	Grado en Ingeniería Informática	Tiempo Estimado
	Álgebra y Matemática Discreta	Previo: 30 min.
	Unidades del anillo $\mathbb{Z}_n$ y Fórmula de Euler	Clase: 30 min.

Vídeo : <https://youtu.be/nNbVAaxtKd8>

## 1. Resumen

**Definición 1.** Sea  $n$  un entero positivo, denotaremos  $\mathbb{Z}_n^*$  al conjunto de las unidades de  $\mathbb{Z}_n$ , es decir, aquellos elementos  $u \in \mathbb{Z}_n$  tales que existe  $v \in \mathbb{Z}_n$  cumpliendo que  $uv \equiv 1 \pmod{n}$ .

Por ejemplo:

$$\begin{aligned}\mathbb{Z}_{10}^* &= \{1, 3, 7, 9\} \\ \mathbb{Z}_{15}^* &= \{1, 2, 4, 7, 8, 11, 13, 14\}\end{aligned}$$

**Proposición 2.** El producto de unidades es una unidad.

*Demostración.* Si  $u$  y  $v$  son unidades es porque existen  $u^{-1}, v^{-1} \in \mathbb{Z}_n$  y por lo tanto

$$(uv)(v^{-1}u^{-1}) = u(vv^{-1})u^{-1} = uu^{-1} = 1 \pmod{n}.$$

Esto prueba que el inverso de  $uv$  es  $v^{-1}u^{-1}$  y por lo tanto el producto de dos elementos que tienen inverso, lo tiene también.  $\square$

**Proposición 3.** Sea  $n$  un entero positivo y  $a \in \mathbb{Z}_n$ . Entonces  $a \in \mathbb{Z}_n^*$  (es decir, tiene inverso) si y solo si  $\text{mcd}(a, n) = 1$ .

*Demostración.* Si  $\text{mcd}(a, n) = 1$  entonces por la Identidad de Bézout sabemos que existen  $u, v \in \mathbb{Z}$  tales que  $au + nv = 1$ , pero entonces  $1 = au + nv \equiv au \pmod{n}$  porque podemos sumar y restar múltiplos de  $n$  en la congruencia. Esto demuestra que  $u$  es el inverso de  $a$  módulo  $n$  y por lo tanto  $a$  es invertible.

En el otro sentido, si  $a$  es un elemento de  $\mathbb{Z}_n^*$ , entonces existe  $u \in \mathbb{Z}_n$  tal que  $au \equiv 1 \pmod{n}$ . Dicho de otra forma  $au - 1$  es un múltiplo de  $n$  que llamaremos  $au - 1 = nt$ . Entonces  $1 = au - nt$  y si  $d = \text{mcd}(a, n)$ , como  $d$  divide a  $a$  y a  $n$ , dividirá a  $au - nt = 1$ , pero el único divisor positivo de 1 es 1. Esto prueba que  $d = 1$ .  $\square$

**Definición 4.** Sea  $n$  un entero positivo. Llamaremos  $\varphi(n)$  al número de unidades de  $\mathbb{Z}_n$ , es decir, el número de elementos de  $\mathbb{Z}_n^*$ . Esta función  $\varphi$  se llama función  $\varphi$  de Euler.

**Proposición 5.** Si  $p$  es un número primo,  $\mathbb{Z}_p$  es un cuerpo porque todos los elementos distintos de 0 son invertibles. El número de unidades es pues  $\varphi(p) = p - 1$ .


*Demostración.* Como  $p$  es primo,  $\text{mcd}(a, p)$  es un divisor de  $p$  y sólo puede ser 1 ó  $p$ . Si  $a$  no es una unidad es porque dicho divisor es  $p$ , pero  $p$  no divide a ninguno de los  $\{1, 2, \dots, p - 1\}$  que están entre  $p \cdot 0 = 0$  y  $p \cdot 1 = p$ , por tanto todos estos serán unidades.  $\square$

La función  $\varphi$  de Euler se puede calcular fácilmente si tenemos una factorización de  $n$  en primos distintos  $n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$  porque cumple las siguientes propiedades:

- $\varphi(p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}) = \varphi(p_1^{t_1}) \varphi(p_2^{t_2}) \cdots \varphi(p_k^{t_k})$  si los  $p_i$  son primos distintos.
- $\varphi(p^t) = p^t - p^{t-1}$  si  $p$  es primo.

Así, por ejemplo,  $\varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2) \varphi(3) = (2^2 - 2^1)(3^1 - 3^0) = (4 - 2)(3 - 1) = 4$ .

**Proposición 6** (Fórmula de Euler). Sea  $n$  un entero positivo y  $a$  un entero tal que  $\text{mcd}(a, n) = 1$ . Entonces  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

	Grado en Ingeniería Informática	Tiempo Estimado
	Álgebra y Matemática Discreta	Previo: 30 min.
	Unidades del anillo $\mathbb{Z}_n$ y Fórmula de Euler	Clase: 30 min.

*Demostración.* Sea  $t = \varphi(n)$  y denotemos  $\{a_1, a_2, \dots, a_t\}$  a las unidades de  $\mathbb{Z}_n$ . Como  $a$  es coprimo con  $n$ , será una de estas unidades y como el producto de unidades es una unidad, el conjunto  $\{aa_1, aa_2, \dots, aa_t\}$  son todas unidades de  $\mathbb{Z}_n$ . Pero si  $aa_i = aa_j$  multiplicando por la izquierda por  $a^{-1}$  deducimos que  $a_i = a_j$  y por lo tanto las  $\{aa_1, aa_2, \dots, aa_t\}$  son todas diferentes y como son  $t$ , han de ser las mismas que  $\{a_1, a_2, \dots, a_t\}$  cambiadas de orden.

Como en el producto no importa el orden, tenemos que

$$(aa_1)(aa_2) \cdots (aa_t) \equiv a_1 a_2 \cdots a_t \pmod{n}$$

Pero entonces podemos agrupar las  $a$ 's y escribir

$$a^t (a_1 a_2 \cdots a_t) \equiv 1 (a_1 a_2 \cdots a_t) \pmod{n}$$

Multiplicando por el inverso de  $(a_1 a_2 \cdots a_t)$  por ambos lados, concluimos que  $a^t \equiv 1 \pmod{n}$  tal y como queríamos probar.  $\square$

## 2. Erratas

(No detectadas)

## 3. Ejercicios

Con respecto a los ejercicios de este tema, conviene ser capaz de decidir si  $a$  es una unidad módulo  $n$ , pero esto es equivalente a calcular el máximo común divisor de  $a$  y  $n$ , lo cual hemos hecho ya en muchos ejercicios. Además deberíamos ser capaces de calcular el inverso de  $a$  módulo  $n$ , pero eso nos lo da la relación  $au + nv = 1$  y para calcularla utilizaremos el Algoritmo de Euclides Extendido, lo cual también hemos hecho en muchas ocasiones.

En relación con la función  $\varphi$  de Euler, en el próximo tema de la exponenciación modular, tendremos oportunidad de practicarla, porque formará parte del cálculo de las potencias de  $a$  módulo  $n$ .