(p^\alpha\right)\left(p^{\alpha-1} + p^\alpha\right) \\ &= \left(p^\alpha - p^{\alpha-1}\right)\left(p^{\alpha-1} + p^\alpha\right) \\ &= p^{2\alpha} - p^{2\alpha-2} \\ &= p^{2\alpha}\left(1 - \frac{1}{p^2}\right). \end{aligned}$$

□

Ejercicio 4.10. Sea f una función multiplicativa y definamos F para todo entero positivo n, como

$$F(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Demostrar que si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, entonces

$$F(n) = \prod_{i=1}^{m} \left(f\left(p_i^{\alpha_i}\right) - f\left(p_i^{\alpha_i - 1}\right)\right).$$

Demostración. Como f es multiplicativa, también lo es F. Luego basta comprobar el resultado para $n = p^\alpha$ con p primo y $\alpha \in \mathbb{Z}^+$.

$$\begin{aligned} F\left(p^\alpha\right) &= \sum_{d|p^\alpha} \mu(d) f\left(\frac{p^\alpha}{d}\right) \\ &= \mu(1) f\left(p^\alpha\right) + \mu(p) f\left(p^{\alpha-1}\right) + 0 + 0 + \cdots \\ &= f\left(p^\alpha\right) - f\left(p^{\alpha-1}\right). \end{aligned}$$

□

4.3. Problemas con más de una Función Aritmética

Ejercicio 4.11 (The American Mathematical Monthly, Problema E1962, [41]). Demostrar que $\varphi(n)\tau(n) \geq n$, donde la igualdad solo se tiene para $n = 1$ y $n = 2$.

Demostración 1. Si $n = 1$ es claro que se tiene la igualdad. De ahora en adelante consideramos $n \geq 2$. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, luego

$$\varphi(n)\tau(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) \prod_{i=1}^{m} (\alpha_i + 1)\,.$$

Dado que $p_i \geq 2$, se tiene que $1 - 1/p_i \geq \frac{1}{2}$ y que $\alpha_i + 1 \geq 2$, $\forall i$. Luego $\varphi(n)\tau(n) \geq n \left(\frac{1}{2}\right)^m 2^m = n$. Se ve que la igualdad se tiene, cuando $n \geq 2$, sii $1 - 1/p_i = \frac{1}{2}$ y $\alpha_i + 1 = 2$, $\forall i$, es decir cuando $n = 2$. □

Demostración 2. Si $n = 1$ es claro que se tiene la igualdad. De ahora en adelante consideramos $n \geq 2$. Es claro que $\varphi(n) \geq \varphi(d)$ si $d|n$. Luego

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

La igualdad se tiene, cuando $n \geq 2$, sii

$$n \prod_{p|n} \left(1 - \frac{1}{p}\right) = d \prod_{p|d} \left(1 - \frac{1}{p}\right) \qquad \forall d|n,$$

lo cual solo ocurre si $n = 2$. □

Teorema 4.12. *$\varphi(n)\sigma(n) < n^2$ para $n \geq 2$.*

Demostración. Si $n \geq 2$ con $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, entonces

$$\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{m} \left(\frac{p_i - 1}{p_i}\right)$$

y

$$\sigma(n) = \prod_{i=1}^{m} \left(\frac{p_i^{\alpha_{i+1}} - 1}{p_i - 1}\right).$$

Luego

$$\varphi(n)\sigma(n) = n \prod_{i=1}^{m} \left(\frac{p_i^{\alpha_{i+1}} - 1}{p_i}\right) = n \prod_{i=1}^{m} \left(p_i^{\alpha_i} - \frac{1}{p_i}\right) < n \prod_{i=1}^{m} p_i^{\alpha_i} = n^2.$$

□

Ejercicio 4.13 (The American Mathematical Monthly, Problema 5591, [35]). Para $n \geq 2$, demostrar que

$$\varphi\left(n\left\lfloor\frac{\sigma(n)}{n}\right\rfloor\right) < n.$$

Demostración. Utilizando el lema 2.23 y el teorema anterior, vemos que

$$\varphi\left(n\left\lfloor\frac{\sigma(n)}{n}\right\rfloor\right) \leq \varphi(n)\left\lfloor\frac{\sigma(n)}{n}\right\rfloor \leq \varphi(n)\frac{\sigma(n)}{n} < n.$$

□

Es claro que la anterior desigualdad no solo se tiene para $\left\lfloor\frac{\sigma(n)}{n}\right\rfloor$ sino para cualquier $j \leq \sigma(n)/n$, es decir:

Corolario 4.14. *Si $n \geq 2$ y j es un entero positivo tal que $j \leq \sigma(n)/n$ entonces $\varphi(jn) < n$.*

Teorema 4.15 (The American Mathematical Monthly, Problema E2611, [33]). *n es primo sii $\varphi(n)|(n-1)$ y $(n+1)|\sigma(n)$.*

Demostración. $\Rightarrow$) Evidente, pues si n es primo $\varphi(n) = n-1$ y $\sigma(n) = n+1$.

$\Leftarrow$) Sea n tal que $\varphi(n)|(n-1)$ y $(n+1)|\sigma(n)$, luego $n \geq 2$, pues si $n = 1$ no se tiene que $(n+1)|\sigma(n)$. Si $n = 2$ se tiene entonces que n es primo. Si $n \geq 3$, entonces se tiene que $\varphi(n)$ es par y por lo tanto $n-1$ también, de donde n es impar.

Si $p^r|n$ con p primo y $r \geq 2$ entonces como

$$\varphi(n) = n \prod_{\substack{q|n \\ q \text{ primo}}} \frac{q-1}{q}$$

se tiene que $p^{r-1}|\varphi(n)$, de donde $p^{r-1}|(n-1)$, lo cual es una contradicción pues $(n, n-1) = 1$. Por lo tanto n es libre de cuadrados y $n = p_1p_2\cdots p_m$ donde por ser n impar, los p_i's son primos impares. Como

$$\varphi(n) = (p_1-1)(p_2-1)\cdots(p_m-1)$$

y

$$\sigma(n) = (p_1+1)(p_2+1)\cdots(p_m+1)$$

entonces 2^m divide tanto a $\varphi(n)$ como a $\sigma(n)$.

Si $m \geq 2$ entonces $4|\varphi(n)$ y por lo tanto $4|(n-1)$ de donde se tiene que $4 \nmid (n+1)$,

luego $n+1 = 2r$ con r impar. Sabemos que $2^m|\sigma(n)$ luego existe $t \in \mathbb{Z}^+$ tal que $2^m t = \sigma(n)$, de donde se tiene que

$$2^{m-1}\left(\frac{t}{r}\right) = \frac{2^m t}{2r} = \frac{\sigma(n)}{n+1}$$

$\frac{t}{r}$ es entero pues r es impar y $\frac{\sigma(n)}{n+1}$ es entero ya que $n+1|\sigma(n)$ por hipótesis. Luego

$$2^{m-1}|\frac{\sigma(n)}{n+1}$$

de donde

$$2^{m-1} \leq \frac{\sigma(n)}{n+1} < \frac{\sigma(n)}{n}$$

pero sabemos que

$$\begin{aligned}\frac{\sigma(n)}{n} &= \frac{1}{p_1 p_2 \cdots p_m}\left(\frac{p_1^2-1}{p_1-1}\right)\cdots\left(\frac{p_1^2-1}{p_1-1}\right)\\ &= \left(\frac{p_1+1}{p_1}\right)\cdots\left(\frac{p_m+1}{p_m}\right)\\ &= \left(1+\frac{1}{p_1}\right)\cdots\left(1+\frac{1}{p_m}\right)\end{aligned}$$

y al ser los p_i's impares, se tiene que

$$\frac{1}{p_i} \leq \frac{1}{3} \qquad \forall i.$$

Luego

$$\frac{\sigma(n)}{n} < \left(\frac{4}{3}\right)^m$$

De donde

$$\begin{aligned}2^{m-1} &< \left(\frac{4}{3}\right)^m\\ \frac{2^m}{2} &< \left(\frac{4}{3}\right)^m\\ \frac{1}{2} &< \left(\frac{2}{3}\right)^m\end{aligned}$$

Al ser $m \geq 2$ se tiene entonces que $\frac{1}{2} < \frac{4}{9}$, lo cual es una contradicción. Luego $m = 1$ y n primo. □

Ejercicio 4.16 (Olimpiadas matemáticas de China Occidental, 2004).

a) Demostrar que $\tau(n) + \varphi(n) \leq n + 1$.

b) Hallar todos los valores de n para los cuales se tenga que $\tau(n) + \varphi(n) = n$.

c) Hallar todos los valores de n para los cuales se tenga que $\tau(n) + \varphi(n) = n + 1$.

Desarrollo. a) Sea $n \in \mathbb{Z}^+$, definimos:

$$A = \left\{ m \in \mathbb{Z}^+ : m|n \right\}$$

y

$$B = \left\{ m \in \mathbb{Z}^+ : 1 \leq m \leq n, (m, n) = 1 \right\}.$$

Es claro que $\#A \cup B \leq n$ y que $A \cap B = \{1\}$, además sabemos que

$$\#A \cup B = \#A + \#B - \#A \cap B,$$

de donde se tiene que

$$\begin{aligned} \tau(n) + \varphi(n) &= \#A + \#B \\ &= \#A \cup B + \#A \cap B \\ &\leq n + 1. \end{aligned}$$

b) Sea n tal que $\tau(n) + \varphi(n) = n$ entonces $\#A \cup B = n - 1$, luego solo hay número entre 1 y n que no es ni divisor de n, ni primo relativo con n.

i) Si n es par y $n > 8$, es claro que $n-2$ y $n-4$ no son primos relativos con n (ambos son divisibles por 2). Veamos que $n-2$ y $n-4$ tampoco son divisores de n.

Supongamos que $n - 2|n$. Se tiene que

$$\begin{aligned} n &\equiv 0 \mod n - 2 \\ n - (n - 2) &\equiv -(n - 2) \mod n - 2 \\ 2 &\equiv 0 \mod n - 2 \end{aligned}$$

es decir $n - 2|2$, lo cual es una contradicción pues $n > 8$. De las misma forma, si se supone que $n - 4|n$, se llega a la contradicción de que $n - 4|4$.

Luego para n par y $n > 8$, encontramos dos números, $n - 2$ y $n - 4$, entre 1 y n que no son ni divisores de n, ni primos relativos con n, contradiciendo la existencia de solo uno.

ii) Si n es impar, tiene que ser compuesto, pues si n es 1 o un primo, es claro que $\tau(n) + \varphi(n) = n + 1$. Luego $n = pq$ con p y q impares y $1 < p \leq q$. Si $q \geq 5$, entonces $2p$ y $4p$ no son divisores de n por ser este impar, además $2p$, $4p$ y n son divisibles por p, luego $2p$ y $4p$ no son primos relativos con n. Luego todo número impar que se pueda escribir como $n = pq$ con $1 < p \leq q$ y $q \geq 5$ no cumple la ecuación $\tau(n) + \varphi(n) = n + 1$, pues contradice la existencia de un sólo número entre 1 y n que no son ni divisor de n, ni primo relativo con n. Veamos que si n es impar, compuesto y $n > 9$ entonces se puede escribir de la forma anteriormente mencionada.

Supongamos que existe n impar, compuesto y mayor que n que no se puede escribir de tal forma. Se deduce entonces que n tiene que ser de la forma $n = pq$ con $1 < p \leq q < 5$, pero recordemos que $n > 9$, luego $p = q = 4$ pues cualquier otros valores de p y q con $1 < p \leq q < 5$ se tendría que $n \leq 9$. Es decir $n = 16$ pero $16 = 2 \cdot 8$ y $8 \geq 5$, lo cual nos lleva a una contradicción.

De i) y ii) tenemos que los únicos candidatos que quedan para que $\tau(n)+\varphi(n) = n$ son de la forma $n \leq 8$ con n par o $n \leq 9$ con n impar compuesto. Verificando cuales de estos nos sirven, llegamos a que los únicos que cumplen la ecuación son 6, 8 y 9.

c) Sea n tal que $\tau(n) + \varphi(n) = n + 1$, entonces todo los números entre 1 y n son divisores de n o primos relativos con n.

i) Es claro si n es 1 o un primo, entonces cumple la ecuación.

ii) Si n es par y $n > 4$ entonces es claro que $n - 2$ no es primo relativo con n, si suponemos que $n - 2|n$ como vimos antes, se tiene que $n - 2|2$, lo cual es una contradicción por ser $n > 4$, luego $n - 2$ tampoco es un divisor de n. Se llega entonces a una contradicción. Luego si n es par entonces o n es 2 o 4. Verificando estos casos se ve que la ecuación se cumple para ambos.

iii) Si n es impar y compuesto entonces n es de la forma $n = pq$ con $3 \leq p \leq q$, es claro que $2p$ no es divisor de n, ni primo relativo con n, lo cual nos lleva a una contradicción.

De i), ii) y iii) vemos que $\tau(n) + \varphi(n) = n + 1$ solamente si n es 1, 4 o un primo. □

4.4. Otras funciones aritméticas

Ejercicio 4.17 (Hungría, 2003). Para k entero positivo, definimos $P(k)$ como el mayor divisor impar de k. Para $n \in \mathbb{Z}^+$, probar que

$$\frac{2n}{3} < \frac{P(1)}{1} + \frac{P(2)}{2} + \cdots + \frac{P(n)}{n} < \frac{2(n+1)}{3}$$

Demostración. Sea

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

Para $n = 1$ se tiene, pues

$$\frac{2 \cdot 1}{3} = \frac{2}{3} < S(1) = 1 < \frac{2(1+1)}{3} = \frac{4}{3}$$

igual que para $n = 2$

$$\frac{2 \cdot 2}{3} = \frac{4}{3} < S(2) = 1 + \frac{1}{2} = \frac{3}{2} < \frac{2(2+1)}{3} = 2$$

Supongamos que se cumple para todo $m \in \mathbb{Z}^+$ menor que n y probemos que se tiene para $n + 1$.

Es claro que $P(2k) = P(k)$.

i) Si n es par entonces $n = 2k$ para $k \in \mathbb{Z}^+$ $(k < n)$ y $n + 1 = 2k + 1$.

$$\begin{aligned} S(2k+1) &= \left(\frac{P(1)}{1} + \frac{P(3)}{3} + \cdots + \frac{P(2k+1)}{2k+1}\right) + \left(\frac{P(2)}{2} + \frac{P(4)}{4} + \cdots + \frac{P(2k)}{2k}\right) \\ &= (k+1) + \left(\frac{P(1)}{2} + \frac{P(2)}{4} + \cdots + \frac{P(k)}{2k}\right) \\ &= (k+1) + \frac{1}{2}\left(\frac{P(1)}{1} + \frac{P(2)}{2} + \cdots + \frac{P(k)}{k}\right) \\ &= (k+1) + \frac{S(k)}{2} \end{aligned}$$

Por hipótesis de inducción tenemos que

$$(k+1) + \frac{k}{3} < (k+1) + \frac{S(k)}{2} = S(2k+1) < (k+1) + \frac{k+1}{3}$$

Además se tiene que

$$\frac{2(2k+1)}{3} = \frac{4k+2}{3} < \frac{4k+3}{3} = (k+1) + \frac{k}{3}$$

y que

$$(k+1) + \frac{k+1}{3} = \frac{4(k+1)}{3} = \frac{2(2k+1+1)}{3}$$

Luego

$$\frac{2(2k+1)}{3} < S(2k+1) < \frac{2(2k+1+1)}{3}$$

y por lo tanto se tiene para $n + 1$.

ii) Si n es impar, es análogo.

□

Definición 4.18. *Sea $x \in \mathbb{R}$, definimos la parte fraccionaria de x, $\{x\}$, como*

$$\{x\} = x - \lfloor x \rfloor$$

Lema 4.19. *Sean a y b enteros con $b > 0$, q el cociente y r el residuo cuando a es dividido por b, entonces se tiene que $q = \left\lfloor \frac{a}{b} \right\rfloor$ y $r = b\left\{\frac{a}{b}\right\}$.*

Demostración. Veamos que $a = \left\lfloor \frac{a}{b} \right\rfloor b + b\left\{\frac{a}{b}\right\}$.

$$\begin{aligned} \left\lfloor \frac{a}{b} \right\rfloor b + b\left\{\frac{a}{b}\right\} &= \left\lfloor \frac{a}{b} \right\rfloor b + b\left(\frac{a}{b} - \left\lfloor \frac{a}{b} \right\rfloor\right) \\ &= \left\lfloor \frac{a}{b} \right\rfloor b + a - \left\lfloor \frac{a}{b} \right\rfloor b \\ &= a \end{aligned}$$

Además es claro que $0 \leq \left\{\frac{a}{b}\right\} < 1$, de donde se tiene que $0 \leq b\left\{\frac{a}{b}\right\} < b$. Por la unicidad de q y r se tiene que $q = \left\lfloor \frac{a}{b} \right\rfloor$ y $r = b\left\{\frac{a}{b}\right\}$. □

Ejercicio 4.20. Para n entero positivo, definimos $r(n)$ como la suma de los residuos de n al ser dividido por $1, 2, \ldots, n$. Demostrar que existen infinitos enteros positivos n tales que $r(n) = r(n-1)$.

Demostración. Por el lema anterior sabemos que

$$r(n) = \sum_{k=1}^{n} \left\{\frac{n}{k}\right\} k = \sum_{k=1}^{n} \left(n - \left\lfloor \frac{n}{k} \right\rfloor k\right)$$

Luego la condición $r(n) = r(n-1)$ es equivalente a las siguientes condiciones

$$\begin{aligned} &\sum_{k=1}^{n} \left(n - \left\lfloor \frac{n}{k} \right\rfloor k\right) = \sum_{k=1}^{n-1} \left(n - 1 - \left\lfloor \frac{n-1}{k} \right\rfloor k\right) \\ \iff & n + \sum_{k=1}^{n-1} [n - (n-1)] = \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor k - \sum_{k=1}^{n-1} \left\lfloor \frac{n-1}{k} \right\rfloor k \\ \iff & 2n - 1 = n + \sum_{k=1}^{n-1} \left(\left\lfloor \frac{n}{k} \right\rfloor k - \left\lfloor \frac{n-1}{k} \right\rfloor k \right) \end{aligned} \tag{1}$$

Si k no divide a n entonces $\left\lfloor \frac{n}{k} \right\rfloor = \left\lfloor \frac{n-1}{k} \right\rfloor$ y por lo tanto $\left\lfloor \frac{n}{k} \right\rfloor k - \left\lfloor \frac{n-1}{k} \right\rfloor k = 0$. Si k divide a n entonces $\left\lfloor \frac{n}{k} \right\rfloor = \left\lfloor \frac{n-1}{k} \right\rfloor + 1$, de donde se tiene que $\left\lfloor \frac{n}{k} \right\rfloor k - \left\lfloor \frac{n-1}{k} \right\rfloor k = k$. Luego (1) es equivalente a $2n - 1 = \sum_{k|n} k = \sigma(n)$, esta última identidad se tiene para $n = 2^m$ con m entero no negativo pues $2n - 1 = 2^{m+1} - 1 = 1 + 2 + 2^2 + \cdots + 2^m = \sigma(n)$. □

Ejercicio 4.21. Demostrar que

a) Si f es una función aritmética tal que

$$\frac{1}{\tau(n)} \sum_{d|n} f(d) = f(n), \qquad \forall n \in \mathbb{Z}^+,$$

entonces existe $c \in \mathbb{C}$ tal que $f(n) = c$, $\forall n \in \mathbb{Z}^+$.

b) Si f es una función multiplicativa tal que

$$\frac{1}{\tau(n)} \sum_{d|n} f(d) = f(n), \qquad \forall n \in \mathbb{Z}^+,$$

entonces $f(n) = 1$, $\forall n \in \mathbb{Z}^+$.

Demostración.

a) Demostraremos que $f(n) = f(1)$, $\forall n \in \mathbb{Z}^+$ (tomando $c = f(1)$ tendríamos el resultado deseado). Probaremos esto haciendo inducción sobre el número de divisores positivos de n ($\tau(n)$).

Si $\tau(n) = 1$ entonces $n = 1$ y es claro que se tiene el resultado, pues $f(1) = f(1)$. Probaremos ahora que el resultado se tiene para n con $\tau(n)$ divisores positivos, suponiendo que se cumple para todo m con $1, 2, \ldots, \tau(n) - 2$ o $\tau(n) - 1$ divisores positivos.

Vemos que $\sum_{d|n} f(d)$ es la suma de $\tau(n)$ términos, donde $\tau(n) - 1$ son de la forma $f(d)$ con $\tau(d) \leq \tau(n) - 1$ y el último término es $f(n)$. Aplicando la hipótesis de inducción obtenemos que

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

Pero

$$\sum_{d|n} f(d) = \tau(n)f(n),$$

luego $(\tau(n) - 1)f(1) + f(n) = \tau(n)f(n)$, de donde se deduce que $f(n) = f(1)$.

b) Dado que $f(1) = 1$ si f es multiplicativa, se deduce de la demostración de a) que $f(n) = f(1) = 1$, $\forall n \in \mathbb{Z}^+$.

□

Capítulo 5

La Función Parte Entera

La presente sección tiene como propósito presentar algunas propiedades de la función parte entera. Se presupone que el lector ya conoce la definición de parte entera, definida anteriormente (definición 1.34).

5.1. La mayor potencia de un primo que divide a $n!$

Teorema 5.1. *Sean $n \in \mathbb{Z}^+$, p primo y α el mayor entero tal que $p^\alpha | n!$. Se tiene que*

$$\alpha = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

Demostración 1. Sabemos que $\left\lfloor \frac{n}{p^k} \right\rfloor$ es el número de enteros positivos menores que n que son múltiplos de p^k. Luego la suma

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \tag{1}$$

es igual al número de enteros positivos menores que n que son múltiplos de p, más el número de enteros positivos menores que n que son múltiplos de p^2, más ....

Efectivamente (1) es igual a α, pues si m es un entero positivo menor que n que le aporta exactamente k primos p a la factorización como producto de primos de $n! = n \cdots (m+1) \cdot m \cdot (m-1) \cdots 2 \cdot 1$ (es decir $m^k | n$ pero $m^k + 1 \nmid n$), entonces en (1), m se cuenta exactamente k veces: cuando se cuentan los múltiplos de p, cuando se cuentan los múltiplos de p^2, ..., y finalmente cuando se cuentan los múltiplos de p^k. □

Demostración 2. El múmero de enteros positivos que le aportan exactamente k primos p a $n!$ (es decir el número de enteros m con $1 \leq m \leq n$ tales que $m^k | n$ pero $m^{k+1} \nmid n$) es igual a $\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$, en general todos ellos aportan $k\left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor\right)$ primos p a $n!$. Luego es claro que

$$\alpha = 1 \cdot \left(\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor\right) + 2 \cdot \left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor\right) + \cdots .$$

La anterior suma es en realidad finita, pues a partir de cierto punto los términos de la suma se vuelven cero (ver observación que le sigue al teorema), luego podemos agrupar sin problemas y obtener que

$$\begin{aligned} \alpha &= 1 \cdot \left(\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor\right) + 2 \cdot \left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor\right) + \cdots \\ &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \\ &= \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor . \end{aligned}$$

□

Observación. La suma anterior es en realidad una suma finita pues existe un menor $k' \in \mathbb{Z}^+$ tal que $n < p^{k'}$, luego $\left\lfloor \frac{n}{p^{k'}} \right\rfloor = 0$. En general si $N > k'$ entonces $\left\lfloor \frac{n}{p^N} \right\rfloor = 0$, observe además que si $n < p^{k'}$ entonces

$$\begin{aligned} \log n &< k' \log p \\ \frac{\log n}{\log p} &< k'. \end{aligned}$$

Así que en vez de hacer la suma, que calcula α, de $k = 0$ hasta ∞, la podemos hacer hasta $\left\lfloor \frac{\log n}{\log p} \right\rfloor$.

Corolario 5.2.

$$n! = \prod_{\substack{p \leq n \\ p \text{ primo}}} p^{\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor} = \prod_{\substack{p \leq n \\ p \text{ primo}}} p^{\sum_{k=1}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor}$$

Corolario 5.3. *Sean $n \in \mathbb{Z}^+$, $a = p_1 p_2 \cdots p_m$ y α el mayor entero tal que $a^\alpha | n!$, se tiene que*

$$\alpha = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor ,$$

donde $p = \max\{p_1, p_2, \cdots, p_m\}$.

Demostración. Sea $n! = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} h$ donde $p_i \nmid h$, $\forall i = 1, \ldots, m$. Suponiendo que $p_1 < p_2 < \cdots < p_m = p$ es claro que $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_m$, luego existe r_i entero no negativo tal que $\alpha_i = \alpha_m + r_i$, $\forall i = 1, \ldots, m-1$. Luego

$$n! = p_1^{r_1} p_2^{r_2} \cdots p_{m-1}^{r_{m-1}} a^{\alpha_m} h.$$

Por el teorema anterior

$$\alpha = \alpha_m = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

□

Ejercicio 5.4. Sea $n \in \mathbb{Z}^+$, definimos $N(n)$ como el números de ceros que aparecen al final de la expresión decimal de $n!$, por ejemplo:
$N(1) = 0$ pues $1! = 1$
$N(2) = 0$ pues $2! = 2$
$N(3) = 0$ pues $3! = 6$
$\vdots$
$N(10) = 2$ pues $10! = 36288\underbrace{00}_{2}$.
Demostrar que

$$N(n) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{5^k} \right\rfloor = \sum_{k=1}^{\left\lfloor \frac{\log n}{\log 5} \right\rfloor} \left\lfloor \frac{n}{5^k} \right\rfloor.$$

Demostración. Tomar $a = 10$ y aplicar el corolario anterior. □

Ejercicio 5.5. Sea p primo y α el mayor entero tal que $p^\alpha | n!$. Demostrar que

$$\alpha = \frac{n - S_p(n)}{p-1},$$

donde $S_p(n)$ es igual a la suma de los dígitos de n en base p.

Demostración. Sea $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$ donde $a_i \in \{0, 1, \ldots, p-1\}$ $\forall i = 0, 1, \ldots k$.

Teniendo en cuenta que $0 \leq \frac{a_i}{p} < 1$, $\forall i = 0, 1, \ldots, k$, tenemos que

$$\begin{aligned}
n &= a_k p^k + a_{k-1} p^{k-1} + \cdots + a_2 p^2 + a_1 p + a_0 \\
\left\lfloor \frac{n}{p} \right\rfloor &= a_k p^{k-1} + a_{k-1} p^{k-2} + \cdots + a_2 p + a_1 \\
\left\lfloor \frac{n}{p^2} \right\rfloor &= a_k p^{k-2} + a_{k-1} p^{k-3} + \cdots + a_2 \\
&\vdots \\
\left\lfloor \frac{n}{p^{k-1}} \right\rfloor &= a_k p + a_{k-1} \\
\left\lfloor \frac{n}{p^k} \right\rfloor &= a_k
\end{aligned}$$

Luego

$$\begin{aligned}
\alpha &= \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \\
&= \sum_{i=1}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor \\
&= a_k \left(1 + p + \cdots + p^{k-1}\right) + a_{k-1} \left(1 + p + \cdots + p^{k-2}\right) + \cdots + a_2(1 + p) + a_1,
\end{aligned}$$

de donde se tiene que

$$\begin{aligned}
(p-1)\alpha &= a_k \left(p^k - 1\right) + a_{k-1} \left(p^{k-1} - 1\right) + \cdots + a_2 \left(p^2 - 1\right) + a_1(p-1) \\
&= \left(a_k p^k + a_{k-1} p^{k-1} + \cdots + a_2 p^2 + a_1 p\right) - (a_k + a_{k-1} + \cdots + a_2 + a_1) \\
&= \left(a_k p^k + a_{k-1} p^{k-1} + \cdots + a_2 p^2 + a_1 p + a_0\right) - (a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0) \\
&= n - S_p(n),
\end{aligned}$$

es decir

$$\alpha = \frac{n - S_p(n)}{p-1}.$$

□

Lema 5.6. *Sean $a_1, a_2, \ldots, a_r$ enteros no negativos tales que $a_1 + a_2 + \cdots + a_r = n$. Se tiene que*

$$\binom{n}{a_1, a_2, \ldots, a_r} = \frac{n!}{a_1! a_2! \cdots a_r!}$$

es un entero.

Demostración. Sabemos que para $x_1, x_2, \ldots, x_r \in \mathbb{R}$ se tiene que

$$\lfloor x_1 \rfloor + \lfloor x_2 \rfloor + \cdots + \lfloor x_r \rfloor \leq \lfloor x_1 + x_2 + \cdots + x_r \rfloor ,$$

en especial

$$\left\lfloor \frac{a_1}{p_k} \right\rfloor + \left\lfloor \frac{a_2}{p_k} \right\rfloor + \cdots + \left\lfloor \frac{a_r}{p_k} \right\rfloor \leq \left\lfloor \frac{a_1 + a_2 + \cdots + a_r}{p_k} \right\rfloor = \left\lfloor \frac{n}{p_k} \right\rfloor ,$$

para todo primo p y entero positivo k. Luego

$$\sum_{k=1}^{\infty} \left\lfloor \frac{a_1}{p_k} \right\rfloor + \sum_{k=1}^{\infty} \left\lfloor \frac{a_2}{p_k} \right\rfloor + \cdots + \sum_{k=1}^{\infty} \left\lfloor \frac{a_r}{p_k} \right\rfloor \leq \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p_k} \right\rfloor . \tag{1}$$

Si p es primo y α el mayor entero tal que $p^{\alpha} | n!$ y α_i el mayor entero tal que $p^{\alpha_i} | a_i!$, $\forall i = 1, \ldots, r$, entonces es claro, según (1), que

$$\alpha_1 + \alpha_2 + \cdots + \alpha_r \leq \alpha,$$

lo que significa que en $\frac{n!}{a_1! a_2! \cdots a_r!}$, el denominador se cancela con parte del numerador obteniendose así un entero. □

Corolario 5.7. *Si $1 \leq r \leq n$ entonces $\binom{n}{r}$ es un entero.*

Corolario 5.8. *El producto de r enteros positivos consecutivos es divisible por $r!$.*

Demostración. Sean $n, n-1, n-2, \ldots, n-r+1$ los r enteros consecutivos, vemos que

$$\frac{n(n-1)\cdots(n-r+1)}{r!} = \binom{n}{r},$$

el cual es un entero. Luego

$$n(n-1)\cdots(n-r+1) = r!\binom{n}{r},$$

de donde se tiene que $r! | n(n-1)\cdots(n-r+1)$. □

Ejercicio 5.9. Sea p primo y α el mayor entero tal que $p^{\alpha} | \prod_{i=1}^{n} 2i$, demuestre que

$$\alpha = \begin{cases} n + \sum\limits_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor , & \text{si } p = 2 \\ \sum\limits_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor , & \text{si } p \text{ es un primo impar.} \end{cases}$$

Demostración. Sabemos que $\prod_{i=1}^{n} 2i = 2^n n!$, de aquí es claro que

$$\alpha = n + \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor, \qquad \text{si } p = 2.$$

Si p es primo impar entonces $p^\alpha | \prod_{i=1}^{n} 2i$ implica que $p^\alpha | \prod_{i=1}^{n} i = n!$, de donde es claro que

$$\alpha = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

□

Ejercicio 5.10.

a) Sea p primo y α el mayor entero tal que $p^\alpha | \prod_{i=0}^{n}(2i+1)$, demuestre que

$$\alpha = \begin{cases} 0, & \text{si } p = 2 \\ \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n+1}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor \right), & \text{si } p \text{ es un primo impar.} \end{cases}$$

b) Demostrar que

$$n = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n+1}{2^k} \right\rfloor - \left\lfloor \frac{n}{2^k} \right\rfloor \right), \qquad \forall n \in \mathbb{Z}^+$$

Demostración.

a)

i) Si $p = 2$ es claro que $\alpha = 0$, pues $\prod_{i=0}^{n}(2i+1)$ es el producto de enteros impares.

ii) Sea p primo impar, es claro que

$$\prod_{i=0}^{n}(2i+1) = 1 \cdot 3 \cdots (2n+1) = \frac{(2n+1)!}{2^n n!},$$

de aquí es fácil ver que

$$\alpha = \sum_{k=1}^{\infty} \left\lfloor \frac{2n+1}{p^k} \right\rfloor - \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

b) Calculando α para $p = 2$ de la misma forma como se calculó α para p primo impar en ii), se tiene que

$$\alpha = \sum_{k=1}^{\infty} \left\lfloor \frac{2n+1}{2^k} \right\rfloor - \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor - n,$$

pero por a) (i)) se tiene que $\alpha = 0$, luego

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

□

5.2. Ejercicios Adicionales

Lema 5.11. *Sea $x \in \mathbb{R}$ y n un entero positivo, se tiene que*

a) $\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor$.

b) $\left\lfloor \frac{x}{n} \right\rfloor + \left\lfloor \frac{x+1}{n} \right\rfloor + \cdots + \left\lfloor \frac{x+n-1}{n} \right\rfloor = \lfloor x \rfloor$.

Demostración.

a) Sea $x = \lfloor x \rfloor + \frac{\alpha}{n}$, donde $0 \leq \alpha < n$ con $\alpha \in \mathbb{R}$, se tiene entonces que

$$\lfloor nx \rfloor = \lfloor n \lfloor x \rfloor + \alpha \rfloor = n \lfloor x \rfloor + \lfloor \alpha \rfloor . \tag{1}$$

Vemos que

$$\begin{aligned}
\sum_{k=0}^{n-1} \left\lfloor x + \frac{k}{n} \right\rfloor &= \sum_{k=0}^{n-1} \left\lfloor \lfloor x \rfloor + \frac{\alpha + k}{n} \right\rfloor \\
&= n \lfloor x \rfloor + \sum_{k=0}^{n-1} \left\lfloor \frac{\alpha + k}{n} \right\rfloor \\
&= n \lfloor x \rfloor + \sum_{k=1}^{n} \left\lfloor \frac{\alpha + n - k}{n} \right\rfloor \\
&= n \lfloor x \rfloor + \sum_{k=1}^{\lfloor \alpha \rfloor} \left\lfloor \frac{\alpha + n - k}{n} \right\rfloor \qquad \left(\text{pues } \left\lfloor \frac{\alpha + n - k}{n} \right\rfloor = 0, \text{ si } \lfloor \alpha \rfloor + 1 \leq k \leq n\right) \\
&= n \lfloor x \rfloor + \sum_{k=1}^{\lfloor \alpha \rfloor} 1 \\
&= n \lfloor x \rfloor + \lfloor \alpha \rfloor \\
&= \lfloor nx \rfloor . \qquad (\text{por } (1))
\end{aligned}$$

b) Se obtiene de a) reemplazando x por $\frac{x}{n}$.

□

Ejercicio 5.12. Sean $x, y \in \mathbb{R}$ y $n \in \mathbb{Z}^+$, demostrar que

$$\lfloor x \rfloor + \lfloor y \rfloor + n \lfloor x + y \rfloor \leq \lfloor (n+1)x \rfloor + \lfloor (n+1)y \rfloor$$

Demostración. Sean $x = \lfloor x \rfloor + a$ con $0 \leq a < 1$ y $y = \lfloor y \rfloor + b$ con $0 \leq b < 1$. Por un lado tenemos que

$$\begin{aligned} \lfloor x \rfloor + \lfloor y \rfloor + n \lfloor x + y \rfloor &= \lfloor x \rfloor + \lfloor y \rfloor + n \lfloor \lfloor x \rfloor + \lfloor y \rfloor + a + b \rfloor \\ &= \lfloor x \rfloor + \lfloor y \rfloor + n (\lfloor x \rfloor + \lfloor y \rfloor) + n \lfloor a + b \rfloor \\ &= (n+1) (\lfloor x \rfloor + \lfloor y \rfloor) + n \lfloor a + b \rfloor . \end{aligned}$$

Por el otro lado tenemos que

$$\begin{aligned} \lfloor (n+1)x \rfloor + \lfloor (n+1)y \rfloor &= \lfloor (n+1) \lfloor x \rfloor + (n+1)a \rfloor + \lfloor (n+1) \lfloor y \rfloor + (n+1)b \rfloor \\ &= (n+1) \lfloor x \rfloor + \lfloor (n+1)a \rfloor + (n+1) \lfloor y \rfloor + \lfloor (n+1)b \rfloor \\ &= (n+1) (\lfloor x \rfloor + \lfloor y \rfloor) + \lfloor (n+1)a \rfloor + \lfloor (n+1)b \rfloor . \end{aligned}$$

Luego basta con demostrar que

$$n \lfloor a + b \rfloor \leq \lfloor (n+1)a \rfloor + \lfloor (n+1)b \rfloor . \tag{1}$$

Si $0 \leq a + b < 1$, es claro que se cumple la desigualdad (1). Si $a + b \geq 1$, $\lfloor a + b \rfloor = 1$ (recordemos que $a, b < 1$ luego $a + b < 2$) y por lo tanto (1) es equivalente a

$$n \leq \lfloor (n+1)a \rfloor + \lfloor (n+1)b \rfloor . \tag{2}$$

Para $a + b \geq 1$, se tiene que $(n+1)a + (n+1)b = (n+1)(a+b) \geq n+1$, luego $\lfloor (n+1)a + (n+1)b \rfloor \geq n+1$. Recordemos que para x' y y' reales se tiene que $\lfloor x' \rfloor + \lfloor y' \rfloor \geq \lfloor x' + y' \rfloor - 1$, luego

$$\lfloor (n+1)a \rfloor + \lfloor (n+1)b \rfloor \geq \lfloor (n+1)a + (n+1)b \rfloor - 1 \geq n,$$

obteniendo así (2). □

Ejercicio 5.13. Sea x un real y $n \in \mathbb{Z}^+$, demostrar que

$$\lfloor \sqrt[n]{x} \rfloor = \left\lfloor \sqrt[n]{\lfloor x \rfloor} \right\rfloor .$$

Demostración. Sabemos que

$$\lfloor \sqrt[n]{x} \rfloor \leq \sqrt[n]{x} < \lfloor \sqrt[n]{x} \rfloor + 1.$$

Luego

$$\left\lfloor \sqrt[n]{x} \right\rfloor^n \leq x < \left(\left\lfloor \sqrt[n]{x} \right\rfloor + 1 \right)^n,$$

de donde se tiene

$$\left\lfloor \sqrt[n]{x} \right\rfloor^n \leq \lfloor x \rfloor \leq x < \left(\left\lfloor \sqrt[n]{x} \right\rfloor + 1 \right)^n.$$

Luego

$$\left\lfloor \sqrt[n]{x} \right\rfloor \leq \sqrt[n]{\lfloor x \rfloor} < \left\lfloor \sqrt[n]{x} \right\rfloor + 1,$$

es decir

$$\left\lfloor \sqrt[n]{\lfloor x \rfloor} \right\rfloor = \left\lfloor \sqrt[n]{x} \right\rfloor.$$

□

Ejercicio 5.14. Sean $0 < k < n$ enteros positivos, demostrar que

$$\sum_{j=1}^{k} \left\lfloor \frac{n-j}{k} \right\rfloor = n - k.$$

Demostración. Como $0 < k < n$, existen q y r enteros positivos con $n = qk + r$, $0 \leq r < k$. Luego

$$\begin{aligned}
\sum_{j=1}^{k} \left\lfloor \frac{n-j}{k} \right\rfloor &= \sum_{j=1}^{k} \left\lfloor q + \frac{r-j}{k} \right\rfloor \\
&= \sum_{j=1}^{k} \left(q + \left\lfloor \frac{r-j}{k} \right\rfloor \right) \\
&= qk + \sum_{j=1}^{k} \left\lfloor \frac{r-j}{k} \right\rfloor \\
&= qk + \sum_{j=r+1}^{k} \left\lfloor \frac{r-j}{k} \right\rfloor \qquad \left(\text{pues } \left\lfloor \frac{r-j}{k} \right\rfloor = 0 \text{ si } 1 \leq j \leq r \right) \\
&= qk + \sum_{j=1}^{k-r} \left\lfloor \frac{-j}{k} \right\rfloor \\
&= qk + (k-r)(-1) \\
&= qk - k + r \\
&= (qk + r) - k \\
&= n - k.
\end{aligned}$$

□

Ejercicio 5.15. Sea $n \in \mathbb{Z}^+$, demostrar que

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} - \frac{1}{2} \right\rfloor = n.$$

Demostración. Por el lema 5.11, parte a), sabemos que $\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor$, es decir $\left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor - \lfloor x \rfloor$. Tomando $x = \frac{2}{2^{k+1}}$ con k entero no negativo, se tiene que

$$\left\lfloor \frac{n}{2^{k+1}} \right\rfloor + \left\lfloor \frac{1}{2} \right\rfloor = \left\lfloor \frac{n}{2^k} \right\rfloor - \left\lfloor \frac{n}{2^{k+1}} \right\rfloor,$$

luego

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} - \frac{1}{2} \right\rfloor = \sum_{k=0}^{\infty} \left\lfloor \frac{n}{2^{k+1}} - \frac{1}{2} \right\rfloor = \sum_{k=0}^{\infty} \left(\left\lfloor \frac{n}{2^k} \right\rfloor - \left\lfloor \frac{n}{2^{k+1}} \right\rfloor \right).$$

Observe que $\left\lfloor \frac{n}{2^k} \right\rfloor - \left\lfloor \frac{n}{2^{k+1}} \right\rfloor$ es el número de enteros positivos menores que n que son divisibles por 2^k, pero no por 2^{k+1}, luego

$$\sum_{k=0}^{\infty} \left(\left\lfloor \frac{n}{2^k} \right\rfloor - \left\lfloor \frac{n}{2^{k+1}} \right\rfloor \right) = n,$$

pues para todo entero positivo m menor que n, existe un único entero k no negativo (que depende de m) tal que $2^k | m$ pero $2^{k+1} \nmid m$. □

Ejercicio 5.16. Sean $n \in \mathbb{Z}^+$ y $H_n = \{(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid xy \leq n\}$, demostrar que

$$\#H_n = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor = 2 \sum_{k=1}^{\lfloor \sqrt{n} \rfloor} \left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \sqrt{n} \right\rfloor^2.$$

Demostración. La desigualdad $xy \leq n$ es equivalente a $x \leq \frac{n}{y}$, luego para un y fijo, el número de enteros x tales que $x \leq \frac{n}{y}$ es igual a $\left\lfloor \frac{n}{y} \right\rfloor$, variando y entre 1 y n se tiene entonces que

$$\#H_n = \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor.$$

Para demostrar la segunda identidad, observemos primero que si $x > \lfloor \sqrt{n} \rfloor$ y $y > \lfloor \sqrt{n} \rfloor$ entonces $x \geq \lfloor \sqrt{n} \rfloor + 1 > \sqrt{n}$ y $y \geq \lfloor \sqrt{n} \rfloor + 1 > \sqrt{n}$, luego $xy > n$. Así que $H_n = A \cup B$, donde

$$A = \left\{ (x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid xy \leq n \text{ y } 1 \leq x \leq \left\lfloor \sqrt{n} \right\rfloor \right\}$$

y

$$B = \left\{ (x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid xy \leq n \text{ y } 1 \leq y \leq \left\lfloor \sqrt{n} \right\rfloor \right\}.$$

Sea x con $1 \leq x \leq \lfloor \sqrt{n} \rfloor$, es claro que el número de y's tales que $xy \leq n$ es igual a $\left\lfloor \frac{n}{x} \right\rfloor$, luego

$$\#A = \sum_{k=1}^{\lfloor \sqrt{n} \rfloor} \left\lfloor \frac{n}{k} \right\rfloor.$$

Análogamente se obtiene que

$$\#B = \sum_{k=1}^{\lfloor \sqrt{n} \rfloor} \left\lfloor \frac{n}{k} \right\rfloor.$$

Por otro lado se observa que si $1 \leq x \leq \lfloor \sqrt{n} \rfloor$ y $1 \leq y \leq \lfloor \sqrt{n} \rfloor$ entonces se tiene que $xy \leq n$, luego

$$A \cap B = \left\{ (x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid 1 \leq x, y \leq \lfloor \sqrt{n} \rfloor \right\}$$

y por lo tanto $\#A \cap B = \lfloor \sqrt{n} \rfloor^2$.

Finalmente tenemos que

$$\begin{aligned} \#H_n &= \#A + \#B - \#A \cap B \\ &= 2 \sum_{k=1}^{\lfloor \sqrt{n} \rfloor} \left\lfloor \frac{n}{k} \right\rfloor - \lfloor \sqrt{n} \rfloor^2. \end{aligned}$$

□

Ejercicio 5.17. Demostrar que para todo entero no negativo n, se tiene que

$$\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{8} \right\rfloor + \left\lfloor \frac{n+8}{16} \right\rfloor + \cdots = n.$$

Demostración. Si $n = 0$, es claro que se cumple. Si $n > 0$, representando a n en base 2, $n = a_0 + a_1 2 + a_2 2^2 + \cdots + a_m 2^m$ donde los $a_i \in \{0, 1\}$ para $i = 1, \cdots, m-1$ y

$a_m = 1$. Vemos que

$$\begin{aligned}
\left\lfloor \frac{n+1}{2} \right\rfloor &= \left\lfloor \frac{n}{2} + \frac{1}{2} \right\rfloor = \left\lfloor \frac{a_0}{2} + a_1 + a_2 2 + \cdots + a_m 2^{m-1} + \frac{1}{2} \right\rfloor \\
&= a_1 + a_2 2 + \cdots + a_m 2^{m-1} + \left\lfloor \frac{a_0}{2} + \frac{1}{2} \right\rfloor \\
\left\lfloor \frac{n+2}{4} \right\rfloor &= \left\lfloor \frac{n}{4} + \frac{1}{2} \right\rfloor = \left\lfloor \frac{a_0}{4} + \frac{a_1}{2} + a_2 + a_3 2 + \cdots + a_m 2^{m-2} + \frac{1}{2} \right\rfloor \\
&= a_2 + a_3 2 + \cdots + a_m 2^{m-2} + \left\lfloor \frac{a_0}{4} + \frac{a_1}{2} + \frac{1}{2} \right\rfloor \\
&\vdots \\
\left\lfloor \frac{n+2^{m-1}}{2^m} \right\rfloor &= a_m + \left\lfloor \frac{a_0}{2^m} + \frac{a_1}{2^{m-1}} + \cdots + \frac{a_{m-1}}{2} + \frac{1}{2} \right\rfloor \\
\left\lfloor \frac{n+2^m}{2^{m+1}} \right\rfloor &= \left\lfloor \frac{a_0}{2^{m+1}} + \frac{a_1}{2^m} + \cdots + \frac{a_m}{2} + \frac{1}{2} \right\rfloor .
\end{aligned}$$

Probaremos entonces que si $1 \leq k \leq m+1$, entonces

$$\left\lfloor \frac{a_0}{2^k} + \frac{a_1}{2^{k-1}} + \cdots + \frac{a_{k-1}}{2} + \frac{1}{2} \right\rfloor = a_{k-1}.$$

Sabemos que

$$\begin{aligned}
\frac{a_0}{2^k} + \frac{a_1}{2^{k-1}} + \cdots + \frac{a_{k-2}}{2^2} &\leq \sum_{i=2}^{k} \left(\frac{1}{2}\right)^i \\
&< \sum_{i=2}^{\infty} \left(\frac{1}{2}\right)^i \\
&= \sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i - \left(1 + \frac{1}{2}\right) \\
&= 2 - \left(1 + \frac{1}{2}\right) \\
&= \frac{1}{2}.
\end{aligned}$$

Luego es claro que si $a_{k-1} = 0$, entonces

$$\left\lfloor \frac{a_0}{2^k} + \frac{a_1}{2^{k-1}} + \cdots + \frac{a_{k-1}}{2} + \frac{1}{2} \right\rfloor = 0,$$

y si $a_{k-1} = 1$, entonces

$$\left\lfloor \frac{a_0}{2^k} + \frac{a_1}{2^{k-1}} + \cdots + \frac{a_{k-1}}{2} + \frac{1}{2} \right\rfloor = 1.$$

Es decir

$$\left\lfloor \frac{a_0}{2^k} + \frac{a_1}{2^{k-1}} + \cdots + \frac{a_{k-1}}{2} + \frac{1}{2} \right\rfloor = a_{k-1}.$$

Luego

$$\begin{aligned}
\left\lfloor \frac{n+1}{2} \right\rfloor &= a_0 + a_1 + a_2 2 + a_3 2^2 + \cdots + a_{m-1} 2^{m-2} + a_m 2^{m-1} \\
\left\lfloor \frac{n+2}{4} \right\rfloor &= a_1 + a_2 + a_3 2 + \cdots + a_{m-1} 2^{m-3} + a_m 2^{m-2} \\
&\vdots \\
\left\lfloor \frac{n+2^{m-1}}{2^m} \right\rfloor &= a_{m-1} + a_m \\
\left\lfloor \frac{n+2^m}{2^{m+1}} \right\rfloor &= a_m,
\end{aligned}$$

de donde se tiene que

$$\begin{aligned}
\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \cdots + \left\lfloor \frac{n+2^m}{2^{m+1}} \right\rfloor &= a_0 + a_1(1+1) + a_2(1+1+2) + a_3(1+1+2+2^2) \\
&\quad + \cdots + a_{m-1}(1+1+2+2^2+\cdots+2^{m-2}) \\
&\quad + a_m(1+1+2+2^2+\cdots+2^{m-1}) \\
&= a_0 + a_1 2 + a_2 2^2 + \cdots + a_{m-1} 2^{m-1} + a_m 2^m \\
&= n.
\end{aligned}$$

Para completar el ejercicio, basta con probar que si $k > m+1$, entonces

$$\left\lfloor \frac{n+2^{k-1}}{2^k} \right\rfloor = 0.$$

Observe que

$$\begin{aligned}
\left\lfloor \frac{n+2^{k-1}}{2^k} \right\rfloor &\iff \frac{n+2^{k-1}}{2^k} < 1 \\
&\iff n + 2^{k-1} < 2^k \\
&\iff n < 2^{k-1} \\
&\iff \log_2 n < k-1 \\
&\iff \log_2 n + 1 < k. \qquad (1)
\end{aligned}$$

Como k es entero, (1) ocurre sii

$$\lfloor \log_2 n + 1 \rfloor < k \iff \lfloor \log_2 n \rfloor + 1 < k \iff m+1 < k,$$

que es lo que estábamos buscando. □

Teorema 5.18. *Sean m y n enteros positivos tales que $(m,n)=d$. Se tiene que*

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

En especial si $(m,n)=1$, entonces

$$\sum_{k=1}^{n-1}\left\lfloor\frac{mk}{n}\right\rfloor=\frac{(m-1)(n-1)}{2}.$$

Demostración. Consideremos los siguientes conjuntos

$$\begin{aligned}R&=\left\{\langle x,y\rangle\in\mathbb{Z}^+\times\mathbb{Z}^+\mid 1\leq x<n, 1\leq y<m\right\}\\ R_1&=\left\{\langle x,y\rangle\in R\mid y=\frac{mx}{n}\right\}\\ R_2&=\left\{\langle x,y\rangle\in R\mid y\leq\frac{mx}{n}\right\}\\ R_3&=\left\{\langle x,y\rangle\in R\mid y\geq\frac{mx}{n}\right\}.\end{aligned}$$

Es claro que $\#R=(m-1)(n-1)$. Para k, con $1\leq k\leq n-1$, existen $\left\lfloor\frac{mk}{n}\right\rfloor$ elementos de R entre el segmento que une $\langle k,0\rangle$ y $\left\langle k,\frac{mk}{n}\right\rangle$. Luego

$$\#R_2=\sum_{k=1}^{n-1}\left\lfloor\frac{mk}{n}\right\rfloor.$$

Por simetría se tiene que $\#R_2=\#R_3$.

Como $(m,n)=d$ entonces existen $(a,b)=1$ tales que $m=ad$ y $n=bd$, por lo tanto si $\langle x,y\rangle\in R_1$, entonces $y=\frac{mx}{n}=\frac{a}{b}x$. Es claro que para que y sea un entero positivo, x tiene que ser un múltiplo de b. Dado que $1\leq x\leq n-1$, los valores de x que nos sirven son $b,2b,\cdots,(d-1)b$, luego $\#R_1=d-1$.

Como $R=R_2\cup R_3$ y $R_2\cap R_3=R_1$, entonces

$$\#R=\#R_2+\#R_3-\#R_1,$$

es decir

$$(m-1)(n-1)=2\sum_{k=1}^{n-1}\left\lfloor\frac{mk}{n}\right\rfloor-d-1.$$

Despejando, debidamente, obtenemos el resultado deseado. □

Corolario 5.19. *Para todos los enteros positivos m y n, se tiene que*

$$(m,n)=2\sum_{k=1}^{n-1}\left\lfloor\frac{mk}{n}\right\rfloor+m+n-mn.$$

Demostración. Consecuencia inmediata del teorema anterior. □

Ejercicio 5.20. Sea $\alpha \in \mathbb{R}$, demostrar que

$$\lim_{n\to\infty} \frac{\lfloor n\alpha \rfloor}{n} = \alpha.$$

Demostración. Sea $n\alpha = \lfloor n\alpha \rfloor + \beta$ con $0 \leq \beta < 1$, de donde $n\alpha - \beta = \lfloor n\alpha \rfloor$. Luego

$$\lim_{n\to\infty} \frac{\lfloor n\alpha \rfloor}{n} = \lim_{n\to\infty} \left(\alpha - \frac{\beta}{n}\right) = \alpha.$$

□

Ejercicio 5.21. Demostrar que

$$\lim_{n\to\infty} \left\lfloor \cos^2(n!\pi x) \right\rfloor = \begin{cases} 1, & \text{si } x \in \mathbb{Q} \\ 0, & \text{si } x \in \mathbb{R} - \mathbb{Q}. \end{cases}$$

Demostración.

i) Sea $x \in \mathbb{Q}$, luego $\frac{a}{b}$ con $a, b \in \mathbb{Z}$ y $b \neq 0$, luego $bx \in \mathbb{Z}$ y por lo tanto $b!x$ también, en general si $n \geq b$, entonces $n!x \in \mathbb{Z}$ y por lo tanto $\lfloor \cos^2(n!\pi x) \rfloor = cos^2(n!\pi x) = 1$ (la sucesión se vuelve constante para $n \geq b$), luego $\lim_{n\to\infty} \lfloor \cos^2(n!\pi x) \rfloor = 1$.

ii) Si $x \in \mathbb{R} - \mathbb{Q}$ entonces $n!x \in \mathbb{R} - \mathbb{Q}$, de donde se tiene que $0 \leq \cos^2(n!\pi x) < 1$, luego $\lfloor \cos^2(n!\pi x) \rfloor = 0, \forall n \in \mathbb{Z}$, de donde se tiene que $\lim_{n\to\infty} \lfloor \cos^2(n!\pi x) \rfloor = 0$.

□

Capítulo 6

Los Teoremas de Euler, Fermat y Wilson

El presente capítulo tiene como objetivo presentar algunas consecuencias de los teoremas de Euler, Fermat y Wilson, se presupone que el lector ya conoce estos teoremas.

6.1. Consecuencias de estos Teoremas

Ejercicio 6.1. Sea $n = a_1 a_2 \cdots a_m$ donde los a_k's son enteros positivos tales que $(a_i, a_j) = 1$, si $i \neq j$. Demostrar que

$$a_1^{\varphi(n)/\varphi(a_1)} + a_2^{\varphi(n)/\varphi(a_2)} + \cdots + a_m^{\varphi(n)/\varphi(a_m)} \equiv m - 1 \mod n.$$

Demostración. Por el Teorema de Euler se tiene que $a_i^{\varphi(a_j)} \equiv 1 \mod a_j$, para $i \neq j$. Utilizando el hecho de que $\varphi(n) = \varphi(a_1)\varphi(a_2)\cdots\varphi(a_m)$ por ser φ multiplicativa, vemos que

$$\left(a_i^{\varphi(a_j)}\right)^{\frac{\varphi(n)}{\varphi(a_i)\varphi(a_j)}} \equiv 1^{\frac{\varphi(n)}{\varphi(a_i)\varphi(a_j)}} \mod a_j,$$

es decir $a_i^{\varphi(n)/\varphi(a_i)} \equiv 1 \mod a_j$, para $i \neq j$.

Si $i = j$ entonces $a_i^{\varphi(n)/\varphi(a_i)} \equiv 0 \mod a_j$. Luego para un j fijo, se tiene que

$$a_1^{\varphi(n)/\varphi(a_1)} + a_2^{\varphi(n)/\varphi(a_2)} + \cdots + a_m^{\varphi(n)/\varphi(a_m)} \equiv m - 1 \mod a_j.$$

Como $(a_i, a_j) = 1$, si $i \neq j$, entonces

$$a_1^{\varphi(n)/\varphi(a_1)} + a_2^{\varphi(n)/\varphi(a_2)} + \cdots + a_m^{\varphi(n)/\varphi(a_m)} \equiv m - 1 \mod n.$$

□

Lema 6.2. *Si p y q son primos distintos y a un entero tal que $a^p \equiv a \bmod q$ y $a^q \equiv a \bmod p$, entonces $a^{pq} \equiv a \bmod pq$.*

Demostración. Utilizando el Pequeño Teorema de Fermat tenemos que $a^{pq} \equiv (a^p)^q \equiv a^p \bmod q$, además sabemos que por hipótesis $a^p \equiv a \bmod q$, luego $q|a^{pq} - a$. Análogamente tenemos que $p|a^{pq} - a$. Por ser $(p, q) = 1$ entonces $pq|a^{pq} - a$, luego $a^{pq} \equiv a \bmod pq$. □

Ejercicio 6.3. Sean $a, b \in \mathbb{Z}$ tales que $a^p \equiv b^p \mod p$, con p primo, demostrar que $a^p \equiv b^p \mod p^2$.

Demostración. Por el Pequeño Teorema de Fermat sabemos que

$$\begin{aligned} a^p &\equiv a \mod p \\ b^p &\equiv b \mod p. \end{aligned}$$

Luego $a \equiv b \mod p$ pues $a^p \equiv b^p \mod p$, luego existe $k \in \mathbb{Z}$ tal que $a = b + kp$, de donde se tiene que

$$\begin{aligned} a^p &= (b + kp)^p \\ &= b^p + \binom{p}{1} b^{p-1} kp + \binom{p}{2} b^{p-2} k^2 p^2 + \cdots + k^p p^p \\ &= b^p + b^{p-1} kp^2 + p^2 \left[\binom{p}{2} b^{p-2} k^2 + \cdots + k^p p^{p-2} \right]. \end{aligned}$$

Luego $a^p \equiv b^p \mod p^2$. □

Ejercicio 6.4. Sean p primo y a un entero cualquiera, demostrar que

$$p|a^p + a(p-1)!.$$

Demostración. Por el Pequeño Teorema de Fermat y por el Teorema de Wilson tenemos respectivamente que $a^p \equiv a \mod p$ y que $a(p-1)! \equiv -a \mod p$, luego $a^p + a(p-1)! \equiv 0 \mod p$. □

Ejercicio 6.5. Demostrar que para $n \in \mathbb{Z}$ y p, q primos se tiene que

$$\frac{n^p}{p} + \frac{n^q}{q} + \frac{(pq - p - q)n}{pq}$$

es un entero

Demostración. Observemos que

$$n - \frac{n}{p} - \frac{n}{q} = \frac{(pq - p - q)n}{pq}.$$

Luego

$$\frac{n^p}{p} + \frac{n^q}{q} + \frac{(pq - p - q)n}{pq} = \frac{n^p - n}{p} + \frac{n^q - n}{q} + n$$

es un entero pues $p|n^p - n$ y $q|n^q - n$ por el Pequeño Teorema de Fermat. □

Teorema 6.6. *Sean* $(m,n)=1$*, luego*

$$n^{\varphi(m)}+m^{\varphi(n)}\equiv 1 \mod mn$$

.

Demostración. Por el Teorema de Euler se tiene que

$$\begin{aligned} n^{\varphi(m)} &\equiv 1 \mod m \\ m^{\varphi(n)} &\equiv 1 \mod n, \end{aligned}$$

además es claro que

$$\begin{aligned} m^{\varphi(n)} &\equiv 0 \mod m \\ n^{\varphi(m)} &\equiv 0 \mod n. \end{aligned}$$

Luego

$$n^{\varphi(m)}+m^{\varphi(n)}\equiv 1 \mod m$$

y

$$n^{\varphi(m)}+m^{\varphi(n)}\equiv 1 \mod n,$$

como $(m,n)=1$, entonces

$$n^{\varphi(m)}+m^{\varphi(n)}\equiv 1 \mod mn$$

. □

Corolario 6.7. *Si* p *y* q *son primos entonces* $p^{q-1}+q^{p-1}\equiv 1 \mod pq$.

Teorema 6.8. *Sean* a *y* n *enteros positivos con* $a\neq 1$ *y* $(a,n)=(a-1,n)=1$*. Se tiene que*

$$1+a+a^2+\cdots+a^{\varphi(n)-1}\equiv 0 \mod n.$$

Demostración. Como $(a,n)=1$ entonces por el Teorema de Euler se tiene que

$$n|a^{\varphi(n)}-1=(a-1)\left(1+a+a^2+\cdots+a^{\varphi(n)-1}\right).$$

Como $(a-1,n)=1$ entonces $n|1+a+a^2+\cdots+a^{\varphi(n)-1}$. □

Lema 6.9. *Sea* p *un primo tal que* $p\nmid a$*. Se tiene que*

$$a^{k(p-1)}\equiv 1 \mod p,$$

donde $k\in\mathbb{Z}^+$.

Demostración. Por el Pequeño Teorema de Fermat obtenemos que $a^{p-1} \equiv 1 \mod p$. Luego

$$a^{k(p-1)} \equiv \left(a^{p-1}\right)^k \equiv 1 \mod p.$$

□

Ejercicio 6.10. Sea p un primo tal que $p \nmid a$. Demostrar que $a^{(p-1)!} \equiv 1 \mod p$.

Demostración. Utilizar el lema anterior con $k = p!$. □

Ejercicio 6.11. Demostrar que:

a) Si p es un primo entonces $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \mod p$.

b) Si p es un primo impar entonces $1^p + 2^p + \cdots + (p-1)^p \equiv 0 \mod p$.

Demostración.

a) Es claro que por el Pequeño Teorema de Fermat,

$$\begin{aligned} 1^{p-1} &\equiv 1 \mod p \\ 2^{p-1} &\equiv 1 \mod p \\ &\vdots \\ (p-1)^{p-1} &\equiv 1 \mod p. \end{aligned}$$

Luego $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv p - 1 \equiv -1 \mod p$.

b) Es claro que por el Pequeño Teorema de Fermat,

$$\begin{aligned} 1^p &\equiv 1 \mod p \\ 2^p &\equiv 2 \mod p \\ &\vdots \\ (p-1)^p &\equiv p-1 \mod p. \end{aligned}$$

Luego $1^p + 2^p + \cdots + (p-1)^p \equiv 1 + 2 + \cdots + (p-1) \equiv \frac{p(p+1)}{2} \equiv 0 \mod p$ pues p es un primo impar y por lo tanto $\frac{p+1}{2}$ es un entero.

□

Ejercicio 6.12. Sea p primo. Demostrar que

$$\binom{2p}{p} \equiv 2 \mod p.$$

Demostración. Sabemos que

$$\binom{2p}{p} = \frac{2p(2p-1)(2p-2)\cdots(2p-(p-1))}{p!},$$

luego

$$(p-1)!\binom{2p}{p} = 2p(2p-1)(2p-2)\cdots(2p-(p-1)).$$

Además tenemos que

$$\begin{aligned} 2p-1 &\equiv -1 \mod p \\ 2p-2 &\equiv -2 \mod p \\ &\vdots \\ 2p-(p-1) &\equiv -(p-1) \mod p. \end{aligned}$$

Luego

$$(p-1)!\binom{2p}{p} \equiv 2(-1)^{p-1}(p-1)! \mod p.$$

Es claro que el ejercicio se cumple para $p = 2$, así que podemos suponer que p es impar. Luego tenemos que

$$(p-1)!\binom{2p}{p} \equiv 2(p-1)! \mod p$$

y por lo tanto

$$\binom{2p}{p} \equiv 2 \mod p.$$

□

Ejercicio 6.13. Sea p primo y k entero tal que $1 \leq k \leq p-1$. Demostrar que

$$\binom{p-1}{k} \equiv (-1)^k \mod p.$$

Demostración. Tenemos que

$$\binom{p-1}{k} = \frac{(p-1)(p-2)\cdots(p-k)}{k!},$$

luego

$$k!\binom{p-1}{k} = (p-1)(p-2)\cdots(p-k).$$

Además sabemos que

$$\begin{aligned} p-1 &\equiv -1 \mod p \\ p-2 &\equiv -2 \mod p \\ &\vdots \\ p-k &\equiv -k \mod p, \end{aligned}$$

luego

$$k!\binom{p-1}{k} \equiv (-1)^k k! \mod p$$

y por lo tanto

$$\binom{p-1}{k} \equiv (-1)^k \mod p.$$

□

Ejercicio 6.14. Sea p primo y k entero tal que $1 \leq k \leq p-1$. Si $(-1)^k k! \equiv 1 \mod p$, entonces $(p-k-1)! \equiv -1 \mod p$.

Demostración. Tenemos que

$$\begin{aligned} (p-1)! &\equiv (p-1)(p-2)\cdots(p-k)(p-k-1)! \mod p \\ &\equiv (-1)^k (p-k-1)! \mod p \\ &\equiv (p-k-1)! \mod p. \end{aligned}$$

Utilizando el teorema de Wilson obtenemos que

$$(p-k-1)! \equiv (p-1)! \equiv -1 \mod p.$$

□

Ejercicio 6.15. Sea p primo k entero tal que $1 \leq k \leq p-1$. Demostar que

$$(k-1)!(p-k)! \equiv (-1)^k \mod p.$$

Demostración. Por un lado tenemos que

$$(p-1)! \equiv (p-1)(p-2)\cdots(p-(k-1))(p-k)! \equiv (-1)^{k-1}(k-1)!(p-k)! \mod p.$$

Por otro lado tenemos que $(p-1)! \equiv -1 \mod p$. Luego

$$(-1)^{k-1}(k-1)!(p-k)! \equiv -1 \mod p$$

y por lo tanto

$$(k-1)!(p-k)! \equiv (-1)^k \mod p.$$

□

Lema 6.16. *Sean m y n enteros no negativos tales que $m+n+1=p$ para algún p primo, entonces $m!n! \equiv (-1)^{m+1} \mod p$.*

Demostración. Por el Teorema de Wilson tenemos que

$$(m+n)! \equiv (p-1)! \equiv -1 \mod p,$$

luego

$$(m+n)(m+n-1)\cdots(m+n-(n-1))m! \equiv -1 \mod p.$$

Observemos que

$$\begin{aligned} m+n = p-1 &\equiv -1 \mod p \\ m+n-1 = p-2 &\equiv -2 \mod p \\ &\vdots \\ m+n-(n-1) = p-n &\equiv -n \mod p, \end{aligned}$$

de donde se tiene que

$$(-1)^n n!m! \equiv -1 \mod p$$

y por lo tanto

$$(-1)^{m+n} m!n! \equiv (-1)^{m+1} \mod p.$$

Si $p=2$ es claro que se tiene el lema. Si p es impar entonces $m+n=p-1$ es par, luego

$$m!n! \equiv (-1)^{m+1} \mod p.$$

□

Ejercicio 6.17. Sea p primo con $p=4k+1$. Demostrar que $((2k)!)^2 \equiv -1 \mod p$.

Demostración. Aplicar el lema anterior a $m=n=2k$. □

Ejercicio 6.18. Sea p un primo impar, demostrar que

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \mod p.$$

Demostración 1. Por el Teorema de Wilson tenemos que $(p-1)! \equiv -1 \mod p$, es decir

$$\left(1\cdot 2\cdots\frac{p-3}{2}\cdot\frac{p-1}{2}\right)\left(\frac{p+1}{2}\cdot\frac{p+3}{2}\cdots(p-2)(p-1)\right) \equiv -1 \mod p,$$

pero

$$\begin{aligned} p-1 &\equiv -1 \mod p \\ p-2 &\equiv -2 \mod p \\ &\vdots \\ \frac{p+3}{2} = p - \frac{p-3}{2} &\equiv -\frac{p-3}{2} \mod p \\ \frac{p+1}{2} = p - \frac{p-1}{2} &\equiv -\frac{p-1}{2} \mod p. \end{aligned}$$

Luego reemplazando en (1),

$$(-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \mod p$$

de donde se tiene que

$$(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p-1}{2}}(-1) \mod p,$$

es decir

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \mod p.$$

□

Demostración 2. Utilizar el ejercicio 6.15 con $k = \frac{p+1}{2}$. □

Demostración 3. Utilizar el lema 6.16 con $m = n = \frac{p-1}{2}$. □

Ejercicio 6.19. Demostrar que para p primo, se tiene que

a) $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \mod p$, si p es de la forma $4k+1$.

b) $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1 \mod p$, si p es de la forma $4k+3$.

Demostración. Consecuencia del ejercicio anterior. □

Ejercicio 6.20. Sea p un primo impar con $p \neq 5$. Demostrar que p divide a infinitos números de la sucesión $1, 11, 111, 1111, \ldots$.

Demostración. Si $p = 3$ entonces p divide a $\underbrace{111}_{3\ 1\text{'s}}, \underbrace{111111}_{6\ 1\text{'s}}, \underbrace{111111111}_{9\ 1\text{'s}}, \ldots$ pues la suma de los dígitos de cada uno de estos números es divisible por 3 (criterio de divisibilidad por 3). Tomemos ahor $p \geq 7$, (es claro que el n-ésimo término de la sucesión $1, 11, 111, 1111, \ldots$ es $\frac{10^n-1}{9}$) como $p \not| 10$, entonces por el Pequeño Teorema de Fermat se tiene que $10^{p-1} \equiv 1 \mod p$ y por lo tanto $10^{k(p-1)} \equiv 1 \mod p$ para $k = 1, 2, 3, \ldots$. Como $p | 10^{k(p-1)} - 1$ y $p \not| 9$ (pues $p \neq 3$), entonces $p | \frac{10^{k(p-1)}-1}{9}$, luego el $k(p-1)$-ésimo elemento de la sucesión es divisible por p, para $k = 1, 2, , 3 \ldots$. □

6.2. Números Pseudoprimos y Números de Carmichael

Definición 6.21. *Sea n un número compuesto y a un entero tal que $(n, a) = 1$. Diremos que n es un pseudoprimo en base a sii $a^{n-1} \equiv 1 \bmod n$. Los pseudoprimos en base 2 se conocen simplemente como pseudoprimos.*

Definición 6.22. *Diremos que n es un número de Carmichael o un pseudoprimo absoluto sii n es un pseudoprimo en base a, para todo entero a.*

Ejercicio 6.23. Demuestre que 341 es un pseudoprimo.

Demostración. Se tiene que $341 = 11 \cdot 33$ y que $2^{10} = 31 \cdot 33 + 1 = 93 \cdot 11 + 1$ de donde se sigue que

$$2^{11} \equiv 2 \cdot 2^{10} \equiv 2 \bmod 31$$

y que

$$2^{31} \equiv 2 \cdot \left(2^{10}\right)^3 \equiv 2 \bmod 11$$

luego por el lema 6.2 se tiene que

$$2^{11 \cdot 31} \equiv 2 \bmod (11 \cdot 31)$$

es decir

$$2^{341} \equiv 2 \bmod 341.$$

Como $(2, 341) = 1$, entonces $2^{340} \equiv 1 \bmod 341$. Luego 341 es un pseudoprimo. □

Lema 6.24. *Si $d|n$ entonces $a^d - 1|a^n - 1$ para todo entero $a \geq 2$.*

Demostración. Como $d|n$, existe $k \in \mathbb{Z}^+$ tal que $dk = n$. Luego

$$a^n - 1 = \left(a^d\right)^k - 1 = \left(a^d - 1\right)\left(a^{d(k-1)} + a^{d(k-2)} + \cdots + a^d + 1\right)$$

de donde se ve que $a^d - 1|a^n - 1$. □

De aquí en adelante para k entero positivo, M_k significara $M_k = 2^k - 1$.

Corolario 6.25. *Si $d|n$ entonces $M_d|M_n$.*

Teorema 6.26. *Si n es un pseudoprimo entonces M_n también lo es.*

Demostración. Como n es pseudoprimo entonces n es compuesto y podemos escribir $n = st$ con $1 < s \leq t$. Por el corolario anterior se tiene que como $s|n$ entonces $M_s|M_n$, luego $2^n - 1$ es un número compuesto.

Sabemos que por hipótesis $2^{n-1} \equiv 1 \bmod n$, es decir $2^n \equiv 2 \bmod n$, de donde se tiene que existe $k \in \mathbb{Z}$ tal que $2^n - 2 = kn$. Se sigue que

$$\begin{aligned} 2^{M_n-1} &\equiv 2^{2^n-2} - 1 \\ &\equiv 2^{kn} - 1 \\ &\equiv (2^n - 1)\left(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1\right) \\ &\equiv M_n\left(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1\right) \\ &\equiv 0 \bmod M_n \end{aligned}$$

Luego

$$2^{M_n-1} \equiv 1 \mod M_n.$$

De donde se tiene que M_n es un pseudopirmo. □

Lema 6.27. *Si $d|n$ y $a \equiv b \mod n$ entonces $a \equiv b \mod d$.*

Demostración. Como $d|n$ y $a \equiv b \mod n$ entonces existen k y k' enteros tales que $dk = n$ y $nk' = a - b$, luego $d(kk') = a - b$ de donde se tiene que $a \equiv b \mod d$. □

Teorema 6.28. *Si n es un número de Carmichael, entonces n es libre de cuadrados.*

Demostración. Supongamos que existe $k > 1$ tal que $k^2|n$. Como n es un número de Carmichael entonces $a^n \equiv a \mod n$ para todo a entero positivo en especial $k^n \equiv k \bmod n$. Por el lema anterior se tiene que $k^n \equiv k \mod k^2$. Como n es compuesto entonces $n \geq 4$, luego $k^2|k^n$, de donde se tiene que $0 \equiv k^n \equiv k \mod k^2$, luego $k^2|k$, lo cual es una contradicción. Se dedude entonces que n tiene que ser libre de cuadrados. □

Teorema 6.29. *Sea $n = p_1p_2\cdots p_m$ donde los p_i son primos diferentes. Si $p_i - 1|n-1$ para $i = 1, 2, ..., m$ entonces n es un número de Carmichael.*

Demostración. Sean $(n, a) = 1$, entonces $p_i \nmid a \; \forall i = 1, 2, ..., m$. Luego podemos aplicar el Pequeño Teorema de Fermat y obtenemos que $p_i|a^{p_i-1} - 1$. Por el lema 6.24 tenemos que como $p_i - 1|n - 1$ entonces $a^{p_i-1} - 1|a^{n-1} - 1$, luego $p_i|a^{n-1} - 1$, $\forall i = 1, 2, ..., m$. Ya que $(p_1, p_2, \ldots, p_m) = 1$ entonces $n = p_1p_2\cdots p_m|a^{n-1} - 1$, de donde se tiene que $a^{n-1} \equiv 1 \mod n$. □

Ejemplo. Como

$$\begin{aligned} 561 &= 3 \cdot 11 \cdot 17 \\ 1729 &= 7 \cdot 13 \cdot 19 \\ 6601 &= 7 \cdot 23 \cdot 41 \\ 10585 &= 5 \cdot 29 \cdot 73 \end{aligned}$$

cumplen con las condiciones del teorema anterior, entonces todos estos son números de Carmichael.

Capítulo 7

Números Perfectos

En esta sección estudiaremos los números perfectos y su relación con los números de Mersenne. A lo largo de la sección, para k entero positivo, M_k significará $M_k = 2^k - 1$. Recordando los números de Mersenne son números de la forma $M_p = 2^p - 1$ con p primo. Si un número de Mersenne es primo, lo llamaremos primo de Mersenne.

Definición 7.1. *Diremos que n es un **número perfecto** sii $\sigma(n) = 2n$.*

A partir de esta definición y el lema 3.1 se obtiene el siguiente corolario.

Corolario 7.2. *n es un número perfecto sii $\sum_{d|n} \frac{1}{d} = 2$.*

De la definción de número perfecto tenemos que para todo número perfecto n, $\sigma(n)$ es par y de los corolarios 3.11 y 3.12 se obtiene el siguiente resultado.

Corolario 7.3.

1) Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ es un número perfecto entonces existe i entre 1 y m tal que p_i y α_i son impares.

2) Un cuadrado perfecto o dos veces un cuadrado perfecto no puede ser un número perfecto.

Teorema 7.4. *Ninguna potencia de un primo p puede ser un número perfecto. Es decir para todo $\alpha \in \mathbb{Z}^+$ y para todo primo p, p^α no es un número perfecto.*

Demostración. Supongamos que existen p primo y α entero positivo tal que $\sigma(p^\alpha) = 2p^\alpha$. Por otro lado sabemos que $\sigma(p^\alpha) = 1 + p + \cdots + p^\alpha$. Luego $1 + p + \cdots + p^\alpha = 2p^\alpha$ y por lo tanto $1 + p + \cdots + p^{\alpha-1} = p^\alpha$. Es decir

$$\frac{p^\alpha - 1}{p - 1} = p^\alpha.$$

Tenemos entonces que $p^\alpha - 1 = p^{\alpha+1} - p^\alpha$. De donde $-1 = p^{\alpha+1} - 2p^\alpha = p^\alpha(p-2) \geq 0$, lo cual es una contradicción. □

Teorema 7.5. *n es un número perfecto par sii existe $k \in \mathbb{Z}^+$ tal que $n = 2^{k-1}\left(2^k - 1\right)$ con $2^k - 1$ primo.*

Demostración. $\Rightarrow$) Sea n un número perfecto par. Sea $n = 2^\alpha m$ donde $\alpha \in \mathbb{Z}^+$ y m es un entero positivo impar. Observamos que

$$2^{\alpha+1}m = 2n = \sigma(n) = \sigma\left(2^\alpha m\right) = \sigma\left(2^\alpha\right)\sigma(m) = \left(2^{\alpha+1} - 1\right)\sigma(m). \tag{1}$$

De donde se tiene que $2^{\alpha+1} - 1 | 2^{\alpha+1}m$, pero $(2^{\alpha+1} - 1, 2^{\alpha+1}) = 1$, luego $2^{\alpha+1} - 1 | m$. Existe entonces $r \in \mathbb{Z}^+$ tal que

$$m = \left(2^{\alpha+1} - 1\right) r. \tag{2}$$

En (1) vemos que

$$\sigma(m) = \frac{2^{\alpha+1}m}{2^{\alpha+1} - 1} = \frac{2^{\alpha+1}\left(2^{\alpha+1} - 1\right) r}{2^{\alpha+1} - 1} = 2^{\alpha+1}r.$$

Como $r|m$ entonces $2^{\alpha+1}r = \sigma(m) \geq m + r = \left(2^{\alpha+1} - 1\right) r + r = 2^{\alpha+1}r$, luego $\sigma(m) = m + r$ y por lo tanto m solo tiene dos divisores: m y r. De donde se deduce que m es primo y $r = 1$. Así que la expresión (2) queda reducida a $m = 2^{\alpha+1} - 1$ y por lo tanto $n = 2^\alpha\left(2^{\alpha+1} - 1\right)$, tomando $k = \alpha + 1$ obtenemos el resultado deseado.

$\Leftarrow$) Sea $n = 2^{k-1}\left(2^k - 1\right)$ para algún $k \in \mathbb{Z}^+$ tal que $2^k - 1$ es primo, es decir $\sigma\left(2^k - 1\right) = 1 + \left(2^k - 1\right) = 2^k$. Por otro lado $\sigma\left(2^{k-1}\right) = 2^k - 1$.

Dado que $\left(2^{k-1}, 2^k - 1\right) = 1$ entonces

$$\begin{aligned}
\sigma(n) &= \sigma\left(2^{k-1}\right)\sigma\left(2^k - 1\right) \\
&= \left(2^k - 1\right) 2^k \\
&= 2\left[2^{k-1}\left(2^k - 1\right)\right] \\
&= 2n.
\end{aligned}$$

Observamos entonces que n es un número perfecto. Dado que $n = 2^{k-1}\left(2^k - 1\right)$, para ver que n es par basta con observar que $k \neq 1$ pues si $k = 1$ entonces $2^k - 1$ no es primo, contradiciendo así la hipótesis. □

Lema 7.6. *Sean $a, n, m \in \mathbb{Z}^+$ con $a \geq 2$. Entonces $n|m$ sii $a^n - 1 | a^m - 1$.*

Demostración.

$\Rightarrow$) Si $n|m$ entonces existe $k \in \mathbb{Z}^+$ tal que $m = nk$ y por lo tanto

$$a^m - 1 = \left(a^n\right)^k - 1 = \left(a^n - 1\right)\left(1 + a^n + a^{2n} + \cdots + a^{(k-1)n}\right).$$

De donde se ve que $a^n - 1 | a^m - 1$.

$\Leftarrow$) Sea $a^n - 1 | a^m - 1$, es claro que $n \leq m$. Aplicando el algoritmo de la división, tenemos que $m = nq + r$ con $0 \leq r < n$. Luego

$$a^m - 1 = a^{nq+r} - a^{nq} + a^{nq} - 1 = a^{nq}(a^r - 1) + a^{nq} - 1.$$

Como $a^n - 1 | a^{nq} - 1 = (a^n - 1)\left(1 + a + a^{2n} + \cdots + a^{(q-1)n}\right)$ y $a^n - 1 | a^m - 1$, entonces $a^n - 1 | a^{nq}(a^r - 1)$. Pero $(a^n - 1, a^{nq}) = 1$, luego $a^n - 1 | a^r - 1$ y dado que $0 \leq r < n$, entonces $r = 0$. □

Lema 7.7. *Si $M_p = 2^p - 1$ es primo entonces p es primo.*

Demostración. Probaremos que si p no es primo tampoco lo es M_p. Es claro para $p = 1$, pues $M_1 = 1$ no es primo. Para $p > 1$ se tiene como consecuencia inmediata del lema anterior si tomamos $a = 2$. □

Teorema 7.8. *n es un número perfecto par sii existe un primo p tal que M_p es primo y $n = 2^{p-1}M_p$.*

Demostración. Consecuencia inmediata del lema anterior y el teorema 7.5. □

Ejercicio 7.9. Demostar que si n es un número perfecto par, entonces $8n + 1$ es un cuadrado perfecto.

Demostración. Veamos en general que si m es de la forma $m = 2^{k-1}\left(2^k - 1\right)$ entonces $8m + 1$ es un cuadrado perfecto (y por lo tanto, por el teorema 7.5, se sigue que si n es un número perfecto par, entonces $8n + 1$ es un cuadrado perfecto). Sea $m = 2^{k-1}\left(2^k - 1\right)$, entonces

$$8m + 1 = 2^3 2^{k-1}\left(2^k - 1\right) + 1 = 2^{k+2}\left(2^k - 1\right) + 1 = 2^{2k+2} - 2^{k+2} + 1 = \left(2^{k+1} - 1\right)^2.$$

□

La demostración del ejercicio anterior nos lleva a la siguiente identidad:

Teorema 7.10. *Sea $n \in \mathbb{Z}^+$, entonces $2^{n+2}M_n + 1 = (M_{n+1})^2$.*

Ejercicio 7.11 (The American Mathematical Monthly, Problema E1755, [45]). Demostrar que 6 es el único número perfecto y libre de cuadrados.

Demostración. Sea n un número perfecto y libre de cuadrados. Como n es libre de cuadrados su factorización como producto de primos es $n = p_1 p_2 \cdots p_m$, en este caso tenemos que

$$\sigma(n) = (p_1 + 1)(p_2 + 1) \cdots (p_m + 1) \tag{1}$$

y como n es un número perfecto entonces

$$\sigma(n) = 2n. \tag{2}$$

Es claro que n debe tener dos o más factores primos ($m \geq 2$) pues ningún primo es un número perfecto, además n tiene que ser par, pues si n es impar en (1) se ve que que $4|\sigma(n)$ y por (2) se tendría entonces que $2|n$ siendo esto una contradicción.

Dado que n es par y perfecto, existe p primo tal que $n = 2^{p-1}M_p$. Como n también es libre de cuadrados necesariamente $p = 2$ y por lo tanto $n = 6$. □

Ejercicio 7.12 (The American Mathematical Mounthly, Problema E3081, [15]). Demostrar que un número perfecto n, con m diferentes divisores primos ($\omega(n) = m$), posee un factor primo menor o igual a m.

Demostración. Sea $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}$ un número perfecto con m diferentes divisores primos (recordemos que $p_1 < p_2 < \cdots < p_m$), supongamos que $p_1 \geq m + 1$. Como $p_i \geq p_1 + (i - 1)$, se tiene que $p_i \geq m + i$, $\forall\ 1 \leq i \leq m$.

Sabemos que $\sigma(n) = (1 + p_1 + \cdots + p_1^{\alpha_1})\cdots(1 + p_m + \cdots + p_m^{\alpha_m})$, luego

$$\begin{aligned}
\frac{\sigma(n)}{n} &= \left(1 + \frac{1}{p_1} + \cdots + \frac{1}{p_1^{\alpha_1}}\right)\cdots\left(1 + \frac{1}{p_m} + \cdots + \frac{1}{p_m^{\alpha_m}}\right) \\
&< \left(\sum_{i=0}^{\infty}\frac{1}{p_1^i}\right)\left(\sum_{i=0}^{\infty}\frac{1}{p_m^i}\right) \\
&< \prod_{i=1}^{m}\left(\frac{1}{1-\frac{1}{p_i}}\right) \\
&= \prod_{i=1}^{m}\left(\frac{p_i}{p_i - 1}\right) \\
&= \prod_{i=1}^{m}\left(1 + \frac{1}{p_i - 1}\right) \\
&\leq \prod_{i=1}^{m}\left(1 + \frac{1}{m + i - 1}\right) \\
&= \prod_{i=1}^{m}\left(\frac{m + i}{m + i - 1}\right) \\
&= \frac{2m}{m} \\
&= 2.
\end{aligned}$$

Luego $\sigma(n) < 2n$, lo que contradice el hecho de que m es un número perfecto. Luego $p_1 \leq m$. □

Ejercicio 7.13. Sea n un número perfecto par. Demostrar que $\tau(n) = \lfloor \log_2 n \rfloor + 2$.

Demostración. Sea n un número perfecto par. Sabemos que existe k primo tal que $n = 2^{k-1}\left(2^k - 1\right)$ con $2^k - 1$ primo. Por lo tanto $\tau(n) = \tau\left(2^{k-1}\right)\tau\left(2^k - 1\right) = 2k$. Sacando $\log_2$ a ambos lados de $n = 2^{k-1}\left(2^k - 1\right)$, tenemos que

$$\begin{aligned}\log_2 n &= k - 1 + \log_2\left(2^k - 1\right)\\ &= k - 1 + \log_2\left(2^k\left(1 - \frac{1}{2^k}\right)\right)\\ &= k - 1 + k + \log_2\left(1 - \frac{1}{2^k}\right)\\ &= 2k - 1 + \alpha,\end{aligned}$$

donde $-1 = \log_2 \frac{1}{2} < \alpha = \log_2\left(1 - \frac{1}{2^k}\right) < \log_2 1 = 0$.

Así que $\tau(n) = \log_2 n + 1 - \alpha$. Como $0 < -\alpha < 1$ entonces $\log_2 n + 1 < \tau(n) < \log_2 n + 2$. De donde se tiene que $\tau(n) = \lfloor \log_2 n + 2 \rfloor = \lfloor \log_2 n \rfloor + 2$. □

Ejercicio 7.14. Demostrar que todo número perfecto par es un número triangular, es decir un número de la forma $\frac{m(m+1)}{2}$.

Demostración. Sea n un número perfecto par, luego existe $k \in \mathbb{Z}^+$ tal que

$$n = 2^{k-1}\left(2^k - 1\right) = \frac{2^k\left(2^k - 1\right)}{2}.$$

Tomando $m = 2^k - 1$ obtenemos el resultado deseado. □

Lema 7.15. *Para todo $m \in \mathbb{Z}^+$, se tiene que $6^m \equiv 6 \mod 10$.*

Demostración. Por inducción.

Para $m = 1$ es claro que el resultado se tiene. Supongamos que se cumple para m y probemos que se tiene para $m + 1$.

$$6^{m+1} = 6 \cdot 6^m \equiv 6 \cdot 6 = 36 \equiv 6 \mod 10.$$

□

Lema 7.16. *Para todo $m \in \mathbb{Z}^+$, se tiene que $16^m \equiv 6 \mod 10$.*

Demostración. Dado que $16 \equiv 6 \mod 10$, entonces $16^m \equiv 6^m \mod 10$. Utilizando el lema anterior se obtiene el resultado deseado. □

Teorema 7.17. *Todo número perfecto par, su último dígito en base 10 es 6 o 8.*

Demostración. Si n es un número perfecto par, entonces $n = 2^{p-1}\left(2^p - 1\right)$ para algún primo p. Si $p = 2$ entonces $n = 6$ y se tiene el teorema. Si $p > 2$ entonces p es de la forma $p = 4m + 1$ o de la forma $p = 4m + 3$.

i) Si $p = 4m + 1$ entonces

$$n = 2^{4m}\left(2^{4m+1} - 1\right) = 16^m\left(2 \cdot 16^m - 1\right) \equiv 6\left(2 \cdot 6 - 1\right) = 66 \equiv 6 \mod 10.$$

ii) Si $p = 4m + 3$ entonces

$$n = 2^{4m+2}\left(2^{4m+3} - 1\right) = 4 \cdot 16^m\left(8 \cdot 16^m - 1\right) \equiv 4 \cdot 6\left(8 \cdot 6 - 1\right) = 24(47) \equiv 4(7)$$
$$= 28 \equiv 8 \mod 10.$$

□

Lema 7.18. *Para $k \in \mathbb{Z}^+$ se tiene que*

$$1^3 + 3^3 + 5^3 + \cdots + (2k-1)^3 = k^2\left(2k^2 - 1\right).$$

Demostración. Sea $S = 1^3 + 3^3 + 5^3 + \cdots + (2k-1)^3$, sabemos que

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Tomando $n = 2k - 1$, obtenemos que

$$S + 2^3 + 4^3 + \cdots + (2k)^3 = \left(\frac{(2k-1)(2k)}{2}\right)^2$$
$$S + 2^3\left(1^3 + 2^3 + \cdots + k^3\right) = k^2(2k-1)^2$$
$$S + 8\left(\frac{k(k+1)}{2}\right)^2 = k^2(2k-1)^2,$$

de donde se tiene que

$$S = k^2\left(4k^2 - 4k + 1\right) - 2k^2\left(k^2 + 2k + 1\right) = k^2\left(2k^2 - 1\right).$$

□

Ejercicio 7.19. Demostrar que para todo número perfecto par n mayor que 6, existe $k \in \mathbb{Z}^+$ tal que

$$n = k^2\left(2k^2 - 1\right) = 1^3 + 3^3 + 5^3 + \cdots + (2k-1)^3.$$

Demostración. La segunda identidad es el lema anterior, luego basta con probar que si $n > 6$ es un número perfecto par entonces existe $k \in \mathbb{Z}^+$ tal que $n = k^2\left(2k^2 - 1\right)$. Sabemos que $n = 2^{p-1}\left(2^p - 1\right)$ para algún p primo. De hecho como $n \neq 6$ entonces $p \neq 2$, luego p es impar de donde $p - 1 = 2\alpha$ para algún $\alpha \in \mathbb{Z}^+$. Tenemos que

$$n = 2^{2\alpha}\left(2^{2\alpha+1} - 1\right) = \left(2^\alpha\right)^2\left(2\left(2^\alpha\right)^2 - 1\right),$$

tomando $k = 2^\alpha$ tenemos el resultado que estabamos buscando. □

Ejercicio 7.20.

a) Demostrar que si n es un número perfecto o un número abundante entonces nk es abundante para todo entero $k \geq 2$.

b) Demostrar que existen infinitos números abundantes.

Demostración.

a) Demostraremos el caso para n perfecto, para n abundante la demostración es similar. Tomemos $m = nk$ con $k \geq 2$. Es claro que n es un divisor propio de m y que por ser n perfecto, $\frac{\sigma(n)}{n} = 2$. Luego aplicando el teorema 3.26, obtenemos que

$$\frac{\sigma(m)}{m} > \frac{\sigma(n)}{n} = 2,$$

de donde se tiene que $\sigma(m) > 2m$. Es decir m es abundante.

b) Consecuencia inmediata de (a).

□

Ejercicio 7.21. Un número n es superperfecto si $\sigma(\sigma(n)) = 2n$. Demostrar que n es un número superperfecto par sii $n = 2^r$ donde r es un entero positivo tal que $M_{r+1} = 2^{r+1} - 1$ es primo.

Demostración. $\Rightarrow$) Sea n un número superperfecto par, $n = 2^r q$ donde q es impar y $r \geq 1$. Tenemos que

$$\begin{aligned} 2^{r+1}q &= 2n \\ &= \sigma(\sigma(n)) \\ &= \sigma(\sigma(2^r)\sigma(q)) \\ &= \sigma\left(\left(2^{r+1}-1\right)\sigma(q)\right). \end{aligned}$$

Es decir

$$\sigma\left(\left(2^{r+1}-1\right)\sigma(q)\right) = 2^{r+1}q. \tag{1}$$

Si $q > 1$ entonces $(2^{r+1}-1)\,\sigma(q)$, $\sigma(q)$ y $2^{r+1}-1$ son divisores de $(2^{r+1}-1)\,\sigma(q)$ y por lo tanto

$$\begin{aligned} \sigma\left(\left(2^{r+1}-1\right)\sigma(q)\right) &\geq \left(2^{r+1}-1\right)\sigma(q) + \sigma(q) + \left(2^{r+1}-1\right) \\ &= 2^{r+1}\sigma(q) + 2^{r+1} - 1 \\ &\geq 2^{r+1}(q+1) + 2^{r+1} - 1 \\ &= 2^{r+1}q + \left(2^{r+2}-1\right) \\ &> 2^{r+1}q. \end{aligned}$$

Es decir

$$\sigma\left(\left(2^{r+1}-1\right)\sigma(q)\right) > 2^{r+1}q. \tag{2}$$

De (1) y (2) se llega a una contradicción. Luego $q = 1$, de donde se tiene que $n = 2^r$ y en (1) se obtiene que

$$\begin{aligned} 2^{r+1} &= \sigma\left(2^{r+1}-1\right) \\ \left(2^{r+1}\right)+1 &= \sigma\left(2^{r+1}-1\right). \end{aligned}$$

Por lo tanto $2^{r+1}-1$ es primo.

$\Leftarrow$) Si $n = 2^r$ con r entero positivo tal que $2^{r+1}-1$ es primo, entonces

$$\begin{aligned} \sigma\left(\sigma(n)\right) &= \sigma\left(2^{r+1}-1\right) \\ &= (2^{r+1}-1)+1 \\ &= 2^{r+1} \\ &= 2n. \end{aligned}$$

□

Ejercicio 7.22. Diremos que n es un número superabundante si $\forall k = 1, 2, \ldots, n-1$ se tiene que

$$\frac{\sigma(n)}{n} > \frac{\sigma(k)}{k}$$

Demostrar que existen infinitos números superabundantes.

Demostración. Supongamos que existen un número finito de números superabundantes, sea m el mayor de ellos. Es claro que $\forall n > m$ se tiene que

$$\frac{\sigma(n)}{n} \leq \frac{\sigma(m)}{m}$$

pues de lo contrario se puede encontrar un n mayor que m que también sea un número superabundante. Luego se tiene que

$$\frac{\sigma(m)}{m} \geq \frac{\sigma(k)}{k}, \qquad \forall k \in \mathbb{Z}^+$$

lo cual contradice el lema 3.2. Se tiene entonces que existen infinitos números superabundantes. □

Ejercicio 7.23. Sean $k, n \in \mathbb{Z}^+$ con $n > 1$. Diremos que n es k-hiperperfecto sii

$$n = 1 + k \sum_{\substack{d|n \\ 1<d<n}} d.$$

(Se entiende que para p primo, $\sum_{\substack{d|p \\ 1<d<p}} d = 0$). Observe que los números 1-hiperperfectos son los mismos números perfectos.

Demostrar que:

a) n es k-hiperperfecto sii $\sigma(n) = n + 1 + \frac{n-1}{k}$.

b) Si n es k-hiperperfecto, entonces $n \equiv 1 \mod k$.

c) Ninguna potencia de un primo puede ser k-hiperperfecto para algún $k \in \mathbb{Z}^+$.

d) Si n es k-hiperperfecto entonces todos los factores primos de n son más grandes que k.

Demostración. a) $\Rightarrow$)

$$n = 1 + k \sum_{\substack{d|n \\ 1<d<n}} d = 1 + k(\sigma(n) - 1 - n) = 1 + k\sigma(n) - k - kn,$$

luego $\sigma(n) = n + 1 + \frac{n-1}{k}$.

$\Leftarrow$) Si $\sigma(n) = n + 1 + \frac{n-1}{k}$, entonces $k(\sigma(n) - 1 - n) = n - 1$, luego

$$n = 1 + k(\sigma(n) - 1 - n) = 1 + k \sum_{\substack{d|n \\ 1<d<n}} d.$$

b) Evidente a partir de la definición de número k-hiperperfecto.

c) Supongamos que existen p primo y $\alpha, k \in \mathbb{Z}^+$ tales que p^α es un número k-hiperperfecto. Es claro que $\alpha \neq 1$, pues de la definición de número k-hiperperfecto se deduce fácilmente que un primo no puede ser k-hiperperfecto, luego $\alpha \geq 2$. Vemos que

$$p^\alpha = 1 + k\left(p + p^2 + \cdots + p^{\alpha-1}\right),$$

es decir

$$p^\alpha - pk\left(1 + p + \cdots p^{\alpha-2}\right) = 1.$$

De donde se tiene que $p|1$, lo cual es una contradicción.

d) Supongamos que existe p primo tal que $p|n$ y $p \leq k$. Como $p \neq n$, pues un primo no puede ser k-hiperperfecto, entonces $\frac{n}{p}$ es un divisor de n diferente a 1 y a n. Luego

$$\sigma(n) \geq n + 1 + \frac{n}{p} \geq n + 1 + \frac{n}{k} > n + 1 + \frac{n-1}{k} = \sigma(n),$$

donde la última igualdad es debida a la parte (a). Como vimos, terminamos en una contradicción.

□

Capítulo 8

Números de Fermat

En la presente capítulo presentaremos algunas propiedades de los números de Fermat, estos son números de la forma $F_m = 2^{2^m}+1$ con $m \in \mathbb{N}$. Recordemos que si un número de Fermat es primo, lo llamaremos primo de Fermat.

Lema 8.1. *Sean $a, n \in \mathbb{Z}^+$ con $a \geq 2$, tales que $a^n + 1$ es primo, entonces a es par y $n = 2^m$ para algún $m \in \mathbb{N}$.*

Demostración. Supongamos que a es impar ($a \neq 1$ pues $a \geq 2$), luego $a^n + 1 \geq 4$ y además $a^n + 1$ tiene que ser par, lo cual es una contradicción ya que $a^n + 1$ es primo. Se tiene entonces que a es par.

Supongamos que n tiene un factor q impar mayor que 1 ($n \geq 3$), luego $n = kq$ para algún $k \in \mathbb{Z}^+$ y por lo tanto

$$a^n + 1 = (a^q)^k + 1 = (a^q + 1)\left(1 - a^q + \cdots - a^{(k-2)q} + a^{(k-1)q}\right).$$

Dado que $k \geq 3$, entonces ambos factores son mayores que 1, contradiciendo la hipótesis de que $a^n + 1$ es primo. Luego n no tiene factores impares mayores que 1, es decir $n = 2^m$ para algún $m \in \mathbb{N}$. □

Ejercicio 8.2. a) Demostrar que para $n \in \mathbb{Z}^+$ se tiene que

$$F_0 F_1 F_2 \cdots F_{n-1} = F_n - 2.$$

b) Utilizando la parte (a), demostrar que $(F_m, F_n) = 1$ si $m \neq n$.

c) Demostrar que todo número de Fermat F_n con $n \geq 1$ es de la forma $6k - 1$.

Demostración.

a) Por inducción. Del hecho de que $F_0 = 3$ y $F_1 = 5$ se puede ver que se cumple para $n = 1$. Supongamos que se cumple para n y probemos que se tiene para $n + 1$.

Vemos que

$$\begin{aligned} F_0F_1F_2\cdots F_{n-1}F_n &= (F_n - 2)\,F_n \\ &= \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) \\ &= 2^{2^{n+1}} - 1 \\ &= \left(2^{2^{n+1}} + 1\right) - 2 \\ &= F_{n+1} - 2. \end{aligned}$$

b) Sean $m, n \in \mathbb{Z}^+$ con $0 \leq n < m$ y $(F_m, F_n) = d$. Es claro que $d \neq 2$, pues los números de Fermat son impares. Utilizando la parte (a) vemos que

$$F_0F_1\cdots F_n\cdots F_{m-1} = F_m - 2.$$

Dado que $d|F_0F_1\cdots F_n\cdots F_{m-1}$ y $d|F_m$, entonces $d|2$, pero como $d \neq 2$, se tiene que $d = 1$.

c) Basta demostrar que $6|F_n + 1$. Para $n = 1$ es evidente, para $n > 1$ vemos, por la parte (a), que

$$F_n + 1 = F_0F_1\cdots F_{n-1} + 3 = 3\left(F_1\cdots F_{n-1} + 1\right),$$

de donde es claro que $6|F_n + 1$ pues la parte dentro del paréntesis es par.

□

Ejercicio 8.3.

a) Demostrar que para n entero positivo, se tiene que $F_n = (F_{n-1} - 1)^2 + 1$.

b) Demostrar que para $n \geq 2$, se tiene que $F_n = F_{n-1}^2 - 2\,(F_{n-2} - 1)^2$.

Demostración.

a) $(F_{n-1} - 1)^2 + 1 = \left(2^{2^{n-1}}\right)^2 + 1 = 2^{2^n} + 1 = F_n$.

b) Es claro que $(F_{n-2} - 1)^2 = F_{n-1} - 1$, luego

$$\begin{aligned} F_{n-1}^2 - 2\,(F_{n-2} - 1)^2 &= F_{n-1}^2 - 2\,(F_{n-1} - 1) \\ &= F_{n-1}^2 - 2F_{n-1} + 2 \\ &= \left(F_{n-1}^2 - 2F_{n-1} + 1\right) + 1 \\ &= (F_{n-1} - 1)^2 + 1 \\ &= F_n. \end{aligned}$$

□

Teorema 8.4. *Para $n \geq 2$ se tiene que el último dígito de F_n en base 10 es 7.*

Demostración. Por inducción. Es claro que se cumple para $n = 2$, pues $F_2 = 2^{2^2} + 1 = 17 \equiv 7 \mod 10$. Supongamos que se cumple para n (con $n \geq 2$) y probemos que se tiene para $n + 1$.

Por hipótesis de inducción tenemos que $F_n = 2^{2^n} + 1 \equiv 7 \mod 10$. Vemos entonces que

$$F_{n+1} = 2^{2^{n+1}} + 1 = \left(2^{2^n}\right)^2 + 1 = \left[\left(2^{2^n} + 1\right) - 1\right]^2 + 1 \equiv (7-1)^2 + 1 = 37 \equiv 7 \mod 10.$$

□

Teorema 8.5. *Si existen $n > 0$ y $a, k \in \mathbb{Z}^+$ tales que $F_n = a^k$, entonces $k = 1$. Es decir, ningún número de Fermat es una potencia perfecta.*

Demostración. Es claro que $F_0 = 3$ no es una potencia perfecta, entonces podemos suponer $n > 1$. Si $F_n = a^k$, de la identidad $F_n = (F_{n-1} - 1)^2 + 1$ vemos que k no puede ser 2 (y por lo tanto k no puede ser par), pues los dos únicos cuadrados perfectos consecutivos son 0 y 1. Luego k tiene que ser impar (a también es impar pues F_n es impar). Vemos que

$$2^{2^n} = F_n - 1 = a^k - 1 = (a-1)\left(a^{k-1} + a^{k-2} + \cdots + 1\right).$$

Como $a^{k-1} + a^{k-2} + \cdots + 1$ es impar y al mismo tiempo divide a 2^{2^n}, entonces $a^{k-1} + a^{k-2} + \cdots + 1 = 1$, de donde se tiene que $k = 1$. □

Ejercicio 8.6. Demostrar que para $n > 1$, F_n no se puede expresar como la suma de dos primos.

Demostración. Si existiese algún F_n que se pudiese expresar como la suma de dos primos, al ser F_n impar, uno de ellos tiene que ser 2 y el otro igual a $F_n - 2$. Pero

$$F_n - 2 = 2^{2^n} - 1 = \left(2^{2^{n-1}} - 1\right)\left(2^{2^{n-1}} + 1\right)$$

es compuesto para $n > 1$. □

Ejercicio 8.7. Demostrar que $\varphi(n) = 2^r$ para algún $r \in \mathbb{N}$ sii $n = 2^\alpha$ o $n = 2^\alpha F_{i_1} F_{i_2} \cdots F_{i_s}$ con $\alpha \in \mathbb{N}$ y $F_{i_1}, F_{i_2}, \ldots, F_{i_s}$ primos de Fermat.

Demostración.

$\Rightarrow$) Si $n = 1$ es claro que es de la forma $n = 2^\alpha$ ($\alpha = 0$).

Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ tal que $\varphi(n) = \varphi\left(p^{\alpha_1}\right) \cdots \varphi\left(p^{\alpha_m}\right) = 2^r$ para algún $r \in \mathbb{Z}^+$.

Para $i \in \{1, \ldots, m\}$ se tiene que $\varphi\left(p_i^{\alpha_i}\right) | 2^r$, luego $\varphi\left(p_i^{\alpha_i}\right) = 2^t$ para algún $t \in \mathbb{Z}^+$. Como

$$\varphi\left(p_i^{\alpha_i}\right) = p^{\alpha-1}(p_i - 1) = 2^t, \tag{1}$$

entonces:

i) Si $\alpha_i > 1$ entonces (1) solo tiene sentido si $p_i = 2$.

ii) Si $\alpha = 1$ entonces en (1) se ve que $p_i - 1 = 2^t$, es decir $p_i = 2^t + 1$. Pero por el lema 8.1, $2^t + 1$ solo es primo si $t = 2^m$ para algún $m \in \mathbb{N}$. Luego $p_i = 2^{2^m} + 1$.

De i) y ii) se deduce que n es de la forma $n = 2^\alpha$ o $n = 2^\alpha F_{i_1} F_{i_2} \cdots F_{i_s}$.

$\Leftarrow$) Si $n = 2^\alpha$ entonces $\varphi(n) = 1$, si $\alpha = 0$ y $\varphi(n) = 2^{\alpha-1}$, si $\alpha > 0$.

Si $n = 2^\alpha F_{i_1} F_{i_2} \cdots F_{i_s}$ con $\alpha > 0$ entonces

$$\begin{aligned}
\varphi(n) &= \varphi\left(2^\alpha\right) \varphi\left(F_{i_1}\right) \varphi\left(F_{i_2}\right) \cdots \varphi\left(F_{i_s}\right) \\
&= 2^{\alpha-1}\left(F_{i_1} - 1\right)\left(F_{i_2} - 1\right) \cdots \left(F_{i_s} - 1\right) \\
&= 2^{\alpha_1} 2^{2^{i_1}} 2^{2^{i_2}} \cdots 2^{2^{i_s}}.
\end{aligned}$$

Si $\alpha = 0$ por un procedimiento análogo llegamos a que $\varphi(n) = 2^{2^{i_1}} 2^{2^{i_2}} \cdots 2^{2^{i_s}}$.

En todos los casos es claro que $\varphi(n) = 2^r$ para algún $r \in \mathbb{N}$. $\square$

Bibliografía

[1] Andreescu, Titu; Andrica, Dorin; Feng, Zuming. *104 Number Theory Problems. From the Training of the USA IMO Team*. Birkhäuser. 2007.

[2] Apostol, Tom. *Introduction to Analytic Number Theory*. Springer-Verlag. 1976.

[3] Bateman, Paul; Diamond, Harold. *Analytic Number Theory. An introductory course*. World Scientific Publishing. 2004.

[4] Bennett, A. A.; Ballantine, Constance R.. *The American Mathematical Monthly*. Vol. 33, No. 2, (Feb., 1926), pp. 106-107.

[5] Bin, Xiong; Yee, Lee Peng. *Mathematical Olympiad in China. Problems and Solutions*. East China Normal University Press. World Scientific Publishing. 2007.

[6] Boju, Valentin; Funar, Louis. *The Math Problems Notebook*. Birkhäuser. 2007.

[7] Brown, J. L., Jr.; Magnuson, E. L.. *The American Mathematical Monthly*. Vol. 71, No. 6, (Jun. - Jul., 1964), pp. 683-684.

[8] Burton, David. *Elementary Number Theory*. Sixth Edition. McGraw-Hill. 2007.

[9] De Koninck, Jean-Marie; Mercier, Armel. *1001 Problems in Classical Number Theory*. American Mathematical Society. 2007.

[10] Caicedo, José Francisco; Castro, Iván. *Temas de Teoría de Cuerpos, Teoría de Anillos y Números Algebraicos. Vol. II*. Segunda Edición. Universidad Nacional de Colombia. 2008.

[11] Demir, Huseyin; Johnston, J. B.. *The American Mathematical Monthly* Vol. 64, No. 1, (Jan., 1957), pp. 45-46.

[12] Dickson, Leonard. *History of the Theory of Numbers. Volume I: Divisibility and Primality*. Dover Publications. 2005.

[13] Djukić, Dušan; Janković, Vladimir; Matić, Ivan; Petrović, Nikola. *The IMO Compendium. A Collection of Problems Suggested for the International Mathematical Olympiads: 1959-2004*. Springer. 2006.

[14] Ecker, Michael W.; Beslin, Scott J.. *The American Mathematical Monthly.* Vol. 93, No. 8, (Oct., 1986), pp. 656-657.

[15] Ehrhart, E.; Pambuccian, Victor. *The American Mathematical Monthly.* Vol. 94, No. 8, (Oct., 1987), pp. 794-795.

[16] Erdős, Paul; Kac, Mark; Breusch, Robert. *The American Mathematical Monthly.* Vol. 61, No. 4, (Apr., 1954), pp. 264-265.

[17] Erdős, Paul; Kelly, J. B.. *The American Mathematical Monthly.* Vol. 60, No. 8, (Oct., 1953), pp. 557-558.

[18] Erdős, Paul; Lambek, J.. *The American Mathematical Monthly.* Vol. 55, No. 2, (Feb., 1948), pp. 103.

[19] Everest, Graham; Ward, Thomas. *An introduction to Number Theory.* Springer-Verlag. 2005.

[20] Fine, Benjamin; Rosenberger, Gerhard. *Number Theory. An Introduction via the Distribution of Primes.* Birkhäuser. 2007.

[21] Gelca, Răzvan; Andreescu, Titu. *Putnam and Beyond.* Springer. 2007.

[22] Heinen, L. R.; Waterhouse, W. C.; Silverman, D. L.. *The American Mathematical Monthly.* Vol. 71, No. 1, (Jan., 1964), pp. 96.

[23] Honsberger, Ross. *In Pólya's Footsteps. Miscellaneous Problems and Essays.* The Mathematical Association of America. 1997.

[24] Honsberger, Ross. *Mathematical Diamonds.* The Mathematical Association of America. 2003.

[25] Iwaniec, Henryk; Kowalski, Emmanuel. *Analytic Number Theory.* American Mathematical Society. 2004.

[26] Kisačanin, Branislav. *Mathematical Problems and Proofs. Combinatorics, Number Theory and Geometry.* Kluwer Academic Publishers. 2002.

[27] Křížek, Michal; Luca, Florian; Somer, Lawrence. *17 Lectures on Fermat Numbers. From Number Theory to Geometry.* Canadian Mathematical Society. Springer-Verlag. 2001.

[28] LeVeque, William. *Topics in Number Theory. Volumes I and II.* Dover Publications. 2002.

[29] Luthar, R.S.; Gerst, Irving. *The American Mathematical Monthly.* Vol. 79, No. 8, (Oct., 1972), pp. 911-912.

[30] Mielke, M. V.; Marsh, D. C. B.; Silverman, D. L.. *The American Mathematical Monthly*. Vol. 69, No. 4, (Apr., 1962), pp. 313-314.

[31] Murty, Ram. *Problems in Analytic Number Theory*. Springer-Verlag. 2001.

[32] Nathanson, Melvyn. *Elementary methods in Number Theory*. Springer-Verlag. 2000.

[33] Nicol, C. A.; Vojta, Paul. *The American Mathematical Monthly*. Vol. 85, No. 3, (Mar., 1978), pp. 199.

[34] Niven, Ivan; Zuckerman, Herbert; Montgomery, Hugh. A*n Introduction to the Theory of Numbers*. Fifth Edition. John Wiley & Sons. 1991.

[35] Oppenheim, A.; Felsinger, Neal. *The American Mathematical Monthly*. Vol. 76, No. 4, (Apr., 1969), pp. 424.

[36] Philipp, Stanton; Chuck, Allan; Goldstein, Peter; Langford, E. S.; Carlitz, Leonard. *The American Mathematical Monthly*. Vol. 73, No. 1, (Jan., 1966), pp. 84-85.

[37] Purdy, George; Brown, J.L., Jr.. *The American Mathematical Monthly*. Vol. 74, No. 5, (May., 1967), pp. 594-595.

[38] Rademacher, Hans; Toeplitz, Otto. *The Enjoyment of Mathematics. Selections from Mathematics for the Amateur*. Princeton University Press. 1957.

[39] Savchev, Svetoslav; Andreescu, Titu. *Mathematical Miniatures*. The Mathematical Association of America. 2003.

[40] Schumer, Peter. *Mathematical Journeys*. John Wiley & Sons. 2004.

[41] Sivaramakrishnan, R.; Beiter, Marion; Greening, M. G.. *The American Mathematical Monthly*. Vol. 75, No. 5, (May., 1968), pp. 550.

[42] Stark, Harold. *An Introduction to Number Theory*. MIT Press. 1998.

[43] Stopple, Jeffrey. *A Primer of Analytic Number Theory. From Pythagoras to Riemann*. Cambridge University Press. 2003.

[44] Tattersall, James. *Elementary Number Theory in Nine Chapters*. Cambridge University Press. 1999.

[45] Vaidya, A. M.; Butter, F. A., Jr.; Prielipp, Robert W.. *The American Mathematical Monthly*. Vol. 73, No. 2, (Feb., 1966), pp. 203.

[46] Venkataraman, C. S.; Clarke, L. E.. *The American Mathematical Monthly*. Vol. 73, No. 9, (Nov., 1966), pp. 1026-1027.

[47] Vinogradov, Ivan. *Fundamentos de la Teoría de Números*. Editorial Mir. 1977.