Introducción a la Teoría Analítica de Números

Pablo De Nápoli

clase 11

1. Introducción

Recordamos que

$$\mathbb{Z}_n^* = \text{unidades del anillo } \mathbb{Z}_n = \{\overline{a} \in \mathbb{Z}_n : (a,n) = 1\}$$

es un grupo abeliano [=conmutativo] (con la operación de producto de clases módulo n). Observamos también que el orden (cantidad de elementos) de este grupo está dado por la función de Euler $\varphi(n)$.

Recordamos también que el orden de un elemento g en un grupo $(G,.)$ con elemento neutro e, se define como el menor entero k tal que $g^k = e$. Coincide con el orden del subgrupo generado por g:

$$< g >= \{g^k : k \in \mathbb{Z}\}$$

En consecuencia, si G es finito, por el teorema de Lagrange el orden de un elemento siempre es un divisor del orden de G. En particular esto dice que:

$$g^{\#(G)} = e \; \forall \; g \in G$$

Aplicando este resultado al grupo $\mathbb{Z}_n^*$ tenemos el siguiente teorema [1]:

Teorema 1.1 (Fermat-Euler) *Si a es coprimo con n, entonces el orden de $\overline{a}$ en $\mathbb{Z}_n^*$ es un divisor de $\varphi(n)$, y en particular:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Definición 1.1 *Un entero $g \in \mathbb{Z}$ se dice una raíz primitiva módulo n si $\overline{g}$ es un generador de $\mathbb{Z}_n^*$, o lo que es equivalente: si el orden de $\overline{g}$ en $\mathbb{Z}_n^*$ es $\varphi(n)$.*

Ejemplo: Consideremos el grupo $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Consideramos $g = 2$, entonces:

$$2^1 = 2, 2^2 = 4, 2^3 = 8 \equiv 3 \pmod{5}, 2^4 = 16 \equiv 1 \pmod{5}$$

[1] Ver también mi apunte de enteros de álgebra I, teorema A.3, para una demostración directa.

En consecuencia, el orden de $\overline{2}$ es $\mathbb{Z}_5^*$ es $4 = \varphi(5)$. Por lo tanto 2 es una raíz primitiva módulo 5.

Nuestro próximo objetivo será estudiar la estructura del grupo $\mathbb{Z}_n^*$. Comenzamos por el caso en que p es primo.

Teorema 1.2 *Si p es primo, entonces el grupo $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ es cíclico, en otras palabras: siempre existen raices primitivas módulo p.*

La prueba que daremos de este teorema se basa en las propiedades de los polinomios ciclótómicos[2].

Recordamos que el polinomio ciclotómico $\Phi_n(X)$ se define como el polinomio mónico (en $\mathbb{C}[X]$) cuyas raices son exactamente las raices primitivas n-ésimas de la unidad:

$$\Phi_n(X) = \prod_{\omega_k \in G_n^*} (X - \omega_k)$$

donde G_n^* designa el conjunto de las raices n-ésimas primitivas de la unidad.

Por ejemplo:

$$\Phi_1(X) = X - 1$$
$$\Phi_2(X) = X + 1$$
$$\Phi_4(X) = (X - i)(X + i) = X^2 + 1$$

Como sabemos que hay exactamente $\varphi(n)$ raices primitivas de la unidad (siendo φ la función de Euler), deducimos que el grado del polinomio $\Phi_n(X)$ es exactamente $\varphi(n)$.

Si G_n denota el conjunto de las raices n-ésimas de la unidad, la descomposición

$$G_n = \bigcup_{d|n} G_d^* \quad \text{(unión disjunta)}$$

proporciona la factorización:

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \tag{1}$$

Los polinomios $\Phi_n(X)$ se pueden calcular recursivamente a partir de la relación (1). Por ejemplo, calculemos $\Phi_5(X)$ y $\Phi_{15}(X)$. Como

$$X^5 - 1 = \phi_1(X)\phi_5(X)$$

tenemos, efectuando la división de polinomios que que:

$$\Phi_5(X) = \frac{X^5 - 1}{X - 1} = X^4 + X^3 + X^2 + X + 1$$

[2]En el libro de Apostol se da una prueba diferente que no los emplea.

y como

$$X^{15}-1=\Phi_1(X)\Phi_3(X)\Phi_5(X)\Phi_{15}(X)=(X^5-1)(X^2+X+1)\Phi_{15}(X)$$

tenemos que:

$$\Phi_{15}(X)=\frac{X^{15}-1}{(X^5-1)(X^2+X+1)}=\frac{X^{10}+X+1}{X^2+X+1}$$

y efectuando la división de polinomios, finalmente encontramos que:

$$\Phi_{15}(X)=X^8-X^7+X^5-X^4+X^3-X+1$$

Es inmediato demostrar por inducción a partir de (1)) que $\Phi_n(X)$ es siempre un polinomio con coeficientes enteros. En particular, es posible evaluarlos en los elementos de $\mathbb{Z}_n$ (o más generalmente, de cualquier anillo).

Lema 1.1 *Sea p un primo, y d un divisor de $p-1$ entonces, en $\mathbb{Z}_p^*$ el polinomio ciclotómico $\Phi_d(X$ tiene exactamente $\varphi(d)$ raices.*

Prueba: Notamos que, por el teorema de Fermat, el polinomio $f=X^{p-1}-1$ se anula en todos los elementos de $\mathbb{Z}_p$. Dicho polinomio admite la factorización

$$f=\prod_{d|p-1}\Phi_d(X)$$

y como $\mathbb{Z}_p$ es un cuerpo, cada raíz de f debe ser raíz de algún Φ_d con $d|p-1$.

Pero no puede ser raíz de estos polinomios ciclotómicos, pues sino f tendría raices múltiples, lo cual no puede ocurrir pues su polinomio derivado (formal) $f'=(p-1)X^{p-2}$ solo se anula en $X=\overline{0}$ (que no está en $\mathbb{Z}_p^*$.

En consecuencia, cada elemento de $\mathbb{Z}_p^*$ es raíz de exactamente un polinomio ciclotómico Φ_d con d divisor de $p-1$. Si designamos por r_d el número de raices de Φ_d en $\mathbb{Z}_p^*$, tendremos en consecuencia:

$$\sum_{d|p-1}r_d=p-1 \tag{2}$$

Por otro lado, recordamos que en un cuerpo un polinomio no puede tener más raices que el grado; por lo tanto:

$$0\leq r_d\leq\varphi(d) \tag{3}$$

y se tiene que:

$$\sum_{d|p-1}\varphi(d)=p-1 \tag{4}$$

Restando (2) y (4), deducimos que:

$$\sum_{d|p-1}\{\varphi(d)-r_d\}=0$$

y como cada término de esta suma es no negativo por 3, se deduce que todos los términos deben ser nulos, es decir $r_d=\varphi(d)$ para cada d que divide a $p-1$, como afirma el lema. □

Lema 1.2 *$\overline{a} \in \mathbb{Z}_p^*$ es raíz de Φ_d (donde $d|p-1$) si y sólo si $\overline{a}$ tiene orden d en $\mathbb{Z}_p^*$.*

Prueba: Si $\overline{a}$ es raíz de Φ_d, entonces la factorización

$$X^d - 1 = \prod_{e|d} \Phi_e(X) \tag{5}$$

implica que $\overline{a}^d = \overline{1}$. Si el orden de $\overline{a}$ fuera menor que d, sería $\overline{a}^e = \overline{1}$ para algún divisor propio $e < d$ de d. Pero entonces como

$$X^e - 1 = \prod_{f|e} \Phi_e(X)$$

(y dado que $\mathbb{Z}_p$ es un cuerpo) $\overline{a}$ sería raíz de Φ_f para algún divisor f de e. Es decir: $\overline{a}$ sería raíz de Φ_d y Φ_e, dos polinomios ciclotómicos correspondientes a dos divisores diferentes de $p-1$, y vimos en el lema anterior que ello no era posible. Esto prueba que el orden de $\overline{a}$ es d.

Recíprocamente, si $\overline{a}$ tiene orden d entonces $\overline{a}^d = 1$, por lo que por (5) $\Phi_e(\overline{a}) = \overline{0}$ para algún e que divide a d, y por lo antes demostrado $d = e$. □

Combinando los resultados de ambos lemas, concluimos que en $\mathbb{Z}_p^*$ hay exactamente $\varphi(d)$ elementos de orden d. En particular, tomando $d = p-1$, vamos que hay $\varphi(p-1)$ raices primitivas módulo p. En particular: $\mathbb{Z}_p$ es cíclico. Esto completa la prueba del teorema.

2. Restos Cuadráticos

En esta sección aplicaremos el resultado anterior, para estudiar algunas propiedades relacionadas con los restos cuadráticos:

Definición 2.1 *Sea p un número primo impar, y a un entero no divisible por p. Decimos que a es un resto cuadrático módulo p si la congruencia*

$$x^2 \equiv a \pmod{p} \tag{6}$$

tiene soluciones, es decir si $\overline{a}$ tiene una raíz cuadrada en $\mathbb{Z}_p$. En caso contrario, decimos que a es un no resto cuadrático módulo p.

Definimos el símbolo de Legendre por:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & si \quad p|a \\ 1 & si \quad p \not| a \text{ y } a \text{ es un resto cuadrático módulo } p \\ 1 & si \quad p \not| a \text{ y } a \text{ es un no resto cuadrático módulo } p \end{cases}$$

Notamos que "ser un resto cudrático" (o no-resto cuadrático) es en realidad una propiedad de la clase $\overline{a} \in \mathbb{Z}_p$, de modo que:

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ si } a \equiv b \pmod{p}$$

Ejemplo: Vimos que $\Phi_4(X) = X^2 + 1$. Si p un primo de la forma $4n+1$, el lema 1.1 implica que Φ_4 tiene dos raices en $\mathbb{Z}_p^*$. En consecuencia, -1 es un resto cuadrático de dichos primpos.

Proposición 2.1 *Sea p un primo impar. Si g es una raíz primitiva módulo p, entonces g^k es un resto cuadrático módulo p si k es par, y un no resto cuadrático módulo p si k es impar. Es decir que:*

$$\left(\frac{g^k}{p}\right) = (-1)^k$$

Prueba: Escribamos $\overline{a} = \overline{g}^k$ y $\overline{x} = \overline{g}^l$ entonces la congruencia (6) es equivalente a:

$$2l \equiv k \pmod{p-1}$$

pues g tiene órden $p-1$. Aquí k es un dato, y l es una incógnita. En consecuencia, esta congruencia tendrá solución si y sólo si el máximo común divisor entre $p-1$ y 2, que es 2, divide a k; es decir, si k es par. □

Corolario 2.1 *En $\mathbb{Z}_p^*$ hay $\frac{p-1}{2}$ restos cuadráticos módulo p, y $\frac{p-1}{2}$ no restos cuadráticos.*

Prueba: Si g es una raíz primitiva, un sistema de representantes de las clases de $\mathbb{Z}_p^*$ es:

$$\{1, g, g^2, \ldots, g^{p-1}\}$$

Por la proposición anterior, las clases correspondientes a las potencias pares de g son restos cudráticos, y las correspondientes a exponentes impares son no restos cuadráticos. □

Corolario 2.2 *El símbolo de Legendre es completamente multiplicativo. Es decir si $a, b \in \mathbb{Z}$:*

$$\left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{ab}{p}\right) \tag{7}$$

Prueba: Si a y b no son divisibles por p, escribimos $\overline{a} = \overline{g}^k$ y $\overline{b} = \overline{g}^l$, siendo g una raíz primitiva módulo p. Entonces:

$$\left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = (-1)^k(-1)^l = (-1)^{k+l} = \left(\frac{ab}{p}\right)$$

pues $\overline{ab} = \overline{g}^{k+l}$.

Por otra parte, si a o b son divisibles por p, entonces ab también lo será y (7) se verifica trivialmente, pues ambos miembros son nulos. □

Teorema 2.1 (Criterio de Euler) *Sea p un primo impar. Entonces*

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Prueba: Supongamos primero que p no divide a a. Nuevamente consideramos una raíz primitiva g módulo p, y escribimos $\overline{a} = \overline{g}^k$. Entonces

$$a^{(p-1)/2} \equiv g^{k(p-1)/2} \equiv b^k \pmod{p}$$

donde $b = g^{(p-1)/2}$. Notamos que:

$$b^2 \equiv g^{p-1} \equiv 1 \pmod{p}$$

por consiguiente $b \equiv \pm 1 \pmod{p}$. Pero como g es una raíz primitiva $b \not\equiv 1 \pmod{p}$ (pues sino el orden de g sería menor o igual que $(p-1)/2$). Luego $b \equiv -1 \pmod{p}$, y por lo tanto:

$$a^{(p-1)/2} \equiv (-1)^k \equiv \left(\frac{a}{p}\right) \pmod{p}$$

por la proposición anterior. Finalmente si p divide a a, el teorema se verifica trivialmente pues p divide a $a^{(p-1)/2}$. □

Ejemplo: Tomando $a = -1$ entontramos que

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si} \quad p \equiv 1 \pmod{4} \\ -1 & \text{si} \quad p \equiv 3 \pmod{4} \end{cases}$$

Es decir que: -1 es un resto cuadrático de los primos de la forma $4n+1$, y un no resto cuadrático de los primos de la forma $4n+3$.

3. El teorema chino del resto

El teorema chino del resto (que se ve en los cursos de álgebra I) permite reducir el problema de estudiar la estructura de $\mathbb{Z}_n^*$ al caso en que n es una potencia de un primo:

Teorema 3.1 (Teorema chino del resto) *Si $m = m_1 m_2$ donde m_1 y m_2 son coprimos, entonces*

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \quad \textit{(isomorfismo de anillos)}$$

En particular mirando el grupo de las unidades de cada anillo se obtiene que

$$\mathbb{Z}_m^* \simeq \quad \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \textit{(isomorfismo de grupos)}$$

(En este enunciado $\oplus$ denota la suma directa de anillos, y $\times$ el producto directo de grupos).

Para la prueba del teorema chino del resto, pueden consultar mi apunte de enteros de álgebra I (teorema 12.1). También pueden encontrar allí una prueba explícita de la segunda afirmación (lema A.1, es fácil ver que la función f construida allí proporciona el isomorfismo buscado), aunque en dicho apunte estos

resultados no están enuciados en el lenguaje de la teoría de grupos. En el curso de álgebra I dicho lema lo utilicé en dicho apunte para probar que la función de Euler φ es multiplicativa, lo cual es una consecuencia inmediata de este teorema, pues siendo isomorfos Z_m^* y $\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^*$ deben tener la misma cantidad de elementos, lo que proporciona la igualdad:

$$\varphi(m) = \varphi(m_1)\varphi(m_2)$$

Este teorema se generaliza al caso de varios factores coprimos dos a dos:

Teorema 3.2 *Si $m = m_1 m_2 \dots m_k$ donde los m_i son coprimos dos a dos, entonces*

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \dots \oplus \mathbb{Z}_{m_k} \quad \textit{(isomorfismo de anillos)}$$

En particular mirando el grupo de las unidades de cada anillo se obtiene que

$$\mathbb{Z}_m^* \simeq \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \dots \times \mathbb{Z}_{m_k}^* \quad \textit{(isomorfismo de grupos)}$$

Deducimos que si m admite la factorización

$$m = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

(donde los p_i son primos distintos), entonces

$$\mathbb{Z}_m^* \simeq \mathbb{Z}_{p_1^{e_1}}^* \times \mathbb{Z}_{m_2^{e^2}}^* \times \dots \times \mathbb{Z}_{p_k^{e_k}}^*$$