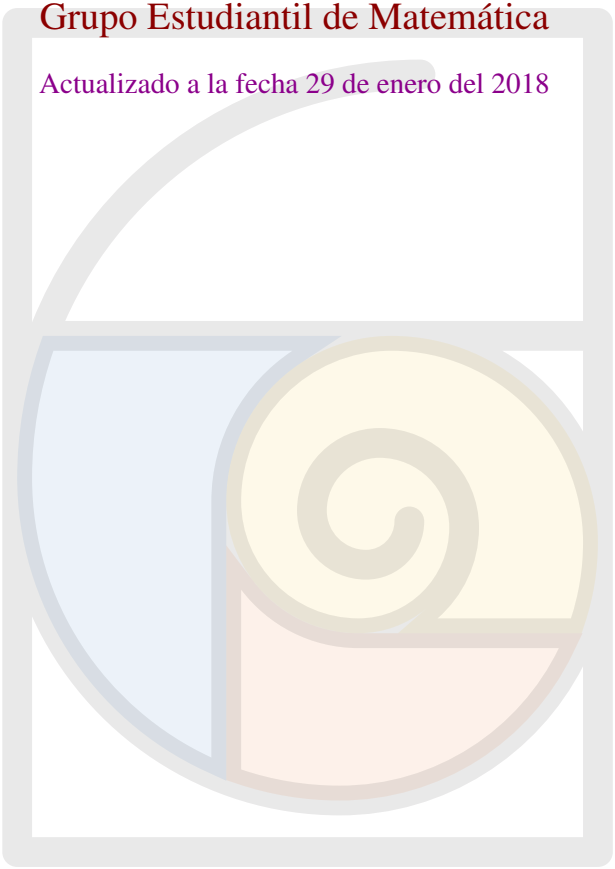
Apuntes de clases de Teoría de números

Grupo Estudiantil de Matemática

Actualizado a la fecha 29 de enero del 2018



Prefacio

Estos son los apuntes de clases de Teoría de números organizado por el Grupo Estudiantil de Matemática durante los meses de enero y febrero del año 2018.

Muchas gracias al Instituto de Matemática y Ciencias Afines por brindarnos sus ambientes para llevar a cabo las clases.

Por favor, cualquier sugerencia o aviso de error escribir a gem@uni.edu.pe o caznaranl@uni.pe.

Carlos Aznarán

Und. Jimmy Espinoza Palacios
Miembro del GEM
Facultad de Ciencias

Und. Bruno Goicochea Vilela
Presidente del GEM
Facultad de Ciencias

Tabla de contenido

Un poco acerca de la historia de la *Teoría de números*

En el año 1912, durante el quinto Congreso Internacional de Matemáticos, el matemático alemán, en tal evento, Edmund Landau listó cuatro problemas básicos acerca de *los números primos* que los calificó como *inabarcable en el estado actual de las matemáticas* y en nuestros días es conocido como los **Problemas de Landau**. Ellos son los siguientes:

1. Conjetura de Goldbach[1]
2. Conjetura de los primos gemelos.
3. Conjetura de Legendre.
4. ¿Existen infinitos números primos de la forma $n^2 + 1$?

Ninguno de los cuatro problemas han sido resultados a la fecha de la edición de los apuntes.

La teoría de números tal como se conoce en la actualidad inició desde Gauss. En el año 2013, el matemático peruano Harald Andrés Helfgott demostró la *Conjetura débil (o ternaria) de Goldbach*

0.1. Harald Andrés Helfgott

Conjetura 1. *Goldbach Todo número impar mayor que cinco es la suma de tres números primos.*

Leonhard Euler, uno de los más grandes matemáticos del siglo XVIII, y de todas las épocas, y su amigo cercano *Christian Goldbach*, quien tenía grandes conocimientos tanto en la ciencia como en las humanidades, mantuvo una regular y copiosa correspondencia. Goldbach hizo una conjetura acerca de los números primos, y Euler rápidamente redujo a la siguiente conjetura, el cual, dijo, Goldbach ya le había dicho: cada entero positivo puede escribirse a lo más, como la suma de tres números primos.

Ahora, podríamos decir que “cada entero mayor que cinco”, ya que no consideramos a 1 como un número primo. Es más, en la actualidad la conjetura se divide en dos casos: la

[1] Helfgott probó la conjetura débil en el año 2013.

conjetura débil o ternaria de Goldbach establece que cada entero impar mayor que cinco se puede escribir como la suma de tres primos y la *conjetura fuerte o binaria de Goldbach* establece que cada entero par mayor que 2 se puede escribir como la suma de dos primos. Como indican sus nombres, la conjetura fuerte implica la débil (fácilmente: reste 3 al número impar n, luego exprese $n-3$ como la suma de dos números primos).

La Olimpiada Internacional de Matemática (IMO) es la Olimpiada científica más grande, más antigua y más prestigiosa para estudiantes de secundaria. La historia de la IMO se remonta a 1959, cuando la primera edición se celebró en Rumanía y participaron siete países: Rumanía, Hungría, Bulgaria, Polonia, Checoslovaquia, Alemania Oriental y la URSS. Desde entonces, el evento se ha celebrado todos los años (excepto 1980) en un país diferente. Actualmente, participan más de 100 países de los 5 continentes. Cada país puede enviar un equipo de hasta seis estudiantes secundarios o individuos que no hayan ingresado a la Universidad o su equivalente,

as of the date of celebration of the Olympiad, plus one team leader, one deputy leader, and observers if desired.

During the competition, contestants have to solve, individually, two contest papers on two consecutive days, with three problems each day. Each problem is worth seven points. Gold, silver, and bronze medals are awarded in the ratio of 1:2:3 according to the overall results — half of the contestants receive a medal. In order to encourage as many students as possible to solve complete problems, certificates of honorable mention are awarded to students (not receiving a medal) who obtained 7 points for at least one problem.

a partir de la fecha de celebración de la Olimpiada, más un líder de equipo, un líder adjunto y observadores si así lo desean. Durante la competencia, los concursantes deben resolver, individualmente, dos documentos del concurso en dos días consecutivos, con tres problemas cada día. Cada problema vale siete puntos. Las medallas de oro, plata y bronce se otorgan en una proporción de 1: 2: 3 de acuerdo con los resultados generales: la mitad de los concursantes reciben una medalla. Con el fin de alentar a tantos estudiantes como sea posible para resolver problemas completos, se otorgan certificados de mención honorífica a los estudiantes (que no reciben una medalla) que obtuvieron 7 puntos por al menos un problema.

Capítulo 1

Introducción

I. *Principio de inducción matemática*

Sea $\mathcal{P}$ un conjunto de números naturales tal que

a) $1 \in \mathcal{P}$.

b) Si $n \in \mathcal{P} \implies n+1 \in \mathcal{P}$.

$\therefore \boxed{\mathcal{P} = \mathbb{N}}$.

II. *Principio del buen orden*

Si $\mathcal{A}$ es un conjunto no vacío de $\mathbb{N}$, entonces $\mathcal{A}$ *posee un elemento mínimo*.

1.1. Divisibilidad

Definición 1.1. *Sean d y n dos números enteros, se denotará*

$$\boxed{d \text{ divide a } n \iff \text{existe } c \in \mathbb{Z} \text{ tal que } n = c \cdot n}$$

como $a \mid n$.
Si d no divide a n, es decir, si $\forall c \in \mathbb{Z}\colon n \neq c \cdot d$, se denotará como $d \nmid n$.

Propiedades de la operación $\mid$

1) $n \mid n$ para cualquier $n \in \mathbb{N}$ (Reflexividad).

2) Si $d \mid n$ y $n \mid m$, entonces $d \mid m$. (Transitividad).

3) Si $d \mid n$ y $d \mid m$, entonces $d \mid an + bm$ $\forall a, b \in \mathbb{Z}$.

4) Si $d \mid n$, entonces $ad \mid an$.

5) Si $ad \mid an$ con $a \neq 0$, entonces $d \mid n$.

6) $1 \mid n$ para cualquier $n \in \mathbb{N}$.

7) $n \mid 0$ para cualquier $n \in \mathbb{N}$.

8) Si $0 \mid n$, entonces $n = 0$.

9) Si $d \mid n$ y $n \neq 0$, entonces $|d| \leqslant |n|$.

10) Si $d \mid n$ y $n \mid d$, entonces $|d| = |n|$.

11) Si $d \mid n$ con $d \neq 0$, entonces $\left(\frac{n}{d}\right) \mid n$.

1.2. Máximo común divisor

Definición 1.2. *Sean a, b y d números enteros. Si $d \mid a$ y $d \mid b$, entonces d es un divisor común de a y b.*

Teorema 1.1. *Dados los números enteros a y b, existe un divisor común d de a y b de la forma $d = ax + by$ para cualesquiera $x, y \in \mathbb{Z}$.*

Prueba: Por inducción matemática en $K = |a| + |b|$.

Si $K = 0$, entonces $a = b = 0$, esto es, $d = 0 \cdot a + 0 \cdot b$. ✓

Supongamos que se cumple para $K = 0, 1, \ldots, n-1$. (Hipótesis de inducción matemática).

Demostraremos para $\boxed{K = n = |a| + |b|}$.

Sin pérdida de generalidad, suponga que $|a| \geqslant |b|$. Así, si $|b| = 0$, entonces $b = 0$ y $|a| = n \implies d = n = (1)(\pm 1) + 0 \cdot b$.

Si $|b| \geqslant 1$, entonces para los números $|a| - |b|$ y $|b|$ se cumple la hipótesis:

$$\underbrace{|a| - |b|}_{\geqslant 0} + |b| = |a| - \cancel{|b|} + \cancel{|b|} = |a| < |a| + |b| = n.$$

Existe $d \in \mathbb{Z}$, $d \mid |a| - |b|$ y $d \mid |b|$. Además:

$$d = (|a| - |b|)\, x' + |b| y' \qquad \forall x', y' \in \mathbb{Z}$$

$$d = |a| \underbrace{x'}_{x''} + |b| \underbrace{y'}_{y''}$$

$$d = \underbrace{|a|}_{a,-a} x'' + \underbrace{|b|}_{b,-b} y''$$

$$d = a \underbrace{x''}_{\pm x'} + b \underbrace{y''}_{\pm y'}$$

Pero $d \mid |a|$ y $d \mid |b|$, así $d \mid |a| - |b|$.

$\therefore$ Esto cumple la condición. ■

Teorema 1.2. *Sean a y b números enteros, existe solo un número $d \in \mathbb{Z}$ tal que*

1) $d \geqslant 0$.

2) $d \mid a$ *y* $d \mid b$.

3) *Si* $e \mid a$ *y* $e \mid b$, *entonces* $e \mid d$ *para cualquier* $e \in \mathbb{Z}$.

Prueba: Por la definición 1.2 y por el teorema 1.1, existe un d con las siguientes propiedades:

$$d \mid a \qquad\qquad d \mid b \qquad\qquad d = ax + by$$

Es claro que $-d$ también cumple esto. Elegimos $|d| = ax' + by'$ que cumpla 1) y 2).
Si $e \mid a$ y $e \mid b$, entonces de la propiedad 3) $e \mid ax' + by' = |d|$.
Así, $e \mid |d|$, en consecuencia $e \mid d$ y $|d|$ satisface 3).
Si existiese un d' que cumpla 1), 2) y 3), entonces de la afirmación 3):

$$d \mid a \text{ y } d \mid b \implies d \mid d'. \tag{1.1}$$

De forma similar:

$$d' \mid a \text{ y } d' \mid b \implies d' \mid d. \tag{1.2}$$

Pero de (1.1) y (1.2) junto con la propiedad 10) se obtiene que $\boxed{d = d'}$. ■

Definición 1.3. *Este número* d *es llamado máximo común divisor de* a *y* b *y se denota como* $\mathrm{mcd}(a, b)$ *o* (a, b).

Observación 1.1. *Si el* $\mathrm{mcd}(a, b) = 1$, *entonces* a *y* b *son llamados coprimos, primos entre sí (PESI) o primos relativos.*

Algunas propiedades del máximo común divisor

1) $(a, b) = (b, a)$.

2) $(a, (b, c)) = ((a, b), c)$.

3) $(ac, bc) = |c|(a, b)$.

4) $(a, 1) = (1, a) = 1$.

5) $(a, 0) = (0, a) = |a|$.

Teorema 1.3. *Si* $a \mid bc$ *y si* $(a, b) = 1$, *entonces* $a \mid c$.

Demostración. Como $(a, b) = 1$, entonces existen $\tilde{x}, \tilde{y} \in \mathbb{Z}$ de modo que

$$1 = a\tilde{x} + b\tilde{y} \tag{1.3}$$

Pero si multiplicamos (1.3) por c resulta

$$c = a(c\tilde{x}) + b(c\tilde{y}) \tag{1.4}$$

Así, $a \mid cx$ y $a \mid cy$ (explicar).

■

1.3. Números primos

Definición 1.4. *El número $n \in \mathbb{N}$ es llamado número primo si sus divisores positivos son 1 y n. Cuando n no es primo, será llamado número compuesto.*

Teorema 1.4. *Cada natural $n > 1$ o es primo o producto de números primos.*

Prueba: Por inducción sobre n.
Para $n = 2$ ✓
Supongamos que se cumple para $n = 2, 3, \ldots, k-1$.
Demostraremos para $n = k$.

***)** Si k es un número primo.

***)** Si k no es un número primo, entonces k tiene por lo menos un divisor $d > 1$, por lo que $k = d \cdot c$ con $1 < c < k$ y $1 < d < k$.

Se cumple la hipótesis para c y d, entonces c y d son primos o productos de primos.

$$\begin{aligned} c &= p_1 p_2 \cdots p_k && (p_i\text{: primo}, k \geqslant 1). \\ d &= q_1 q_2 \cdots q_m && (q_i\text{: primo}, m \geqslant 1). \end{aligned}$$

Así, $n = c \cdot d = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_m$ (se cumple la inducción). ■

Teorema 1.5. *Existen infinitos números primos.*

Prueba: Supongamos que $\boxed{\mathbb{P} = p_1 p_2 \cdots p_k}$ es el conjunto de todos los números primos que existen. Definimos:

$$N = p_1 p_2 \cdots p_k + 1$$

¿Qué tipo de número es N, es un primo o uno compuesto?
Claro está que N es mayor que $p_i, \forall i = 1, \cdots k$.
$N = p_1 p_2 \cdots p_k + 1 = q_1 q_2 \cdots q_t$.

$$\begin{array}{l} q_i \mid p_1 p_2 \cdots p_k + 1 \\ q_i \mid p_1 p_2 \cdots p_k \qquad (-) \\ \hline q_i \mid 1 \quad (\Longrightarrow \Longleftarrow) \end{array}$$

$\therefore$ Existen infinitos números primos. ■

Teorema 1.6. *Si p es un número primo y $p \nmid a$, entonces $(p, a) = 1$.*

Demostración. Sea d el máximo común divisor de p y a (ya que el teorema 1.1 nos asegura su existencia), $d = (p, a)$, entonces

$$d \mid p \quad \text{y} \quad d \mid a.$$

■

Teorema 1.7. *Sea p un número primo. Si $p \mid ab$, entonces $p \mid a$ o $p \mid b$.*

Demostración: Supongamos que $p \nmid a$ ($p \mid a$ ✓), entonces $(p, a) = 1$, en consecuencia, $p \mid ab$.

$$\boxed{a \mid bc \quad \text{y} \quad (a,b) = 1 \implies a \mid c.}$$

$\therefore p \mid b.$ ■

Teorema 1.8. *Cada entero $n > 1$ se representa de forma única como producto de primos no necesariamente distintos, sin importar el orden.*

Prueba: Por inducción en n. Cuando $n = 2$ (se cumple: 2,3,...,n-1.) $n = p_1 p_2 \cdots, p_s = q_1 q_2 \cdots q_t$ $(s = t)$. $(s, t \geqslant 1)$

$p_1 \mid q_1 q_2 \cdots q_t \implies p_1 \mid q_1 \implies p_1 = q_1.$ ■

Observación 1.2. *Si se desea representar a n como producto de primos distintos (donde cabe la posibilidad en que se repitan algún número primo), podemos escribir:*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = \prod_{i=1}^{k} p_i^{a_i}$$

Teorema 1.9. *Si $n = \prod_{i=1}^{r} p_i^{a_i}$, entonces un divisor de n tiene la forma*

$$\prod_{i=1}^{r} = p_i^{c_i}, \quad 0 \leqslant c_i \leqslant a_i.$$

Observación 1.3. *Sea la sucesión de números primos*

$$p_1 = 2, p_2 = 3, p_3 = 5, \ldots,$$

entonces $n = \prod_{i=1}^{\infty} p_i^{a_i}$, $a_i \geqslant 0$.

Teorema 1.10. *Sean $a = \prod_{i=1}^{\infty} p_i^{a_i}$ y $b = \prod_{i=1}^{\infty} p_i^{b_i}$, entonces el máximo común divisor de a y b es*

$$(a, b) = \prod_{i=1}^{\infty} p_i^{c_i} \geqslant 0, \text{ donde } c_i = \text{mín}\{a_i, b_i\} \leqslant a_i, b_i.$$

Demostración: **1.** $\prod_{i=1}^{\infty} p_i^{c_i} \mid a \quad \wedge \quad \prod_{i=1}^{\infty} p_i^{c_i} \mid b.$

2. $e \mid a \quad \wedge \quad e \mid b, e = \prod_{i=1}^{\infty} p_i^{e_i}$.

Pero, $e_i \leqslant a_i$ y $e_i \leqslant b_i$,

$$\Longrightarrow \ e_i \leqslant \text{mín}\{a_i, b_i\} = c_i.$$

$$e = \prod_{i=1}^{\infty} p_i^{e_i} \mid \prod_{i=1}^{\infty} p_i^{c_i} = (a, b).$$

■

Teorema 1.11. *Sean a y b números enteros con $b > 0$, entonces existen únicos $q, r \in \mathbb{Z}$ tal que:*

$$a = bq + r, \quad 0 \leqslant r < b.$$

Además, $r = 0 \iff b \mid a$.

Demostración: Fijando $\underline{b}$ y por inducción en $a \in \mathbb{N}$. Si $a = 0$, entonces $a = b \cdot 0 + 0$. ✓
Supongamos que se cumple para $a = 0, 1, \ldots, k-1$.
Para $a = k$. $k - 1 = b \cdot q' + r', 0 \leqslant r' < b$.

$$\longrightarrow k = bq' + (r' + 1). \quad 1 \leqslant r' + 1 < b + 1.$$

- **•)** Si $1 \leqslant r' + 1 < b$ ✓
- **•)** Si $r' + 1 = b \rightarrow r' = b - 1 \implies$

■

1.4. Ejercicios

Lista N°1

1. Un número racional a/b con $(a, b) = 1$ se llama *fracción reducida*. Si la suma de dos fracciones reducidas es un entero, es decir, si $(a/b) + (c/d) = n$. Demostrar que entonces $|b| = |d|$.

2. Si $(a, b) = 1$, entonces $(a + b, a - b)$ o es 1 o es 2.

3. Si $(a, b) = 1$, entonces $(a + b, a^2 - ab + b^2)$ o es 1 o es 3.

4. Si $(a, b) = 1$, entonces $(a^n, b^k) = 1$ para todo $n \geqslant 1, k \geqslant 1$.

5. Un entero se llama *sin cuadrados* si no es divisible por el cuadrado de ningún primo. Probar que, para cada $n \geqslant 1$, existen $a > 0$ y $b > 0$, unívocamente determinados, tales que $n = a^2 b$, en donde b es sin cuadrados.

6. Probar que $\dfrac{21n+4}{14n+3}$ es irreducible para todo número natural n.

7. Sean $\{a,b,x,y\} \subset \mathbb{N}$. Si $(a,b)=1$ y $ab=c^n$, probar que $a=x^n$ y $b=y^n$ para algunos x,y enteros positivos.

8. Hallar $\left(a^{2^m}+1, a^{2^n}+1\right)$ en función de a.

9. Sean $\{a,b,x,y\} \subset \mathbb{N}$. Si $(a,b)=1$ y $x^a=y^b$ entonces probar que $x=n^b$ e $y=n^a$ para algún entero positivo.

10. Si $\{a,m,n\} \subset \mathbb{N}$ con $a>1$, probar que $(a^m-1, a^n-1) = a^{(m,n)}-1$.

11. Sea n un entero positivo y sea S un conjunto de enteros positivos menores o iguales a $2n$ tal que si a y b están en S y a y b son diferentes, entonces a no divide a b. Hallar el máximo número de elementos de S.

12. Hallar todos los pares de enteros positivos (a,b) tales que $a \mid b+1$ y $b \mid a+1$.

13. Hallar todos los pares de enteros positivos (a,b) tales que $a \mid 8b+1$ y $b \mid 8a+1$.

14. Halle todos los números enteros positivos n tales que el conjunto $\{n, n+1, n+2, n+3, n+4, n+5\}$ puede ser particionado en dos subconjuntos de modo que el producto de los números en cada subconjunto sea igual.

15. Sea m y n números enteros tales que:

$$\frac{m}{n} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319}$$

Probar que m es divisible por 1979. Ayuda: 1979 es un número primo.

1.5. Solución de la lista N°1

1. ***a)*** Dado $n = \dfrac{ad+bc}{bd}$, con b y d que dividen a $ad+bc$. Esto significa que $b \mid bc$ y $d \mid bc$, pero $\mathrm{mcd}(a,b) = \mathrm{mcd}(c,d) = 1$. se tiene que $b \mid b$ y $d \mid b$. Por lo tanto, $|b| = |d|$.

b) Sea $k \in \mathbb{Z}$ y $k = \dfrac{a}{b} + \dfrac{c}{d}$, entonces $\dfrac{c}{d} = k - \dfrac{a}{b} = \dfrac{ck-a}{b}$.
Supongamos por contradicción que $\mathrm{mcd}(kb-a, b) \neq 1$. Además, si $\mathrm{mcd}(kb-a,b) = n$, entonces $n \mid (kb-a)$ y $n \mid b$.

$$kb - a = n\ell_1 \quad \wedge \quad b = n\ell_2$$
$$k(n\ell_2) - a = n\ell_1$$
$$n(k\ell_2 - \ell_1) = a$$

Pero de la última ecuación, se infiere que $n \mid a$ y $n \mid b$, lo cual es una contradicción.

2. Si el $\mathrm{mcd}(a,b)=1$ y el $\mathrm{mcd}(a+b,a-b)=d$, entonces:

$$\begin{aligned} d \mid a+b \ \wedge\ d \mid a-b \ &\Longrightarrow d \mid (a+b)+(a-b) \quad \wedge d \mid (a+b)-(a-b) \\ d \mid a+b \ \wedge\ d \mid a-b \ &\Longrightarrow d \mid 2a \qquad\qquad\qquad\ \wedge d \mid 2b \end{aligned}$$

Por lo tanto $d \mid \mathrm{mcd}(2a,2b) \implies d \mid 2\,\mathrm{mcd}(a,b) \implies d \mid 2$, así, $d = 1 \vee 2$.

3. Si el $\mathrm{mcd}(a,b)=1$ y el $\mathrm{mcd}(a+b,a^2-ab+b^2)=d$, entonces:

$$\begin{aligned} d \mid a+b \ \wedge\ d \mid a^2-ab+b^2 \ &\Longrightarrow d \mid (a+b)^2 \\ d \mid a+b \ \wedge\ d \mid a^2-ab+b^2 \ &\Longrightarrow d \mid a^2+2ab+b^2 \\ d \mid a+b \ \wedge\ d \mid a^2-ab+b^2 \ &\Longrightarrow d \mid \cancel{a^2}+2ab+\cancel{b^2}-(\cancel{a^2}-ab+\cancel{b^2}) \\ d \mid a+b \ \wedge\ d \mid a^2-ab+b^2 \ &\Longrightarrow d \mid 3ab \end{aligned}$$

Por lo tanto, $d \mid 3a(a+b) \implies d \mid 3a^2+3ab$. De esto, $d \mid 3a^2$ y $d \mid 3ab$.

$$d \mid \mathrm{mcd}(3a^2,3ab) \implies d \mid |3a| \cdot \mathrm{mcd}(a,b) \implies d \mid 3a.$$

Como $d \mid a+b \implies d \mid 3a+3b \implies d \mid 3b$. $d \mid \mathrm{mcd}(3a,3b) \implies d \mid 3\underbrace{\mathrm{mcd}(a,b)}_{1} \implies d \mid 3$. Así, $d = 1 \vee 3$.

4. Si el $\mathrm{mcd}(a,b)=1$ y el $\mathrm{mcd}(a^n,b^k)=d>1$, entonces $d \mid a^n$ y $d \mid b^k$. Sea p un número primo de modo que $p \mid d$. Así:

$$p \mid a^n \ \wedge\ p \mid b^k \implies p \mid a \ \wedge\ p \mid b \implies p \mid \underbrace{\mathrm{mcd}(a,b)}_{1}$$

¡Un número primo divide a 1! ($\Longrightarrow \Longleftarrow$). $\therefore d = 1$.

5. Sea el conjunto $\mathbb{N} = \mathcal{A} \bigcup \mathcal{B}$, donde $\mathcal{A} \coloneqq \{n \in \mathbb{N} \mid n \text{ es libre de cuadrados}\}$ y $\mathcal{B} \coloneqq \mathcal{A}^{\complement}$.

Para el caso 1: Sea $\gamma = 1^2 \cdot \gamma$, si $\gamma \in \mathcal{A}$.

Sea $\theta \in \mathcal{B}$, entonces $\exists z^2 \ni \theta = z^2 \cdot \tau$.

Supongamos que τ no es libre de cuadrados:

$$\tau = n^2 \cdot m\checkmark$$

Al reemplazar resulta:

$$\theta = z^2n^2m = (z \cdot n)^2 \cdot m (\Longrightarrow \Longleftarrow)$$

6. Por contradicción y combinación lineal

$$\text{mcd}(a,b) = 1 \text{ y } a \cdot b = c^n$$

donde a y b tienen las siguiente forma:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \text{y} \quad b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}.$$

¡Recuerde que a y b no tiene factores comunes! Así, multiplicando a y b:

$$a \cdot b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \cdot q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell} = c^n,$$

donde

$$c = p_1^{\theta_1} p_2^{\theta_2} \cdots p_k^{\theta_k} \cdot q_1^{\phi_1} q_2^{\phi_2} \cdots q_\ell^{\phi_\ell}$$
$$c^n = p_1^{\theta_1 \cdot n} p_2^{\theta_2 \cdot n} \cdots p_k^{\theta_k \cdot n} \cdot q_1^{\phi_1 \cdot n} q_2^{\phi_2 \cdot n} \cdots q_\ell^{\phi_\ell \cdot n}$$

Por comparación obtenemos las siguientes igualdades:

$$\alpha_1 = \theta_1 \cdot n,\ \alpha_2 = \theta_2 \cdot n,\ \cdots, \alpha_k = \theta_k \cdot n.$$

$$\beta_1 = \phi_1 \cdot n,\ \beta_2 = \phi_2 \cdot n,\ \cdots, \beta_\ell = \phi_\ell \cdot n.$$

Así, $a = \left(\underbrace{p_1^{\theta_1} p_2^{\theta_2} \cdots p_k^{\theta_k}}_{x} \right)^n$ y $b = \left(\underbrace{q_1^{\phi_1} q_2^{\phi_2} \cdots q_\ell^{\phi_\ell}}_{y} \right)^n$.

7. Sea $g = \text{mcd}(\mathfrak{a}^{2^m} + 1, \mathfrak{a}^{2^n} + 1)$. Se define la aplicación $f_\mathfrak{a}$ con la siguiente regla de correspondencia como sigue:

$$f_\mathfrak{a} \colon \mathbb{N} \longrightarrow \mathbb{N}$$
$$k \longmapsto \mathfrak{a}^{2^k} + 1$$

Así, con la notación apropiada, g queda expresada como $\text{mcd}\left(f_\mathfrak{a}(m), f_\mathfrak{a}(n)\right)$. Además $g \mid f_\mathfrak{a}(m)$ y $g \mid f_\mathfrak{a}(n)$.

a) Para el caso en que $m > n$:
Ahora, calculemos:

$$\begin{aligned} f_\mathfrak{a}(m) - 2 &= \mathfrak{a}^{2^m} + 1 - 2 = \mathfrak{a}^{2^m} - 1 \\ &= \left(\mathfrak{a}^{2^n}\right)^{2^{m-n}} - 1 \\ &= \underbrace{\left(\mathfrak{a}^{2^n} + 1\right)}_{f_\mathfrak{a}(n)} \left(\mathfrak{a}^{2^{(m-n-1)}} - 1\right) \end{aligned}$$

Así que $f_\mathfrak{a}(n) \mid f_\mathfrak{a}(m) - 2$. Pero, como $g \mid f_\mathfrak{a}(n) \implies g \mid f_\mathfrak{a}(m) - 2$.
$\therefore g \mid -\cancel{f_\mathfrak{a}(m)} + 2 + \cancel{f_\mathfrak{a}(m)} \implies g \mid 2.$

- Si a es par, entonces $f_{\mathfrak{a}}(m)$ es impar y $g = 1$.
- Si a es impar, entonces $f_{\mathfrak{a}}(m)$ es par y $g = 2$.

b) Para el caso en que $m = n$:

c) Para el caso en que $m < n$:

8. Si el $\mathrm{mcd}(a, b) = 1$ y los números a y b tiene la siguiente representación:

$$a = p_1^{\theta_1} p_2^{\theta_2} \cdots p_k^{\theta_k} = \prod_{i=1}^{k} {p_i}^{\alpha_i}$$

$$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell} = \prod_{i=1}^{\ell} {q_i}^{\beta_i}$$

Pero $x^a =$

Capítulo 2

Funciones aritméticas

Definición 2.1. *Una **función aritmética** es cualquiera función* $f\colon \mathbb{Z}^+ \to \mathbb{C}$.

Algunas funciones aritméticas son:

1. Función de Möbius $\mu(n)$

$$\mu\colon \mathbb{Z}^+ \longrightarrow \{-1, 0, 1\}$$

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \text{ (D.C) con } \alpha_1 = \alpha_2 = \cdots = \alpha_k = 1; \\ 0 & \text{en otro caso.} \end{cases}$$

Observación 2.1. *$\mu(n) = 0$ si y solo si n posee un divisor cuadrado perfecto mayor que 1.*

Ejemplo 2.1. *Algunos valores de la función $\mu(n)$:*

n:	1	2	3	4	5	6	7	8	9	10
$\mu(n)$:	1	-1	-1	0	-1	1	-1	0	0	1

Teorema 2.1. *Si $n \geqslant 1$ y $d > 0$, entonces* $\displaystyle\sum_{d\,|\,n} \mu(d) = \begin{cases} 1 & \textit{si } n = 1, \\ 0 & \textit{si } n > 1. \end{cases}$

Demostración. *a)* Si $n = 1$: $\underbrace{\mu(1)}_{\sum_{d\,|\,1} \mu(d)} = 1$ ✓

b) Si $n > 1$, entonces $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (D.C). Si $d \mid n$ y d posee un factor cuadrado perfecto mayor que 1, entonces $\mu(d) = 0$.

$$\sum_{d\,|\,n} \mu(d) = \underbrace{\sum_{d\,|\,n} \mu(d)}^{0} + \underbrace{\sum_{d\,|\,n} \mu(d)}$$

d posee algún factor $k^2 > 1$ $\quad$ d no posee factor $k^2 > 1$

$d \mid n$ y d no poseen factor $k^2 > 1$.

$\implies d = p_{i1}p_{i2}\cdots p_{is}$

$$\implies \sum_{d\mid n}\mu(d) = \mu(1) + \mu(p_1) + \mu(p_2) + \cdots + \mu(p_k) +$$

$$\mu(p_1p_2) + \cdots + \mu(p_{k-1}p_k) + \cdots \mu(p_1p_2\cdots p_k)$$

$$= 1\binom{k}{0} + (-1)\binom{k}{1} + (-1)^2\binom{k}{2} + \cdots + (-1)^k\binom{k}{k}$$

$$= (1 + (-1))^k = 0.$$

■

2. Función indicador de Euler.

$$\varphi\colon \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$$

$\varphi(n)$: cantidad de números menores o iguales que n y coprimos con n.

Ejemplo 2.2. *Algunos valores de la función* $\varphi(n)$:

n:	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$:	1	1	2	2	4	2	6	4	6	4

Teorema 2.2. *Si* $n \geqslant 1$, *entonces* $\sum_{d\mid n}\varphi(d) = n$.

Demostración. Para cada d tal que $d \mid n$. Sea:

$$\mathcal{A}_d \coloneqq \{k\colon \operatorname{mcd}(k,n) = d, 1 \leqslant k \leqslant n\}.$$

$a \in \mathcal{A}_d, \mathcal{A}_{d'} (d \neq d')$

$\implies \operatorname{mcd}(a,n) = d, \operatorname{mcd}(a,n) = d' (\implies \impliedby)$.

$\implies \mathcal{A}_d \bigcap \mathcal{A}_{d'} = \varnothing (\forall d \neq d')$

Sea $f(d)$ la cantidad de elementos de $\mathcal{A}_d$.

$$\bigcup_{d\mid n}\mathcal{A}_d = \{1, 2, \ldots, n\}.$$

Porque si $k \leqslant n \implies \operatorname{mcd}(k,n) = d$ en donde $d \mid n \implies \mathcal{A}_d \subset \bigcup_{d\mid n}\mathcal{A}_d \implies \sum_{d\mid n} f(d) = n$. Pero $\operatorname{mcd}(k,n) = d \implies \operatorname{mcd}\left(\frac{k}{d}, \frac{n}{d}\right) = 1$.

$$\mathcal{A}_d \coloneqq \left\{k\colon \left(\frac{k}{d}, \frac{n}{d}\right) = 1, 1 \leqslant k \leqslant n\right\}$$

$$\mathcal{B}_d \coloneqq \left\{q\colon \left(q, \frac{n}{d}\right) = 1, 1 \leqslant q \leqslant \frac{n}{d}\right\}$$

$\implies |\mathcal{A}_d| = |\mathcal{B}_d| = f(d) = \varphi\left(\frac{n}{d}\right)$

$$\boxed{\implies \sum_{d\mid n}\varphi\left(\frac{n}{d}\right) = n.}$$

■

2.1. Relación entre μ y φ

Teorema 2.3. *Si $n \geqslant 1$, entonces* $\varphi(n) = \sum_{d\,|\,n} \mu(d)\left(\frac{n}{d}\right)$.

Demostración.

$$\varphi(n) = \sum_{k=1}^{n} i(k), \text{ donde } i(k) = \begin{cases} 1 & \text{si } \operatorname{mcd}(n,k) = 1, \\ 0 & \text{si } \operatorname{mcd}(n,k) \neq 1. \end{cases}$$

Por el teorema:

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

$$\sum_{d\,|\,\operatorname{mcd}(n,k)} \mu(d) = \begin{cases} 1 & \text{si } i(k) = 1, \\ 0 & \text{si } i(k) = 0. \end{cases}$$

$$\sum_{d\,|\,\operatorname{mcd}(n,k)} \mu(d) = i(k)$$

$$\implies \varphi(n) = \sum_{d\,|\,\operatorname{mcd}(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d\,|\,n \\ d\,|\,k}} \mu(d)$$

Fijamos un divisor d en n. Entonces, el divisor d de n aparecerá siempre y cuando k sea múltiplo de d ($k = qd$). Por lo tanto,

$$d \leqslant k \leqslant n \implies 1 \leqslant q \leqslant \frac{n}{d}.$$

Hay $\frac{n}{d}$ múltiplos de k.

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

■

Fórmula para $\varphi(n)$

Teorema 2.4. *Si $n > 1$, entonces* $\varphi(n) = n\prod\left(1 - \frac{1}{p}\right)$.

Demostración. Usar el principio de inclusión y exclusión. Sean $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \ldots, \mathcal{A}_k$ conjuntos (puede haber algún conjunto vacío).

$$\implies \left|\bigcup_{i=1}^{k} \mathcal{A}_i\right| = \sum_{i=1}^{k} |\mathcal{A}_i| - \sum_{\substack{i,j=1 \\ i\neq j}}^{k} \left|\mathcal{A}_i \bigcap \mathcal{A}_j\right| + \sum_{i,j,\ell=1} \left|\mathcal{A}_i \bigcup\right|$$

$$\left|\mathcal{A}_1 \bigcup \mathcal{A}_2 \bigcup \cdots \bigcup \mathcal{A}_k\right| = \sum_{i=1}^{k} (-1)^{i+1} \left| \bigcap_{k=1}^{i} \mathcal{A}_{\tilde{t}} \right|_{1 \leqslant t_1 \leqslant t_2 \leqslant \cdots \leqslant t_i \leqslant k}$$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (D.C)

$$\begin{aligned}
\mathcal{A}_1 &= \{ \text{múltiplos } p_1 \leqslant n\}, & |A_1| &= \frac{n}{p_1} \\
\mathcal{A}_2 &= \{ \text{múltiplos } p_2 \leqslant n\}, & |A_2| &= \frac{n}{p_2} \\
\mathcal{A}_3 &= \{ \text{múltiplos } p_3 \leqslant n\}, & |A_3| &= \frac{n}{p_3} \\
\vdots &= \vdots, & |A_1| &= \frac{n}{p_1} \\
\mathcal{A}_k &= \{ \text{múltiplos } p_k \leqslant n\}, & |A_k| &= \frac{n}{p_k}
\end{aligned}$$

El conjunto $\mathcal{A}_1 \bigcup \mathcal{A}_2 \bigcup \mathcal{A}_3 \bigcup \cdots \bigcup \mathcal{A}_k$ tiene algún factor común con n. Por lo tanto, $(\mathcal{A}_1 \bigcup \mathcal{A}_2 \bigcup \mathcal{A}_3 \bigcup \cdots \bigcup \mathcal{A}_k)'$: elementos coprimos con n y $\leqslant n$.

$\implies \varphi(n) = \left|(\mathcal{A}_1 \bigcup \mathcal{A}_2 \bigcup \mathcal{A}_3 \bigcup \cdots \bigcup \mathcal{A}_k)'\right| = n - |\mathcal{A}_1 \bigcup \mathcal{A}_2 \bigcup \mathcal{A}_3 \bigcup \cdots \bigcup \mathcal{A}_k|$

Pero:

$$\left|\mathcal{A}_1 \bigcup \mathcal{A}_2 \bigcup \mathcal{A}_3 \bigcup \cdots \bigcup \mathcal{A}_k\right| = |\mathcal{A}_1| + |\mathcal{A}_2| + \cdots + |\mathcal{A}_k| - \left(\left|\mathcal{A}_1 \bigcup \mathcal{A}_2\right| + \cdots + \left|\mathcal{A}_{k-1} \bigcup \mathcal{A}_k\right|\right) +$$

El conjunto:

$$\mathcal{A}_{i_1} \bigcap \mathcal{A}_{i_2} \bigcap \cdots \bigcap \mathcal{A}_{i_t} = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_t}}$$

$$\left|\mathcal{A}_1 \bigcap \mathcal{A}_2 \bigcap \cdots \bigcap \mathcal{A}_k\right| = \frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_k} - \left(\frac{n}{p_1 p_2} + \cdots + \frac{n}{p_{k-1} p_k}\right) + \cdots + (-1)^{k-1} \left(\frac{n}{p_1 p_2 \cdot}\right.$$

$$\begin{aligned}
\implies \varphi(n) &= n - \left|\mathcal{A}_1 \bigcup \mathcal{A}_2 \bigcup \cdots \bigcup \mathcal{A}_k\right| \\
&= n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_k}\right) + \left(\frac{n}{p_1 p_2} + \cdots + \frac{n}{p_{k-1} p_k}\right) - + \cdots + (-1)^{k-1} \cdot \frac{}{p_1}
\end{aligned}$$

$$\begin{aligned}\varphi(n) &= n\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)\\ &= n\prod_{\substack{p\mid n\\ p:\text{ primo}}}\left(1-\frac{1}{p}\right)\end{aligned}$$

■

Algunas propiedades de la función indicador

1. $\varphi\left(p^{\alpha}\right) = p^{\alpha} - p^{\alpha-1}$
2. $\varphi\left(mn\right) = \varphi(m)\varphi(n)\left(\frac{d}{\varphi(d)}\right)$
3. $\varphi\left(mn\right) = \varphi(m)\varphi(n)$, si $\operatorname{mcd}(m,n) = 1$.
4. Si $a \mid b$, entonces $\varphi(a) \mid \varphi(b)$.
5. $\varphi(n)$ es par para cada $n \geqslant 3$. Más aún:

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} \implies 2^k \mid \varphi(n)$$

2.2. Funciones multiplicativas

Definición 2.2. *Una función aritmética $f\colon \mathbb{Z}^+ \to \mathbb{C}$ es llamada multiplicativa si f no es idénticamente nula y si*

$$f(mn) = f(m)f(n) \quad \forall m,n \in \mathbb{Z}^+, \quad \operatorname{mcd}(a,b) = 1.$$

Definición 2.3. *Una función multiplicativa $f\colon \mathbb{Z}^+ \to \mathbb{C}$ es completamente multiplicativa si:*

$$f(mn) = f(m)f(n) \quad \forall m,n \in \mathbb{Z}^+.$$

Ejemplo 2.3. *$\varphi(n)$ es multiplicativa, pero no es completamente multiplicativa $\forall n \in \mathbb{Z}^+$.*

Teorema 2.5. *Si f es multiplicativa, entonces $f(1) = 1$.*

Demostración.

$$\cancel{f(n)} = f(n\cdot 1) \overset{\text{def}}{=} \cancel{f(n)}f(1) \implies f(1) = 1.$$

■

Teorema 2.6. *Sea $f\colon \mathbb{Z}^+ \to \mathbb{C}$ con $f(1) = 1$.*

1. *f es multiplicativa* $\iff f\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right) = f\left(p_1^{\alpha_1}\right) \cdot f\left(p_2^{\alpha_2}\right) \cdot \cdots \cdot f\left(p_k^{\alpha_k}\right) \quad \forall p_1 p_2 \cdots p_k$ *primos y* $\alpha_1, \alpha_2, \ldots, \alpha_k \leqslant 1 \in \mathbb{Z}^+$.

2. *Si f es multiplicativa, entonces*

$$f \text{ es completamente multiplicativa} \iff f\left(p^{\alpha}\right) = \left(f(p)\right)^{\alpha}$$

$\forall p$: *primo y* $\tilde{\alpha} \in \mathbb{Z}^+$.

Mis notas de estudio

Divisibilidad

Definición 2.4. *Un entero b es divisible por un entero a, no cero, si existe un entero x tal que $b = ax$ y se escribe $a \mid b$. En el caso en que b no sea divisible por a se escribe $a \nmid b$.*

Teorema 2.7. *Sean $\{a, b, c, x, y\} \subset \mathbb{Z}$, las siguientes proposiciones son verdaderas:*

1) *Si $a \mid b$, entonces $a \mid bc$ para cualquier entero c.*

Prueba:

De la definición (2.7) se sigue que existe algún entero m tal que $b = a \cdot m$. Ahora, sea $c \in \mathbb{Z}$ fijo y arbitrario. Así, el número $bc = a \cdot m(c)$ y de (2.7) existe un entero $d = m(c)$ tal que $b = a \cdot d$, por lo tanto $a \mid bc$. ■

1) *Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*

Prueba:

De la definición (2.7) se sigue que existen los entero m_1 y m_2 tales que $b = a \cdot m_1$ y $c = b \cdot m_2$. Pero c es igual a $b \cdot m_2 = (a \cdot m_1) \cdot m_2 = a \cdot (m_1 \cdot m_2)$, es decir, existe un entero $m_3 = m_1 \cdot m_2$ tal que $c = a \cdot m_3$, por lo tanto, de (2.7) $a \mid c$. ■

1) *Si $a \mid (b_1, b_2, \ldots, b_n)$ para algún $n \in \mathbb{N}$, entonces $a \mid \sum_{j=1}^{n} b_j x_j$ para cualesquiera x_j.*

Prueba:

De la definición (2.7) se sigue que existen n números $m_1, m_2, \ldots, m_n$ tales que $b_j = a \cdot m_j$ cuando $j \in \{1, 2, \ldots, n\}$. ■

1) *Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$.*

Prueba:

■

Algunos códigos

Un divisor positivo de n, el cual ni es 1 ni n, es llamado un **divisor propio**, y un **primo** es un entero mayor que 1 que no tiene divisores propios.