PRÁCTICA 4: LA ESTRUCTURA DE $\mathbb{Z}_n^*$, LOS CARACTERES Y EL TEOREMA DE DIRICHLET

Ejercicio 1.

i) Probar que si g es una raíz primitiva del primo p, entonces $-g$ también lo es cuando $p \equiv 1 \pmod 4$, pero que si $p \equiv 3 \pmod 4$ entonces $\overline{g}$ tiene orden $(p-1)/2$ en $\mathbb{Z}_p^*$.

ii) Probar que 2 es una raíz primitiva módulo p si p es un primo de la forma $2^n + 1$ con $n > 1$.

iii) Probar que 3 es una raíz primitiva módulo p si p es un primo de la forma $4q + 1$, donde q es un primo impar.

iv) Si p es de la forma $4q + 1$ donde q es un primo impar, demostrar que cada no resto cuadrático de p es una raíz primitiva, salvo las dos soluciones de la congruencia $x^2 \equiv -1 \pmod p$ que también son no restos cuadráticos.

Ejercicio 2.

i) Sea p un primo impar, $\alpha \geq 1$ y g una raíz primitiva. Probar que los caracteres de Dirichlet módulo p^α vienen dados por la fórmula

$$\chi_h(n) = \begin{cases} e^{2\pi i h b(n)/\varphi(p^\alpha)} & \text{si} \quad p \nmid n \\ 0 & \text{si} \quad p | n \end{cases}$$

donde $b(n)$ es el único entero que satisface las relaciones

$$n \equiv g^{b(n)} \pmod{p^\alpha}, \quad 0 \leq b(n) < \varphi(p^\alpha)$$

ii) Mostrar que existen exactamente dos caracteres de Dirichlet reales módulo p^α.

iii) Probar que χ_h es primitivo módulo p^α si y sólo si p no divide a h.

iv) Mostrar que existen exactamente cuatro caracteres de Dirichlet reales módulo 2^α.

Ejercicio 3. Es posible demostrar que en la progresión aritmética $nk + 1$ ($k \in \mathbb{Z}$) hay infinitos primos (caso particular del teorema de Dirichlet) mediante un argumento algebraico que generaliza al de Euclides. Este argumento utiliza los polinomios ciclotómicos $\Phi_n(X)$.

i) Supongamos que p no divide a n. Probar que p divide a $\Phi_n(a)$ si y sólo si $\overline{a}$ tiene orden n en Z_p^*. (En clase demostramos esto pero suponiendo que n dividía a $p-1$. No obstante el resulado es cierto en general). Sugerencia: si $p|\Phi_n(a)$ y $\overline{a}$ tiene orden $d_0 < n$ en $\mathbb{Z}_p^*$, ver que:

$$a^n - 1 \equiv (a+p)^n - 1 \equiv 0 \pmod{p^2}$$

ii) Si p no divide a n, p divide a $\Phi_n(a)$ para algúbn $a \in \mathbb{Z}$, si y sólo si $p \equiv 1 \pmod{n}$.

iii) Para $n \geq 1$, existen infinitos primos tales que $p \equiv 1 \pmod{n}$. Sugerencia: si sólo hubiera finitos primos, $p_1, p_2, \ldots, p_r$ congruentes a 1 módulo n, considerar $M = np_1p_2 \cdots p_r$ y probar que para $N \in \mathbb{Z}$ suficientemente grande $\Phi_n(NM)$ es divisible por algún otro primo que por ii) también debe ser congruente a 1 módulo n.

Ejercicio 4. Sean $q \geq 1$ y a coprimo con q.

i) Probar que si χ no es el caracter principal:

$$\sum_{p \leq x} \frac{\chi(p) \log p}{p} = O(1)$$

(donde la suma recorre los primos menores o iguales que x. Sugerencia: relacionar esta suma con la L-serie $L(s, \chi)$.

ii) Demostrar que:

$$\sum_{p \leq x, p \equiv a \pmod{q}} \frac{\log p}{p} = \frac{1}{\varphi(q)} \log x + O(1)$$

(Esto proporciona otra prueba del teorema de Dirichlet diferente de la vista en clase).

Ejercicio 5. Sea χ_1 un caracter de Dirichlet complejo (i.e: χ no toma sólo valores reales). Este ejercicio propone una prueba de que $L(1, \chi_1) \neq 0$ diferente de la vista en clase.

i) Si $L(1, \chi_1) = 0$. entonces $L(1, \overline{\chi}) = 0$.

ii) Introduzcamos La función

$$F(s) = \prod_{\chi \mod q} L(s, \chi)$$

donde el producto recorre los caracteres de Dirichlet módulo q, Entonces si suponemos que $L(1, \chi_1) = 0$, tenemos que:

$$\lim_{s \to 1^+} F(s) = 0$$

ii) $F(s)$ admite un desarrollo en serie de Dirichlet

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

válido si $\mathrm{Re}(s) > 1$, donde $a_n \in \mathbb{R}$, $a_1 = 1$ y $a_n \geq 0$ para $n \geq 1$.

iv) A partir de ii) y iii) probar por reducción al absurdo que $L(s, \chi_1) \neq 0$.

Ejercicio 6. El siguiente ejercicio proporciona una prueba alternativa a la vista en clase de que $L(1, \chi) \neq 0$ si χ es un caracter real.

i) Probar que la función

$$G(s) = \frac{\zeta(s}{\zeta(2s)} L(s, \chi)$$

admite el desarrollo en serie de Dirichlet:

$$G(s) = \sum_{n=1}^{\infty} \frac{(|\mu| * \chi)(n)}{n^s}$$

válido si $\mathrm{Re}(s) > 1$. Probar que los coeficientes de este desarrollo son números reales no negativos.

iii) Teorema de Landau: Sea $f(s)$ una función definida por una serie de Dirichlet

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad (*)$$

convergente en un semiplano $\sigma = \mathrm{Re}(s) > c$, con coeficientes no negativos. Probar que si la función f admite una prolongación analítica a un entorno de c, entonces existe un $\varepsilon > 0$ tal que la serie de Dirichlet de f converge también en el semiplano $\sigma > c - \varepsilon$

Sugerencia: utilizar el desarrollo de Taylor de f en un entorno de c y sustituir en él la expresion de las derivadas $f^{(k)}(c)$ calculadas derivando la serie (*), para probar que dicha serie converge en $s = c - \varepsilon$.

iii) Probar que si $L(1, \chi) = 0$ entonces la serie de Dirichlet de G converge si $\mathrm{Re}(s) > 1/2 - \varepsilon$ para algún $\varepsilon > 0$, y por lo tanto

$$\liminf_{s \to (1/2)^+} G(s)$$

existe y es mayor o igual que 1.

iv) Concluir por reducción al absurdo, que $L(s, \chi) \neq 0$.

Ejercicio 7. Este ejercicio propone una generalización del argumento visto en clase para probar que $\zeta(s) \neq 0$ y más generalmente $L(s, \chi) \neq 0$ cuando $\mathrm{Re}(s) = 1$, debida a Kumar Murty:

i) Probar la siguiente identidad trigonométrica:

$$(2m+1) + 2\sum_{j=0}^{2m-1} (j+1)\cos\left((2m-j)\theta\right) = \left(\frac{\sin\left(\left(m+\frac{1}{2}\right)\theta\right)}{\sin(\theta/2)}\right)^2$$

(Sugerencia: utilizar exponenciales complejas)

ii) Sea $f(s)$ una función de variable compleja que satisface:

a) f es holomorfa en $\mathrm{Re}(s) > 1$.

b) $\log f(s)$ admite un desarrollo en serie de Dirichlet

$$\log f(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

con $b_n \geq 0$ para $\mathrm{Re}(s) > 1$.

c) En la recta $\mathrm{Re}(s) = 1$, f es holomorfa falvo un polo de orden $e \geq 0$ en $s = 1$.

entonces si f tiene un cero en la recta $\mathrm{Re}(s) = 1$, el orden de este cero es menor o igual que $\frac{e}{2}$.

iii) Aplicando este resultado a la función

$$F(s) = \prod_{\chi \mod q} L(s, \chi)$$

definida en el item ii) del ejercicio 4, probar de otra manera que $L(s, \chi) \neq 0$ si $\mathrm{Re}(s) = 1$ para cualquier caracter χ.

Ejercicio 8.

i) Sea χ un caracter primitivo no prinicipal módulo q. Consideramos su suma de Gauss

$$G(n, \chi) = \sum_{m=1}^{q} \chi(m) e^{2\pi i m n/q}$$

Demostrar que:

$$L(1, \chi) = -\frac{G(1, \chi)}{q} \sum_{k=1}^{q} \overline{\chi(k)} \log(1 - \omega^k)$$

donde $\omega = e^{2\pi i/q}$ y log denota la rama principal del logaritmo.

ii) Probar que si χ es par:

$$L(1, \chi) = -\frac{G(1, \chi)}{q} \sum_{k=1}^{q} \overline{\chi(k)} \log \operatorname{sen} \frac{\pi q}{k}$$

mientras que si χ es impar:

$$L(1, \chi) = \frac{i\pi G(1, \chi)}{q} \sum_{k=1}^{q} \overline{\chi(k)} k$$