En este documento eventualmente estarán mis apuntes para las charlas sobre las funciones zeta aritméticas. Favor de contactarme por cualquier corrección, duda, pregunta, etc.

Índice

Parte I Funciones zeta de Dedekind

Esta parte introductoria contiene material bastante conocido y sirve más bien para motivar el resto de mis charlas. Voy a tratar de dar algunos ejemplos, pero para las pruebas refiero a [Neu1999].

1 Función zeta de Riemann

08/10/19

El prototipo de las funciones zeta aritméticas es por supuesto la función zeta de Riemann.

1.1. Definición. La **función zeta de Riemann** se define mediante la serie

$$\zeta(s) := \sum_{n\ge 1} \frac{1}{n^s}. \tag{1.1}$$

La serie de arriba converge absolutamente si $\operatorname{Re} s > 1$: note por ejemplo que si $s = a + bi$, entonces $|n^{-s}| = n^{-a}$, y luego $\int_1^\infty x^{-a}\,dx < \infty$ para $a > 1$. Para $s = 1$ se obtiene la serie armónica $\sum_{n\ge 1} \frac{1}{n}$ que es divergente.

Otra expresión importante para la función zeta de Riemann es la **fórmula del producto de Euler**.

1.2. Proposición. *Se tiene*

$$\zeta(s) = \prod_{p\ primo} \frac{1}{1 - p^{-s}}. \tag{1.2}$$

Demostración de Euler. El mismo Euler probaba esta expresión por el siguiente argumento con series formales. Si

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \cdots,$$

entonces se puede escribir

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \frac{1}{12^s} + \cdots,$$

y restando las dos expresiones, se obtiene

$$\left(\frac{2^s - 1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \cdots$$

De esta manera de los denominadores desaparecen los múltiplos de 2. El mismo truco aplicado para el primo 3 nos da

$$\left(\frac{2^s - 1}{2^s}\right)\left(\frac{3^s - 1}{3^s}\right)\zeta(s) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \frac{1}{17^s} + \cdots$$

Aplicando este razonamiento a todo primo p, se obtiene la expresión

$$\left(\prod_{p \text{ primo}} \frac{p^s - 1}{p^s}\right)\zeta(s) = 1,$$

de donde se sigue la fórmula (1.2). A este argumento le faltan algunas justificaciones, pero notamos que lo que está detrás es la factorización única de $n \in \mathbb{Z}$ en números primos. ■

1.3. Teorema. *La función zeta admite una prolongación meromorfa a todo $s \in \mathbb{C}$ con un único polo simple en $s = 1$ de residuo 1:*

$$\lim_{s\to 1} (s-1)\,\zeta(s) = 1.$$

*La prolongación meromorfa también se denota por $\zeta(s)$ y satisface la **ecuación funcional***

$$\zeta(s) = 2^s \pi^{s-1} \operatorname{sen}\left(\frac{\pi s}{2}\right) \Gamma(1-s)\,\zeta(1-s). \tag{1.3}$$

Demostración. [Neu1999, Chapter VII, Corollary (1.7)]. ■

Aquí $\Gamma(s)$ es la **función gamma** que se define mendiante la integral $\int_0^\infty x^s\, e^{-x}\, \frac{dx}{x}$ para $\operatorname{Re} s > 0$. Esta también admite una prolongación meromorfa, con la ecuación funcional correspondiente

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

Recordemos que

$$\Gamma(n+1) = n! \quad \text{para } n = 0,1,2,3,\ldots$$

La función gamma tiene polos simples en $s = -n$ para $n = 0,1,2,\ldots$ de residuo $\frac{(-1)^n}{n!}$.

1.4. Ejemplo. Usando la ecuación funcional para la ζ y Γ, se puede calcular que

$$\zeta(0) = -\frac{1}{2}.$$

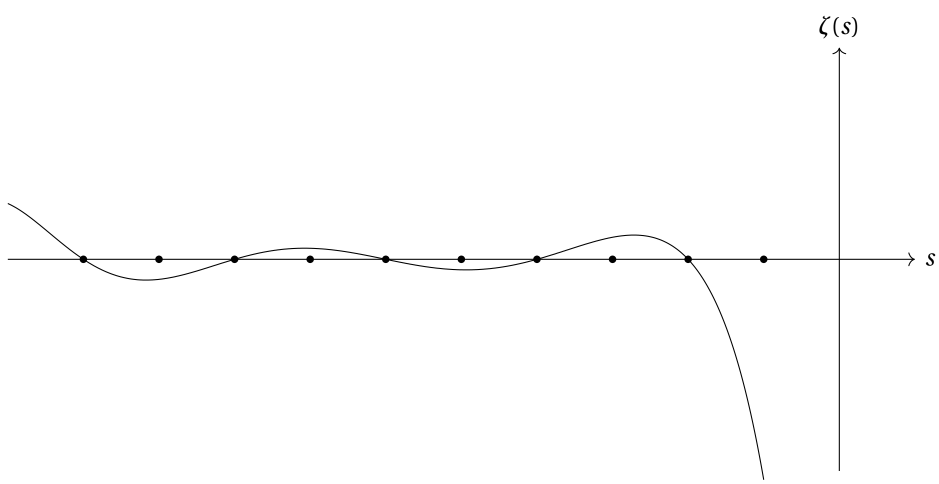
De hecho, tenemos

$$-1 = \lim_{s\to 1}(1-s)\,\zeta(s) = \lim_{s\to 1} 2\, \underbrace{(1-s)\Gamma(1-s)}_{\Gamma(2-s)}\, \zeta(0) = 2\zeta(0),$$

de donde $\zeta(0) = -\frac{1}{2}$. ▲

1.5. Comentario. De la ecuación funcional se ve que hay ceros simples $\zeta(-2n) = 0$ para $n = 1,2,3,\ldots$ Estos ceros se conocen como los **ceros triviales** de ζ. La **hipótesis de Riemann** afirma que los ceros no triviales tienen $\operatorname{Re} s = \frac{1}{2}$.

Entre los ceros triviales la función zeta cambia el signo.



Para $s > 1$ la serie (1.1) converge muy lentamente, así que en el siglo XVII se hizo famoso el **problema de Basilea** que consistía en calcular con una buena precisión el valor de $\zeta(2)$. Un siglo después Euler encontró la respuesta exacta $\zeta(2) = \frac{\pi^2}{6}$*, y la siguiente fórmula general.

*Véase http://empslocal.ex.ac.uk/people/staff/rjchapma/etc/zeta2.pdf para una colección de pruebas.

1.6. Proposición. *Se tiene*

$$\zeta(2k) = (-1)^{k+1}\, B_{2k}\, \frac{2^{2k-1}}{(2k)!}\, \pi^{2k} \quad \text{para } k \ge 1. \tag{1.4}$$

*Aquí $B_{2k} \in \mathbb{Q}$ son los **números de Bernoulli** que pueden ser definidos mediante la función generatriz exponencial*

$$\sum_{k\ge 0} \frac{B_k}{k!}\, t^k = \frac{t\, e^t}{e^t - 1} \quad \text{en } \mathbb{Q}[[t]]. \tag{1.5}$$

Demostración. Hay muchas pruebas de este resultado. Véase por ejemplo [AIK2014, Theorem 5.4] o [Neu1999, Chapter VII, Corollary (1.10)]. ■

1.7. Ejemplo. En particular, se tiene

$$B_0 = 1,\ B_1 = \frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0,\ B_4 = -\frac{1}{30},\ B_5 = 0,\ B_6 = \frac{1}{42},\ B_7 = 0,\ B_8 = -\frac{1}{30},\ B_9 = 0,\ B_{10} = \frac{5}{6},\ \ldots \qquad \blacktriangle$$

1.8. Comentario. En general, $B_{2k+1} = 0$ para $k \ge 1$ y los signos de los B_{2k} se alternan. El signo en la fórmula de Euler (1.4) se debe a esto. Otros múltiplos en la fórmula son en cierto sentido artefactos de la ecuación funcional: usando (1.3) se obtiene una fórmula más bonita

$$\zeta(1-n) = -\frac{B_n}{n} \quad \text{para } n \ge 1. \tag{1.6}$$

1.9. Ejemplo. Tenemos

$$\zeta(0) = -\frac{1}{2}, \quad \zeta(-1) = -\frac{1}{12}, \quad \zeta(-2) = 0, \quad \zeta(-3) = \frac{1}{120}, \quad \zeta(-4) = 0, \quad \zeta(-5) = -\frac{1}{252}, \quad \zeta(-6) = 0, \quad \ldots \qquad \blacktriangle$$

1.10. Comentario. Los valores en los enteros positivos *impares* son más misteriosos. En 1977 Roger Apéry demostró que

$$\zeta(3) = 1{,}202056903159594285399738161511449990 8\ldots$$

es un número irracional. Refiero a [vdP7879] para una exposición de este resultado. Los métodos de Apéry no se generalizan a $\zeta(5)$, $\zeta(7)$, etc.

Un teorema de Rivoal [Riv2000] afirma que hay un número infinito de $k \ge 1$ tales que $\zeta(2k+1)$ es irracional. Otro resultado curioso pertenece a Zudilin [Zud2001] y dice que por lo menos un número entre

$$\zeta(5),\ \zeta(7),\ \zeta(9),\ \zeta(11)$$

es irracional, aunque ¡la prueba no revela cuál!

Todo este progreso analiza la irracionalidad de los valores $\zeta(2k+1)$, pero se sospecha que estos números son trascendentes y algebraicamente independientes entre sí*.

2 Campos de números y sus anillos de enteros

2.1. Definición. Un **campo de números** es una extensión finita $F/\mathbb{Q}$.

Denotemos por $d := [F:\mathbb{Q}]$ el grado de la extensión. En este caso hay d diferentes encajamientos $\sigma\colon F \hookrightarrow \mathbb{C}$. Para cada encajamiento σ también se tiene su conjugado $\overline{\sigma}$. Cuando $\sigma = \overline{\sigma}$, se dice que σ es **real**, y en el caso contrario se dice que σ es **complejo**. Vamos a denotar por r_1 el número de los encajamientos reales y por $2r_2$ el número de encajamientos complejos (que vienen en pares conjugados). Se tiene entonces

$$d = r_1 + 2r_2.$$

Para estudiar la aritmética, se considera el anillo de enteros de F.

*Los $\zeta(2k)$ son también trascendentes, pero por una razón tonta que es el factor π^{2k}.

2.2. Definición. Para un campo de números F, el **anillo de enteros** es la cerradura entera de $\mathbb{Z}$ en F:

$$\mathcal{O}_F := \{\alpha \in F \mid f(\alpha) = 0 \text{ para algún } f \in \mathbb{Z}[x] \text{ mónico}\}.$$

He aquí un par de ejemplos importantes.

2.3. Ejemplo. Si D es un entero libre de cuadrados, la extensión $F = \mathbb{Q}(\sqrt{D})$ se llama un **campo cuadrático**.

Si $D < 0$, se dice que F es **imaginario**. En este caso $r_1 = 0$ y $r_2 = 1$. Hay dos encajamientos:

$$\sigma\colon a + b\sqrt{D} \mapsto a + b\sqrt{D} \quad \text{y} \quad \overline{\sigma}\colon a + b\sqrt{D} \mapsto a - b\sqrt{D}.$$

Si $D > 0$, se dice que F es **real**. En este caso $r_1 = 2$ y $r_2 = 0$, y hay dos encajamientos reales

$$\sigma\colon a + b\sqrt{D} \mapsto a + b\sqrt{D} \quad \text{y} \quad \tau\colon a + b\sqrt{D} \mapsto a - b\sqrt{D}.$$

Es un buen ejercicio calcular que

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{D}], & \text{si } D \equiv 2,3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right], & \text{si } D \equiv 1 \pmod 4. \end{cases}$$

De hecho, se ve que si $D \equiv 1 \pmod 4$, entonces el elemento $\alpha = \frac{1+\sqrt{D}}{2}$ satisface la ecuación

$$\alpha^2 - \alpha - \frac{D-1}{4} = 0,$$

donde $\frac{D-1}{4} \in \mathbb{Z}$, así que hay que considerar el anillo más grande $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ en lugar de $\mathbb{Z}[\sqrt{D}]$.

Los campos cuadráticos han sido estudiados extensivamente a partir de Gauss. ▲

2.4. Ejemplo. La extensión de la forma $F = \mathbb{Q}(\zeta_n)$, donde $\zeta_n := e^{2\pi i/n}$ y $n > 2$, se llama un **campo ciclotómico**. El grado de extensión es $[F:\mathbb{Q}] = \phi(n)$. En este caso $r_1 = 0$ y todos los encajamientos son complejos. Se tiene

$$\mathcal{O}_F = \mathbb{Z}[\zeta_n]$$

—véase [Neu1999, Chapter I, Proposition (10.2)] o [Was1997, Theorem 2.6].

Los campos ciclotómicos fueron estudiados por Gauss y Kummer y representan una familia muy importante de campos de números. Un buen libro sobre el tema es [Was1997]. ▲

He aquí algunas propiedades básicas de los anillos de enteros.

2.5. Proposición. *a)* $\mathcal{O}_F$ *es un* $\mathbb{Z}$*-módulo libre de rango* $d = [F:\mathbb{Q}]$.

b) $\mathcal{O}_F$ *es un* ***dominio de Dedekind****; es decir, un dominio noetheriano, enteramente cerrado, de dimensión de Krull* 1*. Lo último quiere decir que todo ideal primo* $\mathfrak{p} \ne 0$ *es maximal.*

$$\begin{tikzcd} \mathcal{O}_F/\mathfrak{p} \arrow[d, dash, "<\infty"] & \mathcal{O}_F \arrow[l, two heads] \arrow[d, dash] & \supset & \mathfrak{p} \arrow[d, dash] \\ \mathbb{F}_p & \mathbb{Z} \arrow[l, two heads] & \supset & (p) \end{tikzcd}$$

c) Para todo ideal no nulo $\mathfrak{a} \subseteq \mathcal{O}_F$ *el cociente* $\mathcal{O}_F/\mathfrak{a}$ *es finito. El número*

$$N(\mathfrak{a}) := \#(\mathcal{O}_F/\mathfrak{a})$$

se llama la ***norma*** *de* $\mathfrak{a}$.

d) *En general, $\mathcal{O}_F$ no es un dominio de factorización única. Lo que sí es cierto es que todo* ideal $\mathfrak{a} \neq (0),(1)$ *admite una factorización única en ideales primos*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_s.$$

Demostración. a) [Neu1999, Chapter I, Proposition (2.10)].

b) [Neu1999, Chapter I, Theorem (3.1)].

c) [Neu1999, Chapter I, Proposition (2.12)].

d) [Neu1999, Chapter I, Theorem (3.3)].

■

2.6. Definición. Si $\alpha_1,\dots,\alpha_d$ es una base de $\mathcal{O}_F$ sobre $\mathbb{Z}$, entonces el **discriminante** de F viene dado por:

$$d_F = \det((\sigma_i \alpha_j)_{ij})^2.$$

Este es un número entero que no depende de la elección de base.

2.7. Ejemplo. Si $F = \mathbb{Q}(\sqrt{D})$ es un campo cuadrático, entonces en el caso de $D \equiv 2,3 \pmod 4$ se tiene

$$d_F = \det\begin{pmatrix} 1 & 1 \\ \sqrt{D} & -\sqrt{D} \end{pmatrix}^2 = 4D,$$

y si $D \equiv 1 \pmod 4$, entonces

$$d_F = \det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{D}}{2} & \frac{1-\sqrt{D}}{2} \end{pmatrix}^2 = D.$$

▲

2.8. Ejemplo. Para $F = \mathbb{Q}(\zeta_n)$ se tiene

$$d_F = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p\mid n} p^{\phi(n)/(p-1)}}$$

—véase [Was1997, Proposition 2.7]. ▲

El discriminante refleja propiedades importantes aritméticas de $\mathcal{O}_F$ (véase [Neu1999, §§I.8, III.2]), pero para no distraernos, no vamos a entrar en los detalles.

Veamos también un par de ejemplos de factorización en $\mathcal{O}_F$.

2.9. Ejemplo. En el anillo $\mathbb{Z}[\sqrt{10}]$ la factorización no es única, como por ejemplo demuestra la fórmula

$$2 \cdot 5 = (\sqrt{10})^2.$$

Sin embargo, al nivel de factorización en ideales primos, se tiene

$$(2) = (2,\sqrt{10})^2, \quad (5) = (5,\sqrt{10})^2, \quad (\sqrt{10}) = (2,\sqrt{10}) \cdot (5,\sqrt{10}).$$

Los ideales $(2,\sqrt{10})$ y $(5,\sqrt{10})$ son primos y no son principales. ▲

2.10. Ejemplo. Para los campos ciclotómicos, el primer anillo entre $\mathbb{Z}[\zeta_n]$ que no tiene factorización única ocurre para $n = 23$*. Este famoso ejemplo fue encontrado por Kummer. En particular, uno puede calcular que en $\mathbb{Z}[\zeta_{23}]$ se cumple

$$(1+\zeta_{23}^2+\zeta_{23}^4+\zeta_{23}^5+\zeta_{23}^6+\zeta_{23}^{10}+\zeta_{23}^{11})(1+\zeta_{23}+\zeta_{23}^5+\zeta_{23}^6+\zeta_{23}^7+\zeta_{23}^9+\zeta_{23}^{11}) =$$
$$2x^{17}+2x^{16}+2x^{15}+2x^{13}+2x^{12}+6x^{11}+2x^{10}+2x^9+2x^7+2x^6+2x^5.$$

Aquí tenemos dos números que no son divisibles por 2, que es irreducible en $\mathbb{Z}[\zeta_{23}]$, pero su producto sí es divisible por 2.

*Véase también https://en.wikipedia.org/wiki/23_enigma

```
? a = 1 + x^2 + x^4 + x^5 + x^6 + x^10 + x^11;
? b = 1 + x + x^5 + x^6 + x^7 + x^9 + x^11;
? lift (Mod (a*b, polcyclo (23)))
% = 2*x^17 + 2*x^16 + 2*x^15 + 2*x^13 + 2*x^12 + 6*x^11 + 2*x^10 + 2*x^9
      + 2*x^7 + 2*x^6 + 2*x^5
```

▲

3 Grupo de clases

Un invariante algebraico importante asociado a $F/\mathbb{Q}$ es su grupo de clases. La definición clásica es la siguiente.

3.1. Definición. Un **ideal fraccionario** $\mathfrak{a} \subseteq F$ es un $\mathcal{O}_F$-submódulo finitamente generado no nulo. Estos ideales forman un grupo abeliano J_F respecto a la multiplicación. Los inversos vienen dados por*

$$\mathfrak{a}^{-1} = \{x \in \mathcal{O}_F \mid x \cdot \mathfrak{a} \subseteq \mathcal{O}_F\},$$

y la identidad es el ideal $\mathcal{O}_F$.

Los ideales fraccionarios **principales** son los de la forma $\alpha\mathcal{O}_F$ para $\alpha \in F^\times$. Estos forman un subgrupo $P_F \subseteq J_F$. Luego, el **grupo de clases** de F es el cociente

$$Cl_F := J_F/P_F.$$

3.2. Comentario. Por la definición, se tiene entonces una sucesión exacta

$$1 \to \mathcal{O}_F^\times \to F^\times \xrightarrow{\alpha \mapsto \alpha\mathcal{O}_F} J_F \to Cl_F \to 1$$

De hecho, esta sucesión exacta se parece bastante a la sucesión para una curva C/k

$$1 \to \overline{k}^\times \to \overline{k}(C)^\times \xrightarrow{div} \operatorname{Div}^0(C) \to \operatorname{Pic}^0(C) \to 0$$

(véase §18). En realidad, Cl_F es el grupo de Picard del anillo $\mathcal{O}_F$ (= clases de isomorfismo de $\mathcal{O}_F$-módulos que son invertibles respecto a $- \otimes_{\mathcal{O}_F} -$):

$$Cl_F \cong \operatorname{Pic}(\mathcal{O}_F) \cong H^1(\operatorname{Spec}\mathcal{O}_F, \mathbb{G}_m).$$

3.3. Teorema. *El grupo Cl_F es finito para cualquier campo de números F.*

Demostración. [Neu1999, Chapter I, Theorem (6.3)]. ■

3.4. Definición. El orden del grupo de clases

$$h_F := \#Cl_F$$

se llama el **número de clases** de F.

En cierto sentido, el número h_F mide qué tan lejos $\mathcal{O}_F$ está de tener factorización única.

3.5. Proposición. *Las siguientes propiedades son equivalentes:*

a) $h_F = 1$*;*

b) $\mathcal{O}_F$ *es un dominio de ideales principales;*

---

*Al principio el concepto de ideal fraccionario se ve raro, pero este sirve precisamente para introducir los inversos.

c) $\mathcal{O}_F$ *es un dominio de factorización única.*

Demostración. La equivalencia entre a) y b) más o menos está clara desde la definición del grupo de clases. La implicación b)⇒c) se cumple en cualquier caso. Para los dominios de Dedekind se tiene también c)⇒b): note que A es un DIP si y solo si es un DFU y todo primo no nulo $\mathfrak{p} \subset A$ es maximal. ■

Los cálculos particulares de Cl_F son bastante tediosos, pero para un campo específico $F/\mathbb{Q}$ no es difícil calcular Cl_F con la computadora*. Solo voy a dar algunos ejemplos con campos cuadráticos y ciclotómicos.

3.6. Ejemplo. Consideremos los campos cuadráticos imaginarios $\mathbb{Q}(\sqrt{D})$ para $D < 0$:

D:	-1	-2	-3	-5	-6	-7	-10	-11	-13	-14
Cl:	1	1	1	C_2	C_2	1	C_2	1	C_2	C_4
D:	-15	-17	-19	-21	-22	-23	-26	-29	-30	-31
Cl:	C_2	C_4	1	$C_2 \times C_2$	C_2	C_3	C_6	C_6	$C_2 \times C_2$	C_3
D:	-33	-34	-35	-37	-38	-39	-41	-42	-43	-46
Cl:	$C_2 \times C_2$	C_4	C_2	C_2	C_6	C_4	C_8	$C_2 \times C_2$	1	C_4
D:	-47	-51	-53	-55	-57	-58	-59	-61	-62	-65
Cl:	C_5	C_2	C_6	C_4	$C_2 \times C_2$	C_2	C_3	C_6	C_8	$C_4 \times C_2$
D:	-66	-67	-69	-70	-71	-73	-74	-77	-78	-79
Cl:	$C_4 \times C_2$	1	$C_4 \times C_2$	$C_2 \times C_2$	C_7	C_4	C_{10}	$C_4 \times C_2$	$C_2 \times C_2$	C_5
D:	-82	-83	-85	-86	-87	-89	-91	-93	-94	-95
Cl:	C_4	C_3	$C_2 \times C_2$	C_{10}	C_6	C_{12}	C_2	$C_2 \times C_2$	C_8	C_8
D:	-97	-101	-102	-103	-105	-106	-107	-109	-110	-111
Cl:	C_4	C_{14}	$C_2 \times C_2$	C_5	$C_2 \times C_2 \times C_2$	C_6	C_3	C_6	$C_6 \times C_2$	C_8
D:	-113	-114	-115	-118	-119	-122	-123	-127	-129	-130
Cl:	C_8	$C_4 \times C_2$	C_2	C_6	C_{10}	C_{10}	C_2	C_5	$C_6 \times C_2$	$C_2 \times C_2$
D:	-131	-133	-134	-137	-138	-139	-141	-142	-143	-145
Cl:	C_5	$C_2 \times C_2$	C_{14}	C_8	$C_4 \times C_2$	C_3	$C_4 \times C_2$	C_4	C_{10}	$C_4 \times C_2$
D:	-146	-149	-151	-154	-155	-157	-158	-159	-161	-163
Cl:	C_{16}	C_{14}	C_7	$C_4 \times C_2$	C_4	C_6	C_8	C_{10}	$C_8 \times C_2$	1

El **teorema de Heegner–Stark** afirma que para $D < 0$ se tiene

$$h_{\mathbb{Q}(\sqrt{D})} = 1 \iff D = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

También se sabe que

$$h_{\mathbb{Q}(\sqrt{D})} \xrightarrow{D \to -\infty} +\infty.$$

El último resultado fue conjeturado por Gauss quien estudiaba los grupos de clases de campos cuadráticos. Para mayor información recomiendo el artículo [Gol1985]. ▲

3.7. Ejemplo. La situación con los campos cuadráticos reales es más complicada. He aquí una tabla de $Cl_{\mathbb{Q}(\sqrt{D})}$ para $D > 1$.

*Por ejemplo, en PARI/GP; véase https://pari.math.u-bordeaux.fr/ Todos los cálculos que siguen fueron realizados en PARI/GP.

D:	2	3	5	6	7	10	11	13	14	15
Cl:	1	1	1	1	1	C_2	1	1	1	C_2
D:	17	19	21	22	23	26	29	30	31	33
Cl:	1	1	1	1	1	C_2	1	C_2	1	1
D:	34	35	37	38	39	41	42	43	46	47
Cl:	C_2	C_2	1	1	C_2	1	C_2	1	1	1
D:	51	53	55	57	58	59	61	62	65	66
Cl:	C_2	1	C_2	1	C_2	1	1	1	C_2	C_2
D:	67	69	70	71	73	74	77	78	79	82
Cl:	1	1	C_2	1	1	C_2	1	C_2	C_3	C_4
D:	83	85	86	87	89	91	93	94	95	97
Cl:	1	C_2	1	C_2	1	C_2	1	1	C_2	1
D:	85	86	87	89	91	93	94	95	97	101
Cl:	C_2	1	C_2	1	C_2	1	1	C_2	1	1
D:	102	103	105	106	107	109	110	111	113	114
Cl:	C_2	1	C_2	C_2	1	1	C_2	C_2	1	C_2
D:	115	118	119	122	123	127	129	130	131	133
Cl:	C_2	1	C_2	C_2	C_2	1	1	$C_2 \times C_2$	1	1
D:	134	137	138	139	141	142	143	145	146	149
Cl:	1	1	C_2	1	1	C_3	C_2	C_4	C_2	1

Una conjetura de Gauss, todavía abierta, afirma que $h_{\mathbb{Q}(\sqrt{D})} = 1$ para un número infinito de $D > 1$. La **heurística de Cohen–Lenstra** [CL1984] sugiere que $h_{\mathbb{Q}(\sqrt{p})} = 1$ para aproximadamente 76% de los primos, y es algo que se puede verificar con la computadora (solo hay que tomar bastantes primos). ▲

3.8. Ejemplo. Para los campos ciclotómicos, notamos que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ si n es impar (demostración: $\zeta_{2n} = -\zeta_n^{(n+1)/2}$). Por esto para evitar redundancias, se pueden considerar solamente los n tales que $n \not\equiv 2 \pmod 4$. He aquí una pequeña tabla de $Cl_{\mathbb{Q}(\zeta_n)}$. Note que estos grupos son bastante explosivos.

n:	1	3	4	5	7	8	9	11
Cl:	1	1	1	1	1	1	1	1
n:	12	13	15	16	17	19	20	21
Cl:	1	1	1	1	1	1	1	1
n:	23	24	25	27	28	29	31	32
Cl:	C_3	1	1	1	1	$C_2 \times C_2 \times C_2$	C_9	1
n:	33	35	36	37	39	40	41	43
Cl:	1	1	1	C_{37}	C_2	1	$C_{11} \times C_{11}$	C_{211}
n:	44	45	47	48	49	51	52	53
Cl:	1	1	C_{695}	1	C_{43}	C_5	C_3	C_{4889}
n:	55	56	57	59	60	61	63	64
Cl:	C_{10}	C_2	C_9	C_{41241}	1	C_{76301}	C_7	C_{17}
n:	65	67	68	69	71	72	73	75
Cl:	$C_4 \times C_4 \times C_2 \times C_2$	C_{853513}	C_8	C_{69}	$C_{3882809}$	C_3	$C_{11957417}$	C_{11}
n:	76	77	79	80	81	83	84	85
Cl:	C_{19}	$C_{20} \times C_4 \times C_4 \times C_4$	$C_{100146415}$	C_5	C_{2593}	$C_{838216959}$	1	C_{6205}

Se sabe que $h_{\mathbb{Q}(\zeta_n)} = 1$ solo para un número finito de n. He aquí la lista completa de tales n que cumplen $n \not\equiv 2 \pmod 4$ [Was1997, Chapter 11]:

$$1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.$$ ▲

4 Teorema de unidades de Dirichlet y el regulador

4.1. Teorema (El teorema de unidades de Dirichlet). *El grupo de unidades*

$$\mathcal{O}_F^\times = \{\alpha \in \mathcal{O}_F \mid \alpha \textit{ es invertible}\} = \{\alpha \in \mathcal{O}_F \mid N_{F/\mathbb{Q}}(\alpha) = \pm 1\}$$

es finitamente generado y

$$\operatorname{rk} \mathcal{O}_F^\times = r_1 + r_2 - 1.$$

La prueba no es fácil, pero voy a dar la idea (siguiendo [Neu1999, Chapter I, §§5,7]) porque en el camino surge otro invariante importante que es el regulador. Consideremos

$$\prod_{\sigma\colon F \hookrightarrow \mathbb{C}} \mathbb{C}^\times,$$

donde el producto es sobre los d encajamientos de F en $\mathbb{C}$. El grupo de Galois $G_\mathbb{R} := \operatorname{Gal}(\mathbb{C}/\mathbb{R})$ actúa sobre $\prod_\sigma \mathbb{C}^\times$ conjugando las coordenadas y además permutando la coordenada σ con $\overline{\sigma}$. De la misma manera, podemos considerar $\prod_\sigma \mathbb{R}$ con la acción de $G_\mathbb{R}$ por la permutación de coordenadas. Tenemos el siguiente diagrama conmutativo.

$$\begin{tikzcd}
F^\times \arrow[r, "\alpha \mapsto (\sigma(\alpha))"] \arrow[d, "N_{F/\mathbb{Q}}"'] & \prod_\sigma \mathbb{C}^\times \arrow[r, "(z_\sigma) \mapsto (\log|z_\sigma|)"] \arrow[d, "\prod"] & \prod_\sigma \mathbb{R} \arrow[d, "\sum"] \\
\mathbb{Q}^\times \arrow[r, hook] & \mathbb{C}^\times \arrow[r, "z \mapsto \log|z|"] & \mathbb{R}
\end{tikzcd}$$

Aquí las flechas denotadas por $\prod$ y $\sum$ corresponden al producto y suma de coordenadas respectivamente. Todas las aplicaciones son $G_\mathbb{R}$-equivariantes (donde la acción sobre $F^\times$ y $\mathbb{Q}^\times$ es trivial), y tomando los $G_\mathbb{R}$-invariantes, se obtiene

$$\begin{tikzcd}
\mathcal{O}_F^\times \arrow[r] \arrow[d, hook] \arrow[rr, bend left, "=:\lambda"] & S \arrow[r] \arrow[d, hook] & H \arrow[d, hook] \\
F^\times \arrow[r] \arrow[d, "N_{F/\mathbb{Q}}"'] & \left(\prod_\sigma \mathbb{C}^\times\right)^{G_\mathbb{R}} \arrow[r] \arrow[d, "\prod"] & \left(\prod_\sigma \mathbb{R}\right)^{G_\mathbb{R}} \arrow[d, "\sum"] \\
\mathbb{Q}^\times \arrow[r, hook] & \mathbb{R}^\times \arrow[r] & \mathbb{R}
\end{tikzcd}$$

Aquí

$$S := \Big\{ (x_i) \in \Big(\prod_\sigma \mathbb{C}^\times \Big)^{G_\mathbb{R}} \;\Big|\; \prod_i x_i = \pm 1 \Big\},$$

$$H := \Big\{ (x_i) \in \Big(\prod_\sigma \mathbb{R}^\times \Big)^{G_\mathbb{R}} \;\Big|\; \sum_i x_i = 0 \Big\}.$$

Es fácil ver que

$$\dim_\mathbb{R} \Big(\prod_\sigma \mathbb{R}^\times \Big)^{G_\mathbb{R}} = r_1 + r_2,$$

y luego

$$\dim_\mathbb{R} H = r_1 + r_2 - 1.$$

Denotemos

$$\Lambda := \lambda(\mathcal{O}_F^\times) \subseteq H.$$

Resulta que Λ es un retículo en H (subgrupo discreto del rango completo $r_1 + r_2 - 1$) y se tiene una sucesión exacta corta

$$1 \to \mu(F) \to \mathcal{O}_F^\times \xrightarrow{\lambda} \Lambda \to 0 \tag{4.1}$$

Aquí $\mu(F)$ denota la parte de torsión en $\mathcal{O}_F^\times$ que consiste en raíces de la unidad:

$$\mu(F) = \mu_\infty(\mathbb{C}) \cap F.$$

Es fácil ver que F solo puede contener un número finito de raíces de la unidad*, así que $\mu(F)$ es un grupo finito. Esto nos da otro invariante importante de F:

$$\omega_F := \#\mu(F) = \#(\mathcal{O}_F^\times)_{tors}.$$

La sucesión exacta (4.1) se escinde y nos dice que

$$\mathcal{O}_F^\times \cong \Lambda \oplus \mu(F).$$

Puesto que Λ es un retículo en H, tiene sentido calcular su (co)volumen.

4.2. Definición. El número

$$R_F := \frac{1}{\sqrt{r_1 + r_2}} \operatorname{covol}(\Lambda)$$

se llama el **regulador de Dirichlet**.

4.3. Ejemplo. Si $F = \mathbb{Q}(\sqrt{D})$ con $D < 0$ es un campo cuadrático imaginario, entonces $r_1 = 0$ y $r_2 = 1$, así que $\mathcal{O}_F^\times$ es un grupo finito. En este caso ponemos $R_F = 1$. ▲

4.4. Ejemplo. Si $F = \mathbb{Q}(\sqrt{D})$ con $D > 0$ es un campo cuadrático real, entonces $r_1 = 2$ y $r_2 = 0$, así que el teorema de unidades afirma que

$$\mathcal{O}_F^\times = \langle \epsilon \rangle \times \{\pm 1\},$$

donde ϵ es un generador de la parte libre de $\mathcal{O}_F^\times$. Podemos asumir que $\epsilon > 1$, y esta condición define ϵ de manera única. Se dice que ϵ es la **unidad fundamental** para $\mathbb{Q}(\sqrt{D})$. He aquí una pequeña tabla de las unidades fundamentales, donde

$$\alpha := \begin{cases} \sqrt{D}, & \text{si } D \equiv 2,3 \pmod{4}, \\ \frac{1+\sqrt{D}}{2}, & \text{si } D \equiv 1 \pmod{4}. \end{cases}$$

D:	2	3	5	6	7	10	11	13	14	15
ϵ:	$1+\alpha$	$2+\alpha$	α	$5+2\alpha$	$8+3\alpha$	$3+\alpha$	$10+3\alpha$	$1+\alpha$	$15+4\alpha$	$4+\alpha$

En el caso de los campos cuadráticos reales, hay dos encajamientos reales $\sigma_{1,2}\colon F \hookrightarrow \mathbb{C}$ dados por

$$a + b\sqrt{D} \mapsto a \pm b\sqrt{D}.$$

La aplicación $\lambda\colon \mathcal{O}_F^\times \to H \subset \mathbb{R}^2$ va a enviar el generador $\epsilon \in \mathcal{O}_F^\times$ al punto $(\log|\sigma_1(\epsilon)|, \log|\sigma_2(\epsilon)|) \in H$. El regulador correspondiente será

$$R_F = \frac{1}{\sqrt{2}} \sqrt{(\log|\sigma_1(\epsilon)|)^2 + (\log|\sigma_2(\epsilon)|)^2}.$$

Usando la relación $N(\epsilon) = \sigma_1(\epsilon)\,\sigma_2(\epsilon) = \pm 1$ (puesto que $\epsilon \in \mathcal{O}_F^\times$), se ve que

$$R_F = \log \epsilon.$$ ▲

* $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, y entonces si $\zeta_n \in F$, el número $\phi(n)$ debe dividir a $[F : \mathbb{Q}]$.

4.5. Comentario (Teoría K algebraica de $\mathcal{O}_F$). El grupo de clases y el grupo de unidades surgen en la teoría K algebraica del anillo $\mathcal{O}_F$. Se tiene

$$K_0(\mathcal{O}_F) \cong \mathbb{Z} \oplus Cl_F, \quad K_1(\mathcal{O}_F) \cong \mathcal{O}_F^\times.$$

Aquí el primer isomorfismo se deduce de las propiedades básicas de anillos de Dedekind (véase por ejemplo [Mil1971, §1]), mientras que el segundo es más aritmético y se sigue de un resultado de Bass, Milnor y Serre (véase [Mil1971, §16]).

Al introducir los grupos K superiores, el mismo Quillen probó la generación finita de $K_n(\mathcal{O}_F)$ para todo $n = 0, 1, 2, 3, \ldots$ [Qui2010], y en [Bor1974] Borel calculó los rangos exactos:

$$\operatorname{rk} K_n(\mathcal{O}_F) = \begin{cases} 1, & \text{si } n = 0, \\ r_1 + r_2 - 1, & \text{si } n = 1, \\ 0, & \text{si } n > 0 \text{ es par}, \\ r_1 + r_2, & \text{si } n > 1,\ n \equiv 1 \pmod 4, \\ r_2, & \text{si } n \equiv 3 \pmod 4. \end{cases} \tag{4.2}$$

Este cálculo generaliza el teorema de unidades de Dirichlet y servía a Borel para definir los **reguladores superiores**. Una buena exposición se encuentra en [BG2002]. Para los cálculos de la torsión en $K_n(\mathcal{O}_F)$, véase [Wei2005].

5 Funciones zeta de Dedekind

5.1. Definición. La **función zeta de Dedekind** de un campo de números $F/\mathbb{Q}$ se define mediante la serie

$$\zeta_F(s) := \sum_{\mathfrak{a} \subseteq \mathcal{O}_F} \frac{1}{N(\mathfrak{a})^s},$$

donde la suma es sobre todos los ideales no nulos en $\mathcal{O}_F$.

La serie converge para $\operatorname{Re} s > 1$.

5.2. Comentario. Notamos que en particular $\zeta_\mathbb{Q} = \zeta$, así que se trata de una generalización de la función zeta de Riemann.

5.3. Proposición. *Se cumple la fórmula del producto de Euler*

$$\zeta_F(s) = \prod_{(0) \ne \mathfrak{p} \in \operatorname{Spec} \mathcal{O}_F} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \prod_{\mathfrak{m} \in \operatorname{Specm} \mathcal{O}_F} \frac{1}{1 - N(\mathfrak{m})^{-s}}.$$

Demostración. Se sigue de la factorización de ideales en $\mathcal{O}_F$ en ideales primos y la multiplicatividad de la norma: si $\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_s^{v_s}$, entonces $N(\mathfrak{a}) = N(\mathfrak{p}_1)^{v_1} \cdots N(\mathfrak{p}_s)^{v_s}$. ∎

5.4. Teorema. *$\zeta_F(s)$ admite una prolongación meromorfa a todo $s \in \mathbb{C}$ con un polo simple en $s = 1$, que cumple la ecuación funcional*

$$\zeta_F(1-s) = |d_F|^{s-1/2} \left(\cos \frac{\pi s}{2}\right)^{r_1+r_2} \left(\operatorname{sen} \frac{\pi s}{2}\right)^{r_2} (2 \cdot (2\pi)^{-s} \Gamma(s))^d \zeta_F(s).$$

Demostración. [Neu1999, Chapter VII, Corollary (5.11)]. ∎

10/10/19

5.5. Proposición. *$\zeta_F(s)$ tiene ceros en $s = -n$ para $n = 0, 1, 2, 3, \ldots$ y sus órdenes correspondientes son*

$$d_{-n} = \begin{cases} r_1 + r_2 - 1, & \textit{si } n = 0, \\ r_2, & \textit{si } n \ge 1 \textit{ es impar}, \\ r_1 + r_2, & \textit{si } n \ge 2 \textit{ es par}. \end{cases}$$

Demostración. Se ve de la ecuación funcional. ■

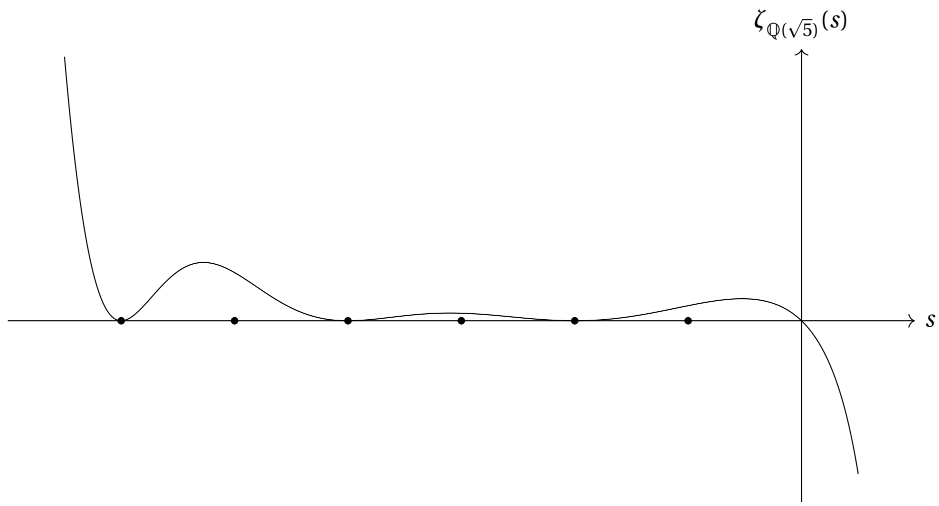
5.6. Comentario. Note que milagrosamente, los números de arriba son los mismos que aparecen en (4.2).

En los enteros negativos pares, ζ_F siempre tiene ceros, mientras que en los enteros negativos impares, no habrá ceros solamente cuando $r_2 = 0$. En este caso se dice que F es un campo **totalmente real**.

Los ceros de ζ_F en los enteros negativos se conocen como los **ceros triviales**. La **hipótesis de Riemann extendida** (ERH)* afirma que los ceros no triviales tienen $\operatorname{Re} s = \frac{1}{2}$.

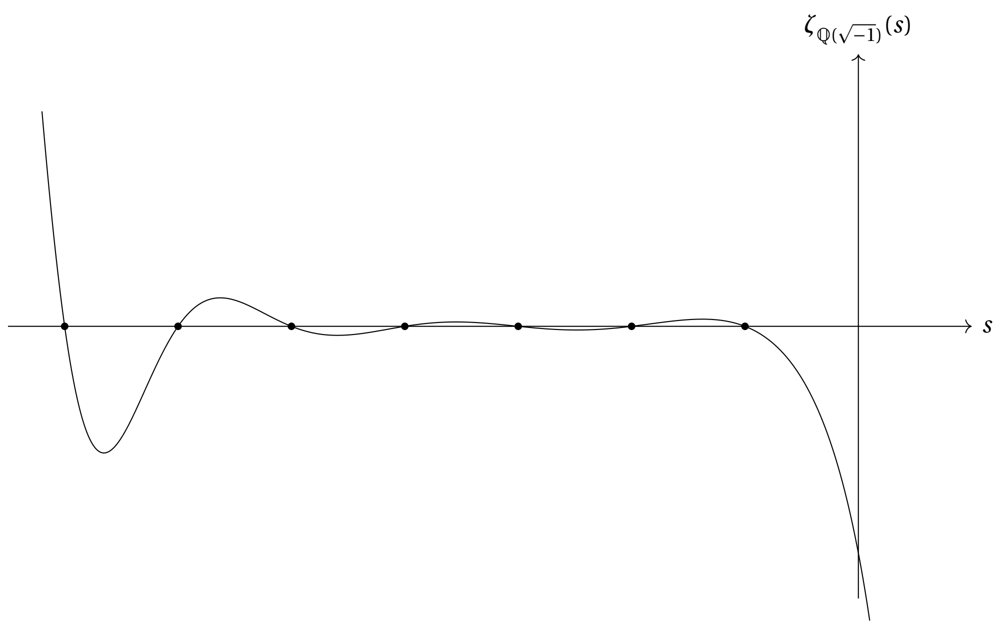
Podemos ver un par de ejemplos del comportamiento de $\zeta_F(s)$ para $s < 0$.

5.7. Ejemplo. Consideremos el campo cuadrático real $F = \mathbb{Q}(\sqrt{5})$. Note que los ceros tienen orden 2.



▲

5.8. Ejemplo. Consideremos el campo imaginario $F = \mathbb{Q}(\sqrt{-1})$. En este caso se tienen ceros simples.



*También hay hipótesis de Riemann **generalizada** (GRH), pero la última se trata de las series L y es más general que la extendida.

▲

5.9. Comentario. Para calcular $\zeta_F(s)$ en PARI/GP, se puede usar el comando `lfun(`f`,`s`)`, donde $F \cong \mathbb{Q}[x]/(f)$. Por ejemplo, `lfun (x^2-5,-1)` devuelve `0.03333...`

6 Teorema de Siegel–Klingen

6.1. Teorema (Siegel–Klingen). *Se tiene* $\zeta_F(-n) \in \mathbb{Q}$ *para todo* $n = 0, 1, 2, 3, \ldots$

Demostración. [Neu1999, Chapter VII, Corollary (9.9)]. ■

6.2. Comentario. El resultado se refiere literalmente a los valores $\zeta_F(-n)$ y no a los residuos correspondientes, así que este tiene interés solo cuando F es un campo totalmente real (con $r_2 = 0$). En el caso contrario $\zeta_F(-n) = 0$ para todo $n = 1, 2, 3, \ldots$

6.3. Ejemplo. En ciertos casos particulares se puede entender cuáles son estos números racionales $\zeta_F(-n)$. Por ejemplo, en el caso de $F = \mathbb{Q}(\sqrt{D})$, usando las series L de Dirichlet

$$L(s,\chi) := \sum_{n\ge 1} \frac{\chi(n)}{n^s},$$

se puede expresar

$$\zeta_{\mathbb{Q}(\sqrt{D})}(s) = L(s,1)\cdot L(s,\chi_D) = \zeta(s)\cdot L(s,\chi_D),$$

donde $\chi_D := \left(\frac{D}{\cdot}\right)$ es el **símbolo de Kronecker.**

Luego, para la serie L de arriba existe una fórmula muy parecida a (1.6):

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n} \quad (n \ge 1).$$

Aquí $B_{n,\chi}$ son los los números de Bernoulli **generalizados** (torcidos por el carácter χ). Estos pueden ser definidos por una función generatriz similar a (1.5):

$$\sum_{n\ge 0} B_{n,\chi}\frac{t^n}{n!} = \sum_{1\le a\le N} \frac{\chi(a)\,t\,e^{at}}{e^{Nt}-1},$$

donde $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ es un carácter de Dirichlet módulo N. Para más detalles y las pruebas, véase [AIK2014, Chapter 4 + Theorem 9.10].

Entonces,

$$\zeta_{\mathbb{Q}(\sqrt{D})}(1-n) = \frac{B_n}{n}\frac{B_{n,\chi_D}}{n}.$$

Para dar un ejemplo particular, si $D = 5$, para $\chi = \chi_5 = \left(\frac{5}{\cdot}\right)$ se tiene

$$\chi(1) = +1, \quad \chi(2) = -1, \quad \chi(3) = -1, \quad \chi(4) = 1,$$

y de la función generatriz uno puede calcular, por ejemplo,

$$B_{2,\chi} = \frac{4}{5}, \quad B_{4,\chi} = -8, \quad B_{6,\chi} = \frac{804}{5}.$$

Recordando los números de Bernoulli habituales

$$B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42},$$

calculamos

$$\zeta_{\mathbb{Q}(\sqrt{5})}(-1) = \frac{1}{30}, \quad \zeta_{\mathbb{Q}(\sqrt{5})}(-3) = \frac{1}{60}, \quad \zeta_{\mathbb{Q}(\sqrt{5})}(-5) = \frac{67}{630}.$$

Podemos comprobar nuestros cálculos en PARI/GP:

```
? lfun (x^2-5, -1)
% = 0.03333333333333333333333333333333333333
? lfun (x^2-5, -3)
% = 0.01666666666666666666666666666666666667
? lfun (x^2-5, -5)
% = 0.1063492063492063492063492063492063492
? 67/630.0
% = 0.1063492063492063492063492063492063492
```

▲

7 Fórmula de clases de Dirichlet

La función $\zeta_F(s)$ tiene cero en $s = 0$ de orden $r_1 + r_2 - 1$. Sin embargo, se puede preguntar cuál es el coeficiente mayor de la serie de Taylor correspondiente.

7.1. Teorema (Fórmula de clases de Dirichlet). *Se tiene*

$$\zeta_F^*(0) := \lim_{s\to 0} s^{-(r_1+r_2-1)}\,\zeta_F(s) = -\frac{h_F}{\#\mu(F)}\,R_F. \tag{7.1}$$

Demostración. [Neu1999, Chapter VII, Corollary (5.11)]. ■

Aquí en la parte izquierda está algo analítico, mientras que en la parte derecha están invariantes algebraicos: el número de clases, el número de las raíces de unidad en $\mathcal{O}_F$ y el regulador. Además, la fórmula nos dice que por alguna razón misteriosa, los tres invariantes están enlazados entre sí.

7.2. Comentario. La ecuación funcional relaciona el cero en $s = 0$ de orden $r_1 + r_2 - 1$ con el polo simple en $s = 1$. De esta manera la fórmula de clases puede ser reescrita como

$$\zeta_F^*(1) := \lim_{s\to 1}(s-1)\,\zeta_F(s) = \frac{2^{r_1}\,(2\pi)^{r_2}\,h_F}{\#\mu(F)\cdot\sqrt{|d_F|}}\,R_F.$$

7.3. Ejemplo. Si $F = \mathbb{Q}$, entonces la fórmula nos da

$$\zeta(0) = \zeta^*(0) = -\frac{1}{2}.$$

▲

7.4. Ejemplo. Si $F = \mathbb{Q}(\sqrt{D})$ con $D > 0$ es un campo cuadrático real y ϵ es la unidad fundamental correspondiente (véase 4.4), entonces la fórmula de clases nos da

$$\zeta_F^*(0) = -\frac{h_F}{2}\,\log\epsilon.$$

En particular, si $F = \mathbb{Q}(\sqrt{10})$, entonces $h_F = 2$, $R_F = \log(3+\sqrt{10})$ y $\mu(F) = \{\pm 1\}$, y

$$\zeta_F^*(0) = -\log(3+\sqrt{10}).$$

Podemos comprobarlo en PARI/GP (note qué estamos haciendo para sacar $\zeta_F^*(0)$ en lugar de $\zeta_F(0)$):

```
? lfun (x^2-10, 0)
% = 0
? lfun (x^2-10, 0 + O (x^10))
% = -1.818446459232066823483698963560708993 8*x + O(x^2)
? log (3+sqrt(10))
% = 1.8184464592320668234836989635607089938
```

▲

7.5. Ejemplo. Si $F = \mathbb{Q}(\sqrt{D})$ con $D < 0$ es un campo cuadrático imaginario, entonces $\mathcal{O}_F^\times = \{\pm 1\}$ y $R_F = 1$, y la fórmula de clases nos da

$$\zeta_F^*(0) = -\frac{h_F}{2}.$$

▲

7.6. Comentario. Uno de los problemas importantes en la teoría de números moderna ha sido generalizar la fórmula (7.1) a algo como

$$\zeta_F^*(1-n) := \lim_{s \to 1-n} (s - (1-n))^{-d_{1-n}} \zeta_F(s) = -\frac{h_n}{\omega_n} R_{F,n}$$

para todo $n = 1, 2, 3, \ldots$ Aquí h_n, ω_n, $R_{F,n}$ deben ser ciertos invariantes superiores asociados a $\mathcal{O}_F$. Hay varias conjeturas de cómo hacerlo.

Parte II Funciones zeta de Hasse–Weil

Por el momento vamos a dejar de lado las funciones zeta de Dedekind $\zeta_F(s)$ y familiarizarnos con las funciones zeta de Hasse–Weil $Z(X,t)$. Más adelante veremos que ambos tipos de funciones zeta son casos particulares de las funciones zeta de esquemas aritméticos.

8 Recordatorio sobre los campos finitos

En esta sección vamos a enumerar algunas propiedades básicas de campos finitos $\mathbb{F}_q$.

1. Para todo $q = p^n$, donde p es primo, hay un único campo finito de q elementos *salvo isomorfismo*. Por abuso de notación, vamos a escribir simplemente "$\mathbb{F}_q$".
2. En particular, para todo m hay una extensión única $k/\mathbb{F}_q$ de grado m, salvo isomorfismo. Por abuso de notación, normalmente se escribe simplemente $k = \mathbb{F}_{q^m}$.
3. El grupo multiplicativo $\mathbb{F}_q^\times$ es cíclico.
4. El grupo de Galois $\operatorname{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ es cíclico de orden m, generado por el automorfismo de Fronenius $F\colon a \mapsto a^q$.

Para un elemento $a \in \mathbb{F}_{q^m}$, su **traza** y **norma** sobre $\mathbb{F}_q$ vienen dadas por

$$T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) := \sum_{\sigma\in\operatorname{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(a) = a + a^q + \cdots + a^{q^{m-1}},$$

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) := \prod_{\sigma\in\operatorname{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(a) = a\,a^q \cdots a^{q^{m-1}},$$

Se cumplen las siguientes propiedades:

a) $T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a), N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) \in \mathbb{F}_q$ para todo $a \in \mathbb{F}_{q^m}$;

b) la traza $T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\colon \mathbb{F}_{q^m} \to \mathbb{F}_q$ es un aplicación $\mathbb{F}_q$-lineal, mientas que la norma $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ es un homomorfismo multiplicativo $\mathbb{F}_{q^m}^\times \to \mathbb{F}_q^\times$;

c) la traza $T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\colon \mathbb{F}_{q^m} \to \mathbb{F}_q$ y norma $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}\colon \mathbb{F}_{q^m}^\times \to \mathbb{F}_q^\times$ son sobreyectivas.

9 Definición de $Z(X,t)$ y primeros ejemplos

Sea X una variedad algebraica sobre un campo finito $\mathbb{F}_q$. Por una **variedad** (algebraica) vamos a entender un esquema reducido de tipo finito sobre $\operatorname{Spec}\mathbb{F}_q$.* Los puntos de X sobre $k/\mathbb{F}_q$ son por la definición

$$X(k) := \operatorname{Hom}_{\operatorname{Spec}\mathbb{F}_q}(\operatorname{Spec} k, X).$$

Si k y k' son dos extensiones de grado m, entonces el isomorfismo $k \cong k'$ sobre $\mathbb{F}_q$ induce una biyección natural $X(k) \cong X(k')$.

*El lector que todavía no conoce la teoría de esquemas debe tener un poco de paciencia: muy pronto se tratará de ejemplos muy explícitos donde basta saber qué es una variedad afín o proyectiva sobre $\mathbb{F}_q$.

Si $X = \operatorname{Spec} \mathbb{F}_q[x_1,\ldots,x_n]/(f_1,\ldots,f_s)$ es afín, entonces

$$X(k) \cong \{x \in \mathbb{A}^n(k) \mid f_1(x) = \cdots = f_s(x) = 0\}.$$

En particular, notamos que para una extensión finita $k/\mathbb{F}_q$ el conjunto $X(k)$ es finito. Para una variedad general, podemos llegar a la misma conclusión tomando un recubrimiento abierto afín.

La discusión de arriba significa que están bien definidos los números de puntos

$$\# X(\mathbb{F}_{q^m}) \quad \text{para } m = 1,2,3,\ldots$$

(es decir, son finitos y no dependen de la elección de $\mathbb{F}_{q^m}/\mathbb{F}_q$).

La función zeta de Hasse–Weil de una variedad $X/\mathbb{F}_q$ es una especie de función generatriz de la sucesión de números $\# X(\mathbb{F}_{q^m})$ para $m = 1,2,3,\ldots$

9.1. Definición. La **función zeta de Hasse–Weil** de una variedad $X/\mathbb{F}_q$ es la función generatriz

$$Z(X,t) := \exp\left(\sum_{m\ge 1} \frac{\# X(\mathbb{F}_{p^m})}{m}\, t^m\right) \in \mathbb{Q}[[t]].$$

Vamos a considerar $Z(X,t)$ como una serie formal en el anillo $\mathbb{Q}[[t]]$. Está claro que de la serie $Z(X,t)$ se pueden extraer todos los números $\# X(\mathbb{F}_{p^m})$:

$$\# X(\mathbb{F}_{q^m}) = \frac{1}{(m-1)!}\, \frac{d^m}{dt^m} \log Z(X,t)\Big|_{t=0}.$$

Más adelante veremos por qué se considera esta función generatriz particular.

9.2. Definición. La **exponencial** y el **logaritmo formal** vienen dados por las series

$$\exp(t) = \sum_{m\ge 0} \frac{t^m}{m!}, \quad \log(1+t) = \sum_{m\ge 1} (-1)^{m+1}\, \frac{t^m}{m} \in \mathbb{Q}[[t]].$$

Muy a menudo nos servirá también la serie

$$-\log(1-at) = \sum_{m\ge 1} \frac{(at)^m}{m},$$

donde a es algún coeficiente constante.

9.3. Lema. *La exponencial y logaritmo formales cumplen las propiedades habituales:*

a) $\exp(\log(1+t)) = 1+t$*,* $\log(\exp(t)) = t$*;*

b) $\exp(s+t) = \exp(s)\exp(t)$*;*

c) $\log((1+s)(1+t)) = \log(1+s) + \log(1+t)$.

Aquí b) y c) se entienden como identidades en el anillo $\mathbb{Q}[[s,t]]$.

Demostración. Para comprobar a), se pueden calcular las derivadas formales; la propiedad b) se demuestra directamente con la fórmula binomial para $(s+t)^m$, y la propiedad c) se deduce de a) y b) de manera formal. ■

9.4. Ejemplo. Si $X = \mathbb{A}^n_{\mathbb{F}_q}$ es el espacio afín n-dimensional, entonces

$$\# \mathbb{A}^n(\mathbb{F}_{q^m}) = q^{mn},$$

y la función zeta correspondiente es

$$Z(\mathbb{A}^n_{\mathbb{F}_q}, t) = \exp\left(\sum_{m\ge 1} \frac{q^{mn}}{m}\, t^m\right) = \exp(-\log(1-q^n t)) = \frac{1}{1-q^n t}. \qquad \blacktriangle$$

9.5. Ejemplo. Para el espacio proyectivo $\mathbb{P}^n$ se tiene la descomposición

$$\mathbb{P}^n(k) = \mathbb{A}^n(k) \sqcup \cdots \sqcup \mathbb{A}^1(k) \sqcup \mathbb{A}^0(k).$$

Usando esto junto con la identidad $\exp(s+t) = \exp(s)\exp(t)$, se deduce que

$$Z(\mathbb{P}^n_{\mathbb{F}_q}, t) = \prod_{0 \le i \le n} Z(\mathbb{A}^i_{\mathbb{F}_q}, t) = \frac{1}{(1-q^n t)\cdots(1-qt)(1-t)}. \qquad \blacktriangle$$

9.6. Ejemplo. En general, se tiene $(X \times Y)(k) = X(k) \times Y(k)$. Usando esto, calculamos que para $X/\mathbb{F}_q$ se tiene

$$Z(\mathbb{A}^n \times X, t) = \exp\left(\sum_{m\ge 1} \frac{\#X(\mathbb{F}_{q^m}) \cdot q^{mn}}{m}\, t^m\right) = Z(X, q^n t).$$

De modo similar,

$$Z(\mathbb{P}^n \times X, t) = \prod_{0 \le i \le n} Z(X, q^i t). \qquad \blacktriangle$$

9.7. Proposición. *Si X es una variedad sobre $\mathbb{F}_q$, entonces al pasar a la extensión $\mathbb{F}_{q^n}/\mathbb{F}_q$ se obtiene*

$$Z(X/\mathbb{F}_{q^n}, t^n) = \prod_{\zeta^n = 1} Z(X/\mathbb{F}_q, \zeta t),$$

donde el producto es sobre las raíces n-ésimas de la unidad.

Demostración. Tenemos

$$\prod_{\zeta^n=1} Z(X/\mathbb{F}_q, \zeta t) = \exp\left(\sum_{m\ge 1} \frac{\#X(\mathbb{F}_{q^m})}{m}\, t^m \sum_{\zeta^n=1} \zeta^m\right),$$

y basta notar que la suma de ζ^m es nula si $n \nmid m$ y es igual a n si $n \mid m$. La serie de arriba nos da entonces

$$\exp\left(\sum_{m\ge 1} \frac{\#X(\mathbb{F}_{q^{nm}})}{m}\, t^{nm}\right) = Z(X/\mathbb{F}_{q^n}, t^n). \qquad \blacksquare$$

Para las funciones zeta de Hasse–Weil también se tiene una fórmula del producto de Euler.

9.8. Proposición. *Para un punto cerrado $x \in |X|$ el campo residual $\kappa(x) := \mathcal{O}_{X,n}/\mathfrak{m}_{X,x}$ es una extensión finita de $\mathbb{F}_q$, y podemos poner*

$$\deg(x) := [\kappa(x) : \mathbb{F}_q].$$

Luego,

$$Z(X, t) = \prod_{x \in |X|} \frac{1}{1 - t^{\deg(x)}}. \tag{9.1}$$

Esta fórmula se ve un poco diferente del producto de Euler (1.2), pero se vuelve similar si ponemos $\zeta(X,s) := Z(X, q^{-s})$ (más adelante veremos la verdadera definición de $\zeta(X,s)$). Antes de probar (9.1), necesitamos un pequeño lema.

9.9. Lema. *Se tiene*

$$\#X(\mathbb{F}_{q^m}) = \sum_{d\mid m} d \cdot a_d, \quad \text{donde } a_d := \#\{x \in |X| \mid \deg(x) = d\}.$$

Demostración. Se tiene

$$X(\mathbb{F}_{q^m}) = \operatorname{Hom}_{\operatorname{Spec}\mathbb{F}_q}(\operatorname{Spec}\mathbb{F}_{q^m}, X) = \coprod_{x \in |X|} \operatorname{Hom}_{\mathbb{F}_q}(\kappa(x), \mathbb{F}_{q^m}).$$

Entonces, para cada punto cerrado $x \in |X|$ falta entender los homomorfismos $\kappa(x) \hookrightarrow \mathbb{F}_{q^m}$. Tenemos la siguiente situación:

$$\begin{tikzcd} \mathbb{F}_{q^m} \arrow[d, dash] \\ \kappa(x) \arrow[d, dash, "\deg(x)"] \\ \mathbb{F}_q \arrow[uu, bend left, dash, "m"] \end{tikzcd}$$

Habrá d diferentes homomorfismos $\kappa(x) \hookrightarrow \mathbb{F}_{q^m}$ que vienen de la acción del grupo $\operatorname{Gal}(\kappa(x)/\mathbb{F}_q)$ que es cíclico de orden d. ■

Ahora estamos listos para probar la identidad (9.1). La parte derecha puede ser escrita como

$$\prod_{x\in|X|} \frac{1}{1-t^{\deg(x)}} = \prod_{d\ge 1} \frac{1}{(1-t^d)^{a_d}}.$$

Ahora bien,

$$\begin{aligned} \log Z(X,t) := \sum_{m\ge 1} \frac{\# X(\mathbb{F}_{q^m})}{m}\, t^m \stackrel{\text{lema}}{=} \sum_{m\ge 1}\sum_{d\mid m} \frac{d\cdot a_d}{m}\, t^m = \sum_{d\ge 1}\sum_{e\ge 1} \frac{a_d}{e}\, t^{de} &= \sum_{d\ge 1} a_d\,(-\log(1-t^d)) \\ &= \sum_{d\ge 1} \log(1-t^d)^{-a_d} = \log \prod_{d\ge 1} \frac{1}{(1-t^d)^{a_d}}, \end{aligned}$$

y tomando la exponencial de ambas partes, se obtiene precisamente (9.1). ■

De la fórmula del producto se ve que la serie formal $Z(X,t)$ tiene coeficientes *enteros*.

9.10. Corolario. *Se tiene* $Z(X,t) \in \mathbb{Z}[[t]]$.

Demostración. En la fórmula del producto

$$\frac{1}{1-t^d} = \sum_{m\ge 0} t^{dm} \in \mathbb{Z}[[t]].$$ ■

9.11. Corolario. *Si $Z\subset X$ es una subvariedad cerrada y $U := X\setminus Z$ es su complemento abierto, entonces*

$$Z(X,t) = Z(Z,t)\cdot Z(U,t).$$

Demostración. Evidente de la fórmula del producto, puesto que $|X| = |Z| \sqcup |U|$. ■

Terminemos por un par de ejemplos más.

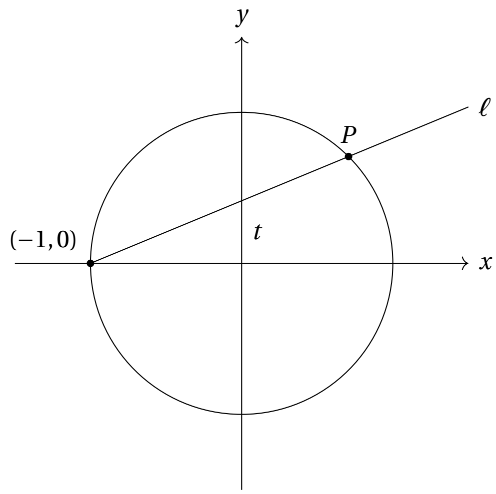
9.12. Ejemplo. Consideremos el círculo unitario afín $X = \operatorname{Spec} \mathbb{F}_q[x,y]/(x^2+y^2-1)$. Primero, notamos que si $\operatorname{char} \mathbb{F}_q = 2$, entonces

$$X(\mathbb{F}_q) = \{(x, \sqrt{1-x^2}) \mid x \in \mathbb{F}_q\},$$

de donde

$$Z(X,t) = Z(\mathbb{A}^1_{\mathbb{F}_q}, t) = \frac{1}{1-qt}.$$

Asumamos entonces que $\operatorname{char} \mathbb{F}_q \neq 2$. Podemos considerar la siguiente parametrización del círculo:



Las coordenadas del punto P son $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ si $t^2 \ne 1$. Esto nos da una biyección

$$\{t \in \mathbb{F}_q \mid t^2 \ne 1\} \cong X(\mathbb{F}_q) \setminus \{(-1,0)\}.$$

Si $q \equiv 1 \pmod 4$, entonces -1 es un cuadrado, y si $q \equiv 3 \pmod 4$, entonces -1 no es un cuadrado. Esto nos da la fórmula

$$\# X(\mathbb{F}_q) = \begin{cases} q-1, & q \equiv 1 \pmod 4, \\ q+1, & q \equiv 3 \pmod 4. \end{cases}$$

Si $q \equiv 1 \pmod 4$, entonces

$$Z(X,t) = \exp\left(\sum_{m\ge 1} \frac{q^m - 1}{m}\, t^m\right) = \frac{1-t}{1-qt}.$$

Si $q \equiv 3 \pmod 4$, entonces

$$Z(X,t) = \exp\left(\sum_{m\ge 1} \frac{q^m}{m}\, t^m + \sum_{m\ge 1} \frac{(-1)^{m+1}}{m}\, t^m\right) = \frac{1+t}{1-qt}. \qquad \blacktriangle$$

Más adelante vamos a calcular la función zeta de la n-esfera $X = \operatorname{Spec}[x_1,\ldots,x_n]/(x_1^2 + \cdots + x_n^2 - 1)$, pero para esto vamos a ocupar otro método más listo.

9.13. Ejemplo. Consideremos la Grassmanniana proyectiva $\mathrm{Gr}(2,n)$ que corresponde a las rectas en $\mathbb{P}^n$. Toda recta en $\mathbb{P}^n(\mathbb{F}_q)$ tiene $q+1$ puntos, y en total $\mathbb{P}^n(\mathbb{F}_q)$ consiste en

$$N = \frac{q^{n+1}-1}{q-1}$$

puntos. Entonces, la fórmula para el número de rectas es

$$\binom{N}{2} \Big/ \binom{q+1}{2} = \frac{N\,(N-1)}{q\,(q+1)} = \frac{(q^{n+1}-1)\,(q^n-1)}{(q^2-1)\,(q-1)}.$$

En general, si ponemos

$$[k]_q := \frac{q^k - 1}{q-1},$$

entonces el número

$$\binom{a}{b}_q := \frac{[a]_q\,[a-1]_q \cdots [a-b+1]_q}{[1]_q\,[2]_q \cdots [b]_q}$$

se llama un **coeficiente q-binomial**. En particular, lo que hemos obtenido es

$$\binom{n+1}{2}_q = \frac{[n+1]_q\,[n]_q}{[1]_q\,[2]_q} = \frac{(q^{n+1}-1)\,(q^n-1)}{(q^2-1)\,(q-1)}.$$

Calculemos ahora la función zeta para $n = 2$ y 3. Si $n = 2$, tenemos

$$\binom{3}{2}_q = \frac{(q^3-1)\,(q^2-1)}{(q^2-1)\,(q-1)} = \frac{q^3-1}{q-1} = q^2+q+1 = \#\mathbb{P}^2(\mathbb{F}_q).$$

Entonces, en este caso la función zeta corresponde a la función zeta de $\mathbb{P}^2$ y es igual a $\frac{1}{(1-q^2 t)\,(1-qt)\,(1-t)}$. Es lo que uno espera, dado que hay una biyección entre los puntos y rectas en el plano proyectivo.

Si $n = 3$, entonces la función zeta es

$$\exp\Bigl(\sum_{m\ge 1} \frac{(q^4-1)\,(q^3-1)}{(q^2-1)\,(q-1)}\,\frac{t^m}{m}\Bigr) = \exp\Bigl(\sum_{m\ge 1} \frac{q^4+q^3+2q^2+q+1}{m}\,t^m\Bigr) = \frac{1}{(1-q^4 t)\,(1-q^3 t)\,(1-q^2 t)^2\,(1-qt)\,(1-t)}.$$

Dejo al lector escribir la expresión general para la función zeta de $\mathrm{Gr}(2,n)$ y analizar el caso de $\mathrm{Gr}(m,n)$.

▲

9.14. Ejercicio. Calcule la función zeta de las siguientes variedades proyectivas sobre $\mathbb{F}_q$ (donde q también puede ser par).

a) $V_{proj}(y^2 z - x^3) \subset \mathbb{P}^2_{\mathbb{F}_q}$,

b) $V_{proj}(y^2 z - x^3 - x^2 z) \subset \mathbb{P}^2_{\mathbb{F}_q}$,

c) $V_{proj}(xy - zw) \subset \mathbb{P}^3_{\mathbb{F}_q}$.

A continuación me gustaría explicar las consideraciones que llevaron a Weil a formular sus célebres conjeturas. La referencia original es [Wei1949], y una buena exposición de este material se encuentra en [IR1990, Chapter 8,10,11]. La idea es obtener algunos cálculos de la función zeta de Hasse–Weil, y las sumas de Gauss y Jacobi nos dan una técnica para hacerlo. 15/10/19

10 Caracteres de $\mathbb{F}_q^\times$

10.1. Definición. Para un campo finito $\mathbb{F}_q$, un **carácter** (**multiplicativo**) es un homomorfismo de grupos $\chi\colon \mathbb{F}_q^\times \to \mathbb{C}^\times$.

El **carácter trivial** $\mathbb{1}\colon \mathbb{F}_q^\times \to \mathbb{C}^\times$ viene dado por $a \mapsto 1$ para todo $a \in \mathbb{F}_q^\times$. A partir de ahora será conveniente extender los caracteres a todo $\mathbb{F}_q$ poniendo

$$\chi(0) := \begin{cases} 0, & \text{si } \chi \ne \mathbb{1}, \\ 1, & \text{si } \chi = \mathbb{1}. \end{cases}$$

He aquí algunas propiedades básicas de los caracteres de $\mathbb{F}_q$:

a) los caracteres forman un grupo respecto al producto punto por punto

$$(\chi\lambda)(a) := \chi(a)\cdot\lambda(a);$$

b) para todo carácter $\chi\colon \mathbb{F}_q^\times \to \mathbb{C}^\times$ y $a \in \mathbb{F}_q^\times$ los números $\chi(a) \in \mathbb{C}^\times$ son $(q-1)$-ésimas raíces de la unidad:

$$\mu_{q-1}(\mathbb{C}) := \{z \in \mathbb{C} \mid z^{q-1} = 1\};$$

c) en particular, se tiene $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$;

d) el grupo de caracteres es cíclico de orden $q-1$:

$$\operatorname{Hom}(\mathbb{F}_q, \mathbb{C}^\times) = \operatorname{Hom}(\mathbb{F}_q, \mu_{q-1}(\mathbb{C})) \cong \operatorname{Hom}(C_{q-1}, C_{q-1}) \cong C_{q-1}.$$

10.2. Ejemplo. Si q es impar, entonces existe un solo carácter no trivial $\chi\colon \mathbb{F}_q^\times \to \mathbb{C}^\times$ que cumple $\chi^2 = \mathbb{1}$. Para $q = p$ primo este carácter se conoce como el **símbolo de Legendre**.

$$\chi(a) = \left(\frac{a}{q}\right) = \begin{cases} +1, & \text{si } a \neq 0 \text{ y } a \text{ es un cuadrado en } \mathbb{F}_q, \\ -1, & \text{si } a \neq 0 \text{ y } a \text{ no es un cuadrado en } \mathbb{F}_q, \\ 0, & \text{si } a = 0 \text{ en } \mathbb{F}_q. \end{cases}$$

Por ejemplo, -1 es un cuadrado en $\mathbb{F}_q$ si y solamente si en el grupo $\mathbb{F}_q^\times$ hay un elemento de orden 4, lo que sucede precisamente si y solo si $q \equiv 1 \pmod 4$. Entonces,

$$\chi(-1) = (-1)^{\frac{q-1}{2}}. \qquad \blacktriangle$$

10.3. Proposición. *Se tiene*

a)

$$\sum_t \chi(t) = \begin{cases} 0, & \text{si } \chi \neq \mathbb{1}, \\ q, & \text{si } \chi = \mathbb{1}, \end{cases}$$

donde χ es un carácter fijo y la suma es sobre $t \in \mathbb{F}_q$;

b)

$$\sum_\chi \chi(a) = \begin{cases} 0, & \text{si } a \neq 1, \\ q-1, & \text{si } a = 1, \end{cases}$$

donde la suma es sobre todos los caracteres de $\mathbb{F}_q^\times$.

Demostración. Si $\chi \neq \mathbb{1}$, entonces existe $a \in \mathbb{F}_q^\times$ tal que $\chi(a) \neq 1$, y la identidad

$$\chi(a) \sum_t \chi(t) = \sum_t \chi(at) = \sum_t \chi(t)$$

implica que $\sum_t \chi(t) = 0$. De manera similar en b), si $a \neq 1$, entonces existe un carácter λ tal que $\lambda(a) \neq 1$, y luego

$$\lambda(a) \sum_\chi \chi(a) = \sum_\chi \lambda\chi(a) = \sum_\chi \chi(a),$$

de donde $\sum_\chi \chi(a) = 0$. ■

10.4. Comentario. A partir de ahora todas las sumas de la forma "$\sum_t(\cdots)$" se entenderán como sumas sobre $t \in \mathbb{F}_q$.

10.5. Proposición. *Para $a \in \mathbb{F}_q$ el número de soluciones de la ecuación $x^n = a$ en $\mathbb{F}_q$ es igual a $\sum_{\chi^d = \mathbb{1}} \chi(a)$, donde $d = \operatorname{mcd}(n, q-1)$ y la suma es sobre todos los caracteres que satisfacen $\chi^d = \mathbb{1}$.*

Demostración. Notamos que en total hay d caracteres χ que satisfacen $\chi^d = \mathbb{1}$. Estos vienen dados por

$$\chi_i\colon c \mapsto \zeta_d^i, \quad i = 0, \ldots, d-1,$$

donde c es un generador de $\mathbb{F}_q^\times$. En particular, $\chi_0 = \mathbb{1}$.

Si $a = 0$, entonces la ecuación $x^n = a$ tiene una solución única $x = 0$. Por otra parte,

$$\chi_0(0) + \chi_1(0) + \cdots + \chi_{d-1}(0) = 1$$

(gracias a nuestra convención de que $\mathbb{1}(0) = 1$).

Ahora si $a \neq 0$, podemos escribir $a = c^m$ para algún $m = 0, \ldots, q-2$. La ecuación $x^n = c^m$ tiene soluciones $x = c^k$, donde $nk \equiv m \pmod{q-1}$. Si $d \mid m$, entonces hay precisamente d soluciones; si $d \nmid m$, entonces no hay soluciones. Calculamos

$$\sum_{0 \le i \le d-1} \chi_i(a) = \sum_{0 \le i \le d-1} (\zeta_d^m)^i.$$

Si $d \mid m$, la suma nos da d; si $d \nmid m$, entonces la suma es igual a $\frac{(\zeta_d^m)^d - 1}{\zeta_d^m - 1} = 0$. ∎

11 Sumas de Gauss

11.1. Definición. Para $a \in \mathbb{F}_q$ y un carácter χ, la expresión

$$g_a(\chi) := \sum_t \chi(t)\, \psi(at), \quad \text{donde } \psi(a) := \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(a)} := \exp\left(\frac{2\pi i}{p}\, T_{\mathbb{F}_q/\mathbb{F}_p}(a)\right)$$

se llama una **suma de Gauss**. En particular, para $a = 1$ se escribe

$$g(\chi) := g_1(\chi) := \sum_t \chi(t)\, \psi(t).$$

Note que el número $\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(a)}$ está bien definido, dado que $T_{\mathbb{F}_q/\mathbb{F}_p}(a) \in \mathbb{F}_p$.

Apuntemos algunas propiedades básicas de la aplicación ψ de arriba.

11.2. Lema. *La aplicación $\psi\colon \mathbb{F}_q \to \mathbb{C}$ definida por $\psi(a) := \zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(a)}$ satisface las siguientes propiedades.*

a) $\psi(a+b) = \psi(a)\,\psi(b)$*;*

b) $\psi(a) \neq 1$ *para algún* $a \in \mathbb{F}_q$*;*

c) $\sum_a \psi(a) = 0$*;*

d) $\sum_a \psi(a(x-y))) = \delta(x,y)\, q = \begin{cases} q, & \text{si } x = y, \\ 0, & \text{si } x \neq y. \end{cases}$

Demostración. a) se sigue de la aditividad de $T_{\mathbb{F}_q/\mathbb{F}_p}\colon \mathbb{F}_q \to \mathbb{F}_p$, mientras que b) se sigue de la sobreyectividad. En c), podemos escoger $b \in \mathbb{F}_q$ tal que $\psi(b) \neq 1$, y luego

$$\psi(b) \sum_a \psi(a) = \sum_a \psi(ba) = \sum_a \psi(a),$$

así que $\sum_a \psi(a) = 0$. La fórmula d) se sigue de c). ∎

11.3. Proposición. *Si $a \neq 0$, entonces*

$$g_a(\chi) = \begin{cases} \chi(a^{-1})\, g(\chi), & \text{si } \chi \neq \mathbb{1}, \\ 0, & \text{si } \chi = \mathbb{1}. \end{cases}$$

Si $a = 0$, entonces

$$g_0(\chi) = \begin{cases} 0, & \text{si } \chi \neq \mathbb{1}, \\ q, & \text{si } \chi = \mathbb{1}. \end{cases}$$

Demostración. Primero calculamos que para $a \neq 0$

$$\chi(a)\, g_a(\chi) = \chi(a) \sum_t \chi(t)\, \psi(at) = \sum_t \chi(at)\, \psi(at) = g(\chi).$$

Si $\chi = \mathbb{1}$, entonces

$$g_a(\mathbb{1}) = \sum_t \psi(at) = \sum_b \psi(b) = 0.$$

En fin, en el caso de $a = 0$ nos queda

$$g_0(\chi) = \sum_t \chi(t).$$

■

11.4. Proposición. *Si $\chi \neq \mathbb{1}$, entonces*

$$|g(\chi)| = \sqrt{q}.$$

Demostración. Primero, calculamos que para todo $a \neq 0$ se tiene

$$g_a(\chi)\, \overline{g_a(\chi)} = \chi(a^{-1})\, g(\chi)\, \overline{\chi(a^{-1})\, g(\chi)} = g(\chi)\, \overline{g(\chi)} = |g(\chi)|^2.$$

Por otra parte, $g_0(\chi) = 0$. Entonces, tomando la suma sobre $a \in \mathbb{F}_q$, se obtiene

$$\sum_a g_a(\chi)\, \overline{g_a(\chi)} = (q-1)\, |g(\chi)|^2.$$

También podemos calcular directamente

$$\sum_a g_a(\chi)\, \overline{g_a(\chi)} = \sum_a \left(\sum_x \chi(x)\, \psi(ax)\right) \overline{\left(\sum_y \chi(y)\, \psi(ay)\right)} = \sum_{x,y} \chi(x)\, \overline{\chi(y)} \sum_a \psi(a\,(x-y)) = \sum_{x,y} \chi(x)\, \overline{\chi(y)}\, \delta(x,y)\, q = (q-1)\, q.$$

Nos queda comparar las dos expresiones para $\sum_a g_a(\chi)\, \overline{g_a(\chi)}$. ■

11.5. Corolario. *Si $\chi \neq \mathbb{1}$, entonces*

$$g(\chi^{-1})\, g(\chi) = \chi(-1)\, q.$$

Demostración. Primero se tiene

$$g(\chi^{-1}) = \chi(-1)^2\, g(\chi^{-1}) = \chi(-1) \sum_t \chi(t)^{-1}\, \psi(-t) = \chi(-1)\, \overline{g(\chi)}.$$

Luego,

$$g(\chi^{-1})\, g(\chi) = \chi(-1)\, g(\chi)\, \overline{g(\chi)} = \chi(-1)\, q.$$

■

11.6. Ejemplo. Consideremos el campo $\mathbb{F}_9 = \mathbb{F}_3[\alpha]/(\alpha^2+1)$. El grupo $\mathbb{F}_9^\times$ es cíclico, generado, por ejemplo, por $\alpha+1$. Sea $\chi\colon \mathbb{F}_9^\times \to \{\pm 1\}$ el carácter cuadrático (definido por $\chi(\alpha+1) = -1$).

a:	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
$T_{\mathbb{F}_9/\mathbb{F}_3}(a)$:	0	2	1	0	2	1	0	2	1
$\chi(a)$:	0	$+1$	$+1$	$+1$	-1	-1	$+1$	-1	-1

Ahora

$$g(\chi) = \zeta_3^2 + \zeta_3 + 1 - \zeta_3^2 - \zeta_3 + 1 - \zeta_3^2 - \zeta_3 = 3.$$

▲

11.7. Ejemplo. En general, para q impar, sea χ el carácter cuadrático de $\mathbb{F}_q^\times$. Usando 11.5, se obtiene

$$g(\chi)^2 = \chi(-1)\, q = (-1)^{\frac{q-1}{2}}\, q.$$

Esto determina a $g(\chi)$ salvo el signo. Un resultado clásico del mismo Gauss dice que para $q = p$ primo se tiene

$$g(\chi) = \sum_{0 \le t \le p-1} \left(\frac{t}{p}\right) \zeta_p^t = \begin{cases} \sqrt{p}, & \text{si } p \equiv 1 \pmod 4, \\ i\sqrt{p}, & \text{si } p \equiv 3 \pmod 4) \end{cases}$$

—véase [IR1990, §6.4]. ▲

12 Sumas de Jacobi

12.1. Definición. Para caracteres $\chi_1,\ldots,\chi_r$ la **suma de Jacobi** correspondiente viene dada por

$$J(\chi_1,\ldots,\chi_r) := \sum_{t_1+\cdots+t_r=1} \chi_1(t_1)\cdots\chi_r(t_r).$$

Aquí la suma es sobre $t_1,\ldots,t_r \in \mathbb{F}_q$ que cumplen $t_1+\cdots+t_r=1$.

De modo similar, pongamos

$$J_0(\chi_1,\ldots,\chi_r) := \sum_{t_1+\cdots+t_r=0} \chi_1(t_1)\cdots\chi_r(t_r).$$

12.2. Comentario. Las sumas de Gauss $g(\chi)$ y de Jacobi $J(\chi_1,\ldots,\chi_r)$ son ciertas sumas de raíces de la unidad, así que son números algebraicos.

Primero hagamos un pequeño cálculo con la suma de Jacobi de dos caracteres.

12.3. Lema. *Para $\chi \ne \mathbb{1}$ se tiene*

$$J(\chi,\chi^{-1}) = -\chi(-1).$$

Demostración.

$$J(\chi,\chi^{-1}) = \sum_{a+b=1} \chi(a)\,\chi(b^{-1}) = \sum_{a\ne 1} \chi\Bigl(\frac{a}{1-a}\Bigr) = \sum_{c\ne -1} \chi(c) = -\chi(-1).$$ ■

12.4. Ejemplo. Asumamos que q es impar. Sea χ el carácter cuadrático de $\mathbb{F}_q^\times$. Luego, el número de soluciones de la ecuación $x^2=a$ es igual a $1+\chi(a)$. Entonces, para el número de soluciones de $x^2+y^2=1$ se tiene

$$\begin{aligned} N(x^2+y^2=1) &= \sum_{a+b=1} N(x^2=a)\,N(x^2=b) = \sum_{a+b=1} (1+\chi(a))\,(1+\chi(b)) \\ &= q + \sum_a \chi(a) + \sum_b \chi(b) + \sum_{a+b=1} \chi(a)\,\chi(b) = q + J(\chi,\chi) = q - \chi(-1) = q - (-1)^{\frac{q-1}{2}}. \end{aligned}$$

Podemos concluir que

$$N(x^2+y^2=1) = \begin{cases} q-1, & q \equiv 1 \pmod 4, \\ q+1, & q\equiv 3 \pmod 4. \end{cases}$$

El resultado, por supuesto, coincide con lo que vimos en 9.12. ▲

Vamos a generalizar el último cálculo al caso de sumas de r cuadrados, pero primero necesitamos analizar algunas propiedades de las sumas de Jacobi.

12.5. Proposición.

a) Para los caracteres triviales se tiene

$$J(\mathbb{1},\ldots,\mathbb{1}) = J_0(\mathbb{1},\ldots,\mathbb{1}) = q^{r-1}.$$

b) Si algunos, pero no todos los χ_i son triviales, entonces

$$J(\chi_1,\ldots,\chi_r) = J_0(\chi_1,\ldots,\chi_r) = 0.$$

c) Si $\chi_r \ne \mathbb{1}$, entonces

$$J_0(\chi_1,\ldots,\chi_r) = \begin{cases} 0, & \text{si } \chi_1\cdots\chi_r \ne \mathbb{1}, \\ \chi_r(-1)\,(q-1)\,J(\chi_1,\ldots,\chi_{r-1}), & \text{si } \chi_1\cdots\chi_r = \mathbb{1}. \end{cases}$$

Demostración. La parte a) es evidente: note que el hiperplano $t_1 + \cdots + t_r = c$ en $\mathbb{A}^r(\mathbb{F}_q)$ contiene q^{r-1} puntos.

En la parte b), asumamos que $\chi_1, \ldots, \chi_s \neq \mathbb{1}$, mientras que $\chi_{s+1} = \cdots = \chi_r = \mathbb{1}$. Entonces,

$$J(\chi_1, \ldots, \chi_r) = \sum_{t_1 + \cdots + t_r = 1} \chi_1(t_1) \cdots \chi_r(t_r) = \sum_{t_1, \ldots, t_{r-1}} \chi_1(t_1) \cdots \chi_s(t_s) = q^{r-s-1} \left(\sum_{t_1} \chi_1(t_1)\right) \cdots \left(\sum_{t_s} \chi_s(t_s)\right) = 0,$$

usando que $\sum_t \chi(t) = 0$. El cálculo para $J_0(\chi_1, \ldots, \chi_r)$ es similar.

En la parte c), primero escribamos

$$J_0(\chi_1, \ldots, \chi_r) = \sum_u \left(\sum_{t_1 + \cdots + t_{r-1} = -u} \chi_1(t_1) \cdots \chi_{r-1}(t_{r-1}) \right) \chi_r(u).$$

Dado que $\chi_r(0) = 0$, podemos asumir que $u \neq 0$ en la suma. Hagamos la sustitución $t_i = -u t_i'$:

$$\begin{aligned} J_0(\chi_1, \ldots, \chi_r) &= \sum_{u \neq 0} \chi_1 \cdots \chi_{r-1}(-u) \left(\sum_{t_1' + \cdots + t_{r-1}' = 1} \chi_1(t_1') \cdots \chi_{r-1}(t_{r-1}') \right) \chi_r(u) \\ &= J(\chi_1, \ldots, \chi_{r-1}) \cdot \chi_1 \cdots \chi_{r-1}(-1) \cdot \sum_{u \neq 0} \chi_1 \cdots \chi_r(u). \end{aligned}$$

Basta recordar que la última suma es nula si $\chi_1 \cdots \chi_r \neq \mathbb{1}$, y es igual a $q - 1$ si $\chi_1 \cdots \chi_r = \mathbb{1}$. ■

Las sumas de Gauss y Jacobi están relacionadas de la siguiente manera.

12.6. Proposición. *Si $\chi_1, \ldots, \chi_r \neq \mathbb{1}$, entonces*

$$g(\chi_1) \cdots g(\chi_r) = \begin{cases} J(\chi_1, \ldots, \chi_r)\, g(\chi_1 \cdots \chi_r), & \text{si } \chi_1 \cdots \chi_r \neq \mathbb{1}, \\ \chi_r(-1) \cdot q \cdot J(\chi_1, \ldots, \chi_{r-1}), & \text{si } \chi_1 \cdots \chi_r = \mathbb{1}. \end{cases}$$

Demostración. Escribamos

$$g(\chi_1) \cdots g(\chi_r) = \left(\sum_{t_1} \chi_1(t_1)\, \psi(t_1)\right) \cdots \left(\sum_{t_r} \chi_r(t_r)\, \psi(t_r)\right) = \sum_u \left(\sum_{t_1 + \cdots + t_r = u} \chi_1(t_1) \cdots \chi_r(t_r) \right) \psi(u).$$

Primero asumamos que $\chi_1 \cdots \chi_r \neq \mathbb{1}$. En este caso podemos asumir que $u \neq 0$ en la suma, dado que

$$\sum_{t_1 + \cdots + t_r = u} \chi_1(t_1) \cdots \chi_r(t_r) = J_0(\chi_1, \ldots, \chi_r) = 0.$$

La sustitución $t_i = u t_i'$ nos da

$$\begin{aligned} g(\chi_1) \cdots g(\chi_r) = \sum_u \left(\chi_1 \cdots \chi_r(u) \sum_{t_1' + \cdots + t_r' = 1} \chi_1(t_1') \cdots \chi_r(t_r') \right) \psi(u) &= J(\chi_1, \ldots, \chi_r) \sum_u \chi_1 \cdots \chi_r(u)\, \psi(u) \\ &= J(\chi_1, \ldots, \chi_r)\, g(\chi_1 \cdots \chi_r). \end{aligned}$$

Ahora asumamos que $\chi_1 \cdots \chi_r = \mathbb{1}$. En este caso $\chi_1 \cdots \chi_{r-1} \neq \mathbb{1}$, y el cálculo de arriba nos da

$$g(\chi_1) \cdots g(\chi_{r-1}) = J(\chi_1, \ldots, \chi_{r-1})\, g(\chi_1 \cdots \chi_{r-1}).$$

Luego,

$$g(\chi_1) \cdots g(\chi_r) = J(\chi_1, \ldots, \chi_{r-1})\, g(\chi_1 \cdots \chi_{r-1})\, g(\chi_r) = J(\chi_1, \ldots, \chi_{r-1})\, g(\chi_r^{-1})\, g(\chi_r).$$

Para terminar la prueba, recordemos de 11.5 que

$$g(\chi_r^{-1})\, g(\chi_r) = \chi_r(-1)\, q.$$

■

12.7. Proposición. *Si* $\chi_1,\dots,\chi_r \ne \mathbb{1}$ *y* $\chi_1\cdots\chi_r = \mathbb{1}$*, entonces*

$$J(\chi_1,\dots,\chi_r) = -\chi_r(-1)\,J(\chi_1,\dots,\chi_{r-1}),$$

donde para $r=2$ *por la definición* $J(\chi_1)=1$.

Demostración. Para $r=2$ este el el contenido de 12.3. Para $r>2$, podemos volver a la prueba de 12.6. Allí en el caso de $\chi_1\cdots\chi_r=\mathbb{1}$ se obtiene la expresión

$$g(\chi_1)\cdots g(\chi_r) = J_0(\chi_1,\dots,\chi_r) + J(\chi_1,\dots,\chi_r)\sum_{u\ne 0}\psi(u) = J_0(\chi_1,\dots,\chi_r) - J(\chi_1,\dots,\chi_r).$$

Nos queda sustituir

$$\begin{aligned} g(\chi_1)\cdots g(\chi_r) &= \chi_r(-1)\,q\,J(\chi_1,\dots,\chi_{r-1}),\\ J_0(\chi_1,\dots,\chi_r) &= \chi_r(-1)\,(q-1)\,J(\chi_1,\dots,\chi_{r-1}). \end{aligned}$$ ■

17/10/19

12.8. Ejemplo. Para q impar sea χ el carácter cuadrático de $\mathbb{F}_q^\times$. Calculemos la suma de Jacobi

$$J(\underbrace{\chi,\dots,\chi}_r).$$

Si r es impar, entonces $\chi^r=\chi$, y tenemos

$$J(\underbrace{\chi,\dots,\chi}_r) = \frac{g(\chi)^r}{g(\chi^r)} = g(\chi)^{r-1} = (g(\chi)^2)^{\frac{r-1}{2}} = (-1)^{\frac{r-1}{2}\frac{q-1}{2}}\,q^{\frac{r-1}{2}},$$

usando el cálculo de 11.7. Si r es par, entonces $\chi^r=\mathbb{1}$, y podemos escribir usando 12.7

$$J(\underbrace{\chi,\dots,\chi}_r) = -\chi(-1)\,J(\underbrace{\chi,\dots,\chi}_{r-1}) = -(-1)^{\frac{r}{2}\frac{q-1}{2}}\,q^{\frac{r}{2}-1}.$$ ▲

13 Ecuaciones $a_1x_1^{\ell_1}+\cdots+a_rx_r^{\ell_r}=b$

El siguiente resultado fue establecido de manera independiente en [Wei1949] y [HV1949].

13.1. Teorema. *Consideremos la ecuación*

$$a_1x_1^{\ell_1}+\cdots+a_rx_r^{\ell_r}=b,$$

donde $a_i\in\mathbb{F}_q^\times$ *y* $b\in\mathbb{F}_q$. *Pongamos* $d_i := \operatorname{mcd}(\ell_i,q-1)$. *Denotemos por* N *el número de soluciones de la ecuación de arriba en* $\mathbb{A}^r(\mathbb{F}_q)$.

- *Si* $b=0$*, entonces*

  $$N = q^{r-1} + \sum_{\chi_1,\dots,\chi_r}\chi_1(a_1^{-1})\cdots\chi_r(a_r^{-1})\,J_0(\chi_1,\dots,\chi_r),$$

  donde la suma es sobre las r*-tuplas* $(\chi_1,\dots,\chi_r)$ *de caracteres de* $\mathbb{F}_q^\times$ *que cumplen* $\chi_i^{d_i}=\mathbb{1}$, $\chi_i\ne\mathbb{1}$ *y* $\chi_1\cdots\chi_r=\mathbb{1}$.

- *Si* $b\ne 0$*, entonces*

  $$N = q^{r-1} + \sum_{\chi_1,\dots,\chi_r}\chi_1\cdots\chi_r(b)\,\chi_1(a_1^{-1})\cdots\chi_r(a_r^{-1})\,J(\chi_1,\dots,\chi_r),$$

  donde la suma es sobre las r*-tuplas* $(\chi_1,\dots,\chi_r)$ *de caracteres de* $\mathbb{F}_q^\times$ *que cumplen* $\chi_i^{d_i}=\mathbb{1}$, $\chi_i\ne\mathbb{1}$.

Demostración. Tenemos
$$N = \sum_{\sum a_i u_i = b} N(x_1^{\ell_1} = u_1) \cdots N(x_1^{\ell_r} = u_r).$$
Recordemos que
$$N(x_i^{\ell_i} = u_i) = \sum_{\chi_i^{d_i} = \mathbb{1}} \chi_i(u_i).$$
Entonces, podemos escribir
$$N = \sum_{\chi_1,\ldots,\chi_r} \sum_{\sum a_i u_i = b} \chi_1(u_1) \cdots \chi_r(u_r),$$
donde la primera suma es sobre los caracteres que satisfacen $\chi_i^{d_i} = \mathbb{1}$.

Ahora si $b = 0$, el cambio de variables $t_i = a_i u_i$ nos permite escribir la segunda suma como
$$\chi_1(a_1^{-1}) \cdots \chi_r(a_r^{-1}) \sum_{\sum t_i = 0} \chi_1(t_1) \cdots \chi_r(t_r) = \chi_1(a_1^{-1}) \cdots \chi_r(a_r^{-1})\, J_0(\chi_1, \ldots, \chi_r).$$
Si $b \ne 0$, el cambio de variables $t_i = b^{-1} a_i u_i$ nos da
$$\chi_1 \cdots \chi_r(b)\, \chi_1(a_1^{-1}) \cdots \chi_r(a_r^{-1})\, J(\chi_1, \ldots, \chi_r).$$
Recordemos de 12.5 que en ambos casos, el término que corresponde a $\chi_1 = \cdots = \chi_r = \mathbb{1}$ contribuye
$$J_0(\underbrace{\mathbb{1}, \ldots, \mathbb{1}}_r) = J(\underbrace{\mathbb{1}, \ldots, \mathbb{1}}_r) = q^{r-1}.$$
Si algunos, pero no todos los χ_i son triviales, el término correspondiente será nulo. Además, se tiene $J_0(\chi_1, \ldots, \chi_r) = 0$ si $\chi_1 \cdots \chi_r \ne \mathbb{1}$. ∎

13.2. Corolario. *Consideremos una hipersuperficie proyectiva $X \subset \mathbb{P}^n_{\mathbb{F}_q}$ definida por la ecuación*
$$a_0 x_0^\ell + a_1 x_1^\ell + \cdots + a_n x_n^\ell = 0,$$
donde $a_i \in \mathbb{F}_q$. Luego,
$$\# X(\mathbb{F}_q) = q^{n-1} + q^{n-2} + \cdots + q + 1 + \frac{1}{q-1} \sum_{\chi_0,\ldots,\chi_n} \chi_0(a_0^{-1}) \cdots \chi_n(a_n^{-1})\, J_0(\chi_0, \ldots, \chi_n),$$
donde la suma es sobre $\chi_i^d = \mathbb{1}$, $d := \operatorname{mcd}(\ell, q-1)$, $\chi_i \ne \mathbb{1}$ y $\chi_0 \chi_1 \cdots \chi_n = \mathbb{1}$.

Además, se tiene
$$\frac{1}{q-1} J_0(\chi_0, \ldots, \chi_n) = \frac{1}{q}\, g(\chi_0) \cdots g(\chi_n).$$

Demostración. Según el teorema de arriba, el número de puntos de la hipersuperficie correspondiente en $\mathbb{A}^{n+1}(\mathbb{F}_q)$ es
$$N = q^n + \sum_{\chi_0,\ldots,\chi_n} \chi_0(a_0^{-1}) \cdots \chi_n(a_n^{-1})\, J_0(\chi_0, \ldots, \chi_n),$$
y el número de los puntos proyectivos viene dado por $\frac{N-1}{q-1}$, lo que nos da la ecuación deseada.

Ahora 12.5 c y 12.6 nos permite escribir
$$\frac{1}{q-1} J_0(\chi_0, \chi_1, \ldots, \chi_n) = \chi_0(-1)\, J(\chi_1, \ldots, \chi_n) = \chi_0(-1)\, \frac{g(\chi_1) \cdots g(\chi_n)}{g(\chi_1 \cdots \chi_n)}.$$
Falta notar que, puesto que $\chi_1 \cdots \chi_n = \chi_0^{-1}$ y $\chi_0 \ne \mathbb{1}$, se tiene
$$g(\chi_0)\, g(\chi_1 \cdots \chi_n) = \chi_0(-1)\, q$$
(véase 11.5). ∎

Por supuesto, las fórmulas del teorema no son muy útiles si uno no sabe calcular las sumas de Jacobi correspondientes. En ciertos casos particulares es posible obtener una sencilla respuesta. Empecemos por un ejemplo particular con q fijo, solo para ver cómo funcionan las cosas.

13.3. Ejemplo. Consideremos la ecuación
$$x^3+y^3=1$$
sobre $\mathbb{F}_4$. El grupo $\mathbb{F}_4^\times=\{1,a,a^3\}$ consiste en 3 elementos, así que la condición $\chi_i^3=\mathbb{1}$ siempre se cumple. Hay dos caracteres no triviales definidos por
$$\chi_1\colon a\mapsto\zeta_3,\quad \chi_2\colon a\mapsto\zeta_3^2.$$
La fórmula nos da
$$4+2\,J(\chi_1,\chi_2)+J(\chi_1,\chi_1)+J(\chi_2,\chi_2).$$
Aquí
$$J(\chi_1,\chi_2)=\sum_{u+v=1}\chi_1(u)\,\chi_2(v)=\chi_1(a)\,\chi_2(a^2)+\chi_1(a^2)\,\chi_2(a)=\zeta_3^2+\zeta_3=-1.$$
De la misma manera, calculamos que
$$J(\chi_1,\chi_1)=\chi_1(a)\,\chi_1(a^2)+\chi_1(a^2)\,\chi_1(a)=2,$$
$$J(\chi_2,\chi_2)=\chi_2(a)\,\chi_2(a^2)+\chi_2(a^2)\,\chi_2(a)=2.$$
Entonces,
$$N(x^3+y^3=1)=6.$$
Y de hecho, en este caso está claro que las soluciones son
$$(1,0),\ (a,0),\ (a^2,0),\ (0,1),\ (0,a),\ (0,a^2).$$ ▲

13.4. Ejemplo. Supongamos que $a_1=\cdots=a_r=1$ y $\ell_1=\cdots=\ell_r=2$. Consideremos primero la ecuación
$$x_1^2+\cdots+x_r^2=1.$$
Hay un solo carácter $\chi\ne\mathbb{1}$ que satisface $\chi^2=\mathbb{1}$; este es el carácter cuadrático. De la fórmula del teorema nos queda simplemente
$$N(x_1^2+\cdots+x_r^2=1)=q^{r-1}+J(\underbrace{\chi,\dots,\chi}_{r}).$$
La suma de Jacobi de arriba fue calculada en 12.8. Se tiene entonces
$$N(x_1^2+\cdots+x_r^2=1)=\begin{cases}q^{r-1}-(-1)^{\frac{r}{2}\,\frac{q-1}{2}}\,q^{\frac{r}{2}-1}, & \text{si } r \text{ es par},\\ q^{r-1}+(-1)^{\frac{r-1}{2}\,\frac{q-1}{2}}\,q^{\frac{r-1}{2}}, & \text{si } r \text{ es impar.}\end{cases}$$
Notamos que para $r=2$ se recupera la fórmula de 12.4.

Ahora consideremos la ecuación afín
$$x_1^2+\cdots+x_r^2=0.$$
Si r es impar, entonces $\chi^r=\chi\ne\mathbb{1}$, y la fórmula nos da simplemente
$$N(x_1^2+\cdots+x_r^2=0)=q^{r-1}.$$
Por otra parte, si r es par, entonces la fórmula nos da
$$N(x_1^2+\cdots+x_r^2=0)=q^{r-1}+J_0(\underbrace{\chi,\dots,\chi}_{r})=q^{r-1}+\chi(-1)\,(q-1)\,J(\underbrace{\chi,\dots,\chi}_{r-1})=q^{r-1}+(q-1)\,(-1)^{\frac{r}{2}\,\frac{q-1}{2}}\,q^{\frac{r}{2}-1}.$$

$$N(x_1^2+\cdots+x_r^2=0)=\begin{cases} q^{r-1}+(q-1)\,(-1)^{\frac{r}{2}\,\frac{q-1}{2}}\,q^{\frac{r}{2}-1}, & \text{si } r \text{ es par},\\ q^{r-1}, & \text{si } r \text{ es impar}\end{cases}$$

En particular, si $r=2$, se obtiene

$$N(x^2+y^2=0)=\begin{cases} 2q-1, & \text{si } q\equiv 1 \pmod 4,\\ 1, & \text{si } q\equiv 3 \pmod 4.\end{cases}$$

Es fácil verlo directamente. Si existe una solución no trivial $(x,y)\neq(0,0)$, entonces $\left(\frac{x}{y}\right)^2=-1$, así que -1 es un cuadrado en $\mathbb{F}_q$. Esto sucede si y solo si $q\equiv 1 \pmod 4$, y en este caso la ecuación se factoriza como $(x-i\,y)\,(x+i\,y)=0$ y se ve fácilmente que hay $2q-1$ soluciones. ▲

14 Relación de Hasse–Davenport y la función zeta de $a_0x_0^\ell+\cdots+a_nx_n^\ell=0$

En 13.2 hemos obtenido la fórmula para el número de puntos en la hipersuperficie proyectiva

$$a_0x_0^\ell+a_1x_1^\ell+\cdots+a_nx_n^\ell=0.$$

A saber,

$$\#X(\mathbb{F}_q)=q^{n-1}+q^{n-2}+\cdots+q+1+\frac{1}{q}\sum_{\chi_0,\ldots,\chi_n}\chi_0(a_0^{-1})\cdots\chi_n(a_n^{-1})\,g(\chi_0)\cdots g(\chi_n), \tag{14.1}$$

donde la suma es sobre $\chi_i^d=\mathbb{1}$, $d:=\operatorname{mcd}(\ell,q-1)$, $\chi_i\neq\mathbb{1}$ y $\chi_0\chi_1\cdots\chi_n=\mathbb{1}$.

Para calcular la función zeta, necesitamos saber cómo este número cambia al pasar de $\mathbb{F}_q$ a una extensión $\mathbb{F}_{q^m}/\mathbb{F}_q$. Notamos que todo carácter $\chi\colon\mathbb{F}_q^\times\to\mathbb{C}^\times$ da lugar a un carácter de $\mathbb{F}_{q^m}$:

$$\begin{tikzcd} \mathbb{F}_{q^m}^\times \arrow[r, "N_{\mathbb{F}_{q^m}/\mathbb{F}_q}"] \arrow[rr, bend right, "\chi'"'] & \mathbb{F}_q^\times \arrow[r, "\chi"] & \mathbb{C}^\times \end{tikzcd}$$

De las propiedades de la norma se deduce que

a) si $\chi_1\neq\chi_2$, entonces $\chi_1'\neq\chi_2'$ (por la sobreyectividad de la norma);

b) si $\chi^d=\mathbb{1}$, entonces $\chi'^d=\mathbb{1}$;

c) $\chi'(a)=\chi(a)^m$ para todo $a\in\mathbb{F}_q$.

Ahora para asegurarnos que

$$d=\operatorname{mcd}(\ell,q-1)=\operatorname{mcd}(\ell,q^m-1),$$

vamos a asumir que $\ell\mid(q-1)$; es decir, que $d=\ell$. Hay d caracteres de $\mathbb{F}_q$ que cumplen $\chi^d=\mathbb{1}$ y d caracteres de $\mathbb{F}_{q^m}$ con la misma propiedad. Tenemos una biyección

$$\{\chi\colon\mathbb{F}_q^\times\to\mathbb{C}^\times\mid\chi^d=\mathbb{1}\}\cong\{\chi'\colon\mathbb{F}_{q^m}^\times\to\mathbb{C}^\times\mid\chi'^d=\mathbb{1}\},$$

dada por $\chi\mapsto\chi':=\chi\circ N$. Gracias a todo esto, la fórmula (14.1) nos da

$$\#X(\mathbb{F}_{q^m})=q^{m(n-1)}+q^{m(n-2)}+\cdots+q^m+1+\frac{1}{q^m}\sum_{\chi_0,\ldots,\chi_n}\chi_0(a_0^{-1})^m\cdots\chi_n(a_n^{-1})^m\,g(\chi_0')\cdots g(\chi_n'),$$

donde la suma es todavía sobre los caracteres de $\mathbb{F}_q$. Falta solo entender la relación entre las sumas de Gauss

$$g(\chi'):=\sum_{t\in\mathbb{F}_{q^m}}\chi'(t)\,\zeta_p^{T_{\mathbb{F}_{q^m}/\mathbb{F}_p}(t)}\quad\text{y}\quad g(\chi):=\sum_{t\in\mathbb{F}_q}\chi(t)\,\zeta_p^{T_{\mathbb{F}_q/\mathbb{F}_p}(t)}.$$

La respuesta está en el siguiente resultado.

14.1. Proposición (Relación de Hasse–Davenport [DH1935]). *Para un carácter $\chi\colon \mathbb{F}_q^\times \to \mathbb{C}^\times$ y el carácter correspondiente $\chi'\colon \mathbb{F}_{q^m}^\times \to \mathbb{C}^\times$ se tiene*

$$-g(\chi') = (-g(\chi))^m.$$

Demostración. La prueba no es difícil, pero algo trabajosa; véase [IR1990, §11.4] o [Wei1949]. ∎

Usando la relación de Hasse–Davenport, podemos escribir

$$\#X(\mathbb{F}_{q^m}) = q^{m(n-1)} + q^{m(n-2)} + \cdots + q^m + 1 + (-1)^{n+1} \sum_{\chi_0,\ldots,\chi_n} \left(\frac{(-1)^{n+1}}{q}\,\chi_0(a_0^{-1})\cdots\chi_n(a_n^{-1})\,g(\chi_0)\cdots g(\chi_n)\right)^m.$$

Calculamos la serie

$$\exp\left(\sum_{\chi_0,\ldots,\chi_n}\left(\frac{(-1)^{n+1}}{q}\,\chi_0(a_0^{-1})\cdots\chi_n(a_n^{-1})\,g(\chi_0)\cdots g(\chi_n)\right)^m \frac{t^m}{m}\right)$$
$$= \prod_{\chi_0,\ldots,\chi_n}\left(1 - \frac{(-1)^{n+1}}{q}\,\chi_0(a_0^{-1})\cdots\chi_n(a_n^{-1})\,g(\chi_0)\cdots g(\chi_n)\,t\right)^{-1}.$$

Todos estos cálculos nos llevan al siguiente resultado.

14.2. Teorema. *Consideremos una hipersuperficie proyectiva $X \subset \mathbb{P}^n_{\mathbb{F}_q}$ definida por la ecuación*

$$a_0 x_0^\ell + a_1 x_1^\ell + \cdots + a_n x_n^\ell = 0,$$

donde $a_i \in \mathbb{F}_q$ y $\ell \mid (q-1)$. Luego,

$$Z(X,t) = \frac{P(t)^{(-1)^n}}{(1-q^{n-1}t)\cdots(1-qt)(1-t)},$$

donde

$$P(t) = \prod_{\chi_0,\ldots,\chi_n}\left(1 - \frac{(-1)^{n+1}}{q}\,\chi_0(a_0^{-1})\cdots\chi_n(a_n^{-1})\,g(\chi_0)\cdots g(\chi_n)\,t\right),$$

y el producto es sobre $\chi_i^\ell = \mathbb{1}$, $\chi_i \ne \mathbb{1}$ y $\chi_0\chi_1\cdots\chi_n = \mathbb{1}$.

14.3. Comentario. Escribamos $P(t) = \prod_i (1-\alpha_i t)$. Los números α_i tienen forma

$$\alpha_i = \pm\zeta_i\,\frac{1}{q}\,g(\chi_0)\cdots g(\chi_n),$$

donde ζ_i es una raíz $(q-1)$-ésima de la unidad. Puesto que $|g(\chi_i)| = \sqrt{q}$, se sigue que

$$|\alpha_i| = q^{(n-1)/2}.$$

Además, gracias a 12.6 se puede escribir

$$\frac{1}{q}\,g(\chi_0)\cdots g(\chi_n) = \chi_n(-1)\cdot J(\chi_0,\ldots,\chi_{n-1}),$$

donde $J(\chi_0,\ldots,\chi_{n-1})$ es un entero algebraico. Entonces, los α_i son enteros algebraicos.

14.4. Ejemplo. Para q impar consideremos la hipersuperficie proyectiva sobre $\mathbb{F}_q$ definida por la ecuación

$$X\colon\ a_0\,x_0^2 + \cdots + a_n\,x_n^2 = 0.$$

Sea χ el carácter cuadrático de $\mathbb{F}_q^\times$. Si n es par, entonces $\chi^{n+1} = \chi \ne \mathbb{1}$, y se tiene $P(t) = 1$, así que

$$Z(X,t) = \frac{1}{(1-q^{n-1}\,t)\cdots(1-q\,t)\,(1-t)} = Z(\mathbb{P}^{n-1}_{\mathbb{F}_q}, t).$$

Por otra parte, si n es impar, las cosas se vuelven más interesantes: se tiene

$$P(t) = 1 - \frac{1}{q}\,\chi(a_0\cdots a_n)\,g(\chi)^{n+1}\,t.$$

En este caso

$$g(\chi)^{n+1} = (g(\chi)^2)^{\frac{n+1}{2}} = (-1)^{\frac{q-1}{2}\,\frac{n+1}{2}}\,q^{\frac{n+1}{2}}$$

(véase 11.5), y entonces la función zeta tiene forma

$$Z(X,t) = \frac{1}{(1-q^{n-1}\,t)\cdots(1-q\,t)\,(1-t)\left(1+(-1)^{\frac{q-1}{2}\,\frac{n-1}{2}}\,\chi(a_0\cdots a_n)\,q^{\frac{n-1}{2}}\,t\right)}.$$

Aquí la expresión $(-1)^{\frac{q-1}{2}\,\frac{n-1}{2}}\,\chi(a_0\cdots a_n)$ es un signo que depende del resto de q y n módulo 4 y también de cuántos números entre $a_0,\ldots,a_n$ son cuadrados en $\mathbb{F}_q$.

Por ejemplo, si $n = 3$ y $q = 3$, y la ecuación es

$$x_0^2 + x_1^2 + x_2^2 + 2x_3^2 = 0,$$

entonces la función zeta será (note que 2 no es un cuadrado módulo 3)

$$\frac{1}{(1-9t)\,(1-3t)\,(1-t)\,(1+3t)}.$$

```
? Z = 1 / ((1-9*t)*(1-3*t)*(1-t)*(1+3*t));
? vector (10, m, polcoeff(m*log (Z),m))
% = [10, 100, 730, 6724, 59050, 532900, 4782970, 43059844, 387420490, 3486902500]
```

▲

14.5. Ejemplo. Consideremos la hipersuperficie proyectiva sobre $\mathbb{F}_4$ definida por la ecuación

$$X\colon\, x_0^3 + x_1^3 + x_2^3 = 0.$$

Según el resultado general, se tiene

$$Z(X,t) = \frac{P(t)}{(1-t)\,(1-4t)},$$

donde

$$P(t) = \prod_{\chi_0,\chi_1,\chi_2}\left(1 + \frac{1}{4}\,g(\chi_0)\,g(\chi_1)\,g(\chi_2)\,t\right),$$

y el producto es sobre (χ_0,χ_1,χ_2) que cumplen $\chi_i^3 = \mathbb{1}$, $\chi_i \ne \mathbb{1}$, $\chi_0\chi_1\chi_2 = \mathbb{1}$. Hay dos caracteres no triviales de $\mathbb{F}_4^\times$:

$$\chi_1\colon\, a \mapsto \zeta_3, \quad \chi_2\colon\, a \mapsto \zeta_3^2.$$

Entonces,

$$P(t) = \left(1 + \frac{1}{4}\,g(\chi_1)^3\,t\right)\left(1 + \frac{1}{4}\,g(\chi_2)^3\,t\right).$$

Falta calcular las sumas de Gauss.

	1	a	a^2
χ_1:	1	ζ_3	ζ_3^2
χ_2:	1	ζ_3^2	ζ_3
$T_{\mathbb{F}_4/\mathbb{F}_2}$:	0	1	1

Se tiene

$$g(\chi_1) = 1 - \zeta_3 - \zeta_3^2 = 2, \quad g(\chi_2) = 1 - \zeta_3^2 - \zeta_3 = 2$$

y

$$P(t) = \left(1 + \frac{1}{4}\, 2^3\, t\right)^2 = (1+2t)^2.$$

La función zeta es entonces

$$Z(X,t) = \frac{(1+2t)^2}{(1-t)\,(1-4t)}.$$

A posteriori, uno puede notar que el número de puntos viene dado por una fórmula bastante sencilla:

$$\begin{aligned}
\#X(\mathbb{F}_4) &= 9 = (2+1)^2,\\
\#X(\mathbb{F}_{4^2}) &= 9 = (2^2-1)^2,\\
\#X(\mathbb{F}_{4^3}) &= 81 = (2^3+1)^2,\\
\#X(\mathbb{F}_{4^4}) &= 225 = (2^4-1)^2,\\
\#X(\mathbb{F}_{4^5}) &= 1089 = (2^5+1)^2,\\
\#X(\mathbb{F}_{4^6}) &= 3969 = (2^6-1)^2,\\
&\cdots
\end{aligned}$$

```
? Z = (1+2*t)^2 / ((1-t)*(1-4*t));
? vector (10, m, polcoeff(m*log(Z),m))
% = [9, 9, 81, 225, 1089, 3969, 16641, 65025, 263169, 1046529]
? vector (10, m, if (m%2 == 1, (2^m+1)^2, (2^m-1)^2))
% = [9, 9, 81, 225, 1089, 3969, 16641, 65025, 263169, 1046529]
```

Sin embargo, no es tan fácil llegar a este resultado sin usar las sumas de Gauss o Jacobi. ▲

14.6. Comentario. La función zeta de una curva puede ser calculada en el programa Magma*.

```
> P<x,y,z> := ProjectiveSpace(GF(4),2);
> ZetaFunction(Curve(P,x^3+y^3+z^3))
(4*t^2 + 4*t + 1)/(4*t^2 - 5*t + 1)
```

14.7. Comentario. Hemos calculado la función zeta de $x^3+y^3+z^3=0$ sobre $\mathbb{F}_4$ y no sobre $\mathbb{F}_2$ porque el argumento con levantamiento de caracteres de $\mathbb{F}_q$ a $\mathbb{F}_{q^m}$ es válido solo cuando $\ell \mid (q-1)$. Sin embargo, este es precisamente el caso más interesante: si $\ell \nmid (q-1)$, entonces la aplicación

$$\mathbb{F}_q^\times \to \mathbb{F}_q^\times, \quad x \mapsto x^\ell$$

es un automorfismo, y todo elemento de $\mathbb{F}_q^\times$ es una ℓ-ésima potencia, así que el número de puntos sobre la hipersuperficie $\sum_i a_i x_i^\ell = 0$ es el mismo que sobre el hiperplano $\sum_i a_i x_i = 0$.

Por ejemplo, si n es impar, entonces $2^n - 1 \equiv 1 \pmod 3$, así que todo elemento en $\mathbb{F}_{2^n}$ es un cubo. Por esto se tiene

$$\#X(\mathbb{F}_{2^n}) = \frac{(2^n)^2-1}{2^n-1} = 2^n+1.$$

*http://magma.maths.usyd.edu.au/calc/

La función generatriz para 2^n con n par ya fue calculada:

$$Z(X/\mathbb{F}_4, t^2)^{1/2} = \frac{1+2t^2}{(1-t^2)^{1/2}\,(1-4t^2)^{1/2}} = \exp\left(\frac{\#X(\mathbb{F}_{2^2})}{2}\,t^2 + \frac{\#X(\mathbb{F}_{2^4})}{4}\,t^4 + \frac{\#X(\mathbb{F}_{2^6})}{6}\,t^6 + \cdots\right).$$

La parte impar corresponde a la función generatriz

$$\exp\left(\sum_{m\ge 0} \frac{2^{2m+1}+1}{2m+1}\,t^{2m+1}\right) = \exp\left(\sum_{m\ge 0} \frac{(2t)^{2m+1}}{2m+1}\right) \exp\left(\sum_{m\ge 0} \frac{t^{2m+1}}{2m+1}\right) = \frac{(1+2t)^{1/2}}{(1-2t)^{1/2}}\,\frac{(1+t)^{1/2}}{(1-t)^{1/2}}.$$

Entonces,

$$Z(X/\mathbb{F}_2, t) = \frac{1+2t^2}{(1-t^2)^{1/2}\,(1-4t^2)^{1/2}}\,\frac{(1+2t)^{1/2}}{(1-2t)^{1/2}}\,\frac{(1+t)^{1/2}}{(1-t)^{1/2}} = \frac{1+2t^2}{(1-t)\,(1-2t)}.$$

La relación de 9.7 nos da en este caso

$$Z(X/\mathbb{F}_4, t^2) = Z(X/\mathbb{F}_2, t)\,Z(X/\mathbb{F}_2, -t).$$

15 Curvas elípticas $y^2z = x^3 + Dz^3$

22/10/19

Consideremos la curva elíptica definida por la ecuación

$$E\colon\ y^2 z = x^3 + Dz^3,$$

El discriminante en este caso es $\Delta = -2^4\cdot 3^3\cdot D^2$, y la curva es lisa para $\operatorname{char}\mathbb{F}_q \ne 2,3$ y $\operatorname{char}\mathbb{F}_q \nmid D$.

Asumamos que $D \in \mathbb{F}_q^\times$, que q es impar y $q \equiv 1 \pmod 3$. Para contar el número de puntos, basta considerar la ecuación afín correspondiente

$$y^2 - x^3 = D$$

y añadir el punto al infinito. La fórmula de 13.1 nos da

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{\chi_1,\chi_2} \chi_1\chi_2(D)\,\chi_2(-1)\,J(\chi_1,\chi_2),$$

donde la suma es sobre los caracteres no triviales que cumplen $\chi_1^2 = \mathbb{1}$ y $\chi_2^3 = \mathbb{1}$. Tenemos

$$J(\chi_1,\chi_2) = \frac{g(\chi_1)\,g(\chi_2)}{g(\chi_1\chi_2)},$$

y la relación de Hasse–Davenport nos da para una extensión $\mathbb{F}_{q^m}/\mathbb{F}_q$

$$J(\chi_1',\chi_2') = \frac{g(\chi_1')\,g(\chi_2')}{g((\chi_1\chi_2)')} = (-1)^{m+1}\,\frac{g(\chi_1)^m\,g(\chi_2)^m}{g(\chi_1\chi_2)^m} = (-1)^{m+1}\,J(\chi_1,\chi_2)^m.$$

Sea χ el carácter cuadrático de $\mathbb{F}_q$ y ρ un carácter cúbico. Notamos que $\rho(-1)^2 = \rho(1) = 1$, así que $\rho(-1) = 1$. Se obtiene la fórmula

$$\#E(\mathbb{F}_{q^m}) = q^m + 1 + (-1)^{m+1}\left(\chi\rho(D)\,J(\chi,\rho)\right)^m + (-1)^{m+1}\left(\chi\rho^2(D)\,J(\chi,\rho^2)\right)^m.$$

Notamos que $\chi = \overline{\chi}$ y $\rho^2 = \overline{\rho}$, así que

$$\chi\rho^2(D)\,J(\chi,\rho^2) = \overline{\chi\rho(D)\,J(\chi,\rho)}.$$

De aquí se sigue que

$$Z(E/\mathbb{F}_q, t) = \frac{(1+\alpha t)\,(1+\overline{\alpha}\,t)}{(1-t)\,(1-qt)},$$

donde

$$\alpha := \chi\rho(D)\, J(\chi,\rho).$$

Tenemos

$$|\alpha| = |\chi\rho(D)| \cdot |J(\chi,\rho)| = \frac{|g(\chi)| \cdot |g(\rho)|}{|g(\chi,\rho)|} = \sqrt{q},$$

y entonces

$$\alpha\,\overline{\alpha} = q.$$

Además, notamos que

$$\alpha + \overline{\alpha} = \#E(\mathbb{F}_q) - q - 1 \in \mathbb{Z}.$$

También es evidente que $\alpha \in \mathbb{Z}[\zeta_3] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, y luego $\alpha + \overline{\alpha} = 2\operatorname{Re}\alpha \in \mathbb{Z}$.

Todos estos cálculos nos llevan al siguiente resultado.

15.1. Teorema. *Para q impar, $q \equiv 1 \pmod 3$ consideremos la curva elíptica*

$$E/\mathbb{F}_q\colon\ y^2 z = x^3 + Dz^3,$$

donde $D \in \mathbb{F}_q^\times$. Luego, la función zeta viene dada por

$$Z(E/\mathbb{F}_q, t) = \frac{(1+\alpha t)\,(1+\overline{\alpha}t)}{(1-t)\,(1-qt)} = \frac{1+at+qt^2}{(1-t)\,(1-qt)},$$

donde

$$\alpha := \chi\rho(D)\, J(\chi,\rho).$$

Además,

$$a = \alpha + \overline{\alpha} = \#E(\mathbb{F}_q) - q - 1 \quad y \quad |a| \le 2\sqrt{q}.$$

15.2. Ejemplo. Para $q = 7$ consideremos la curva

$$E\colon\ y^2 z = x^3 + 2z^3.$$

El carácter cuadrático y cúbico vienen dados por

	1	2	3	4	5	6
χ:	$+1$	$+1$	-1	$+1$	-1	-1
ρ:	1	ζ_3^2	ζ_3	ζ_3	ζ_3^2	1

Calculamos la suma de Jacobi

$$J(\chi,\rho) = \chi(2)\,\rho(6) + \chi(3)\,\rho(5) + \chi(4)\,\rho(4) + \chi(5)\,\rho(3) + \chi(6)\,\rho(2) = 1 - \zeta_3^2 + \zeta_3 - \zeta_3 - \zeta_3^2 = 1 - 2\zeta_3^2.$$

Luego,

$$\alpha = \chi\rho(D)\, J(\chi,\rho) = \zeta_3^2 - 2\zeta_3,$$

de donde

$$a = \alpha + \overline{\alpha} = (\zeta_3^2 - 2\zeta_3) + (\zeta_3 - 2\zeta_3^2) = -\zeta_3 - \zeta_3^2 = 1.$$

La función zeta es entonces

$$Z(E/\mathbb{F}_7, t) = \frac{1+t+7t^2}{(1-t)\,(1-7t)}.$$

La curva tiene 9 puntos sobre $\mathbb{F}_7$:

$$E(\mathbb{F}_7) = \{(0:3:1), (0:4:1), (3:1:1), (3:6:1), (5:1:1), (5:6:1), (6:1:1), (6:6:1), (0:1:0)\},$$

lo que coincide con nuestro cálculo de $a = 9 - 7 - 1 = 1$. ▲

15.3. Comentario. Para una interpretación de $\chi\rho(D)\,J(\chi,\rho)$, véase [IR1990, §18.3].

15.4. Comentario. En general, la función zeta de *cualquier* curva elíptica tiene forma

$$Z(E/\mathbb{F}_q,t) = \frac{1+at+qt^2}{(1-t)\,(1-qt)},$$

donde

$$a = \#E(\mathbb{F}_q) - 1 - q.$$

La **cota de Hasse–Weil** afirma que*

$$|a| \le 2\sqrt{q}.$$

Hemos probado estas propiedades para una familia muy particular de curvas elípticas. Para más detalles sobre las curvas elípticas sobre campos finitos, véase [Sil2009, Chapter V].

16 Curvas elípticas $y^2z = x^3 - Dxz^2$

Ahora consideremos la curva elíptica definida por la ecuación

$$E\colon\ y^2z = x^3 - D\,xz^2.$$

El discriminante en este caso es $\Delta = 2^6\cdot D^3$, y la curva es lisa para $\operatorname{char}\mathbb{F}_q \ne 2$ y $\operatorname{char}\mathbb{F}_q \nmid D$. Vamos a asumir que q es impar y $D\in\mathbb{F}_q^\times$. Olvidando por el momento del punto al infinito $(0:1:0)$, podemos pasar a la curva afín correspondiente

$$C\colon\ y^2 = x^3 - D\,x.$$

Esta no tiene la forma $\sum_i a_i x_i^{\ell_i} = b$, así que nuestra técnica no funciona. Lo que podemos hacer es considerar la curva

$$C'\colon\ u^2 = v^4 + 4D.$$

Se puede verificar que está bien definido el morfismo de curvas

$$\phi\colon C' \to C,\quad (u,v)\mapsto \Bigl(\frac{1}{2}\,(u+v^2),\ \frac{1}{2}\,v\,(u+v^2)\Bigr).$$

Notamos que el punto $(0,0)$ está en la curva C, pero no está en la imagen de ϕ: puesto que

$$4D = (u-v^2)\,(u+v^2),$$

se tiene necesariamente $u+v^2\ne 0$. Podemos definir el morfismo

$$\psi\colon C\setminus\{(0,0)\}\to C',\quad (x,y)\mapsto \Bigl(2x-\frac{y^2}{x^2},\ \frac{y}{x}\Bigr).$$

Se verifica que ϕ y ψ definen una biyección entre C' y $C\setminus\{(0,0)\}$, así que será suficiente analizar el número de puntos sobre C'.

Primero, si $q\equiv 3 \pmod 4$, entonces -1 no es un cuadrado en $\mathbb{F}_q$, todo elemento de $\mathbb{F}_q^\times$ es de la forma $\pm x^2$, y todo cuadrado en $\mathbb{F}_q^\times$ es una cuarta potencia. Luego,

$$\#C'(\mathbb{F}_q) = N(u^2 = v^4+4D) = N(u^2 = v^2+4D) = q-1.$$

*En general, si $C/\mathbb{F}_q$ es una curva proyectiva, lisa, geométricamente irreducible, de género g, entonces la cota de Hasse–Weil es

$$|\#C(\mathbb{F}_q) - 1 - q| \le 2g\sqrt{q}.$$

Esto significa que la curva C tiene q puntos sobre $\mathbb{F}_q$, y luego

$$\#E(\mathbb{F}_q) = q+1, \quad \text{si } q \equiv 3 \pmod 4.$$

Asumamos ahora que $q \equiv 1 \pmod 4$. Sea χ un carácter de orden 4 de $\mathbb{F}_q^\times$. El resultado general nos dice que

$$\#C'(\mathbb{F}_q) = q + \sum_{\chi_1,\chi_2} \chi_1\chi_2(4D)\,\chi_2(-1)\,J(\chi_1,\chi_2),$$

donde la suma es sobre los caracteres no triviales que cumplen $\chi_1^2 = \mathbb{1}$ y $\chi_2^4 = \mathbb{1}$. Sea χ un carácter de orden 4 de $\mathbb{F}_q^\times$. Luego,

$$\#C'(\mathbb{F}_q) = q + \chi^3(4D)\,\chi(-1)\,J(\chi,\chi^2) + \chi^2(-1)\,J(\chi^2,\chi^2) + \chi(4D)\,\chi^3(-1)\,J(\chi^2,\chi^3)$$

(esta fórmula no depende de la elección de χ).

Notamos que $\chi(-1) = \pm 1 = \chi^3(-1)$. Bajo nuestra hipótesis de que $q \equiv 1 \pmod 4$, se tiene

$$\chi^2(-1) = +1, \quad J(\chi^2,\chi^2) = -1$$

(véase 12.8). Además, notamos que

$$J(\chi^2,\chi^3) = \overline{J(\chi,\chi^2)}.$$

Todo esto nos da la fórmula

$$\#C'(\mathbb{F}_q) = q - 1 + \overline{\chi(-4D)}\,J(\chi,\chi^2) + \chi(-4D)\,\overline{J(\chi,\chi^2)}.$$

16.1. Ejemplo. Sean $q = 5$ y $D = 1$. En este caso tenemos

	1	2	3	4
χ:	$+1$	$+i$	$-i$	-1
χ^2:	$+1$	-1	-1	$+1$

Calculamos

$$\chi(-4D) = \chi(1) = 1$$

y

$$J(\chi,\chi^2) = \chi(2)\,\chi^2(4) + \chi(3)\,\chi^2(3) + \chi(4)\,\chi^2(2) = 1 + 2i,$$

así que

$$N(u^2 = v^4 + 4) = 5 - 1 + (1+2i) + (1-2i) = 6.$$

Y en efecto, los puntos de la curva sobre $\mathbb{F}_5$ son

$$(0,1),\ (0,2),\ (0,3),\ (0,4),\ (2,0),\ (3,0).$$

Ahora pongamos $D = 2$. En este caso

$$\chi(-4D) = \chi(2) = i,$$

y luego

$$N(u^2 = v^4 + 3) = 5 - 1 - i\,(1+2i) + i\,(1-2i) = 8.$$

Los puntos correspondientes son

$$(2,1),\ (2,2),\ (2,3),\ (2,4),\ (3,1),\ (3,2),\ (3,3),\ (3,4).$$ ▲

Ahora como en la sección anterior, la relación de Hasse–Davenport nos dice que

$$J(\chi', \chi'^2) = (-1)^{m+1}\, J(\chi, \chi^2)^m,$$

lo que nos lleva a la fórmula

$$\#C'(\mathbb{F}_{q^m}) = q^m - 1 + (-1)^{m+1}\, \alpha^m + (-1)^{m+1}\, \overline{\alpha}^m,$$

donde

$$\alpha := \overline{\chi(-4D)}\, J(\chi, \chi^2).$$

Volviendo a nuestra curva elíptica, tenemos

$$\#E(\mathbb{F}_{q^m}) = q^m + 1 + (-1)^{m+1}\, \alpha^m + (-1)^{m+1}\, \overline{\alpha}^m,$$

Notamos que

$$|\alpha| = |J(\chi, \chi^2)| = \sqrt{q},$$

y luego

$$\alpha\, \overline{\alpha} = q.$$

Además, puesto que $\alpha \in \mathbb{Z}[i]$, es evidente que $\alpha + \overline{\alpha} = 2\operatorname{Re}\alpha \in \mathbb{Z}$, y también se ve que $\alpha + \overline{\alpha} = \#E(\mathbb{F}_q) - q - 1$.

16.2. Teorema. *Para q impar, $q \equiv 1 \pmod 4$, consideremos la curva elíptica*

$$E/\mathbb{F}_q\colon\ y^2 z = x^3 - Dxz^2,$$

donde $D \in \mathbb{F}_q^\times$. Luego, la función zeta viene dada por

$$Z(E/\mathbb{F}_q, t) = \frac{(1 + \alpha t)\,(1 + \overline{\alpha} t)}{(1 - t)\,(1 - qt)} = \frac{1 + at + qt^2}{(1 - t)\,(1 - qt)},$$

donde

$$\alpha := \overline{\chi(-4D)}\, J(\chi, \chi^2).$$

Además,

$$a = \alpha + \overline{\alpha} = \#E(\mathbb{F}_q) - q - 1 \quad \text{y} \quad |a| \le 2\sqrt{q}.$$

16.3. Comentario. Para una interpretación de $\overline{\chi(-4D)}\, J(\chi, \chi^2)$, véase [IR1990, §18.4].

16.4. Comentario. Las curvas que hemos considerado en esta sección y la anterior son bastante especiales: son curvas elípticas con **multiplicación compleja**.

17 Conjeturas de Weil

29/10/19

Alrededor de 1950 André Weil formuló una lista de conjeturas sobre la función zeta $Z(X, t)$.

17.1. Conjetura (Racionalidad). Para cualquier variedad $X/\mathbb{F}_q$ la función zeta es racional:

$$Z(X, t) \in \mathbb{Q}(t).$$

Esta conjetura es un análogo de la continuación meromorfa. Notamos que en todos los ejemplos que hemos visto, la función zeta era racional, lo que confirma la conjetura. La racionalidad fue probada por Dwork en [Dwo1960], usando métodos del análisis p-ádico. Uno de nuestros objetivos será entender esta prueba. Por el momento notamos que la racionalidad tiene el siguiente significado.

17.2. Proposición. *$Z(X,t)$ es una función racional si y solo si existen números complejos α_i y β_j tales que*

$$\#X(\mathbb{F}_{q^m}) = \sum_j \beta_j^m - \sum_i \alpha_i^m.$$

Demostración. Si la propiedad de arriba se cumple, entonces la función zeta correspondiente es

$$\prod_j \exp\left(\sum_{m\ge 1} \frac{(\beta_j t)^m}{m}\right) \Big/ \prod_i \exp\left(\sum_{m\ge 1} \frac{(\alpha_i t)^m}{m}\right) = \frac{\prod_i (1-\alpha_i t)}{\prod_j (1-\beta_j t)}.$$

Viceversa, si $Z(X,t) = \frac{f(t)}{g(t)}$ para algunos polinomios $f,g \in \mathbb{Q}[t]$, entonces $Z(X,0) = \frac{f(0)}{g(0)} = 1$, así que podemos normalizar f y g y asumir que $f(0) = g(0) = 1$. La función zeta se factoriza entonces como

$$Z(X,t) = \frac{\prod_i (1-\alpha_i t)}{\prod_j (1-\beta_j t)}$$

para algunos $\alpha_i, \beta_j \in \mathbb{C}$. Tomando los logaritmos formales, se obtiene

$$\sum_{m\ge 1} \frac{\#X(\mathbb{F}_{q^m})}{m}\, t^m = \sum_i \log(1-\alpha_i t) - \sum_j \log(1-\beta_j t) = \sum_{m\ge 1} \left(\sum_j \beta_j^m - \sum_i \alpha_i^m\right) \frac{t^m}{m}. \qquad \blacksquare$$

Para el resto de las conjeturas, asumamos que $X/\mathbb{F}_q$ una variedad geométricamente irreducible, proyectiva, lisa.

17.3. Conjetura (Ecuación funcional).

$$Z(X, q^{-n} t^{-1}) = \pm q^{n\cdot\chi/2}\, t^\chi\, Z(X,t),$$

donde $n = \dim X$ y $\chi = \chi(X)$ es la **característica de Euler** de X.

17.4. Comentario. Poniendo

$$\zeta_X(s) := Z(X, q^{-s}),$$

podemos reescribir la ecuación funcional como

$$\zeta_X(n-s) = \pm q^{n\chi/2 - s\chi} \cdot \zeta_X(s).$$

17.5. Comentario. La característica de Euler puede ser definida como el número de autointersección

$$\chi(X) := \Delta\cdot\Delta,$$

donde $\Delta \subset X\times X$ es la diagonal. (La misma fórmula funciona si X es una variedad diferenciable compacta y orientable.) La característica de Euler también coincide con la suma alternante de los números de Betti:

$$\chi(X) = \sum_i (-1)^i b_i(X),$$

aquí

$$b_i(X) = \dim_{\mathbb{Q}_\ell} H^i(X,\mathbb{Q}_\ell),$$

y $H^i(X,\mathbb{Q}_\ell)$ denota la **cohomología ℓ-ádica** (para un primo $\ell \ne \operatorname{char}\mathbb{F}_q$). En particular, para una curva de género g se tiene

$$\chi = 2-2g.$$

17.6. Conjetura (Hipótesis de Riemann). Se tiene

$$Z(X,t) = \frac{P_1(t)\,P_3(t)\cdots P_{2n-1}(t)}{P_0(t)\,P_2(t)\cdots P_{2n}(t)},$$

donde $P_i(t) \in \mathbb{Z}[t]$ y

$$P_i(t) = \prod_j (1 - \alpha_{ij}\,t),$$

donde α_{ij} son enteros algebraicos y $|\alpha_{ij}| = q^{i/2}$.

Además, se tiene

$$\deg P_i(t) = b_i(X).$$

En particular,

$$P_0(t) = 1 - t, \quad P_{2n}(t) = 1 - q^n\,t.$$

La conjetura de arriba se llama la hipótesis de Riemann, porque esta nos dice dónde están los ceros y polos de $Z(X,t)$ (resp. $\zeta_X(s)$).

17.7. Conjetura (Especialización). Supongamos que existen una $\mathbb{Z}$-subálgebra finitamente generada $A \subset \mathbb{C}$, un ideal primo $\mathfrak{p} \in \operatorname{Spec} A$ tal que $A/\mathfrak{p} \cong \mathbb{F}_q$ y un esquema proyectivo liso $\widetilde{X}$ sobre $\operatorname{Spec} A$ tal que

$$X \cong \widetilde{X} \times_{\operatorname{Spec} A} \operatorname{Spec}(A/\mathfrak{p}).$$

Lugo,

$$b_i(X) = b_i(\widetilde{X}(\mathbb{C})),$$

donde $\widetilde{X}(\mathbb{C})$ se considera con la topología analítica, y el número de Betti a la derecha se define de la manera habitual.

$$\begin{tikzcd}
X \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner"] & \widetilde{X} \arrow[d] \\
\operatorname{Spec} \mathbb{F}_q \arrow[r] & \operatorname{Spec} A
\end{tikzcd}$$

La ecuación funcional y especialización fueron probadas por Grothendieck y sus colaboradores usando la cohomología ℓ-ádica, desarrollada en [SGA 4] con el propósito de atacar las conjeturas de Weil. La hipótesis de Riemann representa la parte más difícil de las conjeturas, posiblemente porque su análogo clásico para la función zeta de Riemann $\zeta(s)$ no ha sido probado. La prueba para $Z(X,t)$ fue obtenida por Deligne [Del1974].

17.8. Ejemplo. Hemos visto que para el espacio proyectivo se cumple

$$Z(\mathbb{P}^n_{\mathbb{F}_q}, t) = \frac{1}{(1-t)\,(1-q\,t)\cdots(1-q^{n-1}\,t)\,(1-q^n\,t)}.$$

Cohomológicamente, esto corresponde al hecho de que

$$b_i(\mathbb{P}^n) = \begin{cases} 1, & \text{si } 0 \le i \le 2n \text{ es par}, \\ 0, & \text{en el caso contrario}. \end{cases}$$

Tenemos $\chi(\mathbb{P}^n) = n+1$, y se verifica la ecuación funcional:

$$Z(\mathbb{P}^n, q^{-n}\,t^{-1}) = \frac{1}{(1-q^{-n}\,t^{-1})\,(1-q^{-n+1}\,t^{-1})\cdots(1-t^{-1})} = \frac{q\cdot q^2\cdots q^n\cdot t^{n+1}}{(q^n\,t-1)\,(q^{n-1}\,t-1)\cdots(t-1)} = \pm q^{n\cdot(n+1)/2}\,t^{n+1}\,Z(\mathbb{P}^n,t).$$

En este caso

$$\begin{aligned}
P_0(t) &= 1 - t,\\
P_2(t) &= 1 - q\,t,\\
P_4(t) &= 1 - q^2\,t,\\
&\cdots,\\
P_{2n}(t) &= 1 - q^n\,t,
\end{aligned}$$

así que la hipótesis de Riemann sí se cumple. ▲

17.9. Ejemplo. Para las curvas elípticas, hemos visto algunos ejemplos particulares y mencionamos que en cualquier caso se tiene

$$Z(E/\mathbb{F}_q, t) = \frac{1 + at + qt^2}{(1-t)\,(1-qt)},$$

donde $a = \#E(\mathbb{F}_q) - q - 1$.

Cohomológicamente, esto se debe al hecho de que una curva elíptica compleja es un toro, así que los números de Betti no nulos son

$$b_0(E) = 1, \quad b_1(E) = 2, \quad b_2(E) = 1.$$

Por esto en el numerador aparece un polinomio de grado 2. Se tiene $\chi(E) = 0$, y la ecuación funcional es simplemente

$$Z(E, q^{-1}t^{-1}) = \frac{1 + aq^{-1}t^{-1} + q^{-1}t^{-2}}{(1 - q^{-1}t^{-1})\,(1 - t^{-1})} = \frac{qt^2 + at + 1}{(qt-1)\,(t-1)} = Z(E,t).$$

La hipótesis de Riemann significa que si escribimos

$$1 + at + qt^2 = (1 - \alpha t)\,(1 - \overline{\alpha} t),$$

entonces $\alpha\overline{\alpha} = q$, así que $|\alpha| = q^{1/2}$. ▲

18 El caso de curvas

Consideremos la fórmula del producto de Euler

$$Z(X/\mathbb{F}_q, t) = \prod_{x \in |X|} \frac{1}{1 - t^{\deg(x)}} = \prod_{x \in |X|} \Bigl(1 + t^{\deg(x)} + t^{2\deg(x)} + t^{3\deg(x)} + \cdots\Bigr).$$

Al multiplicar todos estos términos, nos sale la suma

$$Z(X/\mathbb{F}_q, t) = \sum_\alpha t^{\deg(\alpha)},$$

donde los α son sumas formales $\sum_{x\in|X|} n_x \cdot x$ con $n_x \in \mathbb{N}$ y $n_x = 0$, salvo un número finito de x, y el grado está definido por

$$\deg\Bigl(\sum_{x\in|X|} n_x \cdot x\Bigr) := \sum_{x\in|X|} n_x \cdot \deg(x).$$

En general, el grupo abeliano libre generado por los puntos cerrados de X se llama el grupo de los **0-ciclos** sobre X, y los 0-ciclos $\sum_{x\in|X|} n_x \cdot x$ con $n_x \geq 0$ se llaman **efectivos**. Entonces, la función zeta es la función generatriz de los 0-ciclos efectivos sobre X.

Divisores y el teorema de Riemann–Roch

Asumamos que $X = C$ es una curva geométricamente irreducible, proyectiva, lisa sobre $\mathbb{F}_q$. En este caso los 0-ciclos son los **divisores** sobre C, y resulta que la racionalidad de la función zeta y la ecuación funcional son consecuencias del teorema de Riemann–Roch[*], y es lo que me gustaría revisar en esta sección. Las referencias son [Lor1996, Chapter VIII] o [Ros2002, Chapter 5]. Algunos detalles sobre el teorema de Riemann–Roch también se encuentran en [Sil2009, Chapter II].

Primero, revisemos todo lo que necesitamos de los divisores sobre curvas y teorema de Riemann–Roch. Para una curva proyectiva lisa C/k denotemos por $\operatorname{Div}(C)$ el grupo de divisores sobre C:

$$\operatorname{Div}(C) := \bigoplus_{x \in |C|} \mathbb{Z} \cdot x.$$

Si para un divisor $D = \sum_x n_x \cdot x$ se tiene $n_x \ge 0$ para todo $x \in |C|$, se dice que D es **efectivo** y se escribe $D \ge 0$.

A cada función racional $f \in \overline{k}(C)^\times$ se asocia un divisor

$$\operatorname{div}(f) := \sum_{x \in |X|} v_x(f) \cdot x,$$

donde $v_x(f)$ es el “orden de anulación de f en x”. Esto nos da un homomorfismo de grupos

$$\operatorname{div}\colon \overline{k}(C)^\times \to \operatorname{Div}(C).$$

Por la definición, el **grupo de Picard** de C es el cociente de $\operatorname{Div}(C)$ por la imagen de este homomorfismo.

Las únicas funciones sin ceros o polos sobre C son constantes, así que

$$\operatorname{div}(f) = 0 \iff f \in \overline{k}^\times.$$

Tenemos entonces una sucesión exacta

$$1 \to \overline{k}^\times \to \overline{k}(C)^\times \xrightarrow{\operatorname{div}} \operatorname{Div}(C) \xrightarrow{D \mapsto [D]} \operatorname{Pic}(C) \to 0$$

Para cualquier $f \in \overline{k}(C)^\times$ se tiene $\deg(\operatorname{div}(f)) = 0$, lo que implica que si para dos divisores $D_1, D_2 \in \operatorname{Div}(C)$ se cumple $[D_1] = [D_2]$ en el grupo de Picard, entonces $\deg D_1 = \deg D_2$. En otras palabras, el homomorfismo del grado está bien definido sobre el grupo de Picard.

$$\begin{tikzcd}
\operatorname{Div}(C) \arrow[d, two heads] \arrow[dr, "\deg"] & \\
\operatorname{Pic}(C) \arrow[r, dashed, "\deg"'] & \mathbb{Z}
\end{tikzcd}$$

Pongamos

$$\operatorname{Div}^0(C) := \{D \in \operatorname{Div}(C) \mid \deg D = 0\},$$
$$\operatorname{Pic}^0(C) := \{[D] \in \operatorname{Pic}(C) \mid \deg D = 0\}.$$

Tenemos entonces una sucesión exacta

$$1 \to \overline{k}^\times \to \overline{k}(C)^\times \xrightarrow{\operatorname{div}} \operatorname{Div}^0(C) \xrightarrow{D \mapsto [D]} \operatorname{Pic}^0(C) \to 0$$

El siguiente resultado es un análogo del teorema de finitud del grupo de clases de un campo de números $F/\mathbb{Q}$ que fue mencionado en §3.

[*] Por otra parte, la hipótesis de Riemann es un asunto más complicado y no la vamos a probar en estos apuntes.

18.1. Teorema. *Para una curva proyectiva lisa $C/\mathbb{F}_q$ el grupo $\operatorname{Pic}^0(C)$ es finito.*

Demostración. Véase por ejemplo [Lor1996, Theorem 7.13]. ∎

El resultado de abajo es el teorema de Riemann–Roch para curvas y algunas de sus consecuencias.

18.2. Teorema. *Sea $C/\mathbb{F}_q$ una curva proyectiva lisa de género g. Para una clase $\mathscr{L} \in \operatorname{Pic}(C)$ consideremos todos los divisores efectivos que representan a $\mathscr{L}$ en el grupo de Picard:*

$$E_{\mathscr{L}} := \{D \in \operatorname{Div}(C) \mid D \ge 0,\ [D] = \mathscr{L}\}.$$

a) Para todo elemento $\mathscr{L} \in \operatorname{Pic}(C)$ existe un entero $h^0(\mathscr{L}) \ge 0$ tal que

$$\# E_{\mathscr{L}} = \frac{q^{h^0(\mathscr{L})} - 1}{q-1}.$$

b) Si $\deg(\mathscr{L}) \ge 2g-1$, entonces $h^0(\mathscr{L}) = \deg(\mathscr{L}) + 1 - g$.

*c) Existe un elemento $\mathscr{K} \in \operatorname{Pic}(C)$ (la **clase canónica**) tal que $\deg(\mathscr{K}) = 2g-2$ y*

$$h^0(\mathscr{L}) = \deg(\mathscr{L}) + 1 - g + h^0(\mathscr{K} - \mathscr{L}).$$

Demostración. Véase [Lor1996, Chapter IX]. ∎

Racionalidad de $Z(C,t)$

Usando la notación de 18.2, podemos escribir

$$Z(C,t) = \sum_{\substack{D \in \operatorname{Div}(C)\\ D \ge 0}} t^{\deg D} = \sum_{\substack{\mathscr{L} \in \operatorname{Pic}(C)\\ \deg \mathscr{L} \ge 0}} \sum_{\substack{D \ge 0\\ [D] = \mathscr{L}}} t^{\deg D} = \sum_{\substack{\mathscr{L} \in \operatorname{Pic}(C)\\ \deg \mathscr{L} \ge 0}} \# E_{\mathscr{L}} \cdot t^{\deg \mathscr{L}}.$$

Primero, si $g = 0$, entonces para cualquier $\mathscr{L}$ con $\deg \mathscr{L} \ge 0$ se tiene

$$\# E_{\mathscr{L}} = \frac{q^{\deg(\mathscr{L})+1} - 1}{q-1},$$

y la función zeta es

$$Z(C,t) = \sum_{d \ge 0} \frac{q^{d+1}-1}{q-1}\, t^d = \sum_{d \ge 0} \sum_{0 \le i \le d} q^i\, t^d = \sum_{m \ge 0} \sum_{i+j=m} (qt)^i\, t^j = \frac{1}{(1-t)\,(1-qt)} = Z(\mathbb{P}^1_{\mathbb{F}_q}, t).$$

Podemos asumir que $g \ge 1$. Como mencionamos, el grupo

$$\operatorname{Pic}^0(C) := \ker(\operatorname{Pic}(C) \xrightarrow{\deg} \mathbb{Z})$$

es finito. Luego, para todo $d \ge 0$ el conjunto

$$\operatorname{Pic}^d(C) := \{\mathscr{L} \in \operatorname{Pic}(C) \mid \deg \mathscr{L} = d\}$$

es vacío, o tiene la misma cardinalidad $h := \operatorname{Pic}^0(C)$. La imagen del homomorfismo $\deg\colon \operatorname{Pic}(C) \to \mathbb{Z}$ es un ideal generado por algún número $e \ge 0$. (En realidad, se tiene $e = 1$ y el homomorfismo es sobreyectivo, pero lo veremos más adelante.)

Escribamos

$$Z(C,t) = \sum_{\substack{\mathscr{L} \in \operatorname{Pic}(C)\\ 0 \le \deg \mathscr{L} \le 2g-2}} \# E_{\mathscr{L}} \cdot t^{\deg \mathscr{L}} + h \sum_{de \ge 2g-1} \frac{q^{de+1-g} - 1}{q-1}\, t^{de}.$$

Aquí la primera suma es algún polinomio de grado $\le 2g-2$. Respecto al segundo término, si ponemos

$$d_0 := \text{mín}\{d \mid de \ge 2g-1\},$$

entonces podemos escribir

$$\frac{h}{q-1}\sum_{de\ge 2g-1}(q^{de+1-g}-1)\,t^{de} = \frac{h\,t^{d_0 e}}{q-1}\left(q^{d_0 e+1-g}\sum_{d\ge 0}(qt)^{de} - \sum_{d\ge 0} t^{de}\right) = \frac{h\,t^{d_0 e}}{q-1}\left(\frac{q^{d_0 e+1-g}}{1-(qt)^e} - \frac{1}{1-t^e}\right). \tag{18.1}$$

De una vez notamos que de la última expresión se sigue que

$$\lim_{t\to 1}(t-1)\,Z(C,t) = \frac{h}{q-1}\lim_{t\to 1}\frac{t-1}{t^e-1} = \frac{h}{(q-1)\,e}. \tag{18.2}$$

En particular, $Z(C,t)$ tiene un polo simple en $t=1$. También observamos que (18.1) nos da la expresión

$$Z(C,t) = f(t^e) + h\,\frac{g(t^e)}{(1-(qt)^e)\,(1-t^e)} = \frac{P(t^e)}{(1-(qt)^e)\,(1-t^e)},$$

donde $f,g,P \in \mathbb{Z}[x]$ y $\deg(f)\le 2g-2$, $\deg(g)\le 2g$, $\deg(P)\le 2g$.

Ahora según 9.7, se cumple la relación

$$Z(C/\mathbb{F}_{q^e}, t^e) = \prod_{\zeta^e=1} Z(C/\mathbb{F}_q, \zeta t) = \left(\frac{P(t^e)}{(1-(qt)^e)\,(1-t^e)}\right)^e.$$

Aquí la parte izquierda tiene un polo simple en $t=1$, mientras que la parte derecha tiene un polo de orden e en $t=1$. Entonces, $e=1$. En particular, esto demuestra que el homomorfismo $\deg\colon \operatorname{Pic}(C)\to\mathbb{Z}$ es sobreyectivo. Todos los cálculos de arriba nos llevan al siguiente resultado.

18.3. Teorema. *Para una curva proyectiva lisa $C/\mathbb{F}_q$ de género g se tiene*

$$Z(C,t) = \frac{P(t)}{(1-t)\,(1-qt)},$$

donde $P(t)\in\mathbb{Z}[t]$ y $\deg(P)\le 2g$. La función zeta tiene un polo simple en $t=1$, donde

$$\lim_{t\to 1}(t-1)\,Z(C,t) = \frac{h}{q-1}, \tag{18.3}$$

y $h = P(1) = \#\operatorname{Pic}^0(C)$.

Notamos que (18.3) es un análogo de la fórmula de clases de Dirichlet mencionada en §7. En realidad, el polinomio $P(t)$ tiene grado precisamente $2g$, como predicen las conjeturas de Weil, pero lo vamos a deducir de la ecuación funcional.

18.4. Ejemplo. Para una curva elíptica $E/\mathbb{F}_q$ se tiene

$$Z(E,t) = \frac{1+at+qt^2}{(1-t)\,(1-qt)},$$

y luego

$$\frac{h}{q-1} = \lim_{t\to 1}(t-1)\,Z(E,t) = \frac{1+a+q}{q-1}.$$

Esto nos dice que

$$h = \#E(\mathbb{F}_q),$$

y de hecho, hay isomorfismo de grupos

$$\operatorname{Pic}^0(E) \cong E(\mathbb{F}_q). \qquad \blacktriangle$$

Ecuación funcional para $Z(C,t)$

31/10/19

Para una curva C de género g, sustituyendo $\chi = 2-2g$ en la conjetura 17.3, se obtiene el siguiente enunciado.

18.5. Teorema. *Se tiene*
$$Z(C,(qt)^{-1}) = (qt^2)^{1-g}\, Z(C,t).$$

Demostración. Usando 18.2, escribamos
$$\begin{aligned}(q-1)\,Z(C,t) &= \sum_{\substack{\mathscr{L}\in \operatorname{Pic}(C)\\ \deg\mathscr{L}\ge 0}} (q-1)\cdot \#E_{\mathscr{L}}\cdot t^{\deg\mathscr{L}} = \sum_{\substack{\mathscr{L}\in \operatorname{Pic}(C)\\ \deg\mathscr{L}\ge 0}} (q^{h^0(\mathscr{L})}-1)\, t^{\deg\mathscr{L}}\\ &= \underbrace{\sum_{\substack{\mathscr{L}\in \operatorname{Pic}(C)\\ 0\le\deg\mathscr{L}\le 2g-2}} q^{h^0(\mathscr{L})}\, t^{\deg\mathscr{L}}}_{=:\alpha(t)} + \underbrace{\sum_{\substack{\mathscr{L}\in \operatorname{Pic}(C)\\ \deg\mathscr{L}\ge 2g-1}} q^{\deg(\mathscr{L})+1-g}\, t^{\deg\mathscr{L}} - \sum_{\substack{\mathscr{L}\in \operatorname{Pic}(C)\\ \deg\mathscr{L}\ge 0}} t^{\deg\mathscr{L}}}_{=:\beta(t)}.\end{aligned}$$

Para comprobar la ecuación funcional, sería suficiente ver que
$$\alpha((qt)^{-1}) = (qt^2)^{1-g}\,\alpha(t), \quad \beta((qt)^{-1}) = (qt^2)^{1-g}\,\beta(t).$$

Primero,
$$\beta(t) = h\sum_{d\ge 2g-1} q^{d+1-g}\, t^d - h\sum_{d\ge 0} t^d = h\left(\frac{q^g\, t^{2g-1}}{1-qt} - \frac{1}{1-t}\right),$$
y es fácil verificar la relación necesaria. Para el polinomio $\alpha(t)$, necesitamos todo el poder del Riemann–Roch. Consideremos el conjunto
$$\{\mathscr{L}\in \operatorname{Pic}(C) \mid 0\le \deg\mathscr{L}\le 2g-2\}.$$
Notamos que $\mathscr{L}\mapsto \mathscr{K}-\mathscr{L}$, donde $\mathscr{K}$ es la clase canónica, define una permutación de sus elementos. En efecto, si $0\le \deg\mathscr{L}\le 2g-2$, entonces
$$0\le \deg(\mathscr{K}-\mathscr{L}) = 2g-2-\deg\mathscr{L}\le 2g-2.$$

Gracias a esto, podemos escribir
$$\alpha(t) = \sum_{\substack{\mathscr{L}\in \operatorname{Pic}(C)\\ 0\le\deg\mathscr{L}\le 2g-2}} q^{h^0(\mathscr{K}-\mathscr{L})}\, t^{\deg(\mathscr{K}-\mathscr{L})}.$$

Ahora la fórmula de Riemann–Roch
$$h^0(\mathscr{L}) = \deg(\mathscr{L}) + 1 - g + h^0(\mathscr{K}-\mathscr{L})$$
nos da en particular
$$h^0(\mathscr{K}-\mathscr{L}) = \deg(\mathscr{K}) - \deg(\mathscr{L}) + 1 - g + h^0(\mathscr{L}) = g-1-\deg(\mathscr{L}) + h^0(\mathscr{L}),$$
así que
$$\alpha(t) = q^{g-1}\, t^{2g-2} \sum_{\substack{\mathscr{L}\in \operatorname{Pic}(C)\\ 0\le\deg\mathscr{L}\le 2g-2}} q^{-\deg(\mathscr{L})+h^0(\mathscr{L})}\, t^{-\deg(\mathscr{L})} = q^{g-1}\, t^{2g-2} \sum_{\substack{\mathscr{L}\in \operatorname{Pic}(C)\\ 0\le\deg\mathscr{L}\le 2g-2}} (qt)^{-\deg(\mathscr{L})}\, q^{h^0(\mathscr{L})}.$$

Por otra parte,
$$\alpha((qt)^{-1}) = \sum_{\substack{\mathscr{L}\in \operatorname{Pic}(C)\\ 0\le\deg\mathscr{L}\le 2g-2}} (qt)^{-\deg(\mathscr{L})}\, q^{h^0(\mathscr{L})}.$$

Esto establece la relación necesaria para $\alpha(t)$. ∎

18.6. Corolario. *Se tiene*

$$Z(C,t) = \frac{P(t)}{(1-t)(1-qt)},$$

donde $P(t) \in \mathbb{Z}[t]$ y $\deg(P) = 2g$.

Demostración. Ya sabemos que $\deg P \le 2g$, y tenemos la ecuación funcional

$$\frac{P((qt)^{-1})}{(1-(qt)^{-1})(1-t^{-1})} = (qt^2)^{1-g} \frac{P(t)}{(1-t)(1-qt)}$$

que implica que

$$P((qt)^{-1}) = (qt^2)^{-g} P(t).$$

Esto es posible solo si $\deg(P) = 2g$. ■

Notamos que

$$P(0) = 1, \quad P(1) = h = \#\operatorname{Pic}^0(C).$$

Escribamos

$$P(t) = 1 + a_1 t + \cdots + a_{2g} t^{2g}.$$

La ecuación funcional nos dice que

$$a_{2g-i} = q^{g-i} a_i. \tag{18.4}$$

Además,

$$\#C(\mathbb{F}_q) = q + 1 + a_1.$$

18.7. Corolario. *Escribamos*

$$P(t) = \prod_{1\le i\le 2g} (1-\alpha_i t).$$

Luego, los α_i son enteros algebraicos y vienen en g parejas $(\alpha_i, q/\alpha_i)$.

Demostración. Primero, los α_i son raíces del polinomio

$$P^\vee(t) := t^{2g} P(t^{-1}) \in \mathbb{Z}[t],$$

que es mónico (su coeficiente mayor es a_0), así que son enteros algebraicos.

De la ecuación funcional se ve que si $P(\alpha_i^{-1}) = 0$, entonces $P(\alpha_i/q) = 0$. Supongamos que hay r parejas con $\alpha_i \ne q/\alpha_i$:

$$\alpha_1, q/\alpha_1, \ldots, \alpha_r, q/\alpha_r, \tag{18.5}$$

Luego, habrá $s+t$ raíces que cumplen $\alpha_i = q/\alpha_i$:

$$\underbrace{+\sqrt{q}, \ldots, +\sqrt{q}}_{s}, \underbrace{-\sqrt{q}, \ldots, -\sqrt{q}}_{t}.$$

Sabemos que

$$\prod_{1\le i\le 2g} \alpha_i = a_{2g} = q^g.$$

El producto de (18.5) también nos da una potencia de q. Esto implica que t es par (sino, tendríamos un signo "−"), pero luego de la relación $2g = 2r + s + t$ podemos concluir que s es también par. ■

Es fácil comprobar que a partir de los números

$$\#C(\mathbb{F}_q), \ldots, \#C(\mathbb{F}_{q^g})$$

se recuperan los coeficientes $a_0, \ldots, a_g$, y luego gracias a (18.4) todos los coeficientes de $P(t)$. Entonces, para recuperar la función zeta completa de C, basta contar los puntos sobre $\mathbb{F}_q, \ldots, \mathbb{F}_{q^g}$.

Hipótesis de Riemann para $Z(C,t)$

La hipótesis de Riemann para las curvas se seguiría de la **cota de Hasse–Weil**

$$|\#C(\mathbb{F}_{q^m}) - q^m - 1| \le 2g \cdot q^{m/2}.$$

18.8. Proposición. *Asumamos que existe una constante $c \in \mathbb{R}$ tal que*

$$|\#C(\mathbb{F}_{q^m}) - q^m - 1| \le c \cdot q^{m/2}$$

para $m \gg 0$. Luego, $|\alpha_i| = \sqrt{q}$ para todo i.

Demostración. Sabemos que

$$\#C(\mathbb{F}_{q^m}) - q^m - 1 = -\sum_{1\le i\le 2g} \alpha_i^m.$$

Consideremos la función

$$\sum_{1\le i\le 2g} \frac{\alpha_i t}{1-\alpha_i t} = \sum_{1\le i\le 2g} \sum_{m\ge 1} (\alpha_i t)^m = \sum_{m\ge 1} \left(\sum_{1\le i\le 2g} \alpha_i^m\right) t^m = \sum_{m\ge 1} \left(q^m + 1 - \#C(\mathbb{F}_{q^m})\right) t^m.$$

La primera serie finita tiene radio de convergencia $\rho := \text{mín}\{|\alpha_i|^{-1} \mid 1 \le i \le 2g\}$, mientras que la última serie converge para $t < 1/\sqrt{q}$ por nuestra hipótesis. Entonces, $|\alpha_i|^{-1} \ge 1/\sqrt{q}$, así que $|\alpha_i| \le \sqrt{q}$. Pero toda raíz recíproca α_i viene junto con q/α_i, así que también $|q/\alpha_i| \le \sqrt{q}$. Entonces, $|\alpha_i| = \sqrt{q}$. ∎

18.9. Comentario. La cota de Hasse–Weil fue probada por Hasse en 1934 para las curvas elípticas (el caso de $g=1$) y por Weil en 1940 para cualquier género.

Stepanov obtuvo en 1969 una prueba elemental para las curvas hiperelípticas, que fue generalizada por Bombieri a todas las curvas. El artículo original de Bombieri es [Bom1974], y una buena exposición de su argumento se encuentra en [Lor1996, Chapter X] o [Ros2002, Appendix]. Otra fuente elemental basada en las ideas de Stepanov es [Sch1976].

Una prueba alternativa de la hipótesis de Riemann para curvas, que también mejora la cota de Hasse–Weil en ciertos casos, pertenece a Stöhr y Voloch [SV1986].

18.10. Comentario. En dimensiones superiores se tiene la **cota de Lang–Weil** [LW1954] que afirma lo siguiente. Si $X \subset \mathbb{P}^n$ es una variedad sobre $\mathbb{F}_q$ de grado d y dimensión r, entonces existe una constante $A(n,d,r)$ tal que

$$|X(\mathbb{F}_q) - q^r| \le (d-1)(d-2)\, q^{r-1/2} + A(n,d,r)\, q^{r-1}.$$

Para las cotas particulares que mejoran la cota de Hasse–Weil, véase por ejemplo [HL2003], [vdG2015], y la página `https://manypoints.org/`

En fin, notamos que la hipótesis de Riemann implica desigualdades para el tamaño de $\#\text{Pic}^0(C)$.

18.11. Proposición. *Se tiene*

$$(1-\sqrt{q})^{2g} \le \#\text{Pic}^0(C) \le (1+\sqrt{q})^{2g}.$$

En particular, $\text{Pic}^0(C) \ne 0$ *para* $q > 4$.

Demostración. Tenemos

$$\#\text{Pic}^0(C) = P(1) = \prod_{1\le i\le 2g} (1-\alpha_i).$$

Ahora si $|\alpha_i| = \sqrt{q}$ para todo i, entonces

$$|1-\sqrt{q}| \le |1-\alpha_i| \le 1+\sqrt{q}.$$ ∎

Referencias

[AIK2014] Tsuneo Arakawa, Tomoyoshi Ibukiyama, and Masanobu Kaneko, *Bernoulli numbers and zeta functions*, Springer Monographs in Mathematics, Springer, Tokyo, 2014, With an appendix by Don Zagier. MR3307736
https://doi.org/10.1007/978-4-431-54919-2

[BG2002] José I. Burgos Gil, *The regulators of Beilinson and Borel*, CRM Monograph Series, vol. 15, American Mathematical Society, Providence, RI, 2002. MR1869655

[Bom1974] Enrico Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430, 1974, pp. 234–241. Lecture Notes in Math., Vol. 383. MR0429903

[Bor1974] Armand Borel, *Stable real cohomology of arithmetic groups*, Ann. Sci. École Norm. Sup. (4) **7** (1974), 235–272 (1975). MR0387496
http://www.numdam.org/item?id=ASENS_1974_4_7_2_235_0

[CL1984] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62. MR756082
https://doi.org/10.1007/BFb0099440

[Del1974] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. (1974), no. 43, 273–307. MR0340258
http://www.numdam.org/item?id=PMIHES_1974__43__273_0

[DH1935] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1935), 151–182. MR1581445
https://doi.org/10.1515/crll.1935.172.151

[Dwo1960] Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648. MR140494
https://doi.org/10.2307/2372974

[Gol1985] Dorian Goldfeld, *Gauss's class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. (N.S.) **13** (1985), no. 1, 23–37. MR788386
https://doi.org/10.1090/S0273-0979-1985-15352-2

[HL2003] E. W. Howe and K. E. Lauter, *Improved upper bounds for the number of points on curves over finite fields*, Ann. Inst. Fourier (Grenoble) **53** (2003), no. 6, 1677–1737. MR2038778
http://aif.cedram.org/item?id=AIF_2003__53_6_1677_0

[HV1949] L. K. Hua and H. S. Vandiver, *Characters over certain types of rings with applications to the theory of equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 94–99. MR28895
https://doi.org/10.1073/pnas.35.2.94

[IR1990] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716
https://doi.org/10.1007/978-1-4757-2103-4

[Lor1996] Dino Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 9, American Mathematical Society, Providence, RI, 1996. MR1376367
https://doi.org/10.1090/gsm/009

[LW1954] Serge Lang and André Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827. MR65218
https://doi.org/10.2307/2372655

[Mil1971] John Milnor, *Introduction to algebraic K-theory*, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1971, Annals of Mathematics Studies, No. 72. MR0349811

[Neu1999] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR1697859
https://doi.org/10.1007/978-3-662-03983-0

[Qui2010] Daniel Quillen, *Finite generation of the groups K_i of rings of algebraic integers*, Cohomology of groups and algebraic K-theory, Adv. Lect. Math. (ALM), vol. 12, Int. Press, Somerville, MA, 2010, pp. 479–488. MR2655185

[Riv2000] Tanguy Rivoal, *La fonction zêta de Riemann prend une infinité de valeurs irrationnelles aux entiers impairs*, C. R. Acad. Sci. Paris Sér. I Math. **331** (2000), no. 4, 267–270. MR1787183
https://doi.org/10.1016/S0764-4442(00)01624-4

[Ros2002] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657
https://doi.org/10.1007/978-1-4757-6046-0

[Sch1976] Wolfgang M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin-New York, 1976. MR0429733

[SGA 4] Michael Artin, Alexander Grothendieck, and Jean-Louis Verdier (eds.), *Séminaire de géométrie algébrique du Bois-Marie 1963–1964 (SGA 4): Théorie des topos et cohomologie étale des schémas*, Lecture Notes in Mathematics, Vol. 269, 270, 305, Springer-Verlag, Berlin-New York, 1972–73, Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat. MR0354652
http://fabrice.orgogozo.perso.math.cnrs.fr/SGA4/

[Sil2009] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094
https://doi.org/10.1007/978-0-387-09494-6

[SV1986] Karl-Otto Stöhr and José Felipe Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** (1986), no. 1, 1–19. MR812443
https://doi.org/10.1112/plms/s3-52.1.1

[vdG2015] Gerard van der Geer, *Counting curves over finite fields*, Finite Fields Appl. **32** (2015), 207–232. MR3293411
https://doi.org/10.1016/j.ffa.2014.09.008

[vdP7879] Alfred van der Poorten, *A proof that Euler missed…Apéry's proof of the irrationality of $\zeta(3)$*, Math. Intelligencer **1** (1978/79), no. 4, 195–203, An informal report. MR547748
https://doi.org/10.1007/BF03028234

[Was1997] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575
https://doi.org/10.1007/978-1-4612-1934-7

[Wei1949] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. MR29393
https://doi.org/10.1090/S0002-9904-1949-09219-4

[Wei2005] Charles Weibel, *Algebraic K-theory of rings of integers in local and global fields*, Handbook of K-theory. Vol. 1, 2, Springer, Berlin, 2005, pp. 139–190. MR2181823
https://doi.org/10.1007/3-540-27855-9_5

[Zud2001] V. V. Zudilin, *One of the numbers $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ is irrational*, Uspekhi Mat. Nauk **56** (2001), no. 4(340), 149–150. MR1861452
https://doi.org/10.1070/RM2001v056n04ABEH000427