Grupos Cíclicos.

Subgrupos generados y grupos cíclicos.

Def. Sea G un grupo y S un subconjunto de G. Se define el subgrupo de G generado por S, denotado por $\langle S\rangle$ como:

$$\langle S\rangle := \bigcap_{H<G,\, H\supseteq S} H$$

Proposición:

Sea G un grupo y $S\subset G$. Entonces:

i) $\langle S\rangle$ es un subgrupo de G.

ii) $S\subset\langle S\rangle$

iii) Si K es un subgrupo de G tal que $S\subset K$, entonces $\langle S\rangle\subset K$.

iv) $\langle\emptyset\rangle=\{e\}=\langle\{e\}\rangle$

v) Si H es un subgrupo de G, $\langle H\rangle=H$.

Dem:

De (i):

Sean $a,b\in\langle S\rangle$, entonces $a,b\in\bigcap_{H<G,\, S\subset H} H$, luego $a,b\in H$, $\forall\, H<G$, $S\subset H$. Como $H<G$, entonces $ab^{-1}\in H$, $\forall\, H<G$, $S\subset H$, luego $ab^{-1}\in\langle S\rangle$.

Por tanto, $\langle S\rangle$ es subgrupo de G.

De (ii):

Veamos que:

$$S=\bigcap_{H<G,\, S\subset H} S\subset\bigcap_{H<G,\, S\subset H} H=\langle S\rangle$$

luego, $S\subset\langle S\rangle$.

De (iii):

Sea $a\in\langle S\rangle$, entonces $a\in H$, $\forall\, H<G$ tal que $S\subset H$, luego $a\in K$, pues $K<G$ y $S\subset K$,

por tanto, $\langle S\rangle \subset K$.

De (iv):

Como $\forall H<G$, $\emptyset\subset H$, entonces

$$\langle\emptyset\rangle=\bigcap_{H<G,\,\emptyset\subset H} H=\bigcap_{H<G} H$$

además $\{e\}\subset H$, $\forall H<G$ y $\{e\}<H$, por lo tanto:

$$\langle\emptyset\rangle=\{e\}$$

pero, también $\forall H<G$, $\{e\}\subset H$ pues $e\in H$. Por tanto:

$$\langle\{e\}\rangle=\bigcap_{H<G,\,\{e\}\subset H} H=\bigcap_{H<G} H=\{e\}$$

$$\therefore \langle\emptyset\rangle=\{e\}=\langle\{e\}\rangle$$

De (v):

Como $H<G$ y $H\subset H$, entonces $\langle H\rangle\subset H$. Como $H\subset\langle H\rangle$, entonces $\langle H\rangle=H$.

q.e.d.

Sea G un grupo y S un subconjunto de G. Al construir $\langle S\rangle$, podemos ya suponer que S es no vacío (por (iv)), y se dice ser que S es un conjunto de generadores del subgrupo $\langle S\rangle$. Por lo que hemos notado, puede suceder que $\exists T\subset G$ tal que $\langle S\rangle=\langle T\rangle$ y $S\neq T$. Si S es finito, constituido por $x_1,x_2,\dots,x_n$, entonces escribimos $\langle x_1,\dots,x_n\rangle$ en lugar de $\langle\{x_1,\dots,x_n\}\rangle$, y decimos que $x_1,\dots,x_n$ son los generadores del subgrupo $\langle S\rangle$. Algo similar sucede cuando S se expresa como $S=\{x\in G \mid x \text{ cumple } P\}$, así escribimos $\langle x\in G\mid x \text{ cumple } P\rangle$.

Proposición.

Sea S un subconjunto no vacío de un grupo G. Entonces

$$\langle S\rangle=\{x_1^{m_1}\cdots x_n^{m_n}\mid x_i\in S \text{ y } m_i\in\mathbb{Z}, \text{ para cada } i\in[\![1,n]\!];\ n\in\mathbb{N}\}$$

Dem:

Sea $H:=\{x_1^{m_1}\cdots x_n^{m_n}\mid x_i\in S \text{ y } m_i\in\mathbb{Z}, \text{ para cada } i\in[\![1,n]\!];\ n\in\mathbb{N}\}$. Entonces, si

$x, y \in H$, con $x = x_1^{m_1} \cdots x_n^{m_n}$ y $y = y_1^{l_1} \cdots y_k^{l_k}$, tenemos que

$$xy^{-1} = x_1^{m_1} \cdots x_n^{m_n} \cdot y_k^{-l_k} \cdots y_1^{-l_1} \in H$$

por como se definió H, luego $H < G$. Ademas $S \subset H$, pues $\forall x \in S$, $x = x^1 \in H$, de esta forma, $\langle S \rangle \subset H$.

Sea ahora $x \in H$, con $x = x_1^{m_1} \cdots x_n^{m_n}$. Como $x_1, \dots, x_n \in S \subset \langle S \rangle$ y $\langle S \rangle < G$, entonces $x_1^{m_1} \cdots x_n^{m_n} \in \langle S \rangle$, así $H \subset \langle S \rangle$. Por lo tanto, $H = \langle S \rangle$.

q.e.d.

Corolario.

Sea S un subconjunto no vacío de G. Entonces

$$\langle S \rangle = \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \mid x_i \in S \text{ y } \varepsilon_i \in \{-1, 1\} \text{ para cada } i \in [\![1, n]\!];\ n \in \mathbb{N}\}$$

Dem:

Sea $K = \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \mid x_i \in S \text{ y } \varepsilon_i \in \{-1, 1\} \text{ para cada } i \in [\![1, n]\!];\ n \in \mathbb{N}\}$. Por la proposición anterior, $K < G$ tal que $S \subset K$, así $\langle S \rangle \subset K$, donde cada elemento de K está en S, luego $K = \langle S \rangle$.

q.e.d.

Corolario.

Sea $x \in G$ arbitrario. Entonces

$$\langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$$

Def. Sea $H < G$.

i) H es *finitamente generado*, si $\exists x_1, \dots, x_n \in H$ tales que $H = \langle x_1, \dots, x_n \rangle$.

ii) H es *cíclico* si $\exists x \in G$ tal que $H = \langle x \rangle$.

Proposición.

Existen grupos cíclicos finitos e infinitos. Más precisamente, sea x un elemento de un grupo G.

i) Si $o(x)<\infty$, $o(x)=n$ (con $n\in\mathbb{N}$), entonces
$$\langle x\rangle=\{e,x,\dots x^{n-1}\}$$
donde $|\langle x\rangle|=n$.

ii) Si x un elemento de un grupo G de orden infinito, entonces
$$\langle x\rangle=\{x^m \mid m\in\mathbb{Z}\}=\{\dots,x^{-2},x^{-1},e,x,x^2,\dots\}$$
donde $x^m\neq x^n$ $\forall$ $m,n\in\mathbb{Z}$, $m\neq n$.

Dem:

De (i):

Sea $H=\{e,x,\dots,x^{n-1}\}$. Probaremos que $H=\langle x\rangle$. Claramente $H\subset\langle x\rangle$. Sea $u\in\langle x\rangle$, entonces $\exists$ $m\in\mathbb{Z}$ tal que $u=x^m$. Por el algoritmo de la división $\exists$ q,r $\in\mathbb{Z}$ tales que
$$m=nq+r,\ \text{donde } 0\leq r<n$$
luego
$$x^m=x^{nq+r}=(x^n)^q x^r=e^q x^r=ex^r=x^r\in H$$
por tanto, $\langle x\rangle\subset H$. Así $H=\langle x\rangle$. Probaremos ahora que $|\langle x\rangle|=n$. Sean $m,l\in\mathbb{Z}$ tales que $0\leq m<l<n$, probaremos que $x^m\neq x^l$.
Suponga que $x^m=x^l$, entonces $x^{l-m}=e$, donde $0<l-m<n$ $\#_c$, pues $o(x)=n$.
por tanto, $x^m\neq x^l$. Así $|\langle x\rangle|=n$.

De (ii):

Basta probar que $x^m\neq x^n$ $\forall$ $m,n\in\mathbb{Z}$, $m\neq n$. Suponga que $\exists$ $m,n\in\mathbb{Z}$, $m<n$ tales que $x^m=x^n$, entonces $x^{n-m}=e$, luego $o(x)=n-m$ $\#_c$, pues x es de orden infinito. Por tanto, $x^m\neq x^n$ $\forall$ $m,n\in\mathbb{Z}$ $\sqcap$ $m\neq n$.

q.e.d.

EJEMPLOS.

1) El conjunto de raíces n-ésimas de la unidad en $\mathbb{C}^*$ es un grupo cíclico infinito de

orden n generado por las raíces n-ésimas primitivas de la unidad.

2) El grupo aditivo $\mathbb{Z}$ de los números enteros es un grupo cíclico infinito generado por 1. También es generado por -1.

3) Podemos utilizar el símbolo $\langle \rangle$ para describir grupos de manera abstracta, pero con propiedades específicas para saber cómo es este. Por ejemplo, cuando expresamos $G = \langle x \mid x^n = e \rangle$, queremos establecer que G es un grupo cíclico generado por x de orden finito n, del cual nos permitió saber cómo son sus elementos de manera precisa.

En general, la manera de expresar los grupos $\langle S \mid R \rangle$ deberá de ser tal que S es un conjunto no vacío y R será un conjunto de relaciones sobre los elementos de S. En el estudio de grupos libres se justifica esta notación.

4) De aquí en adelante, los elementos σ y π de S_3 siempre estarán dados por

$$\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad y \quad \pi := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Entonces, tenemos que

$$S_3 = \langle \pi, \sigma \mid \sigma^2 = e,\ \pi^3 = e \ y \ \pi\sigma = \sigma\pi^2 \rangle = \{ e, \sigma, \pi, \pi^2, \sigma\pi, \sigma\pi^2 \}$$

5) Sea n un entero positivo con $n > 1$. Se define el grupo diédrico de grado n, denotado por D_n, como aquel grupo que satisfaga que

$$D_n := \langle x, y \mid x^2 = e,\ y^n = e,\ yx = xy^{n-1} \rangle$$

Se tiene que D_n tiene $2n$ elementos, a saber

$$D_n = \{ e, x, y, \dots, y^{n-1}, xy, xy^2, \dots, xy^{n-1} \}$$

en particular, tenemos que $S_3 = D_3$.

Proposición.

Sea G un grupo cíclico. Entonces, todo subgrupo de G es cíclico y abeliano.

Dem:

Suponga que G es generado por x, y sea $H < G$, con $H \neq \langle e \rangle$ (pues en tal caso, H sería cíclico generado por e). Sea ahora $h \in H$, con $h \neq e$, como $H < G$, entonces $\exists\, m \in \mathbb{Z} \ni h = x^m$. Como $H < G$, entonces $h, h^{-1} \in H$, así $x^m, x^{-m} \in H$ donde $m \neq 0$. Sea

$$V = \{ n \in \mathbb{N} \mid x^n \in H \}$$

Claramente $V \neq \emptyset$ pues $m \in V$, además como $V \subset \mathbb{N}$, se sigue del principio del buen orden que V tiene elemento mínimo, digamos m_0, sea $a = x^{m_0} \in H$. Afirmamos que $H = \langle a \rangle$. En efecto, como $a \in H$, entonces $\langle a \rangle \subset H$. Sea $z \in H$, entonces $\exists\, k \in \mathbb{Z} \ni z = x^k$. Por el algoritmo de la división $\exists\, q, r \in \mathbb{Z} \ni$

$$k = q m_0 + r, \quad 0 \leq r < m_0$$

así $x^k = x^{q m_0 + r} = (x^{m_0})^q \cdot x^r \Rightarrow x^r = x^k \cdot (x^{m_0})^{-q} \in H$, pues $x^k, (x^{m_0})^{-q} \in H$, así como $r < m_0$, debe suceder que $r = 0$. Por tanto:

$$k = q m_0$$

$$\Rightarrow x^k = (x^{m_0})^q$$

$$\Rightarrow x^k \in \langle a \rangle$$

Por lo tanto, $H = \langle a \rangle$. Claramente H es abeliano.

q.e.d.

Proposición.

Para cada elemento $x \in G$, con G un grupo finito, se cumple que $|x| \mid |G|$.

Dem:

Sea G un grupo finito y $x \in G$ arbitrario. Sea $H = \langle x \rangle$, entonces $|x| = |H|$ pues H es finito, luego por el teorema de Lagrange $|x| = |H| \mid |G|$.

q.e.d.

Corolario

Para cada $x \in G$, G grupo finito, se cumple que $x^{|G|} = e$.

Dem:

Por la proposición anterior, $|x| \mid |G|$, luego si $|x|=m$ y $|G|=n$, entonces $m \mid n$ $\Rightarrow \exists\, K \in \mathbb{Z}$ ∍ $n = mK$, así: $x^{|G|} = x^n = x^{mK} = (x^m)^K = e^K = e$.

q.e.d.

Corolario

Sea G un grupo finito de orden p número primo. Entonces G es grupo cíclico; en particular, todo elemento de G distinto de la identidad, es de orden p.

Dem:

Sea $x \in G$, $x \neq e$, entonces como $|x| \mid |G|$, entonces $|x| \mid p \Rightarrow |x| = 1$ o $|x| = p$. Si $|x| = 1$, entonces $x = e$ #c, así $|x| = p$. Por lo tanto $G = \langle x \rangle$.

q.e.d.

La función de Euler.

Proposición.

Todo grupo cíclico infinito tiene exactamente dos generadores, a saber, si x es un generador, el otro es x^{-1}.

Dem:

Sea G un grupo cíclico infinito con generador x. Claramente $G = \langle x \rangle = \langle x^{-1} \rangle$.

Sea ahora $y \in G$ un generador de G, entonces $\exists\, m, n \in \mathbb{Z}$ ∍ $y = x^m$ y $x = y^n$. Así $x = (x^m)^n = x^{mn} \Rightarrow x^{mn-1} = e$. Como G es de orden infinito, x lo es. Así $mn - 1 = 0$ $\Rightarrow m = \pm 1$. Por tanto $y = x$ ó $y = x^{-1}$.

q.e.d.

Def. Se define la función de Euler $\varphi : \mathbb{N} \to \mathbb{N}$ como sigue: para cada $n \in \mathbb{N}$

$$\varphi(n) := \left| \{ m \in \mathbb{N} \mid 1 \leqslant m \leqslant n,\ (m,n) = 1 \} \right|$$

notemos que si $n \geqslant 2$, entonces

$$\varphi(n)=|\{m\in\mathbb{N} \mid 1\leqslant m\leqslant n,\ (m,n)=1\}|=|\{m\in\mathbb{N} \mid 1\leqslant m\leqslant n-1,\ (m,n)=1\}|$$

Además:

$$\varphi(n)=|(\mathbb{Z}/n\mathbb{Z})^*|$$

para cada $n\in\mathbb{N}$.

Teorema:

La función de Euler cumple las siguientes propiedades:

(i) Para cada p número primo y para cada $m\in\mathbb{N}$

$$\varphi(p^m)=p^m\left(1-\frac{1}{p}\right)=p^m-p^{m-1}$$

(ii) Si $m,n\in\mathbb{N}$, con $(m,n)=1$, entonces $\varphi(mn)=\varphi(m)\cdot\varphi(n)$.

(iii) Si n es un entero positivo y $p_1,\dots,p_t$ son exactamente los distintos números primos que dividen a n, entonces

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_t}\right)$$

Dem:

De (i): Sea $p\in\mathbb{N}$ un número primo arbitrario y $m\in\mathbb{N}$. Sea $K\in\mathbb{N}$ tal que $1\leqslant K\leqslant p^m$. Entonces $(p^m,K)\neq 1 \iff p\mid K$, i.e $\exists\, q\in\mathbb{Z} \ni K=qp$, donde $1\leqslant q\leqslant p^{m-1}$. De aquí que

$$|\{K \mid 1\leqslant K\leqslant p^m,\ (K,p^m)\neq 1\}|=p^{m-1}$$

por lo tanto:

$$\begin{aligned}\varphi(p^m)&=|\{K \mid 1\leqslant K\leqslant p^m,\ (K,p^m)=1\}|\\&=|[\![1,p^m]\!]\setminus\{K \mid 1\leqslant K\leqslant p^m,\ (K,p^m)\neq 1\}|\\&=p^m-p^{m-1}=p^m\left(1-\frac{1}{p}\right)\end{aligned}$$

De (ii): Sean $m,n\in\mathbb{N}$ tales que $(m,n)=1$, entonces $\exists\, r,s\in\mathbb{Z} \ni mr+ns=1$. Sea $f:(\mathbb{Z}/mn\mathbb{Z})^*\to(\mathbb{Z}/m\mathbb{Z})^*\times(\mathbb{Z}/n\mathbb{Z})^*$. Sea $[a]_{mn}\in(\mathbb{Z}/mn\mathbb{Z})^*$, definimos

$$f([a]_{mn})=([a]_m,[a]_n)$$

probaremos que f está bien definida. Sea $[a]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^*$, entonces $(a,mn) = 1$. Luego $(a,m)=(a,n)=1$. Por tanto, $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^*$, y $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^*$.
Sea $a' \in [a]_{mn}$, entonces $mn | a-a' \Rightarrow m|a-a'$ y $n|a-a' \Rightarrow a' \in [a]_m$, $a' \in [a]_n$, luego $([a]_m, [a]_n) = ([a']_m, [a']_n)$. Por tanto $[a]_{mn} = [a']_{mn} \Rightarrow f([a]_{mn}) = f([a']_{mn})$.

Probaremos que f es biyección.

1) f es inyectiva.

Sean $[a]_{mn}, [b]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^*$ m $f([a]_{mn}) = f([b]_{mn})$, entonces $b \in [a]_m$ y $b \in [a]_n$, luego $m|a-b$ y $n|a-b \Rightarrow mn|a-b \Rightarrow b \in [a]_{mn} \Rightarrow [a]_{mn} = [b]_{mn}$.

2) f es supráyectiva.

Sea $([a]_m, [b]_n) \in (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. probaremos que $\exists\ [c]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^*$ m $f([c]_{mn}) = ([a]_m, [b]_n)$, en efecto, tome $c = mrb + nsa \in \mathbb{Z}$. Veamos que $(c, mn) = 1$. En efecto:

Si $(c,mn) \neq 1$, entonces $\exists\ p \in \mathbb{N}$ primo tal que $p|c$ y $p|mn$, lo cual implica que $p|c$ y $p|m$ o $p|c$ y $p|n$.

Si $p|c$ y $p|m$, entonces $p|mrb+nsa$ y $p|m \Rightarrow p|nsa$. Si $p|s$, entonces $p|mr+ns=1$ #c. Si $p|a$, como $p|m$, entonces $(a,m)>1$ #c. Por tanto, $p|n$, luego como $p|m$, entonces $(m,n)>1$ #c. (Si $p|c$ y $p|n$, tenemos un caso análogo).

Por lo tanto, $(c,mn)=1$, así $[c]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^*$.

Veamos ahora que

$$c - a = mrb + nsa - mra - nsa = m(rb - ra)$$
$$\Rightarrow m | c-a \Rightarrow [c]_m = [a]_m, \text{ y}$$
$$c - b = mrb + nsa - mrb - nsb = n(sa - sb)$$
$$\Rightarrow n | c-b \Rightarrow [c]_n = [a]_n$$

Por tanto, $f([c]_{mn}) = ([c]_m, [c]_n) = ([a]_m, [b]_n)$.

Por 1) y 2), f es biyección, luego

$$|(\mathbb{Z}/mn\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^*|\cdot|(\mathbb{Z}/n\mathbb{Z})^*|$$
$$\Rightarrow \varphi(mn) = \varphi(m)\cdot\varphi(n)$$

De (iii): Expresamos: $n = p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_t^{k_t}$, $k_i \in \mathbb{N}, \forall i \in J_t$. Como $(p_i^{k_i}, p_j^{k_j}) = 1$, $\forall$ $i, j \in J_t$, $i \neq j$, entonces:

$$\varphi(n) = \varphi(p_1^{t_1}\cdot p_2^{t_2}\cdot\ldots\cdot p_t^{k_t})$$
$$= \varphi(p_1^{t_1}\cdot\ldots\cdot p_{t-1}^{k_{t-1}})\cdot p_t^{k_t}\cdot\left(1-\frac{1}{p_t}\right)$$
$$= \ldots = p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_t^{k_t}\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_t}\right)$$
$$= n\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_t}\right).$$

q.e.d.

Proposición.

Sea G un grupo cíclico finito de orden n. Entonces G tiene $\varphi(n)$ generadores, más precisamente, Sea $a \in G$ ∋ $G = \langle a \rangle$, entonces para $a \in \mathbb{Z}$ con $1 \leq m \leq n-1$, a^m es generador de $G \Leftrightarrow (m,n) = 1$.

Dem:

Si $n=1$, entonces $G = \langle e \rangle$, y la cantidad de generadores de G es $1 = \varphi(1) = \varphi(n)$.

Suponemos que $n \geq 2$, luego $a^0 = e$ no es generador de G, entonces tomamos $m \in \mathbb{N}$ ∋ $1 \leq m \leq n-1$.

$\Rightarrow$) Suponga que a^m es generador de G, es decir $\langle a^m \rangle = G = \langle a \rangle$, entonces $\exists$ $k \in \mathbb{Z}$ ∋ $a = (a^m)^k = a^{mk} \Rightarrow a^{mk-1} = e$. Luego $n \mid mk-1$, así $\exists$ $t \in \mathbb{Z}$ ∋ $nt = mk-1 \Rightarrow n(-t) + mk = 1$, i.e $(m,n) = 1$.

$\Leftarrow$) Sea $m \in \mathbb{Z}$ con $1 \leq m \leq n-1$ ∋ $(m,n) = 1$. Entonces $\exists$ $r, s \in \mathbb{Z}$ ∋ $mr + ns = 1$. Probemos que $\langle a^m \rangle = G = \langle a \rangle$. Claramente $\langle a^m \rangle \subset \langle a \rangle$. Por otro lado, $a = a^1 = a^{mr+ns} = (a^m)^r\cdot(a^n)^s = (a^m)^r(e)^s = (a^m)^r \in \langle a^m \rangle$. Luego $\langle a^m \rangle \subset \langle a \rangle$.

Así, $\langle a^m \rangle = \langle a \rangle$.

q.e.d.

EJEMPLOS:

1) Sea $n \in \mathbb{N}$ y $n \geq 2$. Definimos el número complejo $w = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{n}\right)$, la cual es una raíz n-ésima de la unidad, i.e es solución al polinomio $x^n - 1 = 0$.

El conjunto de raíces n-ésimas de la unidad, con el producto de complejos, es un grupo multiplicativo cíclico finito de n elementos, generado por w, i.e $\langle w \rangle = \{1, w, w^2, \ldots, w^{n-1}\}$.

Teorema (de Euler).

Sea $a \in \mathbb{Z}$ y $n \in \mathbb{N}$ tal que $(a,n) = 1$. Entonces $a^{\varphi(n)} \equiv 1 \mod n$.

Dem:

Consideremos el grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$, el cual tiene $\varphi(n)$ elementos, como $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$, pues $(a,n) = 1$, entonces

$$[a^{\varphi(n)}] = [a]^{\varphi(n)} = [a]^{|(\mathbb{Z}/n\mathbb{Z})^*|} = [1]$$

por lo tanto, $a^{\varphi(n)} \in [1] \Rightarrow a^{\varphi(n)} \equiv 1 \mod n$.

q.e.d.

Teorema (pequeño) de Fermat.

Sean $m \in \mathbb{Z}$, $p \in \mathbb{N}$ primo. Entonces, $m^p \equiv m \mod p$. En particular, si $p \nmid m$, entonces $m^{p-1} \equiv 1 \mod p$.

Dem:

Si $p \mid m$, entonces $p \mid m^p$ y $p \mid m$, luego $p \mid m^p - m$, por tanto $m^p \equiv m \mod p$.

Si $p \nmid m$ (caso particular), como $(p,m) = 1$, entonces $[m] \in (\mathbb{Z}/p\mathbb{Z})^*$, luego como $|(\mathbb{Z}/p\mathbb{Z})^*| = \varphi(p) = p-1$, entonces

$$[m^{p-1}] = [m]^{p-1} = [1]$$

$$\Rightarrow m^{p-1} \equiv 1 \bmod p.$$

portanto $[m]^{p-1} = [1] \Rightarrow [m^p] = [m]^p = [m] \Rightarrow m^p \equiv m \bmod p.$

q.e.d.