Clase 9

Propiedades de la función φ de Euler

- Recordar que la función φ que aparece en el Teorema de Euler tiene por valor φ(n), con n > 0, el cardinal del conjunto $(\mathbb{Z}/n\mathbb{Z})^*$, que es igual al cardinal de:

$$U_n = \{ a : 1 \leq a \leq n \ y \ mcd(a,n) = 1 \}$$

Veamos ahora propiedades de la función φ que nos permitirán determinar su fórmula en función de la factorización de n en primos.

Antes necesitamos lo siguiente:

Definición: Una función f : $\mathbb{N} \rightarrow \mathbb{R}$ se dice MULTIPLICATIVA si, $\forall \, a, \, b \in \mathbb{N}$ con mcd (a,b) = 1 se tiene f(a·b) = f(a)·f(b).

Propiedad:

(1) φ es multiplicativa

(2) Si p primo: $\varphi(p^r) = p^{r-1}\cdot$ (p-1)

Demostración:

(1) Si a,b $\in \mathbb{N}$ coprimos, queremos ver que φ (a$\cdot$b)= φ(a) $\cdot\varphi$(b).

Recordar que φ(a) es el cardinal de $(\mathbb{Z}/a\mathbb{Z})*$, o lo que es lo mismo, el del conjunto U_a. Y lo mismo es válido para φ(b) y para φ (a$\cdot$b).

Lo que queres pues es demostrar que:

$$\left|(\mathbb{Z}/a\mathbb{Z})*\right| \cdot \left|(\mathbb{Z}/b\mathbb{Z})*\right| = \left|(\mathbb{Z}/a\cdot b\mathbb{Z})*\right| \qquad \text{(I)}$$

(donde $|C|$ denota el cardinal de un conjunto C).

Para probarlo, construyo una función:

$$F : (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^* \to (\mathbb{Z}/ab\mathbb{Z})^*$$

de la siguiente forma : Sea $\overline{C_1} \in (\mathbb{Z}/a\mathbb{Z})^*$ y $\overline{C_2} \in (\mathbb{Z}/b\mathbb{Z})^*$,

Por el teorema Chino del Resto, existe $\overline{C} \in (\mathbb{Z}/ab\mathbb{Z})^*$ con $C \equiv C_1$ $(módulo\ a)$ y $C \equiv C_2$ $(módulo\ b)$. La condición de que $\overline{C} \in (\mathbb{Z}/ab\mathbb{Z})^*$, es decir, que es inversible en $\mathbb{Z}/ab\mathbb{Z}$, se desprende del hecho de que por ser C_1 coprimo con a y C_2 coprimo con b, al ser C solución del sistema C también es coprimo con a y con b, luego con ab, con lo cual mcd(C, ab) =1.

Definimos entonces $F(\overline{C_1}, \overline{C_2}) = \overline{C}$.

- Veamos que F es inyectiva: Si $F(\overline{C_1}, \overline{C_2}) = \overline{C} = F(\overline{C_3}, \overline{C_4}) \Rightarrow$
- $C_1 \equiv C \equiv C_3 \ (módulo\ a) \ \ y \ \ C_2 \equiv C \equiv C_4 \ (módulo\ b)$
- De donde $\overline{C_1} = \overline{C_3} \in (\mathbb{Z}/a\mathbb{Z})^* \ y \ \overline{C_2} = \overline{C_4} \in (\mathbb{Z}/b\mathbb{Z})^*$, es decir, F es inyectiva.
- Veamos que F es exhaustiva: Dado $\overline{C} \in (\mathbb{Z}/ab\mathbb{Z})^*$ consideremos $\overline{C_1}$ la correspondiente clase residual módulo a y $\overline{C_2}$ la correspondiente clase módulo b. Luego, se tiene que: $C \equiv C_1 \ (módulo\ a) \ \ y \ \ C \equiv C_2 \ (módulo\ b)$, y por lo tanto
- $F(\overline{C_1}, \overline{C_2}) = \overline{C}$. Obsérvese que aquí se ha usado el hecho de que como mcd(C, ab)=1 y $C \equiv C_1 \ (módulo\ a) \ \ y \ \ C \equiv C_2 \ (módulo\ b)$, entonces mcd($C_1$, a) = mcd($C_2$, b) = 1, es decir,
- $\overline{C_1} \in (\mathbb{Z}/a\mathbb{Z})^* \ y \ \overline{C_2} \in (\mathbb{Z}/b\mathbb{Z})^*$. Por lo tanto, F es exhaustiva.

- Como F es una función biyectiva del producto $(\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$ en $(\mathbb{Z}/ab\mathbb{Z})^*$, concluimos que la fórmula (I) es cierta, con lo cual queda probado que φ (a · b)= φ(a) · φ (b).
- (2) Sabemos que $\varphi(p^r)$ es el cardinal del conjunto: $U_{p^r} = \{ a : 1 \le a \le p^r, \ mcd(a, p^r) = 1 \}$.
- Como p es primo, la condición $mcd(a, p^r) = 1$ equivale a mcd(a, p)= 1, que a su vez equivale a que a no es múltiplo de p. Como hay un múltiplo de p cada p enteros consecutivos, la cantidad de múltiplos de p en el intervalo $[1, p^r]$ es: $\frac{p^r}{p} = p^{r-1}$, luego:
- $\left| U_{p^r} \right| = p^r - p^{r-1} = p^{r-1}(p-1)$

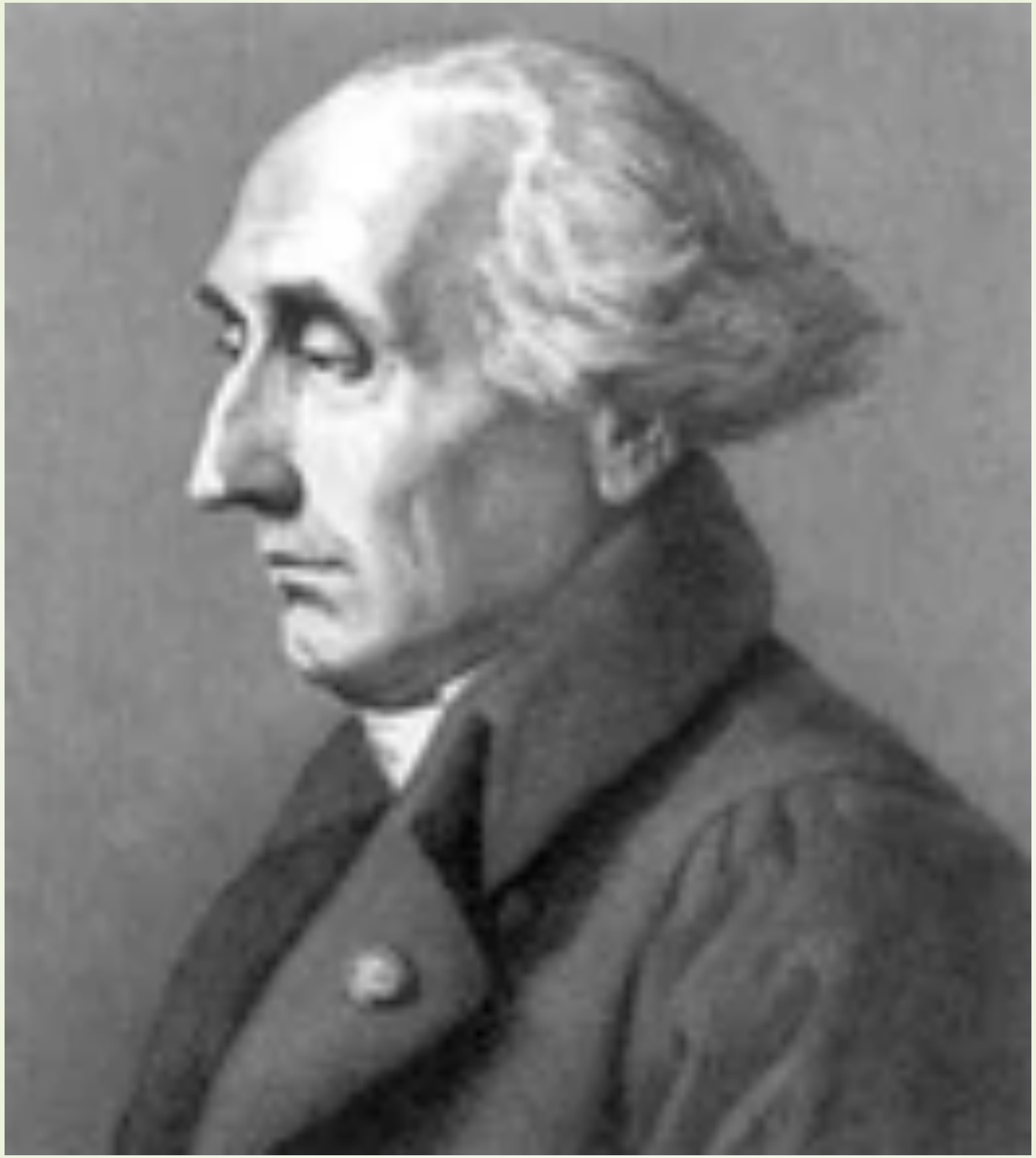
- Corolario: Si $n \geq 1$ con $n = \prod_{i=1}^{r} p_i^{s_i}$ se tiene:
- $\varphi\left(n\right) = n \cdot \prod_{i=1}^{r} \frac{p_i - 1}{p_i}$
- Demostración: La fórmula del enunciado equivale a:
- $\varphi\left(n\right) = \prod_{i=1}^{r} \frac{p_i^{s_i}\left(p_i - 1\right)}{p_i} = \prod_{i=1}^{r} p_i^{s_i - 1}\left(p_i - 1\right)$
- Como φ es multiplicativa, esto se reduce a probar que para cada primo p_i se cumple $\varphi\left(p_i^{s_i}\right) = p_i^{s_i-1}\left(p_i - 1\right)$, que es cierto por (2).

Clase 10

- Teorema de Lagrange: Sea F(x) polinomio a coeficientes enteros de grado d > 0. Sea p un número primo. Supongamos que no todos los coeficientes de F son divisibles por p. El número de clases de congruencia módulo p que son solución de la congruencia:
- $F(x) \equiv 0 \; (\text{módulo } p)$ es menor o igual que d.
- Demostración: Aplicamos inducción en d. Si d=1, ya hemos visto que una congruencia lineal:
- $a\,x + b \equiv 0 \; (\text{módulo } p)$ tiene como máximo una solución módulo p (de hecho, si a no es divisible por p, tiene una y sólo una solución, y si a es divisible por p, la hipótesis implica que b no lo es y por lo tanto la congruencia no tiene solución).
-

- Sea F de grado d > 1 y consideremos $F(x) \equiv 0\ (módulo\ p)$. Si no hubiera ninguna solución, el resultado quedaría probado. Supongamos por lo tanto que existe $x_0\ tal\ que\ F(x_0) \equiv 0\ (módulo\ p)$. Si hacemos la división de polinomios de F(x) entre $(x - x_0)$ obtenemos:
  $F(x) = G(x)\ (x - x_0) + r$ con grado(G(x)) = d -1 y r constante.
  Evaluando en x_0 ambos miembros, obtenemos: $F(x_0)$ = r (estamos probando una vez más el teorema del resto) y como
- $F(x_0) \equiv 0\ (módulo\ p)$ concluimos que $r \equiv 0\ (módulo\ p)$. Por lo tanto nos queda:
- $F(x) \equiv G(x)\ (x - x_0)\ (módulo\ p)$.
- Es evidente que la hipótesis de que no todos los coeficientes de F son divisibles por p también la tiene que cumplir G. Por hipótesis de inducción sabemos que G posee como mucho d-1 raíces módulo p.

- Sea y_0 una solución de $F(y_0) \equiv 0 \ (módulo\ p)$. Como $F(x) \equiv G(x)\ (x - x_0)\ (módulo\ p)$, evaluando en y_0 obtenemos:
- $G(y_0)\ (y_0 - x_0) \equiv F(y_0) \equiv 0\ (módulo\ p)$, que equivale a:
- $p \mid G(y_0)\ (y_0 - x_0)$. Por el Lema Fundamental de la Aritmética, deducimos que p tiene que dividir a alguno de los dos factores:
- $p \mid G(y_0) \quad o \quad p \mid (y_0 - x_0)$, es decir:
  $G(y_0) \equiv 0\ (módulo\ p) \quad o \quad y_0 \equiv x_0\ (módulo\ p)$
- Con lo cual, la clase de congruencia de y_0 ha de ser o bien una de las como mucho d-1 clases que son raíces módulo p de G(x) o bien la clase de la solución inicial x_0. Por lo tanto concluimos que hay como máximo d clases de congruencia que son raíces módulo p de F(x).
- Q. E. D.



- J.L. Lagrange

Revisión: Elementos inversibles módulo m

- Recordemos que hemos definido elementos invisibles módulo m a aquellos a tales que existe solución para la congruencia:
- $$a \cdot x \equiv 1 \ (\textit{módulo } m)$$
- En este caso, a un b tal que se cumple: $a \cdot b \equiv 1 \ (\textit{módulo } m)$ le llamamos inverso de a módulo m.
- Vimos un criterio que nos dice que las clases invisibles módulo m son exactamente aquellas cuyos elementos cumplen mcd(a,m)=1

- Vamos ahora a demostrar de otro modo que en efecto si mcd(a,m)=1 entonces a es inversible módulo m, y hagámoslo de un modo que me permite calcular el elemento inverso: si suponemos mcd(a,m)=1, entonces por la identidad de Bézout existen enteros s y t (y se pueden calcular usando Euclides) tales que:
- $s \cdot a + t \cdot m = 1$ (1)
- De aquí , vemos que se tiene: $1 - s \cdot a = t \cdot m$, de donde:
- $s \cdot a \equiv 1 \left(módulo\ m\right)$. Concluimos que existe el inverso de a módulo m, y que se lo puede calcular resolviendo una identidad de Bézout.
- Recíprocamente, partiendo de la existencia del inverso de a módulo m, se deduce que hay solución para la ecuación (1), de donde se deduce que a es coprimo con m.

- Definamos la noción de orden (módulo m) para aquellos elementos que son inversibles módulo m:
- Definición: Sea $m \geq 1$ y a coprimo con m. Llamamos ORDEN de a módulo m al menor entero positivo e tal que:
- $$a^e \equiv 1 \left(\text{módulo } m\right)$$
- Observación 1: El orden de a módulo m sólo depende de la clase de congruencia de a módulo m, y sólo se define para las clases inversibles módulo m.
- Observación 2: Sabemos por el Teorema de Euler que como mcd(a,m)=1 se tiene: $a^{\varphi(m)} \equiv 1 \left(\text{módulo } m\right)$. Por lo tanto, el orden de a módulo m existe y es menor o igual que $\varphi(m)$.

- Lema: Sea a entero con mcd(a,m)=1 y sea e el orden de a módulo m. Sea k entero positivo tal que $a^k \equiv 1 \left(\text{módulo } m\right)$. Entonces e | k. En particular se tiene que: e | $\varphi(m)$.
- Demostración: Como por definición e es positivo y es minimal se tiene que:
- 0 < e $\leq$ k. Si aplicamos división entera, obtenemos:
- $k = e \cdot q + r$, con q, r enteros y $0 \leq r < e$.
- Como $a^e \equiv 1 \left(\text{módulo } m\right) \Rightarrow a^{eq} \equiv 1 \left(\text{módulo } m\right)$.
- Luego: $a^r \equiv a^r \cdot 1 \equiv a^r \cdot a^{eq} \equiv a^{r+eq} \equiv a^k \equiv 1 \left(\text{módulo } m\right)$.
- Es decir: $a^r \equiv 1 \left(\text{módulo } m\right)$. De aquí, por ser $0 \leq r < e$ de la minimalidad de e se deduce que r = 0. Con lo cual e | k. Como por el Teorema de Euler sabemos que $a^{\varphi(m)} \equiv 1 \left(\text{módulo } m\right)$, en particular concluimos que e | $\varphi(m)$.

- De este lema se deduce fácilmente el siguiente:
- Corolario: Si mcd(a,m) =1 y e es el orden de a módulo m, y se tiene que:
- $a^s \equiv a^t \ (\text{módulo } m)$, entonces: $s \equiv t \ (\text{módulo } e)$.
- Demostración: Hagamos el caso s > t: como de mcd(a,m)=1 se deduce que $mcd(a^t, m) = 1$, podemos aplicar la cancelativa y obtener:
- $a^{s-t} \equiv 1 \ (\text{módulo } m)$. El lema previo implica por lo tanto que e | s - t, y esto equivale a $s \equiv t \ (\text{módulo } e)$.