

Conferencia 6 - Función de Euler

December 15, 2024

Definición. Sea $n \in \mathbb{Z}_+$, la **Función de Euler** que se denota $\varphi(n)$ representa el número de enteros positivos menores o iguales que n primos relativos con n . O sea $\varphi(n) = |\{d \mid 1 \leq d \leq n, (d, n) = 1\}|$.

Para 1 se define $\varphi(1) = 1$

Definición. Se llama **Sistema Residual Reducido módulo n** ($SRR(n)$) a un conjunto de $\varphi(n)$ enteros positivos incongruentes módulo n que son primos relativos con n

O sea, dado un natural positivo n , se dice que un conjunto SRR es un **Sistema Residual Reducido módulo n** si cumple lo siguiente:

1. SRR posee $\varphi(n)$ elementos
2. para cada $a \in SRR$ se cumple $(a, n) = 1$
3. los elementos de SRR son incongruentes módulo de n entre si. O lo que es lo mismo, si $a, b \in SRR$ y $a \not\equiv b \pmod{n}$

Teorema. Sean $n \in \mathbb{Z}_+$, $k \in \mathbb{Z}$, $(k, n) = 1$ y $\{a_1, a_2, \dots, a_{\varphi(n)}\}$ un sistema residual reducido módulo n , entonces $\{ka_1, ka_2, \dots, ka_{\varphi(n)}\}$ es también un sistema residual reducido módulo n .

Demostración

Supongamos que $\{ka_1, ka_2, \dots, ka_{\varphi(n)}\}$ no es un $SRR(n)$
entonces existen i, j tales que $ka_i \equiv ka_j \pmod{n}$
como $(k, n) = 1$ entonces $a_i \equiv a_j \pmod{n}$
luego $\{a_1, a_2, \dots, a_{\varphi(n)}\}$ tampoco es un $SRR(n)$,
por tanto, por contrarecíproco, si $\{a_1, a_2, \dots, a_{\varphi(n)}\}$ es un $SRR(n)$
entonces $\{ka_1, ka_2, \dots, ka_{\varphi(n)}\}$ también lo es

Teorema. $\varphi(p) = p - 1$ si y solo si p es primo

Demostración

Si p es primo entonces significa que todo entero positivo menor que él es primo relativo con él, por tanto $\varphi(p) = p - 1$

Ahora, si $\varphi(p) = p - 1$ y p es compuesto entonces $p = qr$ con $1 < q \leq r < p$ por lo que habría al menos dos números enteros positivo (p, r) , que no serían primos relativos con p por lo que $\varphi(p) \leq p - 2$, lo que es una contradicción y, por tanto, p es primo

Teorema. Si p es primo y $k > 0$ entonces $\varphi(p^k) = p^k - p^{k-1}$

Demostración

Para cualquier número n se tiene que $(n, p^k) = 1$ si y solo si $p \nmid n$. Ahora, entre 1 y p^k hay p^{k-1} enteros que son divisibles por p y que, por tanto, no son primos relativos con p^k . Estos serían $p, 2p, 3p, \dots, p^{k-1}p$. Luego, el conjunto $\{1, 2, 3, \dots, p^k\}$ contendría $p^k - p^{k-1}$ enteros que son primos relativos con p^k y, por tanto, por definición, $\varphi(p^k) = p^k - p^{k-1}$

Teorema. Teorema de Euler Sean $a, n \in \mathbb{Z}$, $n > 0$ y $(a, n) = 1$ entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$

Demostración

Sea $\{n_1, n_2, \dots, n_{\varphi(n)}\}$ un SRR(n), entonces $\{an_1, an_2, \dots, an_{\varphi(n)}\}$ con $a \in \mathbb{Z}$ tal que $(a, n) = 1$ es también un SRR(n), luego se cumple $(an_1)(an_2) \dots (an_{\varphi(n)}) \equiv n_1 n_2 \dots n_{\varphi(n)} \pmod{n}$
 $a^{\varphi(n)} n_1 n_2 \dots n_{\varphi(n)} \equiv n_1 n_2 \dots n_{\varphi(n)} \pmod{n}$
pero como $\forall(i) 1 \leq i \leq \varphi(n) \quad (n_i, n) = 1$
entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$

Definición. Una función se denomina **aritmética** si está definida en los enteros positivos.

Definición. Una función aritmética f se denomina **multiplicativa** si para cualquier m y n tales que $(m, n) = 1$ se cumple que $f(mn) = f(m)f(n)$

Teorema. Si f es una función multiplicativa y n se descompone en primos de la siguiente forma $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ entonces $f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \dots f(p_k^{e_k})$

Demostración

Si n tiene exactamente dos divisores primos distintos, entonces $k = 2$ implica que $n = p_1^{e_1} p_2^{e_2}$ por lo que $f(n) = f(p_1^{e_1} p_2^{e_2})$
ahora como $(p_1, p_2) = 1$ entonces $(p_1^{e_1}, p_2^{e_2}) = 1$
y como f es multiplicativa entonces $f(n) = f(p_1^{e_1} p_2^{e_2}) = f(p_1^{e_1}) f(p_2^{e_2})$
Ahora, supongamos que se cumple para $k = m$,
probemos entonces que se cumple para $k = m + 1$
se tiene que $n = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m} p_{m+1}^{e_{m+1}}$ y como todos los p_i , $1 \leq i \leq m + 1$, son primos relativos 2 a 2, se cumple que $(p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}, p_{m+1}^{e_{m+1}}) = 1$
y como f es multiplicativa entonces $f(n) = f(p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}) f(p_{m+1}^{e_{m+1}})$
pero como se cumple hasta m entonces $f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \dots f(p_m^{e_m}) f(p_{m+1}^{e_{m+1}})$

Teorema. $\varphi(n)$ es multiplicativa

Demostración

Si tenemos la matriz

$$\begin{pmatrix} 1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ m & 2m & 3m & \dots & nm \end{pmatrix} \quad (1)$$

Note que los elementos de una fila son de la forma $cm + r$, $0 \leq c \leq n-1$ y una r fija, $1 \leq r \leq m$,

Ahora, si $(r, m) > 1$ entonces no hay ningún número en esa fila tal que sea primo relativo con m . Entonces eliminamos todas las filas de la matriz tales que $(r, m) > 1$.

Luego, si $(r, m) = 1$ todos los números de esa fila son primos relativos con m . Por tanto hay $\varphi(m)$ filas que me interesan.

Se puede notar que cada una de estas filas es un $SRC(n)$ por lo que hay $\varphi(n)$ números por cada fila que son primos relativos con n .

Entonces, como $\varphi(nm)$ es el número de enteros de la matriz que son primos relativos a nm , y como para que sea multiplicativa, por definición, se tiene que $(n, m) = 1$, entonces como hay $\varphi(m)$ columnas con enteros primos relativos a m y en cada una de ellas $\varphi(n)$ primos relativos con n , se tiene entonces que $\varphi(nm) = \varphi(m)\varphi(n)$

Teorema. Sea $n \in \mathbb{Z}$ con $n > 1$ tal que $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ entonces

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{2}{p_2}) \dots (1 - \frac{1}{p_k})$$

Demostración

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \dots \varphi(p_k^{e_k}) \\ \varphi(n) &= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \dots (p_k^{e_k} - p_k^{e_k-1}) \\ \varphi(n) &= p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} (1 - \frac{1}{p_1})(1 - \frac{2}{p_2}) \dots (1 - \frac{1}{p_k}) \\ \varphi(n) &= n(1 - \frac{1}{p_1})(1 - \frac{2}{p_2}) \dots (1 - \frac{1}{p_k}) \end{aligned}$$

Teorema. Sea $n \in \mathbb{Z}$ tal que $n > 2$ entonces $\varphi(n)$ es par

Demostración

Si $n = 2^k$ con $k > 1$ se tiene que $\varphi(2^k) = 2^k - 2^{k-1}$ y la resta de dos números pares es par.

Si n no es una potencia de 2 entonces lo divide un primo impar p tal que $n = p^d m$ con $(p^d, m) = 1$ por lo que $\varphi(n) = \varphi(p^d)\varphi(m)$ y como $\varphi(p^d) = p^d - p^{d-1} = p^{d-1}(p-1)$, por tanto, $p-1$ es par, luego $\varphi(n)$ es par.

Definición. Sean $a, n \in \mathbb{Z}_+$, $(a, n) = 1$, el menor entero positivo tal que $a^k \equiv 1 \pmod{n}$ se denomina orden de a módulo de n y se denota $\text{ord}_n a$

Note que $\text{ord}_n a \leq \varphi(n)$