INTRODUCCIÓN A LA FUNCIONES ZETA DE HASSE–WEIL

Fernando Rodriguez-Villegas

Mayo 1999

Contenido

0. Introducción

La meta principal de la Teoría de Números es la de resolver ecuaciones en números enteros o racionales. En el mejor de los casos, las soluciones se pueden describir completamente. Por ejemplo, las soluciones racionales a la ecuación

$$x^2 + y^2 = 1 \tag{1}$$

son

$$x = \frac{t^2 - 1}{t^2 + 1}, \qquad y = \frac{2t}{t^2 + 1}, \qquad t \in \mathbb{Q}$$

más el punto $(x, y) = (1, 0)$, que podríamos decir corresponde a $t = \infty$.

Las soluciones racionales a la ecuación

$$x^3 + y^3 = 1, \tag{2}$$

en cambio, son solamente $(x, y) = (1, 0), (0, 1)$ y la ecuación

$$x^2 + y^2 + z^2 = 7 \tag{3}$$

no tiene ninguna solución racional.

Pero estos ejemplos no dan una impresión fidedigna del problema; el hecho es que es extremadamente difícil dar una descripción completa, o aún parcial, de las soluciones racionales de una ecuación arbitraria.

Podemos entonces preguntarnos algo más sencillo: ¿tiene la ecuación *alguna* solución racional?; si las tiene: ¿son un número finito o infinito? Recalquemos la diferencia sutil pero substancial de este punto de vista: no preguntamos *cuáles* son las soluciones si no, esencialmente, *cuántas* hay. Aún este problema simplificado es extremadamente difícil de resolver para una ecuación arbitraria.

Una estrategia básica para probar que una ecuación no tiene soluciones racionales es la de mostrar que no tiene soluciones reales o módulo algún número entero m. La ventaja de cambiar la pregunta es que se vuelve más fácil de contestar.

Por ejemplo, la ecuación

$$x^2 + y^2 = -1$$

visiblemente no tiene soluciones racionales ya que siempre tenemos que

$$x^2 + y^2 \geq 0 > -1.$$

Por otro lado una solución racional a (3) daría una solución

$$u^2 + v^2 + w^2 = 7t^2$$

con u, v, w, t enteros sin factor común, que a su vez daría una solución módulo $m = 8$

$$u^2 + v^2 + w^2 \equiv 7t^2 \bmod 8, \qquad (u, v, w, t) \not\equiv (0, 0, 0, 0) \bmod 2,$$

y es fácil verificar (habiendo solo un número finito de posibilidades para (u, v, w, t) mod 8) que esto no es posible.

Naturalmente nos preguntamos: ¿Qué pasa si la ecuación tiene soluciones reales y módulo cualquier número entero m? ¿Podemos decir que la ecuación tiene entonces una solución racional? Desgraciadamente, la respuesta en general es *no* y en ese caso nuestra estrategia no sirvió de mucho (un ejemplo es la ecuación $x^4 - 17 = y^2$, ver [Ca, p. 57]).

La respuesta es *sí*, sin embargo, para ecuaciones cuadráticas análogas a (3)

$$a_1 x_1^2 + \cdots a_n x_n^2 = a, \qquad a, a_1, \cdots, a_n \in \mathbb{Z}\,;$$

este es el teorema de Hasse–Minkowski ([Se1, chap. IV]).

En todo caso, uno siempre espera poder extraer de la información *local* (módulo enteros, sobre los reales) *algún* tipo de información *global* (sobre los racionales). Una buena manera de codificar toda la información local es formando funciones zeta o L asociadas al objeto aritmético–geométrico en cuestión (podría decirse que estas son el DNA del objeto); uno luego espera que propiedades analíticas de estas funciones, por ejemplo el orden de cero o polo en valores particulares de la variable, reflejen propiedades globales del objeto. Estas funciones son el tópico de esta monografía.

Agradecimientos Quisiera agradecer a A. Sofer y F. Voloch por su valiosos comentarios.

... And though the holes were rather small
They had to count them all
Now they know how many holes it takes to fill the Albert Hall ...

Lennon–McCartney

I – Dimensión 0

§1 Congruencias: número de soluciones

Vamos a estudiar ecuaciones en congruencia módulo un $m \in \mathbb{N}$, es decir, ecuaciones del tipo

$$f(x_1, x_2, \cdots, x_n) \equiv 0 \bmod m \tag{4}$$

(o más generalmente congruencias simultáneas $f_1 \equiv f_2 \equiv \cdots \equiv f_k \equiv 0 \bmod m$).

Para m y f dados el problema es finito; siempre podemos chequear uno a uno todos los mn posibles valores de las variables, $x_j = 0, 1, \cdots, m-1$, $j = 1, \cdots, n$ y ver cuales son soluciones. Este procedimiento, sin embargo, seria muy poco práctico si mn es grande. Buscamos poder decir algo acerca de las soluciones (por ejemplo, cual es su número) de una manera teórica.

Primero notemos que el Teorema Chino del Resto nos permite descomponer (4) en congruencias según las potencias de primos que dividen a m; más precisamente, las soluciones a (4) están en biyección con las soluciones a las congruencias

$$f(x_1, x_2, \cdots, x_n) \equiv 0 \bmod p_j^{e_j}, \qquad j = 1, 2, \cdots, r,$$

donde $m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$ con $p_1, p_2, \cdots, p_r$ primos distintos.

1. Ecuaciones en una variable módulo un primo p

Empecemos por el caso en que m es un número primo p y la ecuación es cuadrática en una variable

$$f(x) = ax^2 + bx + c \equiv 0 \bmod p, \qquad a, b, c \in \mathbb{Z}.$$

Recordemos que como $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo $(\mathbb{Z}/p\mathbb{Z})[x]$ es un dominio de factorización única. Por lo tanto[1] la ecuación $f(x) \equiv 0 \bmod p$ tiene un número $N_p = 0, 1$ o 2 de soluciones. ¿Como podemos distinguir estos tres casos?

Esta pregunta tiene una solución muy bonita, la ley de reciprocidad cuadrática, que es de gran importancia tanto teórica como práctica.

Esta claro que si $p \mid a$ la ecuación es realmente lineal en cuyo caso es fácil de resolver; excluiremos este caso en lo que sigue. Por otro lado, si $p \nmid 2a$ la fórmula cuadrática nos garantiza que N_p es también el número de soluciones de

$$x^2 - \Delta \equiv 0 \bmod p,$$

donde $\Delta = b^2 - 4ac$ es el discriminante de f. Notemos que, si $p \nmid 2a$, $N_p = 1$ si y solo si $p \mid \Delta$.

Podemos ahora formular la ley de reciprocidad cuadrática (LRC) en su versión más débil.

Teorema (LRC, versión débil). *Sean a, b, c enteros sin factor común con $a \neq 0$ y $\Delta = b^2 - 4ac \neq 0$. Entonces, para todo primo $p \nmid a\Delta$ el número de soluciones N_p de la congruencia*

$$f(x) = ax^2 + bx + c \equiv 0 \bmod p,$$

depende solo de $p \bmod \Delta$.

Como ilustración, tomemos la ecuación $f(x) = x^2 + x - 1$ de discriminante $\Delta = 5$. Como $f(3) = 11$ vemos que $N_{11} = 2$ y entonces el teorema nos dice que $N_p = 2$ para todo primo $p \equiv 1 \bmod 5$.

Veremos más adelante la versión más precisa de la LRC detallando como N_p depende de $p \bmod \Delta$.

Tomemos ahora $f \in \mathbb{Z}[x]$ un polinomio de grado d arbitrario con discriminante Δ no nulo. Para simplificar la exposición vamos a asumir de ahora en más que f es mónico (i.e., su coeficiente principal es 1) y que $p \nmid \Delta$. Entonces f se factoriza módulo p como

$$f \equiv f_1 f_2 \cdots f_r \bmod p,$$

con $f_1, f_2, \cdots, f_r$ polinomios irreducibles en $(\mathbb{Z}/p\mathbb{Z})[x]$ distintos de grados $d_1 \leq d_2 \leq \cdots \leq d_r$ respectivamente y $d = d_1 + d_2 + \cdots d_r$. Llamemos $t_p = [d_1, d_2, \cdots, d_r]$ el *tipo* de factorización de $f \bmod p$.

El número de soluciones N_p a la congruencia $f(x) \equiv 0 \bmod p$ es a lo sumo d y se puede expresar en términos del tipo t_p de factorización de $f \bmod p$; en efecto, N_p es el número de factores f_j, $j = 1, \cdots, r$ de grado 1.

En la LRC fijamos un polinomio f de grado $d = 2$ y estudiamos como el número de soluciones N_p de la congruencia $f \equiv 0 \bmod p$ varia con p. ¿Qué pasa para un polinomio arbitrario? Resulta que más que N_p conviene estudiar t_p como función de p. (Para polinomios de grado $d \leq 3$, t_p y N_p se determinan mutuamente pero esto no es cierto en general; por ejemplo, un polinomio de grado 4 con $N_p = 0$ puede tener $t_p = [2, 2]$ o $[4]$.)

Primero vamos a relacionar t_p con el número de soluciones de $f(x) = 0$ sobre un cuerpo finito de característica p.

2. Repaso de cuerpos finitos

Resumimos en esta sección los hechos básicos sobre los cuerpos finitos que vamos a necesitar. El lector podrá encontrar sus demostración en, por ejemplo, [Se1, Ch I, §1].

Al cuerpo de p elementos $\mathbb{Z}/p\mathbb{Z}$ (p un primo) lo vamos a denotar con $\mathbb{F}_p$. Un cuerpo finito $\mathbb{F}$ es una extensión de $\mathbb{F}_p$ para algún primo p, la característica de $\mathbb{F}$. Si $n = [\mathbb{F} : \mathbb{F}_p]$ es el grado de la extensión entonces $\mathbb{F}$ tiene p^n elementos.

Para todo cuerpo F de característica p la aplicación

$$\begin{array}{ccc} \sigma : F & \longrightarrow & F \\ x & \mapsto & x^p \end{array}$$

es un automorfismo de F (el automorfismo de *Frobenius*).

Fijemos $\overline{\mathbb{F}}_p$ una clausura algebraica de $\mathbb{F}_p$. Hay un único cuerpo de $q = p^n$ elementos en $\overline{\mathbb{F}}_p$: el conjunto de puntos de $\overline{\mathbb{F}}_p$ fijados por σ^n. Denotaremos este cuerpo por $\mathbb{F}_q$, es el conjunto de soluciones de $x^q - x = 0$ en $\overline{\mathbb{F}}_p$. $\mathbb{F}_{p^n}$ es una extensión de $\mathbb{F}_{p^m}$ si y solo si $n \mid m$.

Otra forma en la que puede darse un cuerpo finito es como

$$\mathbb{F} = \mathbb{F}_p[x]/(f)$$

donde $f \in \mathbb{F}_p[x]$ es irreducible; el cardinal de $\mathbb{F}$ es p^d donde d es el grado de f. De todas maneras, todo cuerpo finito de $q = p^n$ elementos es isomorfo a $\mathbb{F}_q$.

El grupo multiplicativo $\mathbb{F}_q^*$ de elementos no nulos de $\mathbb{F}_q$ es cíclico de orden $q-1$.

Dada una extensión de cuerpos finitos $\mathbb{F}'/\mathbb{F}$ de grado $n = [\mathbb{F}' : \mathbb{F}]$ y $\mathbb{F}$ de q elementos existen dos aplicaciones importantes: la *traza*

$$T_{\mathbb{F}'/\mathbb{F}}(x) := x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}$$

y la *norma*

$$N_{\mathbb{F}'/\mathbb{F}}(x) := x \cdot x^q \cdot x^{q^2} \cdot \cdots \cdot x^{q^{n-1}}$$

que determinan homomorfismos sobreyectivos

$$T_{\mathbb{F}'/\mathbb{F}} : \mathbb{F}' \longrightarrow \mathbb{F}$$

con respecto a al suma y

$$N_{\mathbb{F}'/\mathbb{F}} : (\mathbb{F}')^* \longrightarrow \mathbb{F}^*$$

con respecto al producto.

3. Ecuaciones en una variable sobre un cuerpo finito

Sea $f \in \mathbb{F}_p[x]$ un polinomio mónico de grado d sin raíces múltiples en $\overline{\mathbb{F}}_p$ (i.e., con discriminante no nulo). Sabemos que f tiene d raíces en $\overline{\mathbb{F}}_p$. ¿Dónde están esas raíces en relación a los diversos cuerpos $\mathbb{F}_q$?

Sea N_q el número de soluciones de $f(x) = 0$ en $\mathbb{F}_q$. Sea como antes $[d_1, d_2, \cdots, d_r]$ su tipo de factorización de f; i.e.,

$$f = f_1 f_2 \cdots f_r,$$

con $f_1, \cdots, f_r \in \mathbb{F}_p[x]$ irreducibles distintos de $\mathrm{gr}(f_1) = d_1, \cdots, \mathrm{gr}(f_r) = d_r$

Sabemos que N_p es el número de $j = 1, 2, \cdots, r$ con $d_j = 1$. Esto se generaliza como sigue.

Lema. *Para todo $n \in \mathbb{N}$ tenemos*

$$N_{p^n} = \sum_{\substack{d_j | n \\ 1 \leq j \leq r}} d_j$$

Demostración. Supongamos primero que f es irreducible y sea $\mathbb{F} = \mathbb{F}_p[x]/(f)$, un cuerpo de p^d elementos. Tenemos que demostrar que $N_{p^n} = d$ si $d \mid n$ y 0 si $d \nmid n$. Cada raíz de f en $\overline{\mathbb{F}}_p$ nos da un morfismo $\tau : \mathbb{F} \longrightarrow \overline{\mathbb{F}}_p$. La imagen de τ es un cuerpo de p^d elementos que por lo que hemos visto debe ser $\mathbb{F}_{p^d}$. Por lo tanto todas las raíces de f están contenidas en $\mathbb{F}_{p^d}$. Si f tiene una raíz en $\mathbb{F}_{p^n}$ este contiene a $\mathbb{F}_{p^d}$ con lo que $d \mid n$ y todas las raíces de f están en $\mathbb{F}_{p^n}$. Recíprocamente, si $d \mid n$, $\mathbb{F}_{p^n}$ contiene $\mathbb{F}_{p^d}$ y entonces todas las raíces de f están en $\mathbb{F}_{p^n}$.

Para probar el caso general basta aplicar el caso anterior a cada factor irreducible f_j (notando que por hipótesis las raíces de f son todas simples). □

A continuación introducimos la función zeta de f que, por el momento, solo veremos como una manera útil de codificar la información sobre todos los números N_{p^n}.

4. Función zeta de un polinomio

Como antes, sea $f \in \mathbb{F}_p[x]$ un polinomio mónico de grado d sin raíces múltiples en $\overline{\mathbb{F}}_p$ y sea N_{p^n} el número de raíces de $f(x) = 0$ contenidas en $\mathbb{F}_{p^n}$. Formamos la serie generatriz en una variable T

$$Z_f(T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_{p^n}}{n} T^n\right),$$

que llamaremos la *función zeta* de f; es una serie de potencias en T con coeficientes racionales.

Estudiemos las propiedades formales de este tipo de serie. Dada una secuencia cualquiera $\mathbf{a} : a_1, a_2, \cdots$ de números complejos definamos de forma análoga

$$Z_{\mathbf{a}}(T) := \exp\left(\sum_{n=1}^{\infty} \frac{a_n}{n} T^n\right).$$

Es fácil de verificar lo siguiente.

(1)

$$Z_{\mathbf{a}+\mathbf{b}}(T) = Z_{\mathbf{a}}(T) Z_{\mathbf{b}}(T),$$

donde

$$\mathbf{a} : a_1, a_2, \cdots, \qquad \mathbf{b} : b_1, b_2, \cdots, \qquad \mathbf{a}+\mathbf{b} : a_1+b_1, a_2+b_2, \cdots,$$

(2)

$$Z_{\mathbf{a}}(T) = (1-\lambda T)^{-1}, \qquad \text{si} \qquad a_n = \lambda^n, \quad n = 1, 2, \cdots,$$

(3) Existen α_j, β_k, para $j = 1, 2, \cdots, r$ y $k = 1, 2, \cdots, s$ tales que

$$a_n = \sum_{j=1}^{r} \alpha_j^n - \sum_{j=1}^{s} \beta_j^n, \qquad n \in \mathbb{N}$$

si y solo si

$$Z_{\mathbf{a}}(T) = \frac{(1-\beta_1 T)(1-\beta_2 T)\cdots(1-\beta_s T)}{(1-\alpha_1 T)(1-\alpha_2 T)\cdots(1-\alpha_r T)}$$

Usando el lema vemos que si f es irreducible en $\mathbb{F}_p[x]$ entonces $N_{p^n} = d$ si $d \mid n$ y 0 si $d \nmid n$ con lo que $Z_f(T) = 1/(1-T^d)$.

En el caso general tenemos entonces que

$$Z_f = Z_{f_1} \cdots Z_{f_r} = \prod_{j=1}^{r} (1-T^{d_j})^{-1},$$

donde como antes

$$f = f_1 f_2 \cdots f_r,$$

con $f_1, \cdots, f_r \in \mathbb{F}_p[x]$ irreducibles distintos de $\mathrm{gr}(f_1) = d_1, \cdots, \mathrm{gr}(f_r) = d_r$. Es claro que la función Z_f (o lo que es lo mismo, la secuencia N_{p^n}) determinan unívocamente el tipo de factorización $[d_1, d_2, \cdots, d_r]$ y recíprocamente.

Destaquemos varios hechos que se deducen de nuestro calculo.

(1) Z_f es una función racional de T con coeficientes en $\mathbb{Z}$.

(2) $Z_f(T)$ es de la forma

$$Z_f(T) = \frac{1}{P(T)}$$

donde

$$P(T) = \prod_{j=1}^{d}(1 - \zeta_j T) \in \mathbb{Z}[T], \qquad |\zeta_j| = 1, \quad j = 1, 2, \cdots, d.$$

(3) $Z_f(1/T) = (-1)^r T^d Z_f(T)$

Ejercicio 1.

(1) Probar que los primeros d elementos $N_p, \cdots, N_{p^d}$ de la secuencia N_{p^n} determinan unívocamente el resto.
(2) Probar[2] que dado $P(T) \in \mathbb{Z}[T]$

$$P(T) = \prod_{j=1}^{d}(1 - \zeta_j T), \qquad |\zeta_j| = 1, \quad j = 1, 2, \cdots, d.$$

si y solo si

$$P(T) = \prod_{j=1}^{r}(1 - T^{d_j})^{-1} \ .$$

5. Polinomios abelianos

Podemos preguntarnos si en general dado un polinomio $f \in \mathbb{Z}[x]$ de grado d y un primo p habrá alguna manera similar a la dada por la LRC de determinar si la ecuación $f(x) \equiv 0 \bmod p$ tiene o no soluciones.

La respuesta es *no* en general, pero si existe un análogo para cierto tipo especial de polinomios que vamos a llamar *abelianos*. Es mas, para un tal polinomio podremos describir no solo el número N_p de soluciones de $f(x) \equiv 0 \bmod p$ como función de p si no también su tipo de factorización t_p.

Sea $f \in \mathbb{Z}[x]$ un polinomio mónico con discriminante Δ no nulo. Denotemos por S el conjunto (finito) de primos que dividen a Δ. Para todo primo $p \notin S$ podemos considerar el polinomio $f \bmod p \in \mathbb{F}_p[x]$ y su correspondiente función zeta que vamos a denotar por $Z_{f,p}(T)$. Como vimos en el n$^{\text{o}}$ 4, el tipo de factorización t_p y la función zeta $Z_{f,p}(T)$ se determinan mutuamente. Consideraremos entonces como varia $Z_{f,p}(T)$ con $p \notin S$.

Diremos que f es *abeliano*[3] si existe un $N \in \mathbb{N}$ tal que $Z_{f,p}(T)$ para $p \notin S$ depende solo de $p \bmod N$. El número N más chico que para el cual esta propiedad de f es valida se llama el *conductor* de f.

El teorema 1 implica que todo polinomio cuadrático $x^2 + rx + s \in \mathbb{Z}[x]$ con $\Delta = r^2 - 4s \neq 0$ es abeliano, basta tomar $N = \Delta$.

Todo polinomio ciclotómico (polinomio minimal de una raíz primitiva de la unidad) es abeliano. Un teorema de Kronecker y Weber garantiza que si f es

un polinomio abeliano irreducible su cuerpo de descomposición $\mathbb{Q}[x]/(f)$ se puede incluir en un cuerpo ciclotómico $\mathbb{Q}(\zeta_N)$ donde ζ_N es una raíz N-ésima primitiva de la unidad (y de hecho el mínimo tal N es el conductor de f). En otras palabras, las raíces de f se pueden expresar en términos de raíces de la unidad.

Estudiemos el caso de raíces de la unidad de orden un primo l.

Proposición. *Para todo primo l el polinomio ciclotómico*

$$\Phi_l(x) = x^l + x^{l-1} + \cdots + x + 1 = (x^l - 1)/(x - 1)$$

es abeliano de conductor l.

Demostración. Las raíces de Φ_l en $\mathbb{C}$ son las $l-1$ raíces primitivas l-ésimas de la unidad. Aunque nos alcanzaría con saber que $S = \{l\}$ probemos que de hecho el discriminante Δ de Φ_l vale $(-1)^{\frac{1}{2}(l-1)} l^{l-2}$.

Para un polinomio mónico $f(x)$ de grado d

$$\operatorname{disc}(f) = (-1)^{\frac{1}{2}(d-1)} \prod_{\alpha} f'(\alpha),$$

donde α recorre las raíces de f y f' es la derivada de f respecto de x.

En nuestro caso

$$\Phi_l'(x) = \frac{lx^{l-1} - \Phi_l(x)}{x - 1}$$

con lo que $\Phi_l'(\zeta) = l\zeta^{l-1}/(\zeta - 1)$ para cada raíz ζ de Φ_l. Es fácil verificar que

$$\prod_{\zeta} \zeta^{l-1} = \Phi_l(0)^{-1} = 1, \qquad \prod_{\zeta} (\zeta - 1) = \Phi_l(1) = (-1)^{l-1} l$$

y encontramos que $\Delta = (-1)^{\frac{1}{2}(l-1)} l^{l-2}$.

Sea p un primo distinto de l y $q = p^n$ para algún $n \in \mathbb{N}$. Supongamos que $a \in \mathbb{F}_q$ es una raíz de Φ_l. No puede ser que $a = 1$ ya que $\Phi_l(1) = l$ y por hipótesis $p \nmid l$. Entonces a es un elemento de orden l del grupo $\mathbb{F}_q^*$ y como este grupo es de orden $q - 1$ tenemos que $l \mid q - 1$.

Reciprocamente, si $l \mid q - 1$ existe un $a \in \mathbb{F}_q^*$ de orden l; como $a^l = 1$ pero $a \neq 1$ tenemos que $\Phi_l(a) = 0$. Por el mismo motivo $\Phi_l(a^j) = 0$ para $j = 1, 2, \cdots, l - 1$ y $\Phi_l(x)$ tiene todas sus raíces en $\mathbb{F}_q$.

En conclusión, $N_q = l$ si $l \mid q - 1$ y $N_q = 0$ si $l \nmid q - 1$. Dejamos al lector verificar que entonces

$$Z_{\Phi_l, p}(T) = (1 - T^m)^{-r}, \qquad l - 1 = mr, \qquad p \neq l,$$

donde m es el orden de p mod l (es decir, la potencia mínima p^n que es congruente a 1 mod l). En particular, $Z_{\Phi_l, p}(T)$ solo depende de p mod l con lo que Φ_l es abeliano (tomando $N = l$ en la definición) de conductor l. $\square$

Notemos que hemos probado que el tipo de factorización t_p de Φ_l para $p \neq l$ es $[m, m, \cdots, m]$ donde m es el orden de $p \bmod l$. En particular, hay tantas posibilidades[4] para t_p como divisores de $l-1$. Esta es una proporción muy pequeña de todos los tipos de factorización posibles para un polinomio arbitrario de grado $l-1$. En general, para un d dado, el número de posibles tipos de factorización de un polinomio de grado d es $p(d)$, el número de particiones $d = d_1 + d_2 + \cdots + d_r$ con $0 < d_1 \leq d_2 \leq d_r$ y se sabe que [Ap]

$$p(d) \sim \frac{e^{\pi\sqrt{2d/3}}}{4\sqrt{3}\, d}, \qquad d \to \infty.$$

Si elegimos al azar un polinomio f, irreducible digamos, de grado d, con alta probabilidad[5] , el tipo de factorización de f módulo p tomará todos estos posibles valores al variar p; un polinomio abeliano en cambio tomará solo una fracción pequeña de estos. La propiedad de ser abeliano es muy especial.

6. Ecuaciones en una variable módulo una potencia p^n de un primo p

Sea $f \in \mathbb{Z}[x]$ un polinomio mónico de discriminante Δ no nulo. Queremos ahora estudiar la ecuación

$$f(x) \equiv 0 \bmod p^r$$

para p primo y $r \in \mathbb{N}$. Lo que veremos es que existe un r_0 tal que las soluciones para $r = r_0$ determinan las soluciones para todo r; si $p \nmid \Delta$ podemos tomar $r_0 = 1$.

Para todo número racional no nulo z vamos a denotar por $v_p(z)$ la *valuación* de z en p, es decir $z = p^{v_p(z)}u$ con u un racional con numerador y denominador no divisibles por p. Como es habitual $f'(x)$ denota la derivada de $f(x)$ con respecto a la variable x.

Lema de Hensel. *Sea $f \in \mathbb{Z}[x]$ y $x_0 \in \mathbb{Z}$ tal que*

$$f(x_0) \equiv 0 \bmod p^{r_0}$$

para un $r_0 \in \mathbb{N}$.

Si $r_0 > 2k$ donde $k = v_p(f'(x_0))$ entonces para todo $n \in \mathbb{N}$ existe un único $x_n \in \mathbb{Z}$ tal que

$$x_n \equiv x_0 \bmod p^{n+r_0-k-1}, \qquad f(x_n) \equiv 0 \bmod p^{r_0+n}$$

Demostración. Sea $m = r_0 - k$. Busquemos t tal que $x_1 = x_0 + tp^m$ cumpla lo requerido. Usando el teorema de Taylor vemos que

$$f(x_1) \equiv f(x_0) + tf'(x_0)p^m \bmod p^{2m}.$$

Dividiendo por p^{r_0}, planteamos la congruencia

$$f(x_0)p^{-r_0} + tf'(x_0)p^{-k} \equiv 0 \bmod p^{2m-r_0}$$

donde $2m - r_0 = r_0 - 2k > 0$ por hipótesis. Como $f'(x_0)p^{-k}$ es un entero coprimo con p podemos resolver la congruencia y encontrar t, que es claramente único módulo p. Dado que $2m = r_0 + (r_0 - 2k) > r_0$ vemos que $f(x_1) \equiv 0 \bmod p^{r_0+1}$.

Por otro lado,

$$f'(x_1) \equiv f'(x_0) + tf''(x_0)p^m \bmod p^{2m}$$

y como $m = r_0 - k > k$ tenemos que $v_p(f'(x_1)) = k$.

Repitiendo el proceso, por inducción, se encuentra la secuencia x_n buscada. Dejamos los detalles al lector. □.

Notemos que si $p \nmid \Delta$ podemos tomar $r_0 = 1$. En efecto, si p dividiera a $f(x_0)$ y $f'(x_0)$ entonces p dividiría a Δ que no es el caso. Por lo tanto si $f(x_0) \equiv 0 \bmod p$ necesariamente $v_p(f'(x_0)) = 0$ y se cumplen las hipótesis del lema con $r_0 = 1$.

En resumen, excepto para los primos $p \mid \Delta$ las soluciones de la congruencia $f(x) \equiv \bmod p^r$ para $r \in \mathbb{N}$ están en biyección con las soluciones de $f(x) \equiv 0 \bmod p$. En particular, hay el mismo número de soluciones a ambas congruencias. Mas aún, el lema nos da un algoritmo[6] para calcular esta biyección.

Por ejemplo, $x^2 + 1 \equiv 0 \bmod 5$ tiene dos soluciones $x_0 = \pm 2$ y por lo tanto $x^2 + 1 \equiv 0 \bmod 5^r$ tiene dos soluciones para todo $r \in \mathbb{N}$; para $r = 15$ las dos soluciones son

$$x = \pm(2+5+2\cdot 5^2+5^3+3\cdot 5^4+4\cdot 5^5+2\cdot 5^6+3\cdot 5^7+3\cdot 5^9+2\cdot 5^{10}+2\cdot 5^{11}+4\cdot 5^{13}+5^{14})$$

El lema de Hensel tambien se puede aplicar a polinomios en cualquier número de variables, por ejemplo, fijando todas las variables salvo una.

Ejercicio 2. Sea a un entero impar. Probar que existe una solución de

$$a \equiv u^2 \bmod 2^r, \qquad \text{para todo } r \in \mathbb{N}$$

si y solo si $a \equiv 1 \bmod 8$.

§2 Funciones Zeta: aspectos analíticos

En esta sección estudiaremos algunos aspectos analíticos de la funciones zeta; dejamos varios detalles, convergencia, intercambio de suma e integral, etc., a cargo del lector.

Sea $f \in \mathbb{Z}[x]$ un polinomio mónico con discriminante Δ no nulo y sea S el conjunto de primos $p \mid \Delta$. Para cada $p \notin S$ tenemos la función zeta $Z_{f,p}(T)$ del

polinomio $f \bmod p$. Ahora vamos a poner juntas todas todas las $Z_{f,p}(T)$ en una sola función de una variable compleja s

$$Z_f(s) = \prod_{p \notin S} Z_{f,p}(p^{-s}),$$

pronto veremos que este producto converge para $\Re(s) > 1$ y $Z_f(s)$ es una función analítica en ese dominio. Empezamos con una instancia particular fundamental.

7. La función zeta de Riemann $\zeta(s)$.

Consideremos el caso en que $f(x) = x$. Desde el punto de vista de la ecuación $x = 0$ que determina no hay mucho por decir: $\Delta = 1$, con lo que $S = \emptyset$, y $Z_{f,p}(T) = 1/(1-T)$ para todo p (el tipo de factorización es [1] para todo p); podríamos decir que en este ejemplo la dirección geométrica es trivial. Sin embargo, queda la dirección aritmética, es decir los números primos; en efecto, la función $Z_f(s)$ es la función *zeta de Riemann*

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}, \qquad \Re(s) > 1\ .$$

Llamamos a esta expresión el *producto de Euler* para ζ y a $1 - p^{-s}$ el *factor de Euler* en p. La función zeta de Riemann también puede darse como

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \qquad \Re(s) > 1$$

y la igualdad de ambas expresiones es equivalente al hecho que todo número natural se escribe en forma única como producto de primos. En efecto, tenemos para todo primo p

$$(1 - p^{-s})^{-1} = 1 + p^{-s} + p^{-2s} + \cdots ;$$

al expandir el producto todo sobre p obtendremos términos de la forma

$$p_1^{-e_1 s} \cdot p_2^{-e_2 s} \cdots p_r^{-e_r s}$$

con $e_1, e_2, \cdots, e_r \in \mathbb{N}$ que corresponden a un único término n^{-s} de la suma. No es difícil formalizar rigurosamente este argumento como vemos a continuación.

Sea $s = \sigma + it$ con $\sigma = \Re(s) > 1$. Usando el criterio de la integral vemos que

$$\left| \sum_{n=1}^{N} n^{-s} \right| \leq \sum_{n=1}^{N} n^{-\sigma} \leq 1 + \int_1^N x^{-\sigma}\, dx = 1 + \frac{1}{\sigma - 1}(1 - \frac{1}{N^{\sigma-1}})$$

con lo que la serie converge uniformemente en la banda $\sigma_1 \leq \sigma \leq \sigma_2$ para todo $1 < \sigma_1, \sigma_2$ y por lo tanto define una función analítica de s en el dominio $\Re(s) > 1$.

Por otro lado, para todo $P \geq 2$ tenemos

$$\prod_{p \leq P} (1 - p^{-s})^{-1} = \prod_{p \leq P} \sum_{e=0}^{\infty} p^{-es} = \sum_{n \in \mathcal{N}_P}^{\infty} n^{-s},$$

donde

$$\mathcal{N}_P = \{n \in \mathbb{N} \,|\, \text{todo primo } p \mid n \text{ satisface } p \leq P\}$$

con lo que el producto converge a la suma.

Combinando este análisis con los resultados del nº 4 se prueba facilemente lo afirmado al final del nº 6 sobre las propiedades de $Z_f(s)$ en general.

Usando otra vez el criterio de la integral vemos que

$$\sum_{n=1}^{N} n^{-s} \geq \int_1^{N+1} x^{-s}\, dx = \frac{1}{s-1}(1 - \frac{1}{N^{s-1}}), \qquad s > 1$$

y tomando $N \longrightarrow \infty$ deducimos que

$$\zeta(s) \geq \frac{1}{s-1}, \qquad s > 1$$

Por lo tanto

$$\lim_{s \searrow 1} \zeta(s) = +\infty \tag{5}$$

y en consecuencia *hay infinitos números primos*! (Si hubiera un número finito de primos la expresión del producto para ζ diría que $\lim_{s \searrow 1} \zeta(s)$ es finito.)

Esta es la demostración de Euler de la infinitud de números primos. Es el paradigma de lo que uno espera de las funciones zeta: propiedades analíticas de la función zeta asociadas a algún objeto aritmético/geométrico (por ejemplo, su orden de cero o polo para ciertos valores de s) deberían reflejar propiedades aritméticas/geométricas de este.

8. Repaso de la función gamma

Incluimos en este nº ciertas propiedades básicas de la función gamma[7] para las que pueden consultarse, por ejemplo, [WW].

La función gamma puede definirse como

$$\Gamma(s) := \int_0^{\infty} e^{-t} t^s\, \frac{dt}{t}, \qquad \Re(s) > 0.$$

En la banda $0 < \sigma_1 \leq s \leq \sigma_2$ tenemos

$$\left| \int_0^1 e^{-t} t^s\, \frac{dt}{t} \right| \leq \int_0^1 e^{-t} t^{\sigma_1}\, \frac{dt}{t} \leq \int_0^1 t^{\sigma_1 - 1}\, dt = \frac{1}{\sigma_1}$$

y

$$\left| \int_1^\infty e^{-t} t^s \, \frac{dt}{t} \right| \leq \int_1^\infty e^{-t} t^{\sigma_2 - 1} \, dt.$$

Es fácil acotar esta última integral por una constante dependiendo solo de σ_2 (por ejemplo, integrando sucesivamente por partes). Por lo tanto la integral que define a $\Gamma(s)$ en efecto converge para $\Re(s) > 0$ y $\Gamma(s)$ es analítica en ese dominio.

La función gamma tiene una extensión meromorfa a todo el plano complejo con solo polos simples en $s = -n$, $n = 0, 1, 2, \cdots$ de residuo $(-1)^n/n!$; satisface la ecuación funcional

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

de donde obtenemos que

$$\Gamma(n+1) = n!, \qquad n = 0, 1, 2, \cdots .$$

$\Gamma(s)$ no se anula para ningún valor de s y satisface la identidad (*fórmula de duplicación*)

$$\Gamma(\tfrac{1}{2}s)\,\Gamma(\tfrac{1}{2}(s+1)) = 2^{1-s}\sqrt{\pi}\,\Gamma(s).$$

Notemos el siguiente hecho útil. El cambio de variables $t \mapsto at$ para $a > 0$ muestra que

$$\Gamma(s)\, a^{-s} = \int_0^\infty e^{-at} t^s \, \frac{dt}{t}. \tag{6}$$

(Una buena razón para escribir dt/t en lugar de simplemente dt es que el diferencial dt/t es invariante por este cambio de variable.)

9. Ecuación funcional: Zeta y Theta

En lo que sigue probaremos que la función $\zeta(s)$ a priori solo definida para $\Re(s) > 1$ tiene una continuación analítica a todo el plano complejo , excepto por un polo simple en $s = 1$. También probaremos que existe una relación entre $\zeta(s)$ y $\zeta(1-s)$; esta *ecuación funcional* es mejor expresarla en términos de la función

$$\zeta^*(s) = \pi^{-\frac{1}{2}s}\Gamma(\tfrac{1}{2}s)\,\zeta(s),$$

para la que es simplemente

$$\zeta^*(1-s) = \zeta^*(s). \tag{7}$$

La demostración de esta ecuación que sigue se debe a Riemann.

Usando (6) con $a = \pi n^2$, $n = 1, 2, \cdots$, reemplazado s por $s/2$, y luego sumando sobre todo n obtenemos

$$\zeta^*(s) = \int_0^\infty \sum_{n=1}^\infty e^{-\pi n^2 t} t^{\frac{1}{2}s} \, \frac{dt}{t}.$$

Introducimos ahora la función θ, definida por la serie rápidamente convergente

$$\theta(t) := \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t}, \qquad t > 0.$$

La ecuación funcional (7) es una consecuencia de la siguiente ecuación funcional para θ

$$\theta(\tfrac{1}{t}) = t^{\frac{1}{2}} \, \theta(t), \qquad t > 0 \tag{8}$$

que probaremos en el siguiente n$^{\text{o}}$. En efecto,

$$\zeta^*(s) = \int_0^\infty \tfrac{1}{2}(\theta(t) - 1) \, t^{\frac{1}{2}s} \, \frac{dt}{t}, \qquad \Re(s) > 0.$$

Escribiendo la integral como $\int_0^1 + \int_1^\infty$, haciendo el cambio de variables $t \mapsto 1/t$ en la primer integral y usando (8) obtenemos

$$\begin{aligned}
\zeta^*(s) &= \tfrac{1}{2} \int_1^\infty (\theta(t) - 1) \, t^{\frac{1}{2}s} \, \frac{dt}{t} + \tfrac{1}{2} \int_1^\infty (t^{\frac{1}{2}}\theta(t) - 1) \, t^{-\frac{1}{2}s} \, \frac{dt}{t} \\
&= -\tfrac{1}{2} \int_1^\infty ((t^{-\frac{1}{2}s} - t^{\frac{1}{2}(1-s)}) \, \frac{dt}{t} + \tfrac{1}{2} \int_1^\infty (\theta(t) - 1) \, (t^{\frac{1}{2}s} + t^{\frac{1}{2}(1-s)}) \, \frac{dt}{t} \\
&= -\frac{1}{s} + \frac{1}{s-1} + \tfrac{1}{2} \int_1^\infty (\theta(t) - 1) \, (t^{\frac{1}{2}s} + t^{\frac{1}{2}(1-s)}) \, \frac{dt}{t}
\end{aligned}$$

La integral en la última expresión converge para todo s, ya que $\theta(t) - 1$ decrece exponencialmente, y define una función entera de s. Los dos primeros términos muestran que $\zeta^*(s)$ tiene polos simples en $s = 0, 1$ de residuo $-1, 1$ respectivamente. Es claro también de la última expresión que $\zeta^*(s)$ satisface la ecuación funcional (7). Como $\Gamma(s)$ no se anula para ningún s y tiene un polo simple en $s = 0$ deducimos que $\zeta(s) = \pi^{\frac{1}{2}s}/\Gamma(s/2)\,\zeta^*(s)$ es analítica excepto por un polo simple en $s = 1$ de residuo 1 (comparar esto último con (5)).

Ejercicio 3.

(1) Verificar que $\zeta(s)$ tiene ceros simples en $s = -2, -4, \cdots$.
(2) ¿Cual es el valor de $\zeta(0)$?

Los valores de las funciones zeta (o L que veremos más adelante) en $s = k$, donde k son ciertos números enteros, juegan un papel importante en la Teoría de Números. No ahondaremos en este tema pero damos de todas maneras una breve descripción de estos valores en el caso de la función zeta de Riemann.

Euler probó que los valores de la función $\zeta(s)$ para $s > 1$ entero par pueden calcularse explícitamente en términos de números de Bernoulli (ver por ejemplo [Se1, p. 149]).

$$\zeta(2k) = (-1)^{k+1}\frac{2^{2k-1}}{(2k)!}B_{2k}\pi^{2k}, \qquad k \in \mathbb{N}\,,$$

donde los números de Bernoulli B_n están definidos por medio de la expansión

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}\,.$$

Sus primeros valores son

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30}, \quad B_6 = \frac{5}{66}\,,$$

y $B_{2k+1} = 0$ para todo $k \in \mathbb{N}$. Como suele ser el caso, la expresión para $\zeta(2k)$ se vuelve mucho más sencilla si se expresa como $\zeta(1-2k)$ por medio de la ecuación funcional,

$$\zeta(1-2k) = -\frac{B_{2k}}{2k}, \qquad k \in \mathbb{N}.$$

¿Qué puede decirse de $\zeta(k)$ para $k \in \mathbb{N}, k > 1$ impar? Pues no mucho; esencialmente lo único que sabemos de la naturaleza de estos números es el resultado[8] relativamente reciente de Apéry que $\zeta(3)$ es irracional.

10. Formula de sumación de Poisson

Nos queda por demostrar la ecuación funcional (8) para $\theta(t)$. Para ello usaremos la sumación de Poisson que es una herramienta fundamental de independiente interés.

Para $x, y \in \mathbb{R}^n$ denotamos con $x \cdot y$ el producto escalar usual.

Formula de sumación de Poisson. *Sea $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ una función C^∞ de decrecimiento rápido y sea*

$$\hat{f}(y) = \int_{\mathbb{R}^n} f(x)e^{-2\pi i x\cdot y}\,dx$$

su transformada de Fourier. Entonces

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

Idea de la demostración. Consideramos la función periódica

$$h(x) = \sum_{m \in \mathbb{Z}^n} f(x+m)$$

y su serie de Fourier

$$h(x) = \sum_{m \in \mathbb{Z}^n} c_m e^{2\pi i m \cdot x}$$

con

$$c_m = \int_{[0,1]^n} h(x)\, e^{-2\pi i m \cdot x}\, dx.$$

Reemplazando la definición de h en términos de f vemos que

$$\begin{aligned} c_m &= \sum_{l \in \mathbb{Z}^n} \int_{[0,1]^n} f(x+l)\, e^{-2\pi i m \cdot x}\, dx \\ &= \int_{\mathbb{R}^n} f(x)\, e^{-2\pi i m \cdot x}\, dx \\ &= \hat{f}(m) \end{aligned}$$

y poniendo $x = 0$ obtenemos

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

que es lo que queríamos probar. □.

Tomemos ahora $f(x) = e^{-\pi x^2 t}$ con $x, t \in \mathbb{R}$ y $t > 0$. No es difícil probar que en ese caso

$$\hat{f}(y) = t^{-\frac{1}{2}} e^{-\frac{\pi y^2}{t}} \tag{9}$$

y la fórmula de Poisson nos da exactamente (8).

Ejercicio 4. Probar (9). (Una manera de hacerlo es usar el teorema de residuos para la integral de $e^{-\pi z^2}$ sobre un rectángulo conveniente tomando luego limite en el tamaño del rectángulo)

§3 Cálculo de algunas funciones zeta

Calcularemos en esta sección la función zeta de algunos polinomios abelianos particulares. Para simplificar la exposición elegimos polinomios con conductor primo.

11. La función zeta de Φ_l

Fijemos un primo $l > 2$. Recordemos que el polinomio ciclotómico

$$\Phi_l(x) = x^l + x^{l-1} + \cdots + x + 1 = (x^l - 1)/(x - 1)$$

tiene

$$Z_{\Phi_l,p}(T) = (1 - T^m)^{-r}, \qquad l - 1 = mr, \qquad p \neq l,$$

donde m es el orden de $p \bmod l$. Sea G el grupo de homomorfismos

$$\chi : (\mathbb{Z}/l\mathbb{Z})^* \longrightarrow \mathbb{C}^*;$$

diremos que χ es un *carácter módulo* l. Abusando un poco la notación llamaremos también χ a la función $\mathbb{Z} \longrightarrow \mathbb{C}^*$ que en $n \in \mathbb{Z}$ vale $\chi(n \bmod l)$ si $l \nmid n$ y 0 si $l \mid n$. Como $(\mathbb{Z}/l\mathbb{Z})^*$ es cíclico de orden $l - 1$ también G es cíclico de ese orden.

Vamos a usar el grupo G de caracteres módulo l para reescribir la función zeta $Z_{\Phi_l,p}(T)$ de una manera más conveniente.

Lema. *Para todo primo $p \neq l$ tenemos*

$$Z_{\Phi_l,p}(T) = \prod_{\chi \in G} (1 - \chi(p)T)^{-1}$$

Demostración. Como antes, sea m el orden de $p \bmod l$ y $p - 1 = mr$. Sea χ_1 un generador de G. Todo $\chi \in G$ se escribe de forma única como $\chi = \chi_1^a(\chi_1^m)^b$ con $0 \leq a < m$ y $0 \leq b < r$. Como p tiene orden m módulo l tenemos que $\chi(p) = \chi_1^a(p)$ y $\chi_1(p) \in \mathbb{C}^*$ es una raíz primitiva m-ésima de la unidad. Por lo tanto

$$\begin{aligned}
\prod_{\chi \in G} (1 - \chi(p)T)^{-1} &= \prod_{0 \leq a < m} \prod_{0 \leq b < r} (1 - \chi_1(p)T)^{-1} \\
&= \prod_{0 \leq a < m} (1 - \chi_1(p)T)^{-r} \\
&= (1 - T^m)^{-r} \\
&= Z_{\Phi_l,p}(T)
\end{aligned}$$

y queda demostrada la igualdad. □

Concluimos entonces que

$$Z_{\Phi_l}(s) = \prod_{p \neq l} \prod_{\chi \in G} (1 - \chi(p)p^{-s})^{-1}, \qquad \Re(s) > 1.$$

12. Funciones L de Dirichlet

Estudiemos los factores de $Z_{\Phi_l}(s)$ correspondientes a cada $\chi \in G$ por separado. Denotemos con χ_0 el carácter trivial de G. Para $\chi \in G$ un carácter no trivial definimos

$$L(\chi, s) := \prod_{p \neq l} (1 - \chi(p)p^{-s})^{-1}, \qquad \Re(s) > 1, \qquad \chi \neq \chi_0,$$

la *función L de Dirichlet*[9] asociada a χ. Argumentos virtualmente idénticos a los de nº 7 muestran que la serie converge uniformemente en bandas verticales de $\Re(s) > 1$ con lo que $L(\chi, s)$ es analítica en ese dominio. También como χ es multiplicativa tenemos que

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n)\ n^{-s}$$

(recordemos que pusimos $\chi(n) = 0$ para n tales que $l \mid n$).

Las funciones $L(\chi, s)$ también se extienden a todo el plano complejo y satisfacen una ecuación funcional análoga a (7). Hay dos casos distintos según que $\chi(-1) = \pm 1$; si $\chi(-1) = 1$ decimos que χ es *par*, y si $\chi(-1) = -1$ que es *impar*.

Sea $\delta = 0, 1$ tal que $\chi(-1) = (-1)^\delta$,

$$\tau(\chi) := \sum_{k=1}^{l-1} \chi(k)\ e^{2\pi i k/l}$$

la *suma de Gauss* asociada a χ y

$$L^*(\chi, s) = \left(\frac{\pi}{l}\right)^{-\frac{1}{2}s} \Gamma(\tfrac{1}{2}(s + \delta))\, L(\chi, s)$$

entonces

$$L^*(\chi, s) = w_\chi L^*(\bar{\chi}, 1 - s),$$

donde

$$w_\chi = \frac{\tau(\chi)}{i^\delta \sqrt{l}}.$$

La demostración de la ecuación funcional es análoga a la de la función zeta de Riemann que vimos en nº 9. La función que cumple el rol de $\theta(t)$ es ahora

$$\theta_\chi(t) = \sum_{n \in \mathbb{Z}} \chi(n)\ n^\delta\ e^{-\pi n^2 t/l}$$

que satisface la ecuación funcional

$$\theta_{\bar{\chi}}(1/t) = w_\chi t^{\delta + \frac{1}{2}}\ \theta_\chi(t), \tag{10}$$

cuya demostración se puede dar, como la de $\theta(t)$, usando la formula de sumación de Poisson. (Nótese que $\sum_{n \in \mathbb{Z}} \chi(n)\ n\ e^{-\pi n^2 t/l}$ si χ es par y $\sum_{n \in \mathbb{Z}} \chi(n)\ e^{-\pi n^2 t/l}$ si χ es impar son idénticamente cero.)

Damos algunos detalles para el caso en que χ es par. Sea $f(x) = e^{-\pi x^2 t}$ con $t > 0$. Con la notación de la demostración de la fórmula de Poisson (ver n$^{\text{o}}$ 10), evaluamos h, no en $x = 0$ como hicimos entonces, si no en $x = k/l$, donde $k = 1, 2, \cdots, l-1$, para obtener

$$\sum_{m\in\mathbb{Z}} e^{-\pi(m+k/l)^2 t} = t^{-\frac{1}{2}} \sum_{m\in\mathbb{Z}} e^{2\pi i m k/l}\, e^{-\pi m^2/t}.$$

Multiplicando ambos lados de la ecuación por $\chi(k)$ y sumando sobre k encontramos que

$$\theta_\chi(t/l) = t^{-\frac{1}{2}} \sum_{m\in\mathbb{Z}} \sum_{k=1}^{l-1} \chi(k)\, e^{2\pi i m k/l}\, e^{-\pi m^2/t}, \qquad \chi(1) = 1. \tag{11}$$

Ahora como χ es un carácter, si $l \nmid m$

$$\chi(m) \sum_{k=1}^{l-1} \chi(k)\, e^{2\pi i m k/l} = \sum_{k=1}^{l-1} \chi(mk)\, e^{2\pi i m k/l} = \tau(\chi)$$

y por lo tanto

$$\sum_{k=1}^{l-1} \chi(k)\, e^{2\pi i m k/l} = \bar{\chi}(m)\, \tau(\chi).$$

Reemplazando t por lt en (11) vemos entonces que

$$\theta_{\bar{\chi}}(1/t) = w_\chi t^{\frac{1}{2}}\, \theta_\chi(t), \tag{12}$$

como queríamos demostrar.

No es difícil ver que

$$\overline{w}_\chi = w_{\bar{\chi}}, \qquad w_\chi w_{\bar{\chi}} = 1, \qquad \chi \neq \chi_0, \tag{13}$$

(para la segunda igualdad se pueden combinar, por ejemplo, las ecuaciones funcionales para χ y $\bar{\chi}$).

Notemos que $\theta_\chi(t)$ con $\chi \neq \chi_0$ no tiene término constante (como serie de potencias en $e^{-\pi t}$) ya que $\chi(0) = 0$ por definición. Este hecho se traduce en que $L(\chi, s)$ se extiende como función *analítica* a todo el plano complejo. (En contraste con $\zeta(s)$ que, como vimos, tiene un polo simple en $s = 1$.)

Ejercicio 5. Dar los detalles de la demostración de (11), (12) y (13).

11. La función zeta de Φ_l nuevamente

En el nº anterior tratamos el caso en que $\chi \in G$ es no trivial. ¿Qué pasa cuando $\chi = \chi_0$? En ese caso $\chi(n) = 1$ si $l \nmid n$ y $\chi(n) = 0$ si $l \mid n$ con lo que tendríamos

$$L(\chi_0, s) = \sum_{\substack{n=1 \\ p \nmid n}}^{\infty} n^{-s}$$

$$= \prod_{p \neq l} (1 - p^{-s})^{-1}$$
$$= (1 - l^{-s})\zeta(s)$$

Para tratar de una forma más uniforme todo los caracteres de G vamos ahora a cambiar la notación. Redefinimos el carácter trivial de G como $\chi_0(n) = 1$ para *todo* n. (Mirado módulo l sigue siendo el carácter trivial de $(\mathbb{Z}/l\mathbb{Z})^*$, lo que hemos cambiado es su levantamiento como función de $\mathbb{Z}$ en $\mathbb{C}$.) Con esta nueva definición tenemos que $L(\chi_0, s) = \zeta(s)$ y

$$Z_{\Phi_l}(s) = (1 - l^{-s}) \prod_{\chi \in G} L(\chi, s).$$

Notemos que para todo carácter χ de G, $L(\chi, s)$ se extiende analíticamente a todo el plano complejo (excepto por un polo simple en $s = 1$ cuando $\chi = \chi_0$) y satisface una ecuación funcional con $s \mapsto 1 - s$. Por lo tanto si definimos

$$Z^*_{\Phi_l}(s) := (2\sqrt{\pi})^{\frac{1}{2}(1-l)} \prod_{\chi \in G} L^*(\chi, s)$$

entonces

$$Z^*_{\Phi_l}(1 - s) = w \; Z^*_{\Phi_l}(s),$$

donde

$$w = \prod_{\chi \in G} w_\chi.$$

Elegimos la constante en la definición de $Z^*_{\Phi_l}$ de tal manera que

$$Z^*_{\Phi_l}(s) = \left[\left(\frac{2\pi}{l} \right)^{-s} \Gamma(s) \right]^{\frac{1}{2}(l-1)} \prod_{\chi \in G} L(\chi, s),$$

una igualdad que se puede probar usando la fórmula de duplicación de $\Gamma(s)$ (ver nº 8).

Mencionemos dos resultados[10] no triviales; para su demostración referimos al lector a [IR].

Teorema.

(1) *Para todo $\chi \in G$ no trivial tenemos*

$$L(\chi, 1) \neq 0, \qquad \chi \neq \chi_0.$$

(2)

$$w = \prod_{\chi \in G} w_\chi = 1$$

Corolario. *La función $Z^*_{\Phi_l}(s)$ es analítica en todo el plano complejo excepto por polos simples en $s = 0, 1$ y satisface la ecuación funcional*

$$Z^*_{\Phi_l}(1 - s) = Z^*_{\Phi_l}(s).$$

Demostración. Sabemos que $L^*(\chi, s)$ es analítica si $\chi \neq \chi_0$ y tiene un polo simple en $s = 1$ si $\chi = \chi_0$. Por el teorema este polo simple no es cancelado por ningún cero en el producto. □

Ejercicio 6.

(1) Mostrar que $w = 1$ es equivalente a que

$$\tau(\chi_*) = \begin{cases} \sqrt{l} & \text{si } l \equiv 1 \bmod 4 \\ i\sqrt{l} & \text{si } l \equiv 3 \bmod 4 \end{cases}$$

donde $\chi_* \in G$ es el único carácter de orden 2.

(2) Encontrar el orden de cero de $\prod_{\chi \in G} L(\chi, s)$ en $s = 0$.

12. La ley de reciprocidad cuadrática

En este nº vamos a enunciar la ley de reciprocidad cuadrática en forma precisa, aunque algo incompleta, en términos de series de Dirichlet. La versión completa de la LRC, incluyendo su demostración, puede encontrase en [Se1].

Fijemos como antes un primo $l > 2$ y sea G el grupo de caracteres módulo l. Denotaremos con χ_* el único carácter en G de orden 2 (recordemos que G es cíclico).

Consideremos polinomios $f(x) = x^2 + rx + s \in \mathbb{Z}[x]$ de discriminante $\Delta = r^2 - 4s = \pm l$.

Ejercicio 7. Probar que para todo número impar d existe un $f(x) = x^2 + rx + s \in \mathbb{Z}[x]$ con discriminante $\Delta = \pm d$ y que para todo tal f necesariamente $\pm = (-1)^{\frac{1}{2}(d-1)}$.

Teorema (LRC). *Sea* $f(x) = x^2 + rx + s \in \mathbb{Z}[x]$ *de discriminante*

$$\Delta = r^2 - 4s = (-1)^{\frac{1}{2}(l-1)} l,$$

con $l > 2$ *primo, y sea* χ_* *el único carácter módulo* l *de orden* 2. *Entonces*

$$Z_f(s) = (1 - l^{-s})\, \zeta(s)\, L(\chi_*, s).$$

Para relacionar esta formulación[11] de la LRC con la tradicional, recordemos la noción de *símbolo de Legendre*. Dado un entero cualquiera d y un primo $p \nmid 2d$ definimos

$$\left(\frac{d}{p}\right) := \begin{cases} 1 & x^2 \equiv d \bmod p \quad \text{tiene solución} \\ -1 & x^2 \equiv d \bmod p \quad \text{no tiene solución} \end{cases}$$

Claramente $\left(\frac{d}{p}\right)$ solo depende de d módulo p.

El tipo de factorización de f para $p \nmid 2l$ es

$$t_p = \begin{cases} [1,1] & \left(\frac{\Delta}{p}\right) = +1 \\ [2] & \left(\frac{\Delta}{p}\right) = -1 \end{cases}$$

Por otro lado, sabemos que

$$t_p = \begin{cases} [1,1] & Z_{f,p}(T) = 1/(1-T)^2 \\ [2] & Z_{f,p}(T) = 1/(1-T^2). \end{cases}$$

Comparando con la expresión para $Z_f(s)$ provista por el teorema deducimos[12] que

$$\left(\frac{\Delta}{p}\right) = \chi_*(p), \qquad p \nmid 2l, \quad \Delta = (-1)^{\frac{1}{2}(l-1)} l.$$

Por ejemplo, si $l = 5$ y $5 \nmid n$ entonces $\chi_*(n) = 1$ si $n \equiv \pm 1 \bmod 5$ y $\chi_*(n) = -1$ si $n \equiv \pm 2 \bmod 5$. Por lo tanto, para todo primo $p \neq 2, 5$, se tiene que 5 es un cuadrado módulo p si y solo si $p \equiv \pm 1 \bmod 5$.

Ejercicio 8. Dar una demostración elemental de que para todo primo $p > 3$, -3 es un cuadrado módulo p si y solo si $p \equiv 1 \bmod 3$.

II – Dimensión 1

Pasamos ahora a estudiar ecuaciones en congruencia en más de una variable donde la geometría jugará un rol mas importante. Empezamos naturalmente con el caso de dos variables. Los ceros de un polinomio en dos variables definen una *curva algebraica*. Nuestro primer ejemplo son unas curvas muy famosas.

13. Curvas de Fermat

Para cada entero $n > 1$ la *curva de Fermat* F_n se define como

$$x^n + y^n = 1.$$

Nos interesa contar el número de soluciones a esta ecuación con x, y en un cuerpo finito. Fijemos entonces un cuerpo finito $\mathbb{F}_q$ con $q = p^r$ para algún primo p y algún $r \in \mathbb{N}$. Para $f \in \mathbb{F}_q[x, y]$ y $a \in \mathbb{F}_q$ denotemos con $N_q(f(x, y) = a)$ el número de soluciones $x, y \in \mathbb{F}_q$ a la ecuación $f(x, y) = a$.

Lema. *Sea $n \in \mathbb{N}$, $a \in \mathbb{F}_q^*$ y $m = \mathrm{mcd}(n, q-1)$. Entonces*

$$N_q(x^n = a) = \sum_{\chi \in G} \chi(a),$$

donde G es el grupo de caracteres $\mathbb{F}_q^* \to \mathbb{C}^*$ de orden dividiendo m.

Demostración. La aplicación $x \mapsto x^k$ en $\mathbb{F}_q^*$ es un isomorfismo si (y solo si) k y $q-1$ son coprimos. Por lo tanto $N_q(x^n = a) = N_q(x^m = a)$ y sin perdida de generalidad podemos asumir que $n = m$. Si $b \in \mathbb{F}_q$ es tal que $b^m = a$ entonces $\chi(a) = \chi(b)^m = 1$ para todo $\chi \in G$ y la suma en la derecha da m, el orden de G (recordemos que $\mathbb{F}_q^*$ es cíclico). También es m el número de tales b ya que $m \mid q-1$ y por lo tanto existen exactamente m elementos en $\mathbb{F}_q^*$ de orden dividiendo a m.

Por otro lado, si no hay una solución a $x^m = a$ en $\mathbb{F}_q$ tomemos $\chi_1 \in G$ de orden m. Usando una vez más que $\mathbb{F}_q^*$ es cíclico es fácil ver que el núcleo de χ_1 consiste de las potencias m-estimas de $\mathbb{F}_q^*$ con lo que $\chi_1(a) \neq 1$. Pero como

$$\sum_{\chi \in G} \chi(a) = \chi_1(a) \sum_{\chi \in G} \chi(a)$$

tenemos que $\sum_{\chi \in G} \chi(a) = 0$. □

Extendemos la definición de $\chi \in G$ a todo $\mathbb{F}_q$ declarando que

$$\chi(0) := \begin{cases} 1 & \chi \text{ es trivial} \\ 0 & \chi \text{ no es trivial} \end{cases}$$

(comparece esto con nº 11). Con esta definición el lema es valido para todo $a \in \mathbb{F}_q$.

Necesitamos las *suma de Jacobi*

$$J(\chi,\chi') := \sum_{a\in\mathbb{F}_q} \chi(a)\chi'(1-a), \qquad \chi,\chi' \in G.$$

Podemos ahora dar una fórmula preliminar para el número de puntos de la curva de Fermat en $\mathbb{F}_q$.

Corolario.

$$N_q(x^n+y^n=1) = \sum_{\chi,\chi'\in G} J(\chi,\chi').$$

Demostración. Es fácil ver que

$$N_q(x^n+y^n=1) = \sum_{\substack{a,b\in\mathbb{F}_q \\ a+b=1}} N_q(x^n=a)N_q(y^n=b),$$

que por el lema puede reescribirse como

$$\sum_{\substack{a,b\in\mathbb{F}_q \\ a+b=1}} \sum_{\chi\in G} \chi(a) \sum_{\chi'\in G} \chi(b) = \sum_{\chi,\chi'\in G} \sum_{\substack{a,b\in\mathbb{F}_q \\ a+b=1}} \chi(a)\chi(b). \quad \square$$

14. Sumas de Gauss y Jacobi

Dado $\chi_1,\chi_2,\cdots,\chi_k$ caracteres de $\mathbb{F}_q^*$ definimos la *suma de Jacobi*

$$J(\chi_1,\chi_2,\cdots,\chi_k) := \sum_{a_1+a_2+\cdots+a_k=1} \chi_1(a_1)\cdot\chi_2(a_2)\cdots\chi_k(a_k).$$

Si $k=1$ definimos $J(\chi_1) := 1$.

Dado un carácter χ de $\mathbb{F}_q^*$ definimos la *suma de Gauss*

$$\tau(\chi) := \sum_{a\in\mathbb{F}_q^*} \chi(a)\psi(a),$$

donde

$$\psi(a) := e^{\frac{2\pi i}{p} T_{\mathbb{F}_q/\mathbb{F}_p}(a)}.$$

(Aquí abusamos la notación, $b = T_{\mathbb{F}_q/\mathbb{F}_p}(a)$ es un elemento de $\mathbb{F}_p$ que visto como $\mathbb{Z}/p\mathbb{Z}$ permite levantar b a un entero $\tilde{b}$ y lo que realmente queremos es $e^{2\pi i\tilde{b}/p}$, cuyo valor es independiente de la elección de $\tilde{b}$.) Notemos que $\psi : \mathbb{F}_q \longrightarrow \mathbb{C}^*$ es un carácter aditivo, es decir, $\psi(a+b) = \psi(a)\psi(b)$. (Ambas sumas[13] generalizan las definidas anteriormente.) Denotamos como antes con χ_0 al carácter trivial.

Ejercicio 9. Probar que

$$\tau(\chi_0) = 0, \qquad |\tau(\chi)| = \sqrt{q}, \qquad \chi \neq \chi_0$$

Veremos ahora como estas sumas están relacionadas.

Teorema.

(1)
$$J(\chi_0, \chi_0, \cdots, \chi_0) = q^{k-1}$$

(2) *Si χ_j es trivial para algún $j = 1, 2, \cdots, k$ pero no todo χ_j es trivial entonces*
$$J(\chi_1, \chi_2, \cdots, \chi_k) = 0$$

(3) *Si ningún χ_j, $j = 1, 2, \cdots, k$ es trivial pero $\prod_j \chi_j = \chi_0$ entonces*
$$J(\chi_1, \chi_2, \cdots, \chi_k) = -\chi_k(-1) J(\chi_1, \chi_2, \cdots, \chi_{k-1}).$$

(4) *Si ningún χ_j, $j = 1, 2, \cdots, k$ es trivial y tampoco $\prod_j \chi_j$ es trivial entonces*
$$J(\chi_1, \chi_2, \cdots, \chi_k) = \frac{\tau(\chi_1)\tau(\chi_2)\cdots\tau(\chi_k)}{\tau(\chi_1\chi_2\cdots\chi_k)}$$

Demostración. Damos la demostración de (4) y dejamos las otras propiedades al lector.

$$\tau(\chi_1)\tau(\chi_2)\cdots\tau(\chi_k) = \sum_{b\in\mathbb{F}_q} \left[\sum_{a_1+a_2+\cdots+a_k=b} \chi_1(a_1)\chi_2(a_2)\cdots\chi_k(a_k) \right] \psi(b)$$

Es fácil ver que la suma interior es 0 para $b = 0$. Par $b \neq 0$ hacemos la substitución $a_j \mapsto ba_j$ para todo $j = 1, 2, \cdots, k$ para obtener

$$\sum_{a_1+a_2+\cdots+a_k=b} \chi_1(a_1)\chi_2(a_2)\cdots\chi_k(a_k) = \chi_1\chi_2\cdots\chi_k(b)\ J(\chi_1, \chi_2, \cdots, \chi_k)$$

y la identidad queda demostrada. □

Corolario. *Si $\chi_1, \chi_2, \cdots, \chi_k$ son no triviales entonces*

$$|J(\chi_1, \chi_2, \cdots, \chi_k)| = \begin{cases} q^{\frac{1}{2}k-1} & \chi_1\chi_2\cdots\chi_k = \chi_0 \\ q^{\frac{1}{2}(k-1)} & \chi_1\chi_2\cdots\chi_k \neq \chi_0 \end{cases}$$

15. La función zeta de F_n

Estamos ahora en condiciones de calcular la función zeta de la curva F_n; para todo primo p tal que $p \nmid n$ esta se define, como en el caso de un polinomio en una variable, como

$$Z_{F_n,p}(T) := \exp\left(\sum_{r=1}^{\infty} \frac{N_{p^r}}{r} T^r \right),$$

donde ahora N_{p^r} es el número de puntos *proyectivos* de F_n sobre $\mathbb{F}_{p^r}$. Es decir, N_{p^r} es el número soluciones de $x^n + y^n = z^n$ con $(x, y, z) \in (\mathbb{F}_{p^r})^3$ excluyendo $(0, 0, 0)$ y contando $\lambda(x, y, z)$ para $\lambda \in \mathbb{F}_{p^r}^*$ solo una vez. (Por lo tanto, $N_{p^r} = (N-1)/(p-1)$ donde N es el número total de soluciones de $x^n + y^n = z^n$ con $(x, y, z) \in (\mathbb{F}_{p^r})^3$.) Asumimos en este nº que $p \equiv 1 \bmod n$ con lo que $n = \mathrm{mcd}(p^r - 1, n)$ para todo $r \in \mathbb{N}$.

Volvemos a usar la notación del nº 13. Para evitar confusión agregamos un índice r donde sea necesario, denotando por ejemplo con G_r el grupo de caracteres de $\mathbb{F}_{p^r}^*$ de orden dividiendo n.

Ejercicio 10. Probar que

$$N_{p^r} = N_{p^r}(x^n + y^n = 1) + \sum_{\chi \in G_r} \chi(-1).$$

Proposición. *Para todo $r \in \mathbb{N}$*

$$N_{p^r} = p^r + 1 + \sum_{\substack{\chi, \chi' \in G_r \\ \chi, \chi', \chi\chi' \neq \chi_0}} J(\chi, \chi')$$

Demostración. Basta usar el corolario al lema del nº 13, el teorema del nº 14 y el ejercicio anterior; dejamos los detalles al lector. □

Corolario. *Para todo $r \in \mathbb{N}$ vale la siguiente desigualdad*

$$|N_{p^r} - p^r - 1| \leq (n-1)(n-2)\, p^{\frac{1}{2}r}, \qquad p \equiv 1 \bmod n.$$

Demostración. La desigualdad se deduce de la proposición gracias al corolario al teorema del nº 14: hay $(n-1)(n-2)$ sumandos en la formula para $N_{p^r} - p^r - 1$ cada uno a lo sumo $p^{r/2}$ en valor absoluto. □

Ejercicio 11. Probar que fijado $n > 2$ para todo primo p suficientemente grande existe una solución de $x^n + y^n \equiv z^n \bmod p$ con $p \nmid xyz$ (comparar con [Hur, II, pp. 430–445]).

Lo que debemos estudiar ahora es la relación entre $\tau(\chi)$ para $\chi \in G_r$ con r distintos. Primero veamos como se relacionan G_r y G_1. A todo carácter χ de $\mathbb{F}_p^*$ le podemos asociar el carácter $\chi^{(r)} := \chi \circ N_{\mathbb{F}_{p^r}/\mathbb{F}_p}$ de $\mathbb{F}_{p^r}^*$.

Ejercicio 12. Probar que la aplicación $\chi \mapsto \chi^{(r)}$ da un isomorfismo $G_1 \longrightarrow G_r$.

Probaremos en el siguiente nº la relación de Hasse–Davenport: para todo carácter χ de $\mathbb{F}_p^*$ y todo $r \in \mathbb{N}$ se tiene que

$$-\tau(\chi^{(r)}) = [-\tau(\chi)]^r \,. \tag{14}$$

Combinando esta relación con lo anterior y usando la propiedades básicas de las funciones zeta (ver el nº 4) deducimos el siguiente

Teorema. *La función zeta de la curva de Fermat F_n*

$$Z_{F_n,p}(T) = \frac{P(T)}{(1-T)(1-pT)}, \qquad p \equiv 1 \bmod n \,,$$

donde

$$P(T) = \prod_{\substack{\chi,\chi' \in G \\ \chi,\chi',\chi\chi' \neq \chi_0}} (1 + \chi\chi'(-1)J(\chi,\chi')T)$$

y G es el grupo de caracteres de $\mathbb{F}_p^*$ de orden dividiendo a n.

16. La relación de Hasse–Davenport

Probamos ahora (14) siguiendo una demostración debida a P. Monsky (ver [IR p. 163]). El automorfismo de Frobenius $\sigma(x) = x^p$ actúa en $\overline{\mathbb{F}}_p$ (ver nº 2). Cada órbita Ω de σ en $\overline{\mathbb{F}}_p$ es finita y las órbitas están en biyección con los polinomios irreducibles mónicos de $\mathbb{F}_p[x]$, asignando a Ω el polinomio $f(x) = \prod_{a\in\Omega}(x-a)$.

Ejercicio 13. Probar que para todo $r \in \mathbb{N}$

$$\mathbb{F}_{p^r} = \bigcup_{|\Omega| \mid r} \Omega \,.$$

Sea ahora χ un carácter cualquiera de $\mathbb{F}_p^*$ y sea ψ el carácter aditivo de $\mathbb{F}_p$

$$\psi(a) = e^{\frac{2\pi i}{p}a}$$

(ver nº 14). Para todo $r \in \mathbb{N}$ definimos los caracteres (multiplicativo y aditivo respectivamente) de $\mathbb{F}_{p^r}$

$$\chi^{(r)} := \chi \circ N_{\mathbb{F}_{p^r}/\mathbb{F}_p}, \qquad \psi^{(r)} := \psi \circ T_{\mathbb{F}_{p^r}/\mathbb{F}_p} \,.$$

Sea $f \in \mathbb{F}_p[x]$ un polinomio mónico irreducible y sea Ω el conjunto de sus raíces en $\overline{\mathbb{F}}_p$ (una órbita de σ). Definimos

$$\lambda(f) := \chi\left(\prod_{a\in\Omega} a\right)\psi\left(\sum_{a\in\Omega} a\right);$$

notemos que cualquiera sea $a \in \Omega$

$$\lambda(f) = \chi^{(r)}(a)\ \psi^{(r)}(a)\ . \tag{15}$$

Extendemos la definición a todo polinomio mónico $f \in \mathbb{F}_p[x]$ multiplicativamente; es decir,

$$\lambda(f) := \prod_{j=1}^{k} \lambda(f_j)^{n_j},$$

si $f = \prod_{j=1}^{k} f_j^{n_j}$ con $f_j \in \mathbb{F}_p[x]$ para $j = 1, 2, \cdots, k$ irreducibles mónicos distintos. La aplicación λ esta bien definida gracias a que $\mathbb{F}_p[x]$ es un dominio de factorización única.

La relación de λ con las sumas de Gauss esta dada por la identidad

$$\tau(\chi^{(r)}) = \sum_{\mathrm{gr}(f)|r} \mathrm{gr}(f)\lambda(f), \tag{16}$$

donde f en la suma es irreducible y mónico. Esta igualdad es una consecuencia del ejercicio 13 y (15).

Ejercicio 14. Probar que si

$$f(x) = x^d - a_1 x^{d-1} + \cdots + (-1)^d a_d \in \mathbb{F}_p[x]$$

entonces

$$\lambda(f) = \chi(a_d)\ \psi(a_1)\ .$$

Consideremos la serie formal

$$Z(T) := \prod_f \left(1 - \lambda(f)\ T^{\mathrm{gr}(f)}\right)^{-1},$$

donde f recorre los polinomios mónicos irreducibles de $\mathbb{F}_p[x]$. Sea

$$Z(T) = 1 + c_1 T + c_2 T^2 + \cdots$$

la expansión en serie de potencias de $Z(T)$.

Ejercicio 15. Probar que

(1) Para todo $k \in \mathbb{N}$

$$c_k = \sum_{\substack{f \in \mathbb{F}_p[x] \\ \mathrm{gr}(f)=k}} \lambda(f) \ .$$

(2) Para todo $k > 1$ se tiene que $c_k = 0$.

Como consecuencia del ejercicio anterior y (16) vemos que

$$Z(T) = 1 + \tau(\chi)T$$

y tomando derivada logarítmica

$$\frac{\tau(\chi)}{1+\tau(\chi)T} = \sum_f \frac{\mathrm{gr}(f)\ \lambda(f)}{1-\lambda(f)\ T^{\mathrm{gr}(f)}}$$

donde f recorre los polinomios mónicos irreducibles de $\mathbb{F}_p[x]$. Finalmente, comparando la potencia de T^r en cada lado de esta igualdad se obtiene la relación de Hasse–Davenport.

17. La curva $x^3 + y^3 = 1$

Estudiemos en más detalle la curva de Fermat F_3 de ecuación $x^3 + y^3 = 1$. Sea $p \equiv 1 \bmod 3$ un primo y χ un carácter de $\mathbb{F}_p^*$ de orden 3. El grupo G de caracteres de $\mathbb{F}_p^*$ de orden dividiendo 3 esta generado por χ. La función zeta de F_3 módulo p tiene numerador

$$P(T) = (1 + J(\chi,\chi)T)(1 + J(\chi^2,\chi^2)T)$$

y como $J(\chi^2,\chi^2) = \overline{J(\chi,\chi)}$ si definimos $\pi := -J(\chi,\chi)$ entonces $\pi\overline{\pi} = p$ (ver n$^{\mathrm{o}}$ 14) y la función zeta se puede escribir como

$$Z_{F_3,p}(T) = \frac{1 - a_pT + pT^2}{(1-T)(1-pT)}, \qquad p \equiv 1 \bmod 3 \tag{17}$$

donde $a_p := \pi + \overline{\pi}$. (El valor de π no es canónico, depende de la elección del generador χ de G, si cambiamos χ por $\overline{\chi}$ entonces π cambia por $\overline{\pi}$, pero por supuesto $Z_{F_3,p}(T)$ no depende de esta elección.)

Ejercicio 16.

(1) Probar que $\pi = a + b\,\zeta_3$ donde $a, b \in \mathbb{Z}$ y $\zeta_3 = e^{2\pi i/3}$ es una raíz primitiva de la unidad de orden 3. Concluir que para todo primo $p \equiv 1 \bmod 3$ existen enteros a, b tales que

$$p = a^2 - ab + b^2 \ .$$

(2) Probar que la función zeta de F_3 para un primo $p \equiv -1 \bmod 3$ es

$$Z_{F_3,p}(T) = \frac{1+pT^2}{(1-T)(1-pT)}, \qquad p \equiv -1 \bmod 3.$$

Como en el caso de polinomios de una variable ponemos ahora todas las funciones $Z_{F_3,p}(T)$ juntas en una función de una variable compleja s. Definimos la función L asociada a F_3 como

$$L(F_3, s) := \prod_{p \neq 3} (1 - a_p\, p^{-s} + p^{1-2s})^{-1}, \qquad \Re(s) > 3/2,$$

donde el factor de Euler en p es el inverso del numerador de la función $Z_{F_3,p}(T)$ evaluado en $T = p^{-s}$ (definiendo $a_p := 0$ para $p \equiv -1 \bmod 3$). Discutiremos la convergencia de este producto en breve.

Nos gustaría expandir el producto como una suma de manera similar a lo que hicimos para la función zeta de Riemann y para ello conviene reescribirlo.

Consideremos[14] el dominio íntegro $\mathbb{Z}[\zeta_3] = \{a + b\,\zeta_3 \,|\, a, b \in \mathbb{Z}\}$. Al igual[15] que $\mathbb{Z}$ el anillo $\mathbb{Z}[\zeta_3]$ es un dominio de factorización única, es decir, todo $\alpha \in \mathbb{Z}[\zeta_3]$ se escribe de manera única como

$$\alpha = u\rho_1\rho_2\cdots\rho_n$$

donde $\rho_1, \rho_2, \cdots, \rho_n$ son irreducibles y $u = \pm\,\zeta_3^k$, con $k = 0, 1, 2$, es una unidad.

Hay tres tipos de irreducibles en $\mathbb{Z}[\zeta_3]$; módulo producto por unidades estos son:

(1) $1 - \zeta_3$
(2) $p \equiv -1 \bmod 3$ un primo de $\mathbb{Z}$
(3) $\pi, \overline{\pi}$ como más arriba con $\pi\overline{\pi} = p \equiv 1 \bmod 3$.

Ejercicio 17.

(1) Encontrar la factorización de 3 en $\mathbb{Z}[\zeta_3]$ (el único irreducible de la lista que divide a 3 es $1 - \zeta_3$).
(2) Probar que las unidades (es decir los elementos inversibles) de $\mathbb{Z}[\zeta_3]$ son $\pm\,\zeta_3^k$, con $k = 0, 1, 2$.

Proposición. *Para todo $p \equiv 1 \bmod 3$ valen en $\mathbb{Z}[\zeta_3]$ las congruencias*

$$\pi \equiv 1 \bmod 3, \qquad \overline{\pi} \equiv 1 \bmod 3.$$

Demostración. Es claro que conjugando obtenemos una congruencia como consecuencia de la otra. Usando la relación entre sumas de Jacobi y Gauss que probamos en el n$^{\text{o}}$ 14 vemos que

$$\pi = -\frac{\tau(\chi)^2}{\tau(\chi^2)}.$$

Como χ es de orden 3, $\chi^2 = \overline{\chi}$. Se verifica fácilmente que $\overline{\tau(\chi)} = \tau(\overline{\chi})$ ya que $\chi(-1) = 1$. Por lo tanto $\tau(\chi^2) = p/\tau(\chi)$ y

$$\pi = -\frac{\tau(\chi)^3}{p}.$$

Reduciendo módulo 3 obtenemos

$$\begin{aligned}
\pi &\equiv -\left[\sum_{a\in\mathbb{F}_p^*} \chi(a)\psi(a)\right]^3 \bmod 3 \\
&\equiv -\sum_{a\in\mathbb{F}_p^*} \chi(a)^3\psi(3a) \bmod 3 \\
&\equiv -\sum_{a\in\mathbb{F}_p^*} \psi(a) \bmod 3 \\
&\equiv 1 \bmod 3
\end{aligned}$$

y la congruencia queda demostrada. □

Corolario. *Para todo primo $p \equiv 1 \bmod 3$ existen enteros A, B, únicos excepto por un signo, tales que*

$$4p = A^2 + 27B^2 \ .$$

El número de soluciones (proyectivas) de

$$x^3 + y^3 + z^3 \equiv 0 \bmod 3$$

es $p + 1 + A$ si elegimos A tal que $A \equiv 1 \bmod 3$.

Demostración. Sabemos que (ejercicio 16) $\pi = a + b\,\zeta_3$ con $a, b \in \mathbb{Z}$ y como $\zeta_3 = (-1 + \sqrt{-3})/2$ tenemos que $\pi = (A + B'\sqrt{-3})/2$ con $A, B' \in \mathbb{Z}$. Por la proposición $\pi \equiv 1 \bmod 3$ con lo que $B' \equiv 0 \bmod 3$. Sea $B = B'/3 \in \mathbb{Z}$. Como $\pi \cdot \overline{\pi} = p$ encontramos que $p = (A^2 + 27B^2)/4$. Dejamos el resto de lo acertado como ejercicio para el lector. □

Este corolario fue probado por Gauss[16] en el articulo 358 de su *Disquisitiones Arithmeticae* [Ga].

Ejercicio 18.

(1) Probar que para todo $\alpha \in \mathbb{Z}[\zeta_3]$ coprimo con 3 existe una unidad única $\phi(\alpha) = \pm\zeta_3^k$, $k = 0, 1, 2$, tal que

$$\phi(\alpha)\,\alpha \equiv 1 \bmod 3.$$

(2) Probar que para α una unidad $\phi(\alpha) = \alpha^{-1}$.

(3) Probar que para todo $\alpha, \beta \in \mathbb{Z}[\zeta_3]$ coprimos con 3 se tiene que

$$\phi(\alpha\beta) = \phi(\alpha)\,\phi(\beta)$$

y por lo tanto ϕ determina un carácter de orden 6 (que denotamos con el mismo nombre)

$$\phi : (\mathbb{Z}[\zeta_3]/3\mathbb{Z}[\zeta_3])^* \longrightarrow \mathbb{C}^*$$

Como hicimos en el nº 7 extendemos la definición de ϕ a todo $\mathbb{Z}[\zeta_3]$ declarando $\phi(\alpha) := 0$ si α no es comprimo con 3.

Normalizamos los irreducibles $\rho \in \mathbb{Z}[\zeta_3]$ coprimos con 3 requiriendo que $\rho \equiv 1 \bmod 3$, con lo que $\rho = -p$ para irreducibles de tipo (2) y $\rho = \pi$ o $\rho = \overline{\pi}$ para irreducibles del tipo (3).

No es ahora difícil verificar que

$$L(F_3, s) = \prod_{\rho \equiv 1 \bmod 3} \left(1 - \frac{\rho}{(\rho\overline{\rho})^s}\right)^{-1} \qquad \Re(s) > 3/2, \tag{18}$$

donde ρ recorre los irreducibles normalizados de $\mathbb{Z}[\zeta_3]$ y al expandir el producto obtenemos

$$L(F_3, s) = \tfrac{1}{6} \sum_{\substack{\alpha \in \mathbb{Z}[\zeta_3] \\ \alpha \neq 0}} \frac{\phi(\alpha)\,\alpha}{(\alpha\overline{\alpha})^s}. \qquad \Re(s) > 3/2. \tag{19}$$

Para la convergencia podemos usar como en el nº 7 el criterio de la integral, ahora en dos variables, comparando la suma con

$$\int_{\substack{x \in \mathbb{R}^2 \\ \|x\| \geq 1}} \|x\|^{1-2\sigma}, \qquad \sigma = \Re(s)\ ,$$

donde $\|x\|$ es la distancia euclídea. Usando coordenadas polares por ejemplo se ve que esta integral converge para $2\Re(\sigma) - 1 > 2$, es decir para $\Re(\sigma) > 3/2$.

Ejercicio 19. Verificar las igualdades (18) y (19).

Probemos ahora que $L(F_3, s)$ se extiende analíticamente a todo s y satisface una ecuación funcional. Los pasos a seguir son los mismos que para $L(\chi, s)$ que vimos en el nº y solamente los indicamos.

Definimos la función theta asociada a $L(F_3, s)$

$$\Theta(t) := \tfrac{1}{6} \sum_{\alpha \in \mathbb{Z}[\zeta_3]} \phi(\alpha)\,\alpha\, e^{-2\pi\alpha\overline{\alpha}\,t/\sqrt{27}}, \qquad t > 0.$$

Usando la fórmula de Poisson en dos variables se prueba que

$$\Theta(1/t) = w\, t^2\, \Theta(t), \tag{20}$$

donde w se expresa en términos de una suma de Gauss para ϕ. Con algo de esfuerzo uno verifica que de hecho $w = 1$.

Definimos

$$L^*(F_3, s) := \left(\frac{2\pi}{\sqrt{27}}\right)^{-s} \Gamma(s)\, L^*(F_3, s)$$

y se tiene que

$$L^*(F_3, s) = \int_0^\infty \Theta(t)\, \frac{dt}{t}$$

que combinada con la ecuación funcional (20) para Θ nos da el siguiente

Teorema. *La función $L^*(F_3, s)$ se extiende a todo el plano complejo y satisface la ecuación funcional*

$$L^*(F_3, 2 - s) = L^*(F_3, s)$$

La función φ que a α le asigna $\phi(\alpha)\alpha$ es multiplicativa y es un ejemplo de un *carácter de Hecke* (en este caso del cuerpo $\mathbb{Q}(\zeta_3)$). Los caracteres de Hecke son una gran generalización de los caracteres de Dirichlet y la función L asociada a cualquier carácter de Hecke tiene[17] una continuación analítica a todo el plano complejo y satisface una ecuación funcional.

La igualdad (19) puede resumirse diciendo que la función L de la curva elíptica (ver n$^{\text{o}}$ 19) F_3 coincide con la función L asociada al carácter de Hecke φ. (Esto es cierto para toda una clase especial de curvas elípticas, aquellas que tienen multiplicación compleja).

18. La conjetura de Weil para curvas

Sea X una curva proyectiva no-singular definida sobre un cuerpo finito $\mathbb{F}_q$, por ejemplo $X \subset \mathbb{P}^2$ dada por una ecuación homogénea

$$X : F(x, y, z) = 0, \qquad F \in \mathbb{F}_q[x, y, z]$$

tal que

$$\frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = \frac{\partial F}{\partial z} = 0$$

no tienen ninguna solución en $\overline{\mathbb{F}}_q$, una clausura algebraica de $\mathbb{F}_q$; diremos también en ese caso que F es *no-singular*. Para todo $r \in \mathbb{N}$ sea N_{q^r} el número de soluciones proyectivas de X definidas sobre $\mathbb{F}_{q^r}$. Definimos, siguiendo a Artin, la función zeta de X como

$$Z_X(T) := \exp\left(\sum_{r=1}^{\infty} \frac{N_{q^r}}{r} T^r\right).$$

Esta definición extiende la que dimos para $X = F_n$ en el nº 13. Notemos que $Z_X(T)$ es una serie de potencias con coeficientes racionales.

Ejercicio 20. Probar que

$$Z_{\mathbb{P}^1}(T) = \frac{1}{(1-T)(1-qT)}.$$

Teorema.

(1) *$Z_X(T)$ es una función racional con coeficientes en $\mathbb{Z}$.*

(2) *Mas precisamente,*

$$Z_X(T) = \frac{P(T)}{(1-T)(1-qT)}$$

con $P(T) \in \mathbb{Z}[T]$ de grado $2g$, donde g es el genero de X y $P(T)$ es de la forma

$$P(T) = \prod_{j=1}^{2g}(1-\alpha_j T), \qquad |\alpha_j| = q^{\frac{1}{2}}, \quad j = 1, 2, \cdots, 2g.$$

(3)

$$Z_X(1/qT) = q^{\frac{1}{2}e}\, T^e\, Z_X(T), \qquad e = 2-2g.$$

El punto (1) se debe a Artin, (2) a Hasse y Weil y (3) a F. K. Schmidt. Para un comentario sobre este resultado fundamental remitimos al lector al nº 21 donde daremos la versión general.

Nota sobre el genero Los puntos $X(\mathbb{C})$ de una curva proyectiva no-singular X definida sobre $\mathbb{C}$ forman, como espacio topológico, una superficie S (es decir una variedad de dimensión 2 sobre $\mathbb{R}$) orientable. El genero de X se puede definir como el número de "agujeros" de esta superficie o más formalmente, usando la identidad $e = 2g-2$, donde e es la *característica de Euler* de S; en todo caso, g es un invariante topológico de S. Para una curva definida sobre un cuerpo finito, sin embargo, el número de "agujeros" no tiene ningún sentido y es necesario definir el genero de otra manera. En la práctica, si X esta dada por $F(x,y,z) = 0$ con F homogéneo de grado n y no-singular entonces $g = \frac{1}{2}(n-1)(n-2)$ (si F es singular el genero sera menor que ese número).

La curva X puede parametrizarse con funciones racionales si y solo si su genero es cero (ver por ejemplo (1) en la introducción).

Si X esta definida por un polinomio homogéneo $F(x,y,z)$ con coeficientes enteros podemos reducir la ecuación módulo un primo p y obtener una curva $\overline{X}$ sobre $\mathbb{F}_p$.

Para todo p excepto un número finito $\overline{X}$ sera no-singular. El teorema nos dice que el invariante topológico g de X se refleja en una propiedad del número de puntos de $\overline{X}$ sobre cuerpos finitos!

Ejercicio 21.

(1) Verificar que el polinomio $x^n + y^n - z^n$ es no-singular con lo que F_n tiene genero $g = \frac{1}{2}(n-1)(n-2)$.
(2) Verificar que $Z_{F_3,p}(T)$ para $p \neq 3$ satisface las propiedades del teorema usando la forma explicita del nº 17.
(3) Probar que $N_1, N_q, \cdots, N_{q^g}$ determinan N_{q^r} para todo $r \in \mathbb{N}$.

El teorema nos da una estimación no trivial del número de puntos de una curva no-singular sobre un cuerpo finito (comparar con la desigualdad análoga del nº 15).

Corolario. *Para todo* $r \in \mathbb{N}$

$$|N_{q^r} - q^r - 1| \leq 2g\sqrt{q}^{\,r}.$$

Demostración. Notemos que por el teorema

$$N_{q^r} = q^r + 1 - \sum_{j=1}^{2g} \alpha_j^r$$

(ver nº 4) y como para cada $j = 1, 2, \cdots, 2g$ sabemos que $|\alpha_j| = \sqrt{q}$ resulta la desigualdad. □.

Vale la pena destacar que $q^r + 1$ es el número de puntos de $\mathbb{P}^1$ en $\mathbb{F}_{q^r}$; el corolario nos dice que el número de puntos de X en $\mathbb{F}_{q^r}$ difiere de ese número por algo acotado por $2g\sqrt{q}^{\,r}$.

Ejercicio 22.

(1) Asumiendo solamente que

$$N_{q^r} = q^r + 1 - \sum_{j=1}^{2g} \alpha_j^r, \qquad r \in N$$

para ciertos números complejos α_j probar que

$$|N_{q^r} - q^r - 1| \leq 2g\sqrt{q}^{\,r}, \qquad r \in N$$

si y solo si $|\alpha_j| = q^{\frac{1}{2}}$ para $j = 1, 2, \cdots, 2g$.

(2) Probar que toda curva (proyectiva, no-singular) sobre un cuerpo finito $\mathbb{F}$ de genero 0 o 1 tiene al menos un punto sobre $\mathbb{F}$.
(3) Probar que la ecuación $y^4 - 17 = x^2$ que mencionamos en la introducción tiene soluciones módulo cualquier número $m \in \mathbb{N}$. (Usar el hecho que para $p \neq 2, 17$ la curva proyectiva, no-singular determinada por la desingularización de $y^4 - 17z^4 = x^2z^2$ sobre $\mathbb{F}_p$ tiene a lo sumo dos puntos más que las soluciones de $y^4 - 17 \equiv x^2 \bmod p$.)

19. Curvas elípticas

Damos en este nº una introducción super breve a una clase de curvas que juegan un rol prominente en la aritmética: las curvas elípticas. Para más detalles referimos el lector a [ST].

Una *curva elíptica* E sobre un cuerpo K es una curva algebraica proyectiva no-singular de genero 1 definida sobre K junto con un punto distinguido O, también definido sobre K. Toda curva elíptica sobre K puede darse[18] en *forma de Weierstrass*, una ecuación afín ($z = 1$) del tipo

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_1, a_2, a_3, a_4, a_6 \in K$$

con punto racional distinguido O de coordenadas proyectivas $(x, y, z) = (0, 1, 0)$.

En la práctica las curvas de genero 1 suelen típicamente darse en alguna una de las siguientes formas:

(1) (elíptica)
$$y^2 = f(x), \qquad f \in K[x], \quad \mathrm{gr}(f) = 3, 4;$$

(2) (cubica general)
$$F(x, y, z) = 0, \qquad F \in K[x, y, z], \text{ homogeneo, } \mathrm{gr}(F) = 3;$$

(3) (intersección de dos cuádricas)
$$\begin{cases} Q_1(x, y, z) = 0 \\ Q_2(x, y, z) = 0 \end{cases} \qquad Q_1, Q_2 \in K[x, y, z], \text{ homogeneos, } \mathrm{gr}(Q_1) = \mathrm{gr}(Q_2) = 2$$

(En el caso general $y^2 = f(x)$ con $\mathrm{gr}(f) = 4$ la curva es singular en infinito, es decir cuando $z = 0$ en $y^2z = z^4f(y/z)$, y la curva que realmente consideramos es su desingularización.)

En general una ecuación de este tipo da una curva de genero 1 definida sobre K pero esta puede no tener ningún punto sobre K y entonces no ser una curva

elíptica. (Sobre un cuerpo finito este problema nunca surge por el ejercicio 22). También, ecuaciones particulares pueden determinar curvas de genero 0 en vez de 1. Por ejemplo, para el caso (1), el genero es 1 si y solo si $\mathrm{disc}(f) \neq 0$.

Ejercicio 23.

(1) Mostrar que si K no tiene característica 2 o 3 existe un cambio de variables lineal que lleva una ecuación de Weierstrass general a una versión simplificada
$$y^2 = x^3 + ax + b\ .$$
(2) Probar que
$$y^2 z = x^3 + axz^2 + bz^3$$
es no-singular (y por lo tanto de genero 1) si y solo si $\mathrm{disc}(x^3 + ax + b) \neq 0$.
(3) Encontrar una parametrización con funciones racionales de las soluciones de
$$y^2 = x^3 + x^2.$$

La curva de Fermat F_3 es una curva elíptica sobre $\mathbb{Q}$ (tiene genero 1 ya que es una ecuación cubica no-singular y, por ejemplo, $(1, 0)$ es un punto racional). Veamos como encontrar una de sus formas de Weierstrass.[19] Primero hacemos el cambio de variables:
$$\begin{cases} x = \frac{1}{2}(u + v) \\ y = \frac{1}{2}(u - v) \end{cases}$$
y obtenemos, después de multiplicar por 4,
$$u^3 + 3uv^2 = 4$$
o en forma homogénea
$$u^3 + 3uv^2 = 4w^3\ .$$
Ahora si multiplicamos por $432 = 4^2 \cdot 3^3$ y ponemos $v = 1$ tenemos que
$$(36v)^2 = (12w)^3 - 432$$
y entonces una forma de Weierstrass de F_3 es $y^2 = x^3 - 432$ (el punto al infinito $O = (0, 1, 0)$ en estas coordenadas corresponde al punto $(1, -1, 0)$ en las coordenadas originales).

Dada una curva elíptica E sobre $\mathbb{Q}$, digamos
$$E : y^2 = x^3 + ax + b, \qquad a, b, \in \mathbb{Z}\ ,$$

podemos estudiar su reducción módulo un primo p. Si p divide al discriminante $\Delta = -4a^3 - 27b^2$ de $x^3 + ax + b$ entonces la ecuación es singular y E tiene genero 0 sobre $\mathbb{F}_p$. Si en cambio $p \nmid \Delta$ obtenemos una curva elíptica sobre $\mathbb{F}_p$. Podría suceder que $p \mid \Delta$ pero sin embargo existe otra forma de Weierstrass de E cuya reducción es no-singular. Por ejemplo, el cambio de variables $x \mapsto p^2x, y \mapsto p^3y$ lleva $y^2 = x^3 + p^4ax + p^6$ a $y^2 = x^3 + ax + b$ y elimina una potencia p^{12} de Δ.

Es un hecho que siempre existe una ecuación de Weierstrass *minimal*[20] en el sentido que su discriminante es el mas chico entre todas las ecuaciones de Weierstrass de E con coeficientes enteros. Llamamos al discriminante de tal ecuación el *discriminante minimal* de E. Los primos que dividen a Δ se llaman *primos de mala reducción* y los que no dividen a Δ *primos de buena reducción*. Por ejemplo, F_3 tiene modelo minimal

$$y^2 + y = x^3 - 7, \qquad \Delta = -3^9,$$

y por lo tanto mala reducción solo para $p = 3$ (en contraste con la ecuación de Weierstrass $y^2 = x^3 + 432$ que tiene reducción singular también módulo $p = 2$).

Denotemos con Δ el discriminante minimal de E. Para todo $p \nmid \Delta$ sea $Z_{E,p}(T)$ la función zeta de la reducción de E módulo p. Como esta reducción tiene genero 1 tenemos (ver n° 18) que el numerador de $Z_{E,p}(T)$ es de la forma

$$1 - a_pT + pT^2, \qquad a_p \in \mathbb{Z}, \quad |a_p| \leq 2\sqrt{p}.$$

Como hicimos con F_3 (ver n° 17) definimos la función L de E

$$L(E,s) := \prod_{p|\Delta} F_p(s)^{-1} \prod_{p\nmid\Delta} \left(1 - a_pp^{-s} + p^{1-2s}\right)^{-1} , \qquad \Re(s) > 3/2 ,$$

donde para un primo $p \mid \Delta$ el factor de Euler es $F_p(s) = 1, (1 \pm p^{-s})$ según el tipo de (mala) reducción que E tenga módulo p (no vale la pena detallar esto aquí). Al expandir el producto obtenemos una serie

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}, \qquad \Re(s) > 3/2,$$

con enteros a_n ahora definidos para todo $n \in \mathbb{N}$. La convergencia del producto y la serie para $\Re(s) > 3/2$ son consecuencia de la cota $|a_p| \leq 2\sqrt{p}$.

Como discutiremos en el siguiente n°, se espera (y se sabe para un colección grande de casos gracias al trabajo de Wiles) que $L(E,s)$ se extienda analíticamente a todo el plano y satisfaga una ecuación funcional con $s \mapsto 2 - s$.

¿Qué información global podemos extraer de la función L de una curva elíptica? En los años 60, Birch y Swinnerton-Dyer, basándose en los resultados de una serie de experimentos numéricos, formularon una conjetura muy importante de la que damos a continuación su versión mas básica.

Conjetura. *(Birch–Swinnerton-Dyer) Sea E una curva elíptica definida sobre $\mathbb{Q}$ y sea $E(\mathbb{Q})$ el conjunto de sus puntos racionales.*

$$E(\mathbb{Q}) \text{ es infinito} \qquad \Longleftrightarrow \qquad L(E,1) = 0$$

Notemos que para que la conjetura tenga algún sentido es necesario saber que $L(E,s)$ se extiende analíticamente a algún dominio que incluya $s = 1$. Notemos también que $s = 1$ es el centro de simetría de $s \mapsto 2 - s$ con lo que si el signo en la ecuación funcional (ver el n$^{\text{o}}$ siguiente) es -1 necesariamente $L(E,1) = 0$ y esperamos entonces que $E(\mathbb{Q})$ sea infinito.

La implicación $\Longrightarrow$ es ahora un teorema (para curvas elípticas con multiplicación compleja debido a Coates y Wiles; para curvas elípticas modulares debido a Kolyvagin y Rubin).

La idea intuitiva que siguieron Birch y Swinnerton-Dyer para conectar el valor $L(E,1)$ y los puntos en $E(\mathbb{Q})$ es la siguiente. Si evaluamos el factor de Euler de $L(E,s)$ correspondiente a un primo $p \nmid N$ en $s = 1$ obtenemos

$$(1 - a_p p^{-s} + p^{1-2s})\big|_{s=1} = \frac{N_p}{p},$$

donde N_p es el número de puntos de E módulo p. Si $E(\mathbb{Q})$ es infinito estos números deberían reflejar este hecho de alguna manera.

El producto de N_p/p sobre todo $p \nmid N$ no converge; Birch y Swinnerton–Dyer compararon como crece

$$\prod_{\substack{p \nmid N \\ p \leq P}} \frac{N_p}{p},$$

al variar P y descubrieron que efectivamente parecía haber una correlación entre el comportamiento de este producto con el número de puntos de $E(\mathbb{Q})$! (Una manipulación analítica permite mostrar que este comportamiento del producto se traduce en que $L(E,1)$ sea nulo o no.)

20. Modularidad

El famoso "último teorema de Fermat" que para todo $n \in \mathbb{N}$ con $n > 2$ la ecuación

$$a^n + b^n = c^n, \qquad xyz \neq 0 \tag{21}$$

no tiene solución en números enteros fue probado recientemente por Wiles. La estrategia, originalmente debida a Hellegouarch y Frey, es la siguiente. Supongamos

sin perdida de generalidad que n es un primo impar p y sea $a, b, c \in \mathbb{Z}$ coprimos una supuesta solución de (21). Consideremos la curva elíptica sobre $\mathbb{Q}$ (curva de Frey)

$$y^2 = x(x - a^p)(x + b^p) \ . \tag{22}$$

La observación fundamental de Frey es que esta curva elíptica es muy "extraña", no parece ser "modular".

Expliquemos brevemente que quiere decir que una curva elíptica E sobre $\mathbb{Q}$ sea modular. Asociada a E tenemos su discriminante minimal Δ y la función $L(E, s)$. Existe otro número importante asociado a E, su *conductor* N. La definición de N es complicada[21] y diremos solamente que sus factores primos son los primos de mala reducción de E, es decir los primos que dividen a Δ. (La relación entre el conductor y discriminante de E es un poco como la relación entre el conductor y discriminante de un polinomio abeliano; por ejemplo, vimos que el conductor de Φ_l es l pero su discriminante es $(-1)^{\frac{1}{2}(l-1)} l^{l-2}$.) Una de las razones por las cuales la curva de Frey es "extraña" es que su discriminante, esencialmente $(abc)^{2p}$, es *mucho*[22] más grande que su conductor, esencialmente el producto de los primos que dividen a abc.

Consideremos la función

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n, \qquad q = e^{2\pi i \tau}, \quad \Im(\tau) > 0 \ ,$$

donde

$$L(E, s) = \sum_{n=1}^{\infty} a_n n^{-s} \ .$$

Una manera de definir que E es *modular* es requerir que f sea una forma modular (newform) de peso 2 y nivel N. Por ejemplo F_3 es modular; usando no más que la fórmula de sumación de Poisson como en el nº 17 se puede probar que Θ es modular de peso 2 y nivel 27. (Esto es cierto en general para toda curva elíptica con multiplicación compleja para las cuales la función L se puede expresar por medio de caracteres de Hecke.) Precisar esta definición de modular nos llevaría demasiado lejos[23] ; damos en cambio una definición en términos de funciones L. La equivalencia (no trivial) de ambas definiciones se debe a Weil.

Para dar al menos una idea de que significa que E sea modular consideremos el siguiente ejemplo

$$y^2 + y = x^3 - x^2 - 10x - 20 \ ;$$

una curva elíptica de discriminante minimal $\Delta = -11^5$ y conductor $N = 11$ (el conductor más pequeño posible para una curva elíptica sobre $\mathbb{Q}$). Esta curva es modular y la forma modular f de peso 2 y nivel 11 puede darse explícitamente como

$$f = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 \cdots$$

Debemos definir un concepto mas. Sea

$$y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Z}$$

una ecuación de Weierstrass de E. Dado un número entero no nulo d consideramos la curva

$$E_d : dy^2 = x^3 + ax + b,$$

que llamaremos el *twist* de E por $\mathbb{Q}(\sqrt{d})$. Notemos que E_d es isomorfa a E sobre el cuerpo $\mathbb{Q}(\sqrt{d})$ (pero no sobre $\mathbb{Q}$ si d no es un cuadrado). Denotemos por N_d al conductor de E_d.

Definición. *La curva elíptica E es modular si y solo si para todo $d \in \mathbb{Z}$ no nulo la función*

$$L^*(E_d, s) = \left(\frac{2\pi}{\sqrt{N_d}}\right)^{-s} \Gamma(s)\, L(E_d, s),$$

se extiende analíticamente a todo el plano complejo y satisface la ecuación funcional

$$L^*(E_d, 2 - s) = w_d\, L^*(E_d, s)$$

para algún $w_d = \pm 1$.

Conjetura. *(Taniyama–Shimura–Weil) Toda curva elíptica sobre $\mathbb{Q}$ es modular.*

Volvamos a la curva de Frey (22) y al teorema de Fermat. Primero Ribet probó que efectivamente la curva de Frey no es modular y después de siete años de intenso trabajo Wiles probó el siguiente

Teorema. *(Wiles) Toda curva elíptica sobre $\mathbb{Q}$, semi-estable es modular.*

Este teorema combinado con el de Ribet implican el teorema de Fermat. (La condición de ser semi-estable es demasiado técnica para que la detallemos; nadie duda que se va a poder eliminar de las hipótesis en el futuro cercano probando la conjetura de Taniyama–Shimura–Weil en todos los casos.)

Seria imposible dar aquí siquiera un resumen inteligible de las muchas ideas y resultados que intervienen en el trabajo de Ribet y Wiles; referimos al lector interesado a alguno de los varios artículos expositorios [O1], [O2], [Ri], [RS], [Sch], [Se2].

III – Dimensión arbitraria

21. Las conjeturas de Weil

Sea X una variedad proyectiva no-singular de dimensión n sobre $\mathbb{F}_q$. Para $r \in \mathbb{N}$ sea N_{p^r} el número de puntos (proyectivos) de X definidos sobre $\mathbb{F}_{p^r}$ y sea

$$Z_X(T) = \exp\left(\sum_{r=1}^{\infty} \frac{N_{q^r}}{r} T^r\right)$$

su función zeta. En 1949 Weil fórmula las siguientes conjeturas acerca de $Z_X(T)$.

Teorema.

(1) *$Z_X(T)$ es una función racional con coeficientes en $\mathbb{Z}$.*

(2) *Mas precisamente,*

$$Z_X(T) = \frac{P_1(T)P_3(T)\cdots P_{2n-1}(T)}{P_0(T)P_2(T)\cdots P_{2n}(T)}$$

con

$$P_k(T) = \prod_{j=1}^{b_k}(1 - \alpha_{j,k}T), \qquad |\alpha_{j,k}| = \sqrt{q}^{\,k}$$

(3)

$$Z_X(1/q^n T) = \pm q^{\frac{1}{2}e}\, T^e\, Z_X(T), \qquad \textit{para algun } e \in \mathbb{Z}$$

(4) *Si X es la reducción módulo p de una variedad proyectiva no singular $\widetilde{X}$, b_k es el k-ésimo número de Betti topológico de $\widetilde{X}$ como variedad compleja.*

El punto (1) fue probado por Dwork, (2) por Deligne y (3), (4) por Grothendieck. Remitimos al lector a [Ka] para más detalles.

Comentarios (a) La propiedad que $|\alpha_{j,k}| = \sqrt{q}^{\,k}$ se conoce en este contexto como la "hipótesis de Riemann". (Si reemplazamos T por q^{-s} las raíces de $P_k(q^{-s})$ tiene parte real $k/2$, una propiedad análoga a la verdadera hipótesis de Riemann.)
(b) La "ecuación funcional" (3) implica que aplicación $\alpha \mapsto q^n/\alpha$ da una biyección entre los $\alpha_{k,j}$ y los $\alpha_{2n-k,j}$. Si reemplazamos a T por q^{-s} obtenemos una ecuación funcional con $s \mapsto n - s$.
(c) Por los números de Betti topológicos b_k de $\widetilde{X}$ entendemos la dimensión de los espacios de cohomología $H^k(\widetilde{X}, \mathbb{C})$. Si X es una curva, por ejemplo, $b_1 = 2g$ donde g es el genero de X (comparar con el enunciado del nº 18). Es notable como invariantes topológicos de la variedad compleja $\widetilde{X}$ aparecen reflejados en propiedades aritméticas de X (una variedad definida sobre un cuerpo finito).

(d) El número $e = \sum_{k=0}^{2n}(-1)^n b_k$ es la característica de Euler de $\widetilde{X}$.

Ejercicio 24. Probar que la función zeta de $\mathbb{P}^n$ es

$$Z_{\mathbb{P}^n}(T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^nT)}$$

y verificar las conjeturas de Weil para $\mathbb{P}^n$.

En general es difícil dar explícitamente la función zeta de una variedad arbitraria. Weil mostró como podía tratarse el caso de una variedad diagonal

$$a_1x_1^{e_1} + a_2x_2^{e_2} + \cdots + a_m^{e_m} = 0$$

usando sumas de Jacobi de una manera análoga al caso particular que tratamos nº 15 [We II p. 63, p. 165, III p. 329].

Si X es una hiper-superficie de grado d y dimensión impar n; es decir, X esta dada por una sola ecuación $f = 0$ con f homogéneo de grado d en $n+1$ variables entonces

$$Z_X(T) = \frac{P(T)}{(1-T)(1-qT)\cdots(1-q^nT)},$$

donde $P(T)$ es un polinomio con coeficientes enteros de grado

$$b = \frac{((d-1)^{n+1}-1)}{d}(d-1)\,.$$

Como en el caso de curvas deducimos que

$$|N_{q^r} - (1 + q^r + \cdots + q^{rn})| \leq b\sqrt{q}^{\,rn}, \qquad r \in \mathbb{N}\,.$$

El siguiente ejemplo se debe a Livné [Li]. Sea $W \subset \mathbb{P}^9$ la variedad algebraica dada por

$$x_1 + x_2 + \cdots x_{10} = 0$$
$$x_1^3 + x_2^3 + \cdots x_{10}^3 = 0$$

y sea N_p el número de soluciones (proyectivas) a estas ecuaciones módulo p. Como W es singular no podemos aplicar las conjeturas de Weil directamente. Las singularidades de W consisten en 126 puntos dobles ordinarios. Aplicando la conjeturas de Weil a una desingularización $\widetilde{W}$ de W (específicamente, el "blow up" de W en sus puntos singulares), más resultados importantes de Faltings y Serre, Livné demuestra que

$$N_p = 1 + p + \cdots + p^7 - 84p^3 + 42p^4 - a_pp^2,$$

donde a_p es el coeficiente p-ésimo de la forma modular de peso 4 y nivel 10

$$f = q + 2q^2 - 8q^3 + 4q^4 + 5q^5 - 16q^6 - 4q^7\cdots$$

que puede acotarse

$$|a_p| \leq 2p^{\frac{3}{2}} \ .$$

La función $L_7(W,s)$ (ver más abajo) coincide con $L(f,s-2)$, donde

$$L(f,s) := \sum_{n=1}^{\infty} a_n n^{-s}$$

es la función L asociada a f, y por lo tanto se extiende analíticamente a todo el plano complejo y satisface una ecuación funcional con $s \mapsto 4-s$.

Si consideramos ahora X una variedad proyectiva no-singular definida, digamos, sobre $\mathbb{Q}$ habrá un conjunto finito S de primos para los cuales la reducción de X módulo p es singular. Para cada $0 \leq k \leq n$ consideramos la k-ésima función L de X dada por

$$L_k(X,s) = \prod_{p \notin S} P_k(p^{-s})^{-1},$$

donde $P_k(T)$ es el correspondiente factor de la función zeta de la reducción de X módulo p. Las conjeturas de Weil parte (2) implican que este producto converge para $\Re(s) > 1 + k/2$. La función *zeta de Hasse–Weil* $\zeta_X(s)$ de X se define como el producto alternado de las L_k.

¿Qué podemos decir sobre $L_k(X,s)$? En general no mucho pero se conjetura lo siguiente:

(1) $L_k(X,s)$ admite una extensión meromorfa a todo s y satisface una ecuación funcional cuando $s \mapsto k+1-s$;
(2) $L_k(X,s)$ es "modular" en un sentido amplio, es decir se puede expresar en términos de formas automorfas (el programa de Langlands, ver [Ge] para una introducción);
(3) $L_k(X,s)$ satisface la *hipótesis de Riemann* (un tema importante del que no hemos hablado), es decir, todo sus ceros no triviales están sobre la linea $\Re(s) = (k+1)/2$ (el centro de simetría de la ecuación funcional).

Se pueden dar muchos ejemplos de variedades para las que $L_k(X,s)$ satisfacen (1) y (2); algunas las describimos en estas notas. En contraste, (3) no se sabe en *ningún* caso.

Notas

(1) La propiedad clave aquí es que para p primo el anillo $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo; una ecuación sobre un anillo cualquiera puede tener mas soluciones que su grado, por ejemplo $x^2 - 1 = 0$ tiene 4 soluciones en $\mathbb{Z}/8\mathbb{Z}$. Nótese que $x^2 - 1 \equiv (x-1)(x+1) \bmod 8$ pero también $x^2 - 1 \equiv (x-3)(x+3) \bmod 8$ y $x^2 - 1 \equiv (x-5)(x+5) \bmod 8$.

(2) Por un teorema de Kronecker si todas las raíces de un polinomio mónico con coeficientes enteros tienen valor absoluto igual a 1 entonces estas son necesariamente raíces de la unidad.

(3) Esta definición de polinomio abeliano esta lejos de ser standard. Una extensión $K/\mathbb{Q}$ se dice *abeliana* si es de Galois y su grupo de Galois es conmutativo. Un polinomio separable f define una álgebra $\mathbb{Q}[x]/(f)$ isomorfa a la suma de los cuerpos de descomposición $K_j = Q[x]/(f_j)$ de los factores irreducibles f_j de f. Nuestra definición equivale a que $K_j/\mathbb{Q}$ sea abeliana para todo j gracias a la ley de reciprocidad de Artin; lo que hemos hecho es tomar una consecuencia de la ley de reciprocidad de Artin como definición. Comparar con [Wy], una exposición elemental sobre la ley de reciprocidad similar a la nuestra.

(4) Un teorema de Chebotarev garantiza que cada uno de los posibles tipos de factorización ocurre para infinitos primos $p \neq l$.

(5) Con alta probabilidad la clausura algebraica del cuerpo de descomposición de f sera el grupo simétrico S_d.

(6) Este el algoritmo es la versión p-ádica del algoritmo de Newton para resolver ecuaciones sobre los números reales.

(7) Creemos imposible hablar de las funciones zeta sin discutir un mínimo la función gamma. Para un tratamiento elemental ver [Ar].

(8) La demostración increible de Apéry (ver [vdP]) es desgraciadamente algo de un hecho aislado y no parece dar ninguna indicación de como probar algo acerca de los otros valores $\zeta(5), \zeta(7), \cdots$

(9) En general se reserva el nombre de función L, más que función zeta, a funciones asociadas a cierta parte del objeto en cuestión (en este caso un polinomio; más adelante veremos funciones L asociadas a variedades de dimensión mayor). Por ejemplo la función $L(\chi, s)$ esta asociada a un carácter particular χ y no a todo el polinomio Φ_l que involucra los demás caracteres también. Para más detalles sobre funciones L de Dirichlet consultar los primeros capítulos de [Wa].

(10) El hecho que $L(\chi, 1) \neq 0$ para un carácter χ no trivial es un ingrediente fundamental de la demostración de Dirichlet de que dados enteros a, m coprimos existen infinitos primos tales que $p \equiv a \bmod m$. La demostración de Dirichlet es análoga a la demostración de Euler de la infinitud de números

primos que discutimos en el n^{o} 7.

Para completar una demostración (su cuarta) de la ley de reciprocidad cuadrática Gauss necesitaba determinar el valor preciso de $\tau(\chi)$ para un carácter cuadrático χ (ver ejercicio 6). No es difícil encontrar el valor excepto por un signo y calcular el signo es un problema difícil. Gauss comenta en una carta a H. Olbers en 1805: "The determination of the sign of the root has vexed me for many years. This deficiency overshadowed everything that I found: over the last four years, there was rarely a week I dod not make one or another attempt, unsuccesfully, to untie the knot. Finally, a few days ago, I succeeded-but not as a result of my search but rather, I should say, through the mercy of God. As lightning strikes, the riddle has solved itself". (Esta traducción del alemán aparece en [Sch-Op].)

(11) La formulación que damos de la LRC en términos de funciones L es en el espíritu de su gran generalización, la ley de reciprocidad de Artin. Citamos a Tate [Ta p. 315]: "How did Artin guess his reciprocity law? He was not looking for it... He was led to the law in trying to show that a new kind of L-series which he introduced was a generalization of the usual L-series... Not only was the idea of Artin's reciprocity law inspired by analysis, but also its proof."

(12) Dos productos de Euler son iguales si y solo si sus factores de Euler coinciden.

(13) Podría decirse que la suma de Gauss es análoga a la función gamma; en ambas se "integra" el producto de un caracter aditivo y uno multiplicativo. Esta analogía es de hecho útil. Desde este punto de vista $J(\chi, \chi')$ sería como la funcion beta (ver el teorema siguiente (4)).

(14) Este anillo es a $\mathbb{Q}(\zeta_3)$ como $\mathbb{Z}$ es a $\mathbb{Q}$; más precisamente: $\mathbb{Z}[\zeta_3]$ es el *anillo de enteros* del cuerpo de números $\mathbb{Q}(\zeta_3)$.

(15) Esta es de hecho una situación especial: los anillos de enteros de cuerpos de números son raramente dominios de factorización única.

(16) De hecho, Weil se inspiro en parte en Gauss para formular sus conjeturas (ver n^{o} 18 y 21) . Citemos a Weil mismo [We III p. 279–302] "In 1947, in Chicago, I felt bored and depressed, and, not knowing what to do, I started reading Gauss's two memoirs on biquadratic residues, which I had never read before. The Gaussian integers occur in the second paper. The first deals essentially with the number of solutions of equations $ax^4 - by^4 = 1$ in the prime field módulo p, and with the connection between these and certain Gaussian sums; actually the method is exactly the same that is applied in the last section of the *Disquisitiones* to the Gaussian sums of order 3 and the equations $ax^3 - by^3 = 1$. Then I noticed that similar principles can be applied to all equations of the form $ax^m + by^n + cz^r + \cdots = 0$, and that

this implies the truth of the so called "Riemann hypothesis"...This led me in turn to conjectures about varieties over finite fields..."

Weil también menciona en ese mismo articulo que en la última nota de su diario Gauss describe una conexión, descubierta "empíricamente", entre el número de soluciones de $x^2+y^2+x^2y^2 \equiv 1 \bmod p$ y enteros a, b tales que $p = a^2 + b^2$ (para $p \equiv 1 \bmod 4$). La nota de Gauss de 1814 describe esta conexión luego de comentar "I have made by induction the most important observation that connects the theory of biquadratic residues most elegantly with the lemmiscatic functions". (Gauss escribía en latín, la traducción al inglés es de J. J. Gray [Gr]; en su época "by induction" quería decir "empíricamente".)

(17) La extensión analítica y ecuación funcional para funciones L asociadas a caracteres de Hecke de un cuerpo de números cualquiera fue probada por Hecke mismo, esencialmente pero naturalmente con mayores dificultades técnicas, como en este nº . J. Tate en su tesis redemostró estos resultados (y mas) usando técnicas de análisis armónico en cuerpos locales. Es imposible exagerar la influencia que la tesis de Tate ha tenido en la teoría de números.

(18) Encontrar la forma de Weierstrass de una curva elíptica puede hacerse en forma sistematica; aunque puede ser tedioso hacerlo a mano existen varios programas de computadora para ello.

(19) Dos formas de Weierstrass que determinan curvas isomorfas difieren de un cambio de variable sencillo. Por ejemplo,

$$y^2 = x^3 + ax + b, \qquad y^2 = x^3 + a_1x + b_1, \qquad a, b, a_1, b_1 \in K$$

determinan curvas isomorfas sobre K si y solo si $a_1 = u^4a, b_1 = u^6b$ para algún $u \in K$ no nulo (el cambio de variable correspondiente es $x \mapsto u^2x, y \mapsto u^3y$).

(20) Un algoritmo de Tate permite encontrar esta ecuación minimal eficientemente en cualquier caso concreto.

(21) En la práctica el conductor se calcula facilmente usando el algoritmo de Tate que mencionamos en (20).

(22) Recordamos una frase de Eichler. "Las cinco operaciones fundamentales de la aritmética son la suma, la resta, el producto, la división, y las formas modulares." La funciones θ y θ_χ de los nº 7 y 9 también son formas modulares. La función L asociada a cualquier newform se extiende como función meromorfa a todo el plano complejo y satisface una ecuación funcional.

(23) Una conjetura de Szpiro predice precisamente que el discriminante no puede ser demasiado grande comparado con el conductor (ver [O1]).

Bibliografía

[Ar] E. Artin, *The Gamma Function*, Holt, Rinehart and Winston, New York, 1964.

[Ap] T. Apostol, *Modular functions and Dirichlet series in number theory*, Springer-Verlag, New York, 1990.

[Ca] J. W. S. Cassels, *Local Fields*, Cambridge University Press, Cambridge, 1986.

[Ga] C. F. Gauss, *Recherches Arithmétiques*, Librairie Scientifique et Technique Albert Blanchard, Paris, 1979.

[Ge] S. Gelbart, *An elementary introduction to the Langlands program*, Bulletin of the AMS **10** (1984), 177–219.

[Gr] J. J. Gray, *A commentary on Gauss's mathematical diary, 1796–1814, with an English translation*, Exposition. Math. **2** (1984), 97–130.

[Hur] A. Hurwitz, *Mathematische Werke*, Birkhäuser, Basel, 1933.

[IR] K. Ireland and M. Rosen, *A Classic Introduction to Number Theory*, Springer Verlag, New York, 1990.

[Ka] N. Katz, *An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields*, Proceedings of Symposia in Pure Mathematics, Mathematical developments arising from Hilbert Problems, vol. 28, Part 1, AMS, Providence, Rhode Island, 1976, pp. 275–306.

[Li] R. Livné, *Cubic exponential sums and Galois representations*, Current Trends in Arithmetical Algebraic Geometry (K. Ribet, ed.), Contemporary Mathematics, vol. 67, AMS, Providence, Rhode Island, 1987, pp. 247–262.

[O1] J. Oesterlé, *Nouvelles approches du "théorème" de Fermat*, Séminaire Bourbaki, 1987/88, Astérisque, vol. 161–162, 1988, pp. 165–186.

[O2] J. Oesterlé, *Travaux de Wiles (et Taylor, ...). II*, Séminaire Bourbaki, 1994/95, Astérisque, vol. 237, 1996, pp. 333–355.

[Ri] K. Ribet, *Wiles proves Taniyama's conjecture; Fermat's last theorem follows*, Notices of the AMS **40** (1993), 575–576.

[RS] K. Rubin and A. Silverberg, *A report on Wiles' Cambridge lectures*, Bulletin of the AMS **31** (1994), 15–38.

[Sch] R. Schoof, *Wiles' proof of Taniyama-Weil conjecture for semi-stable elliptic curves over Q*, Gaz. Math. **66** (1995), 7–24.

[Sch-Op] W. Scharlau and H. Opolska, *From Fermat to Minkowski, Lectures on the Theory of Numbers and Its Historical Development*, Springer Verlag, New York, 1985.

[Se1] J. -P. Serre, *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1970.

[Se2] J. -P. Serre, *Travaux de Wiles (et Taylor, ...). I*, Séminaire Bourbaki, 1994/95, Astérisque, vol. 237, 1996, pp. 319–332.

[ST] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer Verlag, New York, 1992.

[Ta] J. Tate, *The General Reciprocity Law*, Proceedings of Symposia in Pure Mathematics, Mathematical developments arising from Hilbert Problems, vol. 28, Part 2, AMS, Providence, Rhode Island, 1976, pp. 311–322.

[vdP] A. van der Poorten, *A proof that Euler missed... Apéry's proof of the irrationality of* $\zeta(3)$, Math. Intelligencer **1** (1978/79), 195–203.

[Wa] L. Washington, *Introduction to cyclotomic fields*, Springer Verlag, New York, 1997.

[WW] E. T. Whittaker and G. N. Watson, *A Course in Modern Analysis*, Cambridge University Press, Cambridge, 1927.

[We] A. Weil, *Collected Papers*, Springer Verlag, New York, 1980.

[Wy] B. Wyman, *What is a reciprocity law?*, American Mathematical Monthly **79** (1972), 571–586.

Department of Mathematics University of Texas at Austin

Preprint

E-mail address: villegas@math.utexas.edu