

SOBRE LA TEORÍA ANALÍTICA DE NÚMEROS

LUIS ALBERTO LOMELÍ

Impartimos un minicurso introductorio a la teoría analítica de números a los estudiantes de la Facultad de Ciencias de la Universidad Autónoma de Baja California. El curso fué dirigido a estudiantes de licenciatura en su tercer o cuarto año. En total, se impartieron 10 horas frente a grupo en 5 días. La idea inicial del curso era cubrir el material del capítulo VI del libro de J.-P. Serre “Cours d’Arithmétique”, presentando material suplementario, y haciendo el material de las primeras 8 sesiones autocontenido. El prerrequisito necesario es un curso de variable compleja, y muchos estudiantes habían cursado o se encontraban cursando álgebra moderna.

Comenzamos repasando rápidamente, ab initio, las nociones necesarias dentro de la categoría de grupos finitos abelianos y sus caracteres. Se refleja el punto de vista que las nociones cubiertas en este curso se generalizan al incorporar análisis de Fourier en la categoría de grupos abelianos localmente compactos [6]. Un curso subsecuente puede llevar a la teoría analítica de números con el enfoque de la tesis de Tate [9], ver también [4].

También repasamos aspectos básicos sobre funciones holomorfas, además, necesitamos los conceptos de continuidad uniforme y continuación analítica. En las secciones 4–8, cubrimos material estándar siguiendo a Serre [7]. Estudiamos parte de la teoría de funciones L de Dirichlet, y revisamos algunos detalles que surgen de una lectura minuciosa del libro de Serre. Incluimos una demostración de la ecuación funcional de la función ζ de Riemann, en donde encontramos de gran utilidad el libro de Iwaniec [2], además de la referencia original de Riemann [5]. La ecuación funcional para funciones L de Dirichlet y su continuación analítica no la cubrimos, por limitaciones de tiempo, pero con la ecuación funcional para $\zeta(s)$ nos es suficiente para dar demostraciones completas de las aplicaciones provistas.

Para las secciones 9 y 10, inicialmente teníamos contemplado incluir una demostración completa del teorema de los números primos. Sin embargo, la audiencia ya habiendo asimilado el material de las primeras 8 secciones, no debe ser privada del gusto de leer independientemente una demostración elemental que se puede encontrar, por ejemplo, en [2]. En la sección 9, hacemos una selección de temas importantes en la teoría de números y proveemos referencias en donde el lector podrá obtener una buena idea de los temas mencionados. Decidimos concluir con una versión matemática de la impresión de un egresado de la UABC sobre Valparaíso, Chile.

Agradecimientos. Me gustaría dar gracias a Adina Jordan, Brenda de la Rosa, Gloria Rubí, Selene Solorza y a Carlos Yee de la UABC por la invitación a impartir el curso. Me es muy grato agradecer a Alberto Lomelí, quien tomó notas detalladas. Gracias a él, existen estas notas en versión pdf, pues me alentó a escribirlas además de proveer muchos comentarios que fueron incorporados.

1. SOBRE ARITMÉTICA Y ÁLGEBRA

1.1. En Aritmética estudiamos a los números enteros $\mathbb{Z}$ y a los números primos. Para $n \in \mathbb{Z}$, podemos formar una relación de equivalencia

$$x \equiv y \pmod{n},$$

la cual se lee x es congruente a y módulo n , si existe una $z \in \mathbb{Z}$ tal que $x - y = nz$. Definimos

$$\mathbb{Z}/n\mathbb{Z} = \{[x] \mid x \in \mathbb{Z}\},$$

en donde tenemos n clases de equivalencia como elementos $[0], \dots, [n-1]$, y podemos sumar módulo n .

La pregunta que surge es si podemos multiplicar en $\mathbb{Z}/n\mathbb{Z}$? Dados dos enteros m, n , denotamos su máximo común divisor por (m, n) .

Proposición 1.1. *El grupo de elementos invertibles en $\mathbb{Z}/n\mathbb{Z}$ bajo la multiplicación es*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[x] \in \mathbb{Z}/n\mathbb{Z} \mid (x, n) \equiv 1\}.$$

Demostración. Para $x \in \mathbb{Z}$, tenemos que

$$\begin{aligned} (x, n) = 1 &\iff \text{existen } a, b \in \mathbb{Z}, \text{ tales que } ax + bn = 1 \\ &\iff ax \equiv 1 \pmod{n} \\ &\iff [x]^{-1} = [a] \end{aligned}$$

□

Surge la función aritmética ϕ de Euler, como la cardinalidad de este conjunto

$$\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

Observamos que si tomamos p primo

$$\#(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\},$$

i.e., $\phi(p) = p - 1$.

1.2. **Grupos y sus caracteres.** Recordemos rápidamente nociones básicas de grupos.

Definición 1.2. *Un conjunto G es un grupo si tiene una operación*

$$G \times G \rightarrow G, (g_1, g_2) \mapsto g_1 g_2$$

que satisface

- (i) $\exists e \in G \ni ex = xe = x \forall x \in G$.
- (ii) $\forall x \in G \exists x^{-1} \ni x^{-1}x = xx^{-1} = e$.
- (iii) $x(yz) = (xy)z, \forall x, y, z \in G$.

Proposición 1.3. *El elemento identidad es único.*

Demostración. Si e' fuera otro

$$e' = e'e = e$$

□

Decimos que un grupo G es abeliano si además satisface

(iv) $xy = yx, \forall x, y \in G$.

Tenemos la noción de subgrupo H de G , denotado por $H < G$, además de la noción de un grupo cíclico si G , generado por x , escrito

$$G = \langle x \rangle.$$

Denotamos por $\mathcal{G}$ a la categoría cuyos objetos son grupos y sus flechas son homomorfismos de grupos¹

$$H, G \in \mathcal{G}, \quad G \xrightarrow{f} H.$$

Tenemos entonces el conjunto de todas las flechas de G a H en $\mathcal{G}$:

$$\text{hom}(G, H) = \{f : G \rightarrow H \mid f(x, y) = f(x)f(y) \forall x, y \in G, f(e_G) = e_H\}$$

En la categoría $\mathcal{G}$ podemos formar productos

$$G, H \in \mathcal{G} \Rightarrow G \times H \in \mathcal{G}$$

en donde la operación en $G \times H$ está dada por

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

Ejemplo 1.4. Si tenemos $n, m \in \mathbb{Z}$, entonces

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \in \mathcal{G}.$$

Los siguientes dos resultados son básicos en un curso de álgebra moderna. El primero es el Teorema del Residuo Chino y el segundo es un resultado de clasificación.

Teorema 1.5. Si $n = p_1^{a_1} \cdots p_k^{a_k}$ entonces

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z}.$$

Teorema 1.6. Todo grupo finito abeliano G , es de la forma

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_d\mathbb{Z}.$$

Decimos que

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3$$

es exacta si $\ker(f_2) = \text{im}(f_1)$. Recordamos que si $G \xrightarrow{f} H$, tenemos kernel e imagen definidos por

$$\ker(f) = \{y \in G \mid f(y) = e_H\}$$

$$\text{im}(f) = \{f(y) \in H \mid y \in G\}$$

y sabemos que $\ker(f), \text{im}(f) \in \mathcal{G}$.

En $\mathcal{G}$, tenemos las siguientes propiedades para flechas

(i) $G \xrightarrow{f} H$ es inyectiva si

$$1 \rightarrow G \xrightarrow{f} H$$

es exacta.

¹Una categoría es una clase de objetos y flechas, en donde las flechas tienen una ley de composición. Es definida como una clase, para evitar problemas como la paradoja de Russel. La clase de todos los conjuntos, es un ejemplo de una clase que no es un conjunto.

(ii) $G \xrightarrow{f} H$ es sobreyectiva si

$$G \xrightarrow{f} H \rightarrow 1$$

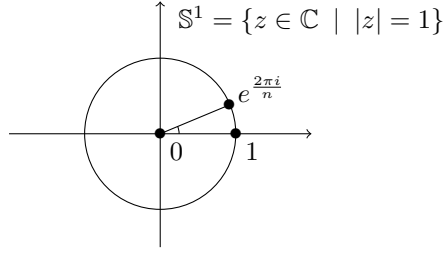
es exacta.

(iii) $G \xrightarrow{f} H$ es un isomorfismo si

$$1 \rightarrow G \xrightarrow{f} H \rightarrow 1$$

es exacta.

Ejemplo 1.7. Sea $\mu_n \in \mathcal{G}$ el grupo multiplicativo de las raíces n -ésimas de la unidad $1 \in \mathbb{C}$.



Tenemos isomorfismos

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{f_k} \mu_n, \quad x \mapsto e^{\frac{2\pi i k x}{n}},$$

para cada k tal que $(k, n) = 1$. Además $\phi(n)$ es el número de generadores del grupo aditivo $\mathbb{Z}/n\mathbb{Z}$.

Proposición 1.8. $n = \sum_{d|n} \phi(d)$.

Demostración. Para cada $d|n$ tenemos que el grupo $\mathbb{Z}/d\mathbb{Z}$ tiene $\phi(d)$ generadores y $n = \#(\mathbb{Z}/n\mathbb{Z})$. Para cada $x \in \mathbb{Z}/n\mathbb{Z}$, formamos el grupo cíclico

$$H_x = \langle x \rangle.$$

Recordamos que para cada $d|n$ existe un único subgrupo cíclico de $\mathbb{Z}/n\mathbb{Z}$ que es isomorfo a $\mathbb{Z}/d\mathbb{Z}$. Ahora, para toda $x \in G$, existe una d tal que $H_x \cong \mathbb{Z}/d\mathbb{Z}$.

Por lo tanto, tenemos la unión disjunta

$$\mathbb{Z}/n\mathbb{Z} = \cup \Phi_d,$$

en donde Φ_d es el conjunto de generadores de $\mathbb{Z}/d\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z}$. Observamos que $\#\Phi_d = \phi(d)$, por lo que concluimos que $n = \sum_{d|n} \phi(d)$ comparando las cardinalidades. $\square$

1.3. Funciones Aritméticas. Una función $f : \mathbb{N} \rightarrow C$ es multiplicativa si

$$f(m, n) = f(m)f(n) \quad \text{para} \quad (m, n) = 1.$$

Como ejemplo, ya nos encontramos con la función ϕ de Euler

$$\phi(n) = \#\{x | 1 \leq x \leq n, (x, n) = 1\},$$

y satisface las siguientes propiedades:

- (i) $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.
- (ii) $n = \sum_{d|n} \phi(d)$.
- (iii) $\phi(n)$ es el número de generadores de $\mathbb{Z}/n\mathbb{Z}$.
- (iv) ϕ es multiplicativa.

$$(v) \phi(n) = n \cdot \prod_{p|n} (1 - \frac{1}{p}).$$

y es un ejercicio completar la demostración de las propiedades no cubiertas en clase.

Un segundo ejemplo es provisto por la función de Ramanujan

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$$

La función τ es una función aritmética que satisface:

$$\tau(mn) = \tau(m)\tau(n),$$

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p\tau(p^{n-1}),$$

p primo. La función $\Delta(z)$ es de importancia aritmética y nos conduce a una forma modular, en donde la variable

$$z \in \mathfrak{h} = \{z \in \mathbb{C} \mid \Im(z) > 0\},$$

varía en el plano hiperbólico $\mathfrak{h}$. No cubriremos formas modulares en este minicurso, y referimos al lector interesado al capítulo VII de [7]. Solamente comentamos que la famosa conjetura de Ramanujan, demostrada por Deligne para formas modulares en los 70's [1], se escribe

$$\tau(n) = O(n^{\frac{1}{2}+\epsilon}), \quad \forall \epsilon > 0,$$

con la notación O para funciones de una variable real: $f(x) = O(g(x))$ si existe una constante M tal que

$$|f(x)| \leq M|g(x)|, \quad \forall x \gg 0.$$

2. CARACTERES DE GRUPOS ABELIANOS FINITOS

Sea $\mathcal{G}_{f.ab.}$ la categoría de grupos finitos abelianos. Para cada $G \in \mathcal{G}_{f.ab.}$, definimos el conjunto sus caracteres

$$\widehat{G} = \text{hom}(G, \mathbb{C}^\times),$$

en donde $\mathbb{C}^\times = \mathbb{C} \setminus \{0\} \in \mathcal{G}_{f.ab.}$ es un grupo multiplicativo, y recordamos que cada

$$G \xrightarrow{\chi} \mathbb{C}^\times$$

es un homomorfismo de grupos. Tenemos el caracter unidad

$$G \xrightarrow{1} \mathbb{C}^\times, \quad x \mapsto 1 \in \mathbb{C}^\times,$$

y vemos que $\widehat{G} \in \mathcal{G}_{f.ab.}$ es un grupo bajo la multiplicación de caracteres

$$\chi_1, \chi_2 \in \widehat{G} \mapsto \chi_1 \chi_2 \in \widehat{G},$$

$$\chi_1 \chi_2(g) = \chi_1(x) \chi_2(x), \quad \forall x \in G.$$

Ejercicio 2.1. *Demostrar que*

- (i) $\widehat{G} = \text{hom}(G, \mathbb{S}^1)$, en donde $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\} \in \mathcal{G}_{f.ab.}$, $\mathbb{S}^1 < \mathbb{C}^\times$.
- (ii) $\chi^{-1} = \bar{\chi} \in \widehat{G}$, en donde $\bar{\chi}$ está dado por

$$\bar{\chi}(x) = \overline{\chi(x)}, \quad \forall x \in G,$$

y denotamos $z \mapsto \bar{z}$ la conjugación en $\mathbb{C}$.

Lema 2.2. *Si $G \in \mathcal{G}$ es cíclico de orden n , entonces*

$$G \cong \mu_n.$$

Demostración. Tomemos $s \in G$ un generador, i.e.,

$$G = \langle s \rangle.$$

Dado $\chi \in \widehat{G}$, tenemos que $\chi(s) = w \in \mathbb{S}^1$, y además

$$\chi^n(s) = w^n = 1.$$

Por lo que $w \in \mu_n$.

Viceversa, si $w \in \mu_n$, entonces

$$\chi(s) = w$$

define un caracter $\chi \in \widehat{G}$. □

Definición 2.3. Dado $\chi \in \widehat{G}$, llamamos $\chi|_H \in \widehat{H}$ la restricción de χ a H . Decimos que un caracter $\chi \in \widehat{H}$ se extiende a uno de G , si existe un caracter $\chi' \in \widehat{G}$ tal que $\chi'|_H = \chi$.

Lema 2.4. Sea $H < G$, entonces todo caracter $\chi \in \widehat{H}$ se extiende a uno de $\widehat{G}$.

Demostración. Si $H = G$, el lema es válido. Supongamos que existe una $x \in G \setminus H$ y tomemos

$$H' = \langle H, x \rangle,$$

por lo que

$$H < H' < G,$$

en donde notamos que $H' \neq H$. Procedemos por inducción en $[G : H]$, el índice de H en G , el caso $[G : H] = 1$ ya cubierto.

Existe un n minimal tal que $x^n \in H$, y vemos que todo $h' \in H'$ es de la forma $h' = hx^a$. Para cada elección de $w \in \mu_n$, podemos definir

$$\chi'(h') = \chi(h)w^a \in \mathbb{S}^1.$$

Entonces podemos verificar que $\chi' \in \widehat{H'}$. Por inducción, χ' se extiende a un caracter de G . □

La operación

$$\chi \in \widehat{G} \mapsto \chi|_H \in \widehat{H}$$

nos da un homomorfismo sobre

$$\widehat{G} \xrightarrow{\rho} \widehat{H} \rightarrow 1$$

con kernel

$$\ker(\rho) = \{\chi \mid \chi|_H = 1\}.$$

Por medio del teorema del homomorfismo, y cocientes, obtenemos una sucesión exacta

$$1 \rightarrow \widehat{G/H} \rightarrow \widehat{G} \rightarrow \widehat{H} \rightarrow 1.$$

Proposición 2.5. Sean $G_1, G_2 \in \mathcal{G}_{\text{f.ab.}}$, entonces

$$\widehat{G_1 \times G_2} \cong \widehat{G_1} \times \widehat{G_2}$$

Demostración. Tenemos proyecciones

$$\begin{array}{ccc}
& \widehat{G_1 \times G_2} & \\
\rho_1 \swarrow & & \searrow \rho_2 \\
\widehat{G_1} & & \widehat{G_2}
\end{array}$$

obtenidas al restringir $\chi \in \widehat{G_1 \times G_2}$ a $G_1 \times 1 \cong G_1$ y a $1 \times G_2 \cong G_2$, respectivamente. Lo cual nos da

$$\begin{aligned}
\widehat{G_1 \times G_2} &\rightarrow \widehat{G_1} \times \widehat{G_2}, \\
\chi &\mapsto (\rho_1 \circ \chi, \rho_2 \circ \chi).
\end{aligned}$$

En dirección contraria, tenemos

$$\begin{aligned}
\widehat{G_1} \times \widehat{G_2} &\rightarrow \widehat{G_1 \times G_2}, \\
(\chi_1, \chi_2) &\mapsto [(x_1, x_2) \mapsto \chi_1(x_1)\chi_2(x_2)].
\end{aligned}$$

□

Proposición 2.6. *Para todo $G \in \mathcal{G}_{\text{f.ab.}}$, tenemos que*

$$\widehat{\widehat{G}} \cong G.$$

Demostración. Sabemos que

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_d\mathbb{Z}.$$

Por la proposición anterior

$$\widehat{G} \cong \widehat{\mathbb{Z}/n_1\mathbb{Z}} \times \cdots \times \widehat{\mathbb{Z}/n_d\mathbb{Z}}.$$

Por el Ejemplo 1.7, tenemos

$$\widehat{G} \cong \mu_{n_1} \times \cdots \times \mu_{n_d}$$

y aplicando el Lema 2.2, concluimos que esto último es

$$\cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_d\mathbb{Z} \cong G.$$

□

2.1. Doble dual. Tenemos un homomorfismo de grupos

$$\begin{aligned}
G &\xrightarrow{\varepsilon} \widehat{\widehat{G}} \\
x \in G &\mapsto [\chi \in \widehat{G} \mapsto \chi(x) \in \mathbb{C}^\times].
\end{aligned}$$

Ejercicio 2.7. *Verificar que, en efecto, ε es un homomorfismo de grupos.*

Proposición 2.8. *ε es un isomorfismo.*

Demostración. Observamos que $\widehat{G}$ y $\widehat{\widehat{G}}$ tienen la misma cardinalidad, por lo que es suficiente demostrar que es 1-1 para concluir que ε es una biyección.

Sea $x \in G$, $x \neq 1$. Si encontramos una $\chi \in \widehat{G}$, tal que

$$\varepsilon(x)(\chi) = \chi(x) \neq 1,$$

entonces podremos concluir que $\ker(\varepsilon) = 1$, lo cual implica 1-1.

Tomemos $H = \langle x \rangle$, el cual es un grupo cíclico, y sea n el orden de H . Para cada $w \in \mu_n$ (en particular, podemos tomar una $w \neq 1$), la relación

$$\chi(x) = w,$$

nos da un caracter en H . Por el Lema 2.4, χ se extiende a un caracter de G . $\square$

Proposición 2.9. *Sea $G \in \mathcal{G}_{f.ab.}$ y $n = \#G$. Entonces*

$$\sum_{x \in G} \chi(x) = \begin{cases} n & \text{si } \chi = \mathbf{1} \\ 0 & \text{si } \chi \neq \mathbf{1} \end{cases}.$$

Demostración. Podemos trasladar la suma por un elemento $x_0 \in G$:

$$\begin{aligned} \sum_{x \in G} \chi(x) &= \sum_{x \in G} \chi(xx_0) = \chi(x_0) \sum_{x \in G} \chi(x) \\ &\implies (1 - \chi(x_0)) \sum_{x \in G} \chi(x) = 0. \end{aligned}$$

Podemos concluir, pues si $\chi \neq 1$, entonces $\exists x_0$ tal que $\chi(x_0) \neq 1$. $\square$

Corolario 2.10. *Sea $G \in \mathcal{G}_{f.ab.}$ y $n = \#G$. Entonces*

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n & \text{si } x = 1 \\ 0 & \sim \end{cases}.$$

2.2. Dualidad en general. Comentamos que el isomorfismo con el doble dual

$$G \cong \hat{\hat{G}}$$

se puede extender a la categoría de grupos abelianos localmente compactos². En esta categoría, este resultado se llama la dualidad de Pontrjagin.

Ejemplo 2.11. *Los grupos $G = \mathbb{R}^n, (\mathbb{R}^\times)^n, \mathbb{C}^n, (\mathbb{C}^\times)^n$ son localmente compactos. Además, para cada primo p , tenemos una métrica p -ádica y el campo de números p -ádicos $\mathbb{Q}_p$.*

Si fijamos un caracter no trivial $\chi \in \hat{G}$, entonces podemos definir la transformada de Fourier

$$\mathcal{F}_\chi(f(x)) = \int_G f(y) \chi(xy) dy,$$

en un espacio adecuado de funciones (espacio de Schwarz), y tenemos inversión de Fourier

$$\mathcal{F}_{\bar{\chi}} \circ \mathcal{F}_\chi(f(x)) = f(x).$$

En el caso de $G = \mathbb{R}$, tenemos el caracter $\chi \in \hat{G}$ dado por $\chi(x) = \exp(x) = e^{2\pi i x}$, y obtenemos la transformada usual de Fourier

$$\mathcal{F}(f(x)) = \int_{\mathbb{R}} f(y) \exp(xy) dy.$$

Este enfoque lleva a muchas direcciones interesantes en la teoría de números moderna, como lo hacen la tesis de Tate [9] y el libro [4], por ejemplo.

3. NOCIONES DE FUNCIONES HOLOMORFAS

Fijamos $U \subset \mathbb{C}$, un conjunto abierto.

²Un grupo topológico es localmente compacto, si para todo elemento $x \in G$ y una vecindad V de x , existe una vecindad U de x con cerradura compacta contenida en V .

3.1. Diferenciación. Decimos que una función

$$f : U \rightarrow \mathbb{C}$$

es diferenciable en $z_0 \in U$ si una de las siguientes tres condiciones equivalentes se cumple:

- (i) $f(z) = f(z_0) + f'(z_0)(z - z_0) + O(z - z_0)$, $f'(z_0) \in \mathbb{C}$, cerca de z_0 ;
- (ii) existe $f'(z_0) = \lim_{z \rightarrow z_0} \frac{f(z) - f(z_0)}{z - z_0}$;
- (iii) si escribimos $z = x + iy$, $x = \Re(z)$, $y = \Im(z)$, tenemos $f(z) = u(x, y) + (iv)(x, y)$, en donde u y v son diferenciables en $\mathbb{R}^2$.

En particular, las funciones u y v de la condición (iii) satisfacen las ecuaciones de Cauchy-Riemann:

$$\begin{aligned} u_x(x, y) &= v_y(x, y) \\ u_y(x, y) &= -v_x(x, y) \end{aligned}$$

y además son funciones armónicas, i.e., si

$$\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$$

es el Laplaciano, entonces

$$\Delta u = \Delta v = 0.$$

3.2. Integración. Para $\gamma : [0, 1] \rightarrow U$, una curva suave, tenemos

$$\int_{\gamma} f(z) dz = \int_0^1 f(\gamma(t)) \gamma'(t) dt.$$

Ejemplo 3.1. Para $\gamma : [0, 1] \rightarrow \mathbb{S}^1$, $t \mapsto e^{2\pi it}$,

$$\int_{\gamma} \frac{dz}{|z|} = 2\pi i.$$

Cauchy-Goursat: Sea U simplemente conexo y $f(z)$ holomorfa en U (i.e. diferenciable para toda $z_0 \in U$). Si γ es una curva cerrada, entonces

$$\int_{\gamma} f(z) dz = 0.$$

$$\implies \int f \text{ es independiente de la trayectoria en } U.$$

Fórmula de Cauchy: Sea $f : U \rightarrow \mathbb{C}$ holomorfa y $\mathcal{D}$ un disco tal que $\overline{\mathcal{D}} \subset U$. Entonces

$$f(z_0) = \frac{1}{2\pi i} \int_{\partial \mathcal{D}} \frac{f(z)}{z - z_0} dz, \quad z_0 \in \mathcal{D}.$$

Además, $f'(z)$ es holomorfa en U , y tenemos

$$f^{(k)}(z_0) = \frac{k!}{2\pi i} \int_{\partial \mathcal{D}} \frac{f(z) dz}{(z - z_0)^{k+1}}, \quad z_0 \in \mathcal{D}.$$

Serie de Taylor: Para f holomorfa, tenemos

$$f(z) = \sum c_n (z - z_0)^n, \quad |z - z_0| \leq R,$$

en donde

$$c_n = \frac{1}{2\pi i} \int_{\partial \mathcal{D}} \frac{f(z) dz}{(z - z_0)^{n+1}}.$$

La serie converge *uniformemente* y absolutamente en $|z - z_0| \leq R$.

3.3. Convergencia uniforme. Una sucesión de funciones, $f_n : U \rightarrow \mathbb{C}$, converge uniformemente en $V \subset U$, a una función $f : V \rightarrow \mathbb{C}$, si

$$\forall \varepsilon > 0 \exists N \ni |f_n(z_1) - f(z_2)| < \varepsilon, \forall z_1, z_2 \in V, n \geq N.$$

Lema 3.2. Sea $f_n : U \rightarrow \mathbb{C}$ una sucesión de funciones holomorfas que converge uniformemente en cada conjunto compacto $K \subset U$ a una $f : U \rightarrow \mathbb{C}$. Entonces, f es holomorfa y $f'_n \rightarrow f'$ uniformemente en cada conjunto compacto $K \subset U$.

Demostración. Sea $\mathcal{D}$ un disco tal que $\overline{\mathcal{D}} \subset U$. Para toda $k \geq 0$, tenemos que

$$f_n^{(k)}(z_0) = \frac{k!}{2\pi i} \int_{\partial \mathcal{D}} \frac{f_n(z) dz}{(z - z_0)^{k+1}} \rightarrow \frac{k!}{2\pi i} \int_{\partial \mathcal{D}} \frac{f(z) dz}{(z - z_0)^{k+1}}$$

uniformemente en $\overline{\mathcal{D}}$, debido a la convergencia uniforme de $f_n \rightarrow f$ en $\overline{\mathcal{D}} \subset U$. En particular, para $k = 1$. $\square$

3.4. Radio de convergencia. Para series de potencias

$$f(z) = \sum a_n z^n,$$

existe una R , $0 \leq R \leq \infty$, con las siguientes propiedades:

- (i) La serie converge absolutamente $\forall z \in \mathbb{C}$ tal que $|z| < R$. Si $\mathcal{D}$ es un disco con radio ρ , $0 \leq \rho \leq R$, entonces la convergencia es uniforme en $\overline{\mathcal{D}}$.
- (ii) Si $|z| > R$, los términos de la serie no son acotados y la serie diverge.
- (iii) La función $f(z)$ es holomorfa para $|z| < R$, y su derivada se obtiene término a término. La serie correspondiente a $f'(z)$ tiene el mismo radio de convergencia.

Nota 3.3. La fórmula de Cauchy para derivadas

$$\implies \left| f^{(n)}(z_0) \right| \leq \frac{n! M}{R^n},$$

en donde

$$M = \max_{|z - z_0| = R} |f(z)|.$$

3.5. Unicidad para funciones analíticas. Sea U una región conexa de $\mathbb{C}$.

Teorema 3.4. Supongamos que f es analítica, i.e. holomorfa, en U . Entonces tenemos una de las dos siguientes posibilidades:

- (i) $f \equiv 0$ en U .
- (ii) El conjunto $\{z \in U \mid f(z) = 0\}$ es aislado en U (no contiene puntos de acumulación).

Corolario 3.5. Sean $f, g : U \rightarrow \mathbb{C}$ holomorfas. Si el conjunto $\{z \in U \mid f(z) = g(z)\}$ no es aislado, i.e. tiene puntos de acumulación, entonces

$$f \equiv g \text{ en } U.$$

Continuación analítica: Sean $U \subset V$ regiones conexas en $\mathbb{C}$ y sea $f : U \rightarrow \mathbb{C}$ una función holomorfa. Si existe una función $g : V \rightarrow \mathbb{C}$ tal que

$$g|_U \equiv f,$$

entonces g es única.

4. SERIES DE DIRICHLET

Sea $\{\lambda_n\}_{n \in \mathbb{Z}_{\geq 0}}$ una sucesión creciente ($\lambda_n < \lambda_{n+1}$) de números reales tales que $\lambda_n \rightarrow \infty$.

Definición 4.1. Una serie de Dirichlet con exponentes $\{\lambda_n\}$ es de la forma

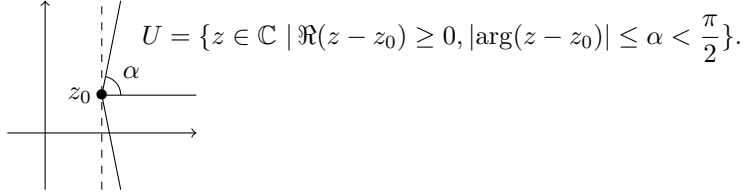
$$f(z) = \sum_{n \in \mathbb{N}} a_n e^{-\lambda_n z}, \quad a_n, z \in \mathbb{C}.$$

(Para fines de convergencia, podemos suponer que $\lambda_n \geq 0$).

Ejemplo 4.2.

- (i) $\lambda_n = n, t = e^{-t} \implies f(t) = \sum a_n t^n$ (Serie de potencias).
- (ii) $\lambda_n = \log n \implies f(s) = \sum \frac{a_n}{n^s}$ (Serie clásica de Dirichlet).

Proposición 4.3. Supongamos que $f(z) = \sum a_n e^{-\lambda_n z}$ converge para $z = z_0$. Entonces converge uniformemente en U^3 :



Demostración. Trasladando, de ser necesario, podemos suponer que $z_0 = 0$.

$$\implies \sum a_n \text{ converge.}$$

Entonces $\forall \varepsilon > 0 \exists N$ tal que

$$|A_{m,m'}| \leq \varepsilon, \quad \text{donde} \quad A_{m,m'} = \sum_{n=m}^{m'} a_n, \quad m' \geq m \geq N.$$

Sea $b_n = e^{-\lambda_n z}$. Para estudiar

$$f(z) = \sum a_n b_n$$

recordamos el siguiente lema de análisis matemático básico.

Lema 4.4 (Abel). Sean $\{a_n\}$ y $\{b_n\}$ sucesiones. Tomemos

$$A_{m,m'} = \sum_{n=m}^{m'} a_n, \quad S_{m,m'} = \sum_{n=m}^{m'} a_n b_n.$$

Entonces

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n} (b_n - b_{n+1}) + A_{m,m'} b_{m'}.$$

³Falta el valor absoluto para $\arg(z - z_0)$ en [7].

En nuestro contexto, el lema de Abel nos dice que

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n} (e^{-\lambda_n z} - e^{-\lambda_{n+1} z}) + A_{m,m'} e^{-\lambda_{m'} z}.$$

Escribimos $z = x + iy$, $x = \Re(z)$, $y = \Im(z)$.

• **Propuesta:**

$$|e^{-\lambda_n z} - e^{-\lambda_{n+1} z}| \leq \frac{|z|}{x} |e^{-\lambda_n x} - e^{-\lambda_{n+1} x}|.$$

Para ver esto, escribimos

$$e^{-\lambda_{n+1} z} - e^{-\lambda_n z} = z \int_{\lambda_n}^{\lambda_{n+1}} e^{-tz} dt.$$

Entonces

$$\begin{aligned} |e^{-\lambda_n z} - e^{-\lambda_{n+1} z}| &\leq |z| \int_{\lambda_n}^{\lambda_{n+1}} e^{-tx} dt \\ &= \frac{|z|}{x} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x}). \end{aligned}$$

Si escribimos z en forma polar, i.e., $z = |z| e^{i\theta}$, $\theta = \arg(z)$. Observamos que

$$\frac{|z|}{x} = \frac{|z|}{|z| \cos \theta} = \sec \theta \leq \sec \alpha, \quad 1 \leq \sec \alpha \leq \infty.$$

Entonces

$$\begin{aligned} |S_{m,m'}| &\leq \varepsilon \left(1 + \frac{|z|}{x} \sum_{n=m}^{m'-1} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x}) \right) \\ &\leq \varepsilon \left(1 + \sec \alpha \sum_{n=m}^{m'-1} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x}) \right) \leq \varepsilon (1 + \sec \alpha). \end{aligned}$$

Lo cual nos da convergencia uniforme en $U \setminus \{0\}$. $\square$

Ejercicio 4.5. Completar la demostración anterior sobre la convergencia uniforme en U , incluyendo $x = 0^4$. ¿Se requiere convergencia absoluta en $x = 0$?

4.1. Consecuencias. Supongamos que $f(z) = \sum a_n e^{-\lambda_n z}$ converge en $z_0 \in \mathbb{C}$. Entonces

- (i) $f(z)$ es holomorfa para $\Re(z) > \Re(z_0)$.
- (ii) La serie converge en un medio plano abierto $\Re(z) > \rho \neq \infty$ maximal, llamado el medio plano de convergencia.
- (iii) En la región

$$U = \{z \mid \Re(z - z_0) \geq 0, |\arg(z - z_0)| \leq \alpha < \frac{\pi}{2}\}$$

tenemos que $f(z)$ es uniformemente continua.

- (iv) $f(z) = 0 \iff a_n = 0 \forall n \in \mathbb{N}$.

⁴Caso omitido en [7].

Demostración de (iv). Supongamos que

$$f(z) = \sum a_n e^{-\lambda_n z} = 0.$$

Entonces

$$f(z)e^{\lambda_0 z} = a_0 + \sum_{n \in \mathbb{Z}_{>0}} a_n e^{-(\lambda_n - \lambda_0)z}.$$

Tomemos $z \rightarrow \infty$ por el eje real positivo. Con un argumento de uniformidad en U , y porque $\{\lambda_n\}$ es estrictamente monótona, tenemos que

$$\sum_{n \in \mathbb{Z}_{>0}} a_n e^{-(\lambda_n - \lambda_0)z} = e^{-(\lambda_1 - \lambda_0)z} \sum_{n \in \mathbb{Z}_{>0}} a_n e^{-(\lambda_n - \lambda_1)z} \rightarrow 0.$$

Entonces $f(z) \rightarrow a_0$, si $z \rightarrow +\infty$. $\therefore a_0 = 0$.

Procedemos inductivamente para demostrar que $a_n = 0$, tomando $e^{\lambda_n z} f(z)$ en cada paso. $\square$

5. SOBRE LA FUNCIÓN ZETA DE RIEMANN

5.1. Transformadas integrales y funciones especiales. Una transformada que encontramos pronto en el estudio de las matemáticas es la transformada de Laplace:

$$f(t) \xrightarrow{\mathcal{L}} F(s)$$

$$\mathcal{L}\{f(t)\} = \int_0^\infty f(t) e^{-st} dt.$$

De importancia en la teoría de números es la transformada de Mellin:

$$f(t) \xrightarrow{\mathcal{M}} \int_{\mathbb{R}_{>0}} f(t) t^s \frac{dt}{t},$$

en donde podemos obtener la función Gamma de Euler

$$\Gamma(s) = \mathcal{M}\{e^{-t}\}.$$

Recordar que

$$\Gamma(s+1) = s\Gamma(s),$$

$$\Gamma(n+1) = n!.$$

5.2. Análisis de Fourier. Podemos integrar sobre un grupo topológico localmente compacto G . Por ejemplo:

- (i) $G = \mathbb{R}$, grupo aditivo, en donde tenemos la integral usual

$$\int_{\mathbb{R}} f(t) dt = \int_{-\infty}^{\infty} f(t) dt.$$

La cual es invariante ante traslación $x \mapsto x + x_0$, $x_0 \in \mathbb{R}$.

- (ii) $G = \mathbb{R}_{>0}$, los reales positivos bajo la multiplicación, en donde tenemos la integral

$$\int_{\mathbb{R}_{>0}} f(t) dt = \int_0^\infty f(t) \frac{dt}{t}.$$

La cual es invariante ante traslación multiplicativa $x \mapsto xx_0$, $x_0 \in \mathbb{R}_{>0}$, además de inversión $x \mapsto x^{-1}$.

Fijemos $G = \mathbb{R}$. La transformada de Fourier se define por medio de un caracter aditivo $\psi : \mathbb{R} \rightarrow \mathbb{S}^1$ en el espacio de Schwarz⁵:

$$\mathcal{S}(\mathbb{R}) \xrightarrow{\mathcal{F}_\psi} \mathcal{S}(\mathbb{R})$$

$$\mathcal{F}_\psi\{f(t)\} = \hat{f}(u) = \int_{\mathbb{R}} f(t)\psi(ut) dt.$$

En particular, fijamos

$$\psi, \bar{\psi} : \mathbb{R} \rightarrow \mathbb{S}^1, \quad \psi(x) = e^{2\pi i x}, \quad \bar{\psi}(x) = e^{-2\pi i x}.$$

Teorema 5.1 (Inversión de Fourier).

$$\mathcal{F}_{\bar{\psi}} \circ \mathcal{F}_\psi\{f(t)\} = f(t).$$

Ejemplo 5.2. Calcular la transformada de Fourier para $f(t) = e^{-\pi t^2 x}$ para $x > 0$.

$$\begin{aligned} \hat{f}(u) &= \int_{\mathbb{R}} e^{-\pi t^2 x - 2\pi i u t} dt = e^{\pi u/x} \int_{\mathbb{R}} e^{\pi x(t + \frac{i u}{x})^2} dt \\ &= e^{\pi u/x} \int_{\mathbb{R}} e^{\pi x t^2} dt = x^{-1/2} e^{-\pi u^2/x} = x^{-1/2} f(u/x). \end{aligned}$$

Teorema 5.3 (Fórmula de Poisson). Si $f \in \mathcal{S}(\mathbb{R})$, entonces

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \hat{f}(n).$$

Ejemplo 5.4. La función

$$\theta(x) = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 x},$$

satisface

$$\theta(x) = x^{-\frac{1}{2}} \theta(x^{-1}).$$

Ejercicio 5.5. Verificar la siguiente observación de Riemann [5]:

$$(5.1) \quad \frac{\pi^{-s/2} \Gamma(s/2)}{n^s} = \int_{\mathbb{R}_{>0}} e^{-\pi n^2 t} t^{s/2} \frac{dt}{t}, \quad n \in \mathbb{N} \setminus \{0\}.$$

5.3. Ecuación Funcional.

Teorema 5.6 (Riemann 1859). Sea $L(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s)$. Entonces

$$L(s) = L(1-s).$$

Demostración. Por la observación (5.1), tenemos

$$\pi^{-s/2} \Gamma(s/2) \sum_{n=1}^{\infty} \frac{1}{n^s} = \int_{\mathbb{R}_{>0}} \sum_{n=1}^{\infty} e^{-\pi n^2 t} t^{s/2} \frac{dt}{t}.$$

Si tomamos

$$\omega(x) = \sum_{n=1}^{\infty} e^{-\pi n^2 x},$$

entonces $\theta(x) = 1 + 2\omega(x)$, y podemos utilizar la fórmula de Poisson, Ejemplo 5.4, para obtener

$$\omega(x^{-1}) = x^{\frac{1}{2}} \omega(x) + \frac{1}{2} \left(x^{\frac{1}{2}} - 1 \right).$$

⁵ $\mathcal{S}(\mathbb{R})$ consiste de funciones analíticas $f(t)$ tales que $|f(t)| \rightarrow 0$ rápidamente, cuando $t \rightarrow \pm\infty$.

Entonces, para $\Re(s) > 1$, tenemos

$$\begin{aligned} L(s) &= \pi^{-s/2} \Gamma(s/2) \zeta(s) = \int_0^\infty \omega(x) x^{s/2} \frac{dx}{x} \\ &= \int_0^1 \omega(x) x^{s/2} \frac{dx}{x} + \int_1^\infty \omega(x) x^{s/2} \frac{dx}{x}. \end{aligned}$$

Utilizando la fórmula para $\omega(x^{-1})$ y haciendo el cambio de variable $x \mapsto x^{-1}$, podemos ver que

$$\int_0^1 \omega(x) x^{s/2} \frac{dx}{x} = \int_1^\infty \left(x^{\frac{1}{2}} \omega(x) + \frac{1}{2} (x^{\frac{1}{2}} - 1) \right) x^{-\frac{s}{2}} \frac{dx}{x}.$$

Entonces

$$L(s) = \int_1^\infty \omega(x) \left(x^{\frac{1-s}{2}} + x^{\frac{s}{2}} \right) \frac{dx}{x} + \frac{1}{2} \int_1^\infty t \left(x^{\frac{1-s}{2}} - x^{-\frac{s}{2}} \right) \frac{dx}{x}.$$

Ahora, es un ejercicio fácil mostrar que

$$\frac{1}{2} \int_1^\infty t \left(x^{\frac{1-s}{2}} - x^{-\frac{s}{2}} \right) \frac{dx}{x} = \frac{1}{s(s-1)}.$$

Por lo tanto

$$L(s) = \int_1^\infty \omega(x) \left(x^{\frac{1-s}{2}} + x^{\frac{s}{2}} \right) \frac{dx}{x} + \frac{1}{s(s-1)}.$$

Esta última fórmula es simétrica bajo $s \mapsto 1-s$. $\square$

Observación 5.7. Formalmente $L(s) = L(1-s)$ nos ayuda a extender la función $\zeta(s)$, originalmente definida en $\Re(s) > 1$, para también incluir $\Re(s) < 0$. Sin embargo, no obtenemos con este razonamiento unicidad en la función meromorfa resultante. Necesitamos más información sobre el comportamiento de $\zeta(s)$ en la franja crítica $0 < \Re(s) < 1$.

5.4. Continuación Analítica.

Teorema 5.8. La función $\zeta(s) = \sum_{n=1}^\infty \frac{1}{n^s}$, satisface:

- (i) $\zeta(s)$ es holomorfa y diferente de cero para $\Re(s) > 1$.
- (ii) $\zeta(s) = \frac{1}{s-1} + \varphi(s)$, en donde $\varphi(s)$ es holomorfa para $\Re(s) > 0$.

Demostración. Para la parte (i), de Análisis Matemático básico, sabemos sobre la convergencia de

$$\sum_{n=1}^\infty \frac{1}{n^x}, \text{ para } x > 0,$$

y observamos que $e^{iy} \in \mathbb{S}^1$.

Para la parte (ii), observamos que

$$\frac{1}{1-s} = \int_1^\infty t^{-s} dt = \sum_{n=1}^\infty \int_n^{n+1} t^{-s} dt, \quad \Re(s) > 0.$$

Escribimos

$$\begin{aligned}\zeta(s) &= \frac{1}{1-s} + \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \int_n^{n+1} t^{-s} dt \right) dt \\ &= \frac{1}{1-s} + \sum_{n=1}^{\infty} \varphi_n(s).\end{aligned}$$

Cada función $\varphi_n(s)$ está bien definida y es holomorfa en $\Re(s) > 0$, y queremos la convergencia uniforme de

$$\varphi(s) = \sum \varphi_n(s).$$

Sea $\varepsilon > 0$. Tenemos

$$|\varphi_n(s)| \leq \sup_{n \leq t \leq n+1} |n^{-s} - t^{-s}| < \infty \quad \text{y} \quad \frac{d}{dt} (n^{-s} - t^{-s}) = st^{-(s+1)}.$$

$$\implies |\varphi_n(s)| \leq \frac{|s|}{n^{x+1}}, \quad x = \Re(s).$$

Finalmente, en todo compacto K dentro de $U = \{s \in \mathbb{C} \mid \Re(s) > 0\}$, la función $|s|$ es acotada. Además, la serie

$$\sum \frac{1}{n^{x+1}}$$

converge absolutamente para toda $x \geq \varepsilon > 0$.

$$\therefore \varphi(s) = \sum \varphi_n(s)$$

converge uniformemente en todo compacto $K \subset U$. □

6. PRODUCTOS INFINITOS Y FUNCIONES L

6.1. Productos infinitos. Sea $\{l_n\}_{n \in \mathbb{N}}$ una sucesión de números complejos, todos diferentes de 0. Decimos que

$$\prod_{n=1}^{\infty} l_n$$

converge si existe una $L \in \mathbb{C} \setminus \{0\}$, tal que

$$\lim_{N \rightarrow \infty} \prod_{n=1}^N l_n = L.$$

Observación 6.1. Así como para series tenemos

$$\sum b_n \text{ converge} \implies b_n \rightarrow 0, \text{ cuando } n \rightarrow \infty,$$

para productos infinitos tenemos

$$\prod l_n \text{ converge} \implies l_n \rightarrow 1, \text{ cuando } n \rightarrow \infty.$$

En la región $\{z \in \mathbb{C} \mid z = |z|e^{i\theta}, -\pi < \theta \leq \pi\}$, tenemos la rama principal de la función logaritmo, que denotamos por $\log$. Para $|z| < 1$, tenemos la identidad

$$(6.1) \quad \log(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3!} - \dots$$

Escribamos $l_n = 1 + a_n$. Para N_0 suficientemente grande, la sucesión $\{a_n\}_{n \geq N_0}$ cae dentro del disco $\mathcal{D} = \{z \in \mathbb{C} \mid |z - 1| < 1\}$. Tomando logaritmo en $\mathcal{D}$, vemos entonces que

$$\prod_{n=1}^{\infty} l_n \text{ converge} \iff \sum_{n \geq N_0} \log l_n \text{ converge},$$

para N_0 suficientemente grande. Ahora, definimos convergencia absoluta para el producto por medio de la suma de la derecha, i.e.,

$$\prod_{n=1}^{\infty} l_n \text{ converge absolutamente} \iff \sum_{n \geq N_0} \log l_n \text{ converge absolutamente}.$$

Notamos que el concepto de convergencia no depende de un número finito de términos que podemos remover tanto el el producto como en la suma.

Proposición 6.2.

$$\prod_{n=1}^{\infty} l_n \text{ converge absolutamente} \iff \sum_{n \geq N_0} a_n \text{ converge absolutamente},$$

para alguna N_0 tal que $a_n \in \mathcal{D}$, $\forall n \geq N_0$.

Demostración. En $\mathcal{D} = \{z \in \mathbb{C} \mid |z - 1| < 1\}$, tenemos que

$$\lim_{z \rightarrow 0} \frac{\log(1+z)}{z} = 1 \implies \forall \varepsilon > 0 \exists N_0 \ni$$

$$(1 - \varepsilon)|a_n| < \log(1 + a_n) < (1 + \varepsilon)|a_n| \quad \forall n \geq N_0.$$

$$\therefore \sum_{n=N_1}^{\infty} |a_n| \text{ converge} \iff \sum |\log(1 + a_n)| \text{ converge}.$$

□

Ejercicio 6.3. *El producto*

$$G(z) = \prod_{n=1}^{\infty} \left(1 + \frac{z}{n}\right) e^{-z/n}$$

converge absolutamente y uniformemente para toda K subconjunto compacto.

De hecho

$$\Gamma(s) = \frac{e^{-\gamma z}}{z} \prod_{n=1}^{\infty} \left(1 + \frac{z}{n}\right) e^{z/n}$$

es la función gamma, y

$$\gamma = \lim_{n \rightarrow \infty} \left(\left(1 + \frac{1}{2} + \frac{1}{3} + \dots\right) - \log n \right).$$

6.2. Producto Euleriano. Sea $\mathcal{P}$ el conjunto de todos los primos. La propiedad de factorización única de los números enteros, y la definición de convergencia para productos infinitos, nos conduce a

$$(6.2) \quad \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \left(\frac{1}{1 - p^{-s}} \right),$$

inicialmente en la región $\Re(s) > 1$.

6.3. Comportamiento cuando $s \rightarrow 1$.

Proposición 6.4. *La serie⁶*

$$\psi(s) = \sum_{p \in \mathcal{P}} \sum_{k=2}^{\infty} \frac{1}{kp^{ks}},$$

define una función holomorfa en $\Re(s) > 1/2$ y permanece acotada cuando $s \rightarrow 1$. La función

$$f(s) = \sum_{p \in \mathcal{P}} p^{-s},$$

inicialmente definida para $\Re(s) > 1$, satisface

$$f(s) + \psi(s) = \log \zeta(s)$$

y tiene continuación meromorfa a $\Re(s) > 1/2$. Cerca de $s = 1$, tenemos

$$\sum_{p \in \mathcal{P}} \frac{1}{p^s} \sim \log \left(\frac{1}{s-1} \right).$$

Demostración. Utilizando el producto euleriano (6.2) para $\zeta(s)$ y la identidad (6.1) para el logaritmo, obtenemos

$$\log \zeta(s) = \sum_{p \in \mathcal{P}} \log(1 - p^{-s})^{-1} = \sum_{p \in \mathcal{P}} \sum_{k \geq 1} \frac{1}{kp^{ks}} = \psi(s) + \sum_{p \in \mathcal{P}} p^{-s}.$$

Esta identidad es válida en $\Re(s) > 1$. Ahora, la función $\psi(s)$, inicialmente definida en $\Re(s) > 1$, satisface

$$|\psi(s)| \leq \sum_{p \in \mathcal{P}} \sum_{k \geq 2} \left| \frac{1}{kp^{ks}} \right| \leq \sum_{p \in \mathcal{P}} \sum_{k \geq 2} \left| \frac{1}{p^{ks}} \right| = \sum_{p \in \mathcal{P}} \left| \frac{1}{p^s(p^s - 1)} \right|.$$

Si escribimos $s = x + iy$, esta última suma es igual a

$$\sum_{p \in \mathcal{P}} \frac{1}{p^x(p^x - 1)} \leq \sum_{n=2}^{\infty} \frac{1}{n^x(n^x - 1)},$$

en donde tenemos convergencia absoluta para $x > 1/2$. Por esto, vemos que la función $\psi(s)$ definida por la serie doble en la proposición, es holomorfa para $\Re(s) > 1/2$. Esto sucede cerca de $s = 1$ y obtenemos el resto de la proposición por medio del Teorema 5.8. $\square$

6.4. Caracteres de Dirichlet. Para simplificar, dado un número entero $m \geq 1$, escribimos⁷

$$Z_m = \mathbb{Z}/m\mathbb{Z}.$$

Un caracter de Dirichlet

$$Z_m^\times \xrightarrow{\chi} \mathbb{S}^1,$$

se extiende a toda $n \in \mathbb{Z}$, primeramente proyectando $\pmod m$

$$\mathbb{Z} \rightarrow Z_m,$$

⁶En [7], $s \rightarrow 1$ por la derecha. En estas notas, hacemos un ajuste para entender el comportamiento en una vecindad de $s = 1$ en $\mathbb{C}$.

⁷No escribimos $\mathbb{Z}_m$, dado que en el caso de un primo p , en teoría analítica de números moderna denotamos por $\mathbb{Z}_p$ a los enteros p -ádicos.

y en Z_m tomamos

$$\xi(n) = 0 \text{ si } (n, m) \neq 1.$$

6.5. Funciones de Dirichlet. Dado un caracter $\chi \in \widehat{Z}_m$, tenemos su función ζ dada por

$$\zeta_\chi(s) = \sum \frac{\chi(n)}{n^s} = \prod \frac{1}{1 - \chi(p)p^{-s}},$$

inicialmente definida para $\Re(s) > 1$, lo cual se demuestra de manera similar que para $\zeta(s)$.

7. DENSIDAD Y PROGRESIÓN ARITMÉTICA

Demostramos la vez anterior que

$$\sum_{p \in \mathcal{P}} \frac{1}{p^s} \sim \log \left(\frac{1}{s-1} \right)$$

cerca de $s = 1$.

Definición 7.1. Sea $\mathcal{A} \subset \mathcal{P}$, definimos la densidad del conjunto de números primos $\mathcal{A}$, $\text{dens}(\mathcal{A})$, $0 \leq \text{dens}(\mathcal{A}) \leq 1$, por medio de

$$\text{dens}(\mathcal{A}) = \lim_{s \rightarrow 1} \frac{\sum_{p \in \mathcal{A}} \frac{1}{p^s}}{\log \left(\frac{1}{s-1} \right)}.$$

Teorema 7.2 (Progresión Aritmética). Sean $a, m \in \mathbb{N} \setminus \{0\}$, $(a, m) = 1$ y sea

$$\mathcal{P}_a = \{p \mid p \equiv a \pmod{m}\}.$$

Entonces

$$\text{dens}(\mathcal{P}_a) = \frac{1}{\phi(m)}.$$

Corolario 7.3. $\mathcal{P}_a$ es un conjunto infinito.

Demostraremos el teorema con ayuda de las funciones L de Dirichlet.

7.1. Funciones de Dirichlet y funciones relacionadas. fijemos un caracter de Dirichlet $\chi \in \widehat{Z}_m$, el cual extendeos a $\mathbb{Z}$ como lo hicimos la vez anterior. Tenemos

$$\zeta_\chi(s) = \sum \frac{\chi(n)}{n^s} = \prod \frac{1}{1 - \chi(p)p^{-s}},$$

inicialmente definida para $\Re(s) > 1$. Observamos que cada término

$$\left| \frac{\chi(p)}{p^s} \right| < 1 \implies \log \frac{1}{1 - \chi(p)p^{-s}} = \sum_n \frac{\chi^n(p)}{np^{ns}}.$$

Obtenemos

$$(7.1) \quad \log \zeta_\chi(s) = \sum_{n,p} \frac{\chi^n(p)}{np^{ns}}.$$

Lema 7.4. *La función auxiliar*

$$f_\chi(s) = \sum_{p \nmid m} \frac{\chi(p)}{p^{-s}},$$

cuenta con el siguiente comportamiento:

- (i) Si $\chi = \mathbf{1}$ entonces $f_\chi \sim \log \left(\frac{1}{s-1} \right)$, cerca de $s = 1$.
- (ii) Si $\chi \neq \mathbf{1}$ entonces $f_\chi(s)$ permanece acotada cuando $s \rightarrow 1$.

Demostración. Escribimos

$$\log \zeta_\chi(s) = f_\chi(s) + \Psi_\chi(s),$$

en donde

$$\Psi_\chi(s) = \sum_{p \in \mathcal{P}} \sum_{n=2}^{\infty} \frac{\chi^n(p)}{np^{ns}}.$$

Al igual que la función $\psi(s)$ de la Proposición 6.4, la función $\Psi_\chi(s)$ converge absolutamente en $\Re(s) > 1/2$.

Ahora, la convergencia de (7.1), nos implica la convergencia de f_χ , sin embargo, inicialmente esto es válido para $\Re(s) > 1$. Si demostramos que para $\chi \neq \mathbf{1}$, $\zeta_\chi(s)$ converge para $\Re(s) > 0$, entonces $f_\chi(s)$ permanece acotada cerca de $s = 1$. Por lo tanto, con la siguiente proposición completamos la demostración del lema. $\square$

Proposición 7.5. *Sea $\chi \in \widehat{Z}_m$, diferente de $\mathbf{1}$. Entonces*

- (i) *Las sumas $A_{l,l'} = \sum_{n=l}^{l'} \chi(n)$ permanecen acotadas.*
- (ii) *La función $\zeta_\chi(s)$ converge para $\Re(s) > 0$.*

Demostración. (i) Por medio del algoritmo de la división de Euclides, escribimos

$$l' = l + mk + r, \quad 0 \leq r < m.$$

Y tenemos que

$$A_{l,l'} = \sum_{n=l}^{l+mk} \chi(n) + \sum_{n=l+mk+1}^{l'} \chi(n) \implies |A_{l,l'}| \leq k \left| \sum_{n \in Z_m} \chi(n) \right| + r.$$

Ahora, por la relación de ortonormalidad de caracteres, Proposición 2.9, entonces

$$\sum_{n \in \mathbb{Z}_m} \chi(n) = 0, \quad \text{si } \chi \neq \mathbf{1}.$$

Por lo tanto

$$|A_{l,l'}| \leq r \leq m-1.$$

(ii) Por el Lema de Abel, Lema 4.4,

$$|S_{k,k'}| \leq \phi(m) \left(\sum_{n=k}^{k'-1} \left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| + \left| \frac{1}{k'^s} \right| \right).$$

Por los resultados del plano de convergencia, podemos suponer que $s = x \in \mathbb{R}_{>0}$. Entonces la suma anterior se vuelve telescópica y hay cancelación, por lo que

$$|S_{k,k'}| \leq \phi(m) \frac{1}{k^s}.$$

$\square$

7.2. Progresión Aritmética – Demostración. Sea

$$g_a(s) = \sum_{p \in \mathcal{P}_a} \frac{1}{p^s}.$$

Lema 7.6.

$$g_a(s) = \frac{1}{\phi(m)} \sum_{\chi \in \hat{Z}_m} \chi^{-1}(a) f_\chi(s)$$

Demostración. Podemos expandir la suma de la derecha

$$\sum_{\chi \in \hat{Z}_m} \chi(a)^{-1} f_\chi(s) = \sum_{p \nmid m} \sum_{\chi \in \hat{Z}_m} \frac{\chi(a)^{-1} \chi(p)}{p^s}.$$

Ahora, por la relación de ortogonalidad, Proposición 2.9,

$$\sum_{\chi \in \hat{Z}_m} \chi(a^{-1}p) = \begin{cases} \phi(m) & \text{si } p \equiv a \pmod{m} \\ 0 & \text{~} \end{cases}.$$

□

Para demostrar el Teorema de Progresión Aritmética, de los Lemas 7.4 y 7.6 concluimos que

$$g_a(s) \sim \frac{1}{\phi(m)} \log \left(\frac{1}{s-1} \right).$$

Y por definición

$$\text{dens}(\mathcal{P}_a) = \frac{1}{\phi(m)}.$$

8. DE GRUPOS A CAMPOS Y RECIPROCIDAD CUADRÁTICA

Comenzamos nuestro estudio con el grupo cíclico $\mathbb{Z}/m\mathbb{Z}$, bajo la adición, y su grupo de unidades $(\mathbb{Z}/m\mathbb{Z})^\times$, bajo la multiplicación. En el caso de $m = p$, un número primo, una mejor notación es

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z},$$

la cual es estándar para campos finitos. Recordamos que

$$\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$$

es un grupo cíclico bajo la multiplicación con $\phi(p) = p-1$ elementos. Una propiedad de este campo, para $p \neq 2$, es que

$$\mathbb{F}_p^\times / (F_p^\times)^2 = \{\pm 1\}.$$

Recordemos rápidamente algunas nociones básicas de campos.

Definición 8.1. Decimos que un conjunto K es un campo si tiene al menos dos elementos $0 \in K$ y $1 \in K^\times = K \setminus \{0\}$, junto con dos operaciones

$$+ : K \times K \rightarrow K, \quad \cdot : K^\times \times K^\times \rightarrow K^\times,$$

que satisfacen

- (i) $(K, +) \in \mathcal{G}_{\text{ab.}}$
- (ii) $(K^\times, \cdot) \in \mathcal{G}_{\text{ab.}}$
- (iii) $x(y+z) = xy + xz, \forall x, y, z \in K.$

Denotamos por $\mathcal{K}$ a la categoría cuyos objetos son campos⁸. Sus flechas son homomorfismos de campos

$$K, L \in \mathcal{K}, \quad K \xrightarrow{f} L,$$

i.e., $f \in \text{hom}(K, L)$ nos da un homomorfismo aditivo en $\mathcal{G}_{ab}$. y $f|_{K^\times} \in \text{hom}(K^\times, L^\times)$ uno multiplicativo en $\mathcal{G}_{ab}$. Denotamos el conjunto de todas las flechas de K a L en $\mathcal{K}$, por $\text{hom}(K, L)$, y esperamos que no haya confusión con la notación con respecto al grupo aditivo.

8.1. Símbolo de Legendre. Sea p un primo diferente de 2. Para cada $x \in \mathbb{F}_p^\times$, tenemos que $x^{p-1} = 1$, y observamos que

$$x^{\frac{p-1}{2}} = \pm 1 \quad \text{en} \quad \mathbb{F}_p^\times.$$

Tenemos el isomorfismo de grupos

$$\{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z},$$

en donde además podemos identificar

$$\{\{\pm 1\} \text{ en } \mathbb{F}_p^\times\} \cong \{\{\pm 1\} \text{ en } \mathbb{C}^\times\}.$$

De hecho, solamente existe un grupo de orden 2, hasta isomorfismo.

Ejercicio 8.2. *Hasta isomorfismo en la categoría correspondiente:*

- (i) *Existe solamente un campo de orden 2.*
- (ii) *Existen dos grupos de orden 4. Uno es un campo y el otro no.*

Definición 8.3. *Dado un primo $p \neq 2$, tenemos un homomorfismo de grupos*

$$\begin{aligned} \mathbb{F}_p^\times &\rightarrow \{\pm 1\}, \\ x &\mapsto \left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}. \end{aligned}$$

Decimos que $\left(\frac{x}{p}\right)$ es el símbolo de Legendre.

Tenemos también un caracter

$$(\mathbb{Z}/4\mathbb{Z})^\times \xrightarrow{\varepsilon} \mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\},$$

definido para $x = 2y + 1$ impar:

$$\varepsilon(x) \equiv y \pmod{2} \equiv \begin{cases} 0 & \text{si } x \equiv 1 \pmod{4} \\ 1 & \text{si } x \equiv 3 \pmod{4} \end{cases}.$$

Extendemos a todo $\mathbb{Z}$, como lo hicimos en la sección anterior, en donde $\varepsilon(x) = 0$ si x es par.

⁸En alemán “Körper”, o del francés “corps”, en contraste con el inglés “fields”.

8.2. Ley de Reciprocidad Cuadrática y aplicaciones. Sean $l, p \neq 2$, números primos. Gauß demostró, temprano en su vida, la siguiente importante ley de reciprocidad:

$$\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right) (-1)^{\varepsilon(p)\varepsilon(l)}.$$

Proposición 8.4. Sea $a \in \mathbb{N} \setminus \{0, 2\}$, libre de cuadrados, y sea $m = 4a$. Existe un caracter

$$Z_m \xrightarrow{\chi_a} \mathbb{S}^1,$$

único con la propiedad

$$(8.1) \quad \chi_a(p) = \left(\frac{a}{p}\right), \quad \forall p \in \mathcal{P}, p \nmid m.$$

Además $\chi_a^2 = \mathbb{1}$ y

$$a \neq 1 \implies \chi_a \neq \mathbb{1}.$$

Demostración. Para mostrar unicidad, vemos que todo entero con $(x, m) = 1$, tiene factorización

$$x = \pm p_1^{e_1} \cdots p_d^{e_d}, \quad p_i \nmid m.$$

Si χ_a satisface (8.4), entonces

$$\chi_a(x) = \chi_a(\pm 1) \chi_a(p_1)^{e_1} \cdots \chi_a(p_d)^{e_d}.$$

Además, de la definición del símbolo de Legendre, esto nos da $\chi_a^2 = \mathbb{1}$.

Tenemos que a cuenta con factorización libre de cuadrados

$$a = \pm l_1 \cdots l_k.$$

Definimos

$$\chi_a(x) = (-1)^{\varepsilon(x)\varepsilon(a)} \prod_i \left(\frac{x}{l_i}\right).$$

Por reciprocidad cuadrática

$$\chi_a(p) = \prod_i \left(\frac{l_i}{p}\right).$$

Supongamos que $a \neq 1$, nos queda por demostrar que χ_a es no trivial. Tomemos x tal que

$$\left(\frac{x}{l_1}\right) = -1, \quad x \equiv 1 \pmod{4l_2 \cdots l_k}.$$

Entonces

$$\chi_a(x) = -1 \implies \chi_a \neq \mathbb{1}.$$

□

Proposición 8.5. Sea $a \in \mathbb{N} \setminus \{0, 2\}$, libre de cuadrados, $m = 4a$ y

$$\mathcal{P}_a = \{p \in \mathcal{P} \mid \left(\frac{a}{p}\right) = 1\}.$$

Entonces $\text{dens}(\mathcal{P}_a) = 1/2$.

Demostración. Tenemos un caracter de Dirichlet $\chi_a \in \widehat{Z}_m$, $\chi_a \neq 1$, con las propiedades de la proposición anterior. Vemos que

$$\left(\frac{a}{p}\right) = 1 \iff p \in \ker \chi_a.$$

Como argumentamos para progresión aritmética, tenemos que

$$\text{dens}(\mathcal{P}_a) = \frac{1}{[Z_m : \ker \chi_a]} = 1/2.$$

□

8.3. Reciprocidad cuadrática – demostración. Fijamos primos $\ell, p \neq 2$. Sea

$$S_p = \left\{1, \dots, \frac{p-1}{2}\right\} \text{ dentro de } \mathbb{F}_p^\times,$$

y observamos que $\mathbb{F}_p^\times = S_p \cup (-S_p)$, unión disjunta.

Para cada $s \in S_p$ y $a \in \mathbb{F}_p^\times$, $\exists e_s(a) = \{\pm 1\}$, $s_a \in S_p$ únicos con la propiedad

$$as = e_s(a)s_a.$$

Observación 8.6. *El mapeo*

$$S_p \rightarrow S_p, s \mapsto s_a$$

es una biyección.

Demostración. Supongamos que tenemos $s \neq s'$ en S_p , pero $s_a = s'_a$. Entonces

$$\begin{aligned} as &= e_s(a)s_a \neq e_{s'}(a)s'_a = as' \\ \implies e_s(a) &= -e_{s'}(a) \implies s = -s'. \end{aligned}$$

Esto último es una contradicción, pues S_p y $-S_p$ son disjuntos. □

Lema 8.7 (Gauß).

$$\left(\frac{a}{p}\right) = \prod_{s \in S_p} e_s(a).$$

Proof.

$$\begin{aligned} a^{\frac{p-1}{2}} \prod_{s \in S_p} s &= \prod_{s \in S_p} e_s(a) \prod_{s \in S_p} s_a = \prod_{s \in S_p} e_s(a) \prod_{s \in S_p} s. \\ \implies a^{\frac{p-1}{2}} &= \prod_{s \in S_p} e_s(a). \end{aligned}$$

□

Ejercicio 8.8. *Sea $m = 2n + 1$ un entero impar, entonces*

$$\frac{\sin mx}{\sin x} = (-4)^n \prod_{1 \leq j \leq n} \left(\sin^2 x - \sin^2 \left(\frac{2\pi j}{2n+1} \right) \right).$$

(Para una pista para este ejercicio, ver el libro de Serre.)

Ahora, combinamos el lema de Gauß con el ejercicio.

$$\sin\left(\frac{2\pi}{p}\ell s\right) = \sin\left(\frac{2\pi}{p}e_s(\ell)s_\ell\right) = e_s(\ell)\sin\left(\frac{2\pi}{p}s_\ell\right)$$

Entonces

$$\begin{aligned}\left(\frac{\ell}{p}\right) &= \prod_{s \in S_p} e_s(\ell) = \prod_{s \in S_p} \frac{\sin\left(\ell \frac{2\pi}{p}s\right)}{\sin\left(\frac{2\pi}{p}s\right)} \\ &= (-4)^{\frac{\ell-1}{2}} \prod_{s \in S_p} \prod_{t \in S_\ell} \left(\sin^2\left(\frac{2\pi s}{p}\right) - \sin^2\left(\frac{2\pi t}{\ell}\right) \right).\end{aligned}$$

Similarmente

$$\begin{aligned}\left(\frac{p}{\ell}\right) &= (-4)^{\frac{p-1}{2}} \prod_{t \in S_\ell} \prod_{s \in S_p} \left(\sin^2\left(\frac{2\pi s}{\ell}\right) - \sin^2\left(\frac{2\pi t}{p}\right) \right). \\ \Rightarrow \left(\frac{\ell}{p}\right) &= \left(\frac{p}{\ell}\right) \prod_{t \in S_\ell} \prod_{s \in S_p} (-1) = \left(\frac{p}{\ell}\right) (-1)^{\frac{\ell-1}{2} \frac{p-1}{2}}. \quad \square\end{aligned}$$

9. SELECCIÓN DE TÓPICOS EN LA TEORÍA DE NÚMEROS

9.1. **Ceros de $\zeta(s)$.** Riemann (1859) estudió la función

$$\zeta(s) = \sum \frac{1}{n^s} = \prod \left(\frac{1}{1 - p^{-s}} \right),$$

en [5]. De hecho, establecimos dos propiedades importantes en § 5:

- (i) Continuación a una función meromorfa en toda $s \in \mathbb{C}$.
- (ii) Ecuación funcional:

$$L(s) = L(1-s),$$

en donde $L(s) = \pi^{s/2} \Gamma(s/2) \zeta(s)$.

Además, Riemann estudió sus propiedades como producto infinito.

Lo que tal vez es el problema abierto más importante en matemáticas puras es la hipótesis de Riemann. Esta predice que los ceros no triviales de $\zeta(s)$ se encuentran en $\Re(s) = \frac{1}{2}$.

Observamos también que conocer regiones de $\mathbb{C}$ en donde $\zeta(s) \neq 0$, nos provee resultados. Por ejemplo, el teorema de números primos es el siguiente.

Teorema 9.1. *Sea*

$$\pi(x) = \# \{p \in \mathcal{P} \mid p \leq x\},$$

entonces

$$\pi(x) \sim \frac{x}{\log x}.$$

Este teorema es equivalente a la afirmación:

$$\zeta(s) \neq 0 \quad \forall s = 1 + it, t \in \mathbb{R},$$

para la cual surgieron dos soluciones simultáneas a finales del siglo XIX por Hadamard y de la Vallée Poissin. Una demostración elemental de este importante teorema, se puede encontrar en [2].

9.2. Campos de Funciones. Estudiamos un caso, en donde obtenemos resultados positivos sobre la hipótesis de Riemann. Sea $\mathbb{F}_p[t]$ es anillo de polinomios en la variable t , con coeficientes en el campo finito $\mathbb{F}_p$.

Observación 9.2. En la teoría de Galois, sabemos que para cada n , existe un campo finito $\mathbb{F}_q$ con $q = p^n$ elementos. Por lo que en lo siguiente podemos reemplazar $\mathbb{F}_p$ por $\mathbb{F}_q$.

Estudiamos el campo de funciones racionales $\mathbb{F}_p(t)$, en donde $h(t) \in \mathbb{F}_p(t)$ si

$$h(t) = \frac{f(t)}{g(t)}, \quad f(t), g(t) \in \mathbb{F}_p[t].$$

Estos, y sus extensiones algebraicas separables, son estudiados en la teoría de números, en donde tenemos dos casos de campos globales.

Campos de funciones	k	Campos de números	k
Campo racional:	$\mathbb{F}_p(t)$		$\mathbb{Q}$
	$\cup$		$\cup$
Anillo de enteros:	$\mathbb{F}_p[t]$		$\mathbb{Z}$

Decimos que nos encontramos en el caso de característica p , cuando estudiamos un campo de funciones, y característica cero en un campo de números.

$\mathbb{F}_p[t]$ es un dominio euclideo, por lo cual es principal y cuenta con factorización única. Cada ideal $\mathfrak{a} \subset \mathbb{F}_p[t]$ es de la forma

$$\mathfrak{a} = (f(t)),$$

end donde $f(t) \in \mathbb{F}_p[t]$ es un polinomio, el cual podemos suponer que es mónico. La factorización única nos da

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k},$$

end donde cada $\mathfrak{p}_i = (p_i(t))$, con $p_i(t) \in \mathbb{F}_p[t]$ es un polinomio irreducible (mónico). Podemos definir la norma de un ideal por

$$N\mathfrak{a} = p^{-\deg f(t)}$$

Definición 9.3. La función ζ_k de un campo de funciones está dada por

$$\zeta_k(s) = \sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}} = \prod_{\mathfrak{p}} \frac{1}{1 - N\mathfrak{p}^{-s}},$$

inicialmente en $\Re(s) > 1$.

$f(t)$ es un polinomio en $\mathbb{F}_p[t]$

Los campos de funciones, surgen en la Geometría Algebraica como el campo de funciones de una curva suave proyectiva X sobre $\mathbb{F}_p$. Weil demostró para curvas:

- (i) (*Racionalidad*). $\zeta_k(s)$ tiene una continuación meromorfa a una función racional en q^{-s} .
- (ii) (*Ecución funcional*). Después de completar a una función L , tenemos

$$L(s) = \varepsilon(s)L(1-s).$$

- (ii) (*Hipótesis de Riemann*) $\zeta_k(s) = 0 \Rightarrow \Re(s) = \frac{1}{2}$.

Las famosas conjeturas de Weil, generalizan estas tres propiedades al contexto de variedades algebraicas. Estas conjeturas fueron demostradas por Deligne [1].

Actualmente, en la teoría de números moderna, estudiamos leyes de reciprocidad generalizadas en el caso abierto para grupos algebraicos no abelianos. Esto es, en el contexto del programa de Langlands, en donde obtenemos funciones L globales, y en el caso de campos de funciones hemos obtenido resultados:

- (i) GL_2 : Drinfeld (1970's).
- (ii) GL_n : L. Lafforgue (2002).
- (iii) Grupos Clásicos: L. Lomelí (2015).

9.3. Problema de la discrepancia de signos de Erdős. Sea $f : \mathbb{N} \rightarrow \{-1, 1\}$ una función estrictamente multiplicativa, i.e., tal que $f(mn) = f(m)f(n)$, $\forall m, n \in \mathbb{N}$. ¿Sabemos si

$$\sup_{N \in \mathbb{N}} \left| \sum_{n=1}^N f(n) \right| = \infty ?$$

De hecho resultó ser peor, como descrito recientemente en [8].

Teorema 9.4 (Tao). *Sea $f : \mathbb{N} \rightarrow \{-1, 1\}$, una función arbitraria. Entonces*

$$\sup_{k, N \in \mathbb{N}} \left| \sum_{n=1}^N f(kn) \right| = \infty.$$

9.4. Progresiones Aritméticas de longitud k . Dado un entero k , desde 1770 Lagrange y Waring se hacen la pregunta si existen k primos en progresión aritmética sin interrupciones?

Este problema tiene una historia interesante, y fué resuelto en este nuevo milenio por los matemáticos Green y Tao, en donde fusionan ideas de la teoría Ergódica con la Teoría de Números. Recomendamos la lectura de [3], para obtener un panorama sobre este tema.

Teorema 9.5 (Green-Tao). *Sea $k \in \mathbb{N}$ y $\mathcal{A} \subset \mathcal{P}$ tal que*

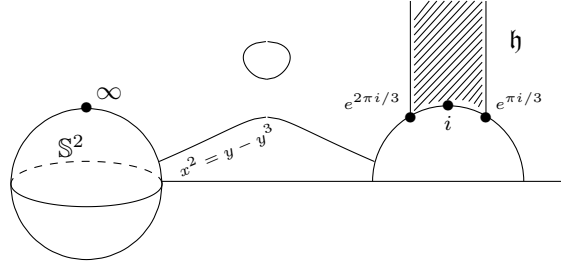
$$\limsup_{N \rightarrow \infty} \frac{\#(\mathcal{A} \cap \{1, \dots, N\})}{\pi(N)} > 0.$$

Entonces $\mathcal{A}$ contiene al menos una progresión aritmética de longitud k .

10. ARITMÉTICA Y GEOMETRÍA EN LOS CERROS DE VALPARAÍSO

En la ciudad de Valparaíso, ver un atardecer y vislumbrar los colores que el océano pacífico junto con el cielo forman parte del día a día. Sin embargo, para un matemático, la pregunta “¿en qué cerro vives?”, puede tomar un sentido muy diferente al de los demás habitantes de la ciudad portuaria.

Para alguien que le interesa el estudio de aritmética y geometría modernas, lo más cercano a vivir en la tierra puede ser la esfera de Riemann. Desde el mirador del cerro Barón se suele vislumbrar el puerto de Valparaíso con el cerro de Playa Ancha en el fondo y el sol o la luna llena en el cielo ...



10.1. Ternas pitagóricas. Comenzamos con un ejercicio en donde se juntan la Aritmética y la Geometría, estudiado por Diofanto en tiempos antiguos. El problema es determinar todas las ternas (x, y, z) que consisten de enteros que satisfacen la ecuación

$$x^2 + y^2 = z^2$$

y tales que su máximo común divisor $(x, y, z) = 1$.

Este problema es equivalente a encontrar todos los puntos racionales en el círculo unitario:

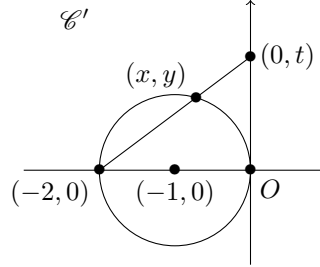
$$\mathbb{S}^1 : x^2 + y^2 = 1, \quad x, y \in \mathbb{Q}.$$

En efecto, uno puede hacer la transición de los puntos racionales del círculo unitario a ternas pitagóricas al incorporar el máximo común divisor, y viceversa, simplemente dividiendo por la tercera variable.

En lenguaje moderno, el problema es encontrar una parametrización racional de círculo unitario. Primero, observamos que parametrizar $\mathbb{S}^1$ sobre los números reales es equivalente a parametrizar

$$\mathcal{C}' : (x+1)^2 + y^2 = 1, \quad x, y \in \mathbb{R}.$$

La siguiente figura

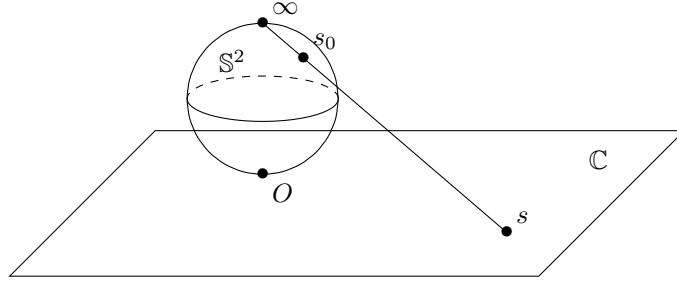


y un poco de álgebra, nos indican que todas las coordenadas $(x(t), y(t)) \in \mathbb{S}^1$ son obtenidas por la parametrización

$$x(t) = \frac{4-t^2}{t^2+4}, \quad y(t) = \frac{4t}{t^2+4}.$$

Un ejercicio es verificar que, ambas $x(t)$, $y(t)$ tienen coordenadas racionales si y solo si $t \in \mathbb{Q}$.

10.2. Proyección estereográfica y puntos racionales. También obtenemos una parametrización para la esfera de Riemann $\mathbb{S}^2$, por medio de la proyección estereográfica a $\mathbb{C}$, ésta incorpora el punto en el infinito ∞ como el polo norte.



Entonces, podemos argumentar como lo hicimos en el caso del círculo unitario para obtener una parametrización racional para los puntos s_0 en la esfera. En verdad, tomamos una esfera unitaria en tres dimensiones con centro $(0, 0, 1)$ e identificamos el punto ∞ con $(0, 0, 2)$. Un punto $s_0 \in \mathbb{S}^2$ corresponde a un punto $s \in \mathbb{C}$. Guiados por la figura y un poco de álgebra, es un ejercicio llegar a

$$s_0(u, v) = \left(\frac{4u}{u^2 + v^2 + 4}, \frac{4v}{u^2 + v^2 + 4}, \frac{2u^2 + 2v^2}{u^2 + v^2 + 4} \right).$$

Además, se debe verificar que $s_0(u, v)$ tiene coordenadas racionales en el espacio euclideo tridimensional si y solo si $(u, v) \in \mathbb{Q}^2$.

10.3. Cerro modular. An example of space endowed with a non-Euclidean geometry, which also provides an example of a Riemann surface is the complex upper half plane

$$\mathfrak{h} = \{z \in \mathbb{C} \mid \Im(z) > 0\}.$$

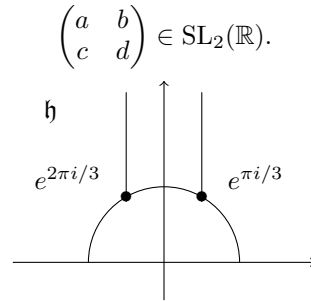
A modular form of weight k is an analytic function

$$f : \mathfrak{h} \rightarrow \mathbb{C}$$

satisfying the relationship

$$f(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right),$$

for



Funciones Δ y τ de Ramanujan. Given $z \in \mathfrak{h}$, we write $q = \exp(2\pi iz)$. Then

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

The τ function appearing in the Fourier expansion of the Δ function is multiplicative

$$\tau(mn) = \tau(m)\tau(n), \text{ g.c.d.}(m, n) = 1$$

and satisfies the following recursive relation on powers of primes

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1}).$$

Ramanujan Conjecture. The τ function satisfies the Ramanujan bound

$$|\tau(p)| \leq 2p^{11/2},$$

for every prime p .

The Ramanujan Conjecture was proved by Deligne, as part of his work on the Weil conjectures [1].

10.4. **Funciones L .** Every modular form of weight k has a ζ -function

$$\zeta(s, f) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s},$$

which is absolutely convergent for $\Re(s) > 2k$. It has an Euler product

$$\prod_p \frac{1}{1 - c(p)p^{-s} + p^{2k-1-2s}}.$$

Completing the ζ -function gives

$$L(s, f) = (2\pi)^{-s} \Gamma(s) \zeta(s, f),$$

which is known to satisfy the functional equation

$$L(s, f) = (-1)^k L(k - s, f).$$

Para mayor información sobre el cerro modular, hacemos referencia al capítulo VII del libro de Serre [7].

10.5. **Cerro elíptico.** Elliptic curves, required for a modern day number theorist, have a Weierstrass form

$$x^2 = y^3 + ay + b,$$

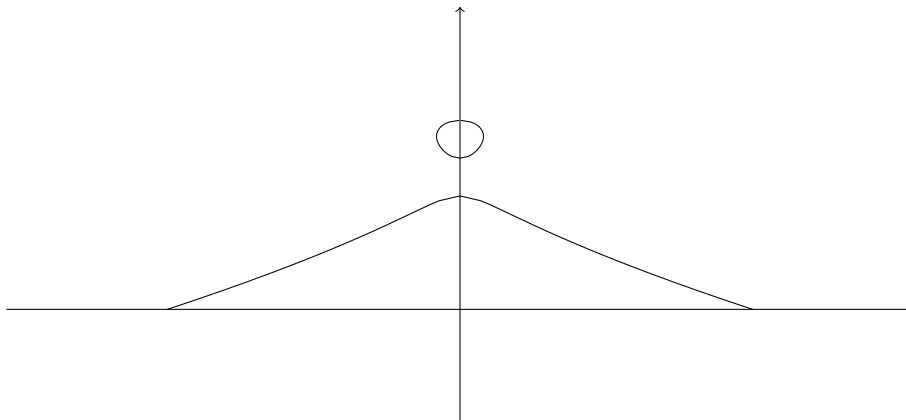
valid not only over $\mathbb{Q}$, but over fields of characteristic different than 2 or 3. They have discriminant and j -invariant

$$\Delta = -16(4a^3 + 27b^2) \quad j = -\frac{1728(4a)^3}{\Delta}.$$

Where we choose the perhaps unconventional setting of interchanging the variables x and y .

Un ejemplo de una curva elíptica es

$$(10.1) \quad E : x^2 = y - y^3$$



L -functions. Let $\#E_p$ denote the number of solutions mod p and take

$$a_p = p + 1 - \#E_p$$

and define

$$\zeta(s, E) = \prod_p \left(\frac{1}{1 - a_p p^{-s} - p^{1-2s}} \right).$$

(We also need to make sense of the cases $p = 2, 3$ in general ...).

By completing the ζ -function we get

$$L(s, E) = (2\pi)^{-s} \Gamma(s) \zeta(s, E).$$

Then we have the functional equation

$$L(s, E) = \varepsilon L(1 - s, E),$$

for a root number $\varepsilon \in \{\pm 1\}$.

REFERENCES

- [1] P. Deligne, *La conjecture de Weil. I & II*, Pub. Math. IHÉS **43**, **52** (1974, 1980), 273-307, 137-252.
- [2] H. Iwaniec, *Lectures on the Riemann Zeta Function*, University Lecture Series **62**, A.M.S., Providence, 2014.
- [3] B. Kra, *The Green-Tao Theorem on Arithmetic Progressions in the Primes: an Ergodic point of view*, Bull. A.M.S. **43**, 3-23.
- [4] D. Ramakrishnan and R. J. Valenza, *Fourier Analysis on Number Fields*, Graduate Texts in Math. **186**, Springer, New York, 1999.
- [5] B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Größe*, Monatsber. Akad. Berlin (1859), 671-680.
- [6] W. Rudin, *Fourier Analysis on Groups*, Dover edition, 2017.
- [7] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Math. **7**, corrected 5th printing, Springer, New York, 1996.
- [8] K. Soundararajan, *Tao's resolution of the Erdős discrepancy problem*, Bull. A.M.S. **55** (2018), 81-92.
- [9] J. T. Tate, *Fourier analysis in number fields and Hecke's zeta-functions*, thesis, Princeton Univ., (1950) (published in [J. W. S. Cassels and A. Fröhlich, editors, Algebraic number theory, 2nd ed., London Mathematical Society, 2010, pp. 305-347]).

LUIS ALBERTO LOMELÍ, INSTITUTO DE MATEMÁTICAS, PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO, BLANCO VIEL 596, CERRO BARÓN, VALPARAÍSO, CHILE
E-mail address: luis.lomeli@pucv.cl