Tema 3

El cuerpo ($\mathbb{Z}_p$, +, .) (p número primo)

3.1 El grupo multiplicativo $\mathbb{Z}_m^*$

En el tema anterior se vio que ($\mathbb{Z}_m$, +, .) es un anillo conmutativo con elementos identidad. No preguntamos ahora para qué elementos existe inverso. A los elementos que poseen inverso se les denomina identidades.

Proposición 3.1 *El conjunto de las unidades del anillo* ($\mathbb{Z}_m$, +, .) *forman un grupo conmutativo, a dicho conjunto lo desinaremos por* $\mathbb{Z}_m^*$. (*En todo anillo conmutativo y con identidad el conjunto de las unidades forman un grupo conmutativo*).

Demostración.

$$\mathbb{Z}_m^* = \{\, \bar{a} \in \mathbb{Z}_m \mid \exists \bar{x} \in \mathbb{Z}_m \; verificando \; \bar{a}.\bar{x} = \bar{1} \,\}$$

- Veamos que la operación multiplicación heredada de $\mathbb{Z}_m$ es interna:

Sean $\bar{a}$,$\bar{b}$$\in \mathbb{Z}_m^*$, esto es, existen $\bar{x}$ e $\bar{y} \in \mathbb{Z}_m$ tales que $\bar{a}.\bar{x} = \bar{1}$ y $\bar{b}.\bar{y} = \bar{1}$. Al ser la operación multiplicación asociativa y conmutativa se verifica que $\bar{1} = (\bar{a}.\bar{x}).(\bar{b}.\bar{y}) = (\bar{a}.\bar{b}).(\bar{x}.\bar{y}) = (\overline{ab}).(\overline{xy})$. Por tanto $(\overline{ab}) \in \mathbb{Z}_m^*$.

- La operación es asociativa y conmutativa por serlo en $\mathbb{Z}_m$.
- La identidad $\bar{1} \in \mathbb{Z}_m^*$.
- Todo $\bar{a} \in \mathbb{Z}_m^*$ tiene inverso. ■

Proposición 3.2 *Un elemento* $a \in \mathbb{Z}_m$ *es unidad si, y sólo si,* $mcd(a, m) = 1$, *es decir,* $\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m \mid mcd(a,m) = 1\}$

Demostración. $\bar{a} \in \mathbb{Z}_m$ es unidad si, y sólo si, existe $\bar{x} \in \mathbb{Z}_m$ tal que $\overline{ax} \equiv 1 (\mathrm{mod}\ m)$, es decir, si y sólo si, $ax + my = 1$ para algún entero y. Esto es, si y sólo si, la ecuación diofántica $ax + my = 1$ tiene solución. Y esto es equivalente a $mcd(a, m) = 1$. ■

Definición 3.3 *Un conjunto K dotado de dos operaciones internas, +, ., verificando:*

- (K, +, .) *es anillo conmutativo con elemento identidad.*
- *Todo elemento de K distinto del 0* (*0 es elemento neutro respecto de la suma*) *tiene inverso respecto de la multiplicación (Ello significa que, K*-{0}, .) *es grupo conmutativo*)

se dice que tiene estructura de ***cuerpo***.

Como consecuencia de la proposición anterior se verifica la siguiente proposición:

Proposición 3.4 ($\mathbb{Z}_m^*$, .) *tiene estructura de grupo.*

Teorema 3.5 *El anillo* $\mathbb{Z}_m$ *es cuerpo si, y sólo si, m es primo.*

Demostración.
Si m es primo, todo entero que no es múltiplo de m es coprimo con m. En consecuencia, $\mathbb{Z}_{\boldsymbol{m}}^{*} = \mathbb{Z}_{\boldsymbol{m}} - \{\bar{0}\}$. Por tanto $\mathbb{Z}_m$ es cuerpo.
Recíprocamente, si $\mathbb{Z}_m$ es cuerpo, $\mathbb{Z}_m^{*} = \{\bar{\boldsymbol{a}} \in \mathbb{Z}_{\boldsymbol{m}} | mcd(a, m) = 1\} = \mathbb{Z}_{\boldsymbol{m}} - \{\bar{0}\}$.
Si m no fuese primo tendría un divisor a distinto de 1 y de m. Se tendría que $mcd(a,m) = a$, $a \neq 1$, $a \neq 0$ y $\bar{a} \notin \mathbb{Z}_m^{*}$. Lo que contradice que , $\mathbb{Z}_{\boldsymbol{m}}^{*} = \mathbb{Z}_{\boldsymbol{m}} - \{\bar{0}\}$. Por tanto m es primo. ■

3.2 Función de Euler

Definición 3.6 *Para un número positivo m, se define la función* $\varphi(m)$ *como el número de enteros entre* 0 *y m que son primos con m. Esta función se dice* ***Función de Euler****.*

$$\varphi(m) = |\mathbb{Z}_m^{*}| \text{ (esto es, el cardinal del conjunto } \mathbb{Z}_m^{*})$$

En lo que sigue se va a encontrar una fórmula que nos de el valor de la Función de Euler. Recordando el teorema fundamental de la aritmética: Todo entero positivo puede expresarse como producto de potencias no triviales de números primos; se va a proceder a calcular $\varphi(m)$ para todo entero positivo m.

Lema 3.7 *Si p es un número primo, se verifica* $\varphi(p) = p - 1$.

Demostración. Si p es un número primo todos los números enteros positivos menores que p son coprimos con p: $1, 2, 3, \ldots, p - 1$. Por tanto $\varphi(p) = p - 1$. ■

Lema 3.8 *Sea q un número positivo potencia de un número primo, esto es, con* $q = p^{\alpha}$*, con p primo.*

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

Demostración.
Los enteros positivos menores que $q = p^{\alpha}$ coprimos con él son los no son divisibles por p.
Los enteros positivos menores que p^{α} divisibles por p son: $p, 2p, 3p, 4p, \ldots.., p^{\alpha} = p^{\alpha-1}p$, hay $p^{\alpha-1}$. Los coprimos con él son todos los números positivos menores o iguales a p^{α} (hay a p^{α}) excepto esos $p^{\alpha-1}$. Por tanto

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha}\left(1 - \frac{1}{p}\right) = q\left(1 - \frac{1}{p}\right) \quad (p \text{ primo}) \qquad ■$$

Lema 3.9 S*i* $mcd(m_1, m_2) = 1$, l*a función* φ *verifica*: $\varphi(m_1.m_2) = \varphi(m_1).\varphi(m_2)$,

Demostración.
$mcd(a, m_1) = 1$ y $mcd(a,m_2) = 1 \Leftrightarrow mcd(a, m_1m_2) = 1$
En el tema anterior se vio que existía una aplicación biyectiva:

$$\psi\colon\ \mathbb{Z}_{m_1m_2}^{*} \rightarrow \mathbb{Z}_{m_1}^{*}\mathbb{Z}_{m_2}^{*}$$

Por tanto, $\varphi(m_1 . m_2) = |\mathbb{Z}^*_{m_1 m_2}| = |\mathbb{Z}^*_{m_1}||\mathbb{Z}^*_{m_2}| = \varphi(m_1) . \varphi(m_2)$ ■

Teorema 3.10 *Sea* $m = \prod_{k=1}^{n} p_k^{\alpha_k}$ *la factorización en potencias de primos de* m, *se verifica*

$$\varphi(m) = m \prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right)$$

Demostración. Teniendo en cuenta los resultados anteriores y mcd$(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$, si $i \neq j$, se verifica

$$\varphi(m) = \prod_{k=1}^{n} \varphi(p_k^{\alpha_k}) = \prod_{k=1}^{n} p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) = m \prod_{k=1}^{n}\left(1 - \frac{1}{p_k}\right)$$ ■

Teorema 3.11 (Euler-Fermat) *Si* a *y* m *son coprimos, se verifica* $a^{\varphi(m)} \equiv 1$ $(mod\ m)$.

Demostración. Sean $k = \varphi(m)$ y $n_1, n_2, \ldots, n_k$ todos los enteros positivos menores que m y primos con m. No son congruentes entre ellos módulo m.
Consideremos ahora $an_1, an_2, \ldots, an_k$. Al ser a primo con m y cada n_i primo con m, se verifica que todos ellos son primos con m.
Además, no son congruentes entre ellos módulo m. En efecto, si $an_i \equiv an_j$ $(mod\ m)$, m dividiría a $a(n_i - n_j)$. Al ser n primo con a tendría que dividir a $(n_i - n_j)$, esto es, $n_i \equiv n_j (mod\ m)$, que contradice el hecho de que entre ellos no sean congruentes módulo n.
En consecuencia, en $\{\overline{an_1}, \ldots, \overline{an_k}\}$ hay k elementos distintos de $\mathbb{Z}_n$ que son coprimos con n. En consecuencia, se verifica

$$\{\overline{n_1}, \ldots, \overline{n_k}\} = \{\overline{an_1}, \ldots, \overline{an_k}\} \text{ y } a^k n_1 \ldots n_k \equiv n_1 \ldots n_k\ (mod\ m)$$

Por hipótesis todos los $\overline{n\iota}$ son inversibles módulo n en $\mathbb{Z}_m$, por lo que, $a^k \equiv 1$ $(mod\ m)$ ■

El teorema anterior es útil si tratamos con potencias de números enteros.

Ejemplo 3.12 *Calcular el resto de la división euclídea de* 2^{1010} *por* 23.
Como 23 es primo, es $\varphi(23) = 22$, y como $1010 = 45.22 + 20$, se tiene:
$2^{1010} \equiv (2^{22})^{45}\, 2^{20} \equiv 2^{20} \equiv (32)^4 \equiv (9)^4 \equiv (9^2)^2 \equiv (81)^2 \equiv (12)^2 \equiv 144 \equiv 6$ (mod 23) ■

Corolario 3.13 (Pequeño Teorema de Fermat) *Si* p *es primo*,

$$a^p \equiv a\ (mod\ p)$$

Demostración. Basta recordar que si p es primo $\varphi(p) = p - 1$.

Algoritmo 3.14 (Algoritmo para el cálculo de potencias)
Supongamos que necesitamos calcular la potencia trigésimo séptima de un entero a.
La manera más ingenua de hacerlo es calcular las potencias sucesivas,

$$a, a^2, a^3, \ldots, a^{36}, a^{37},$$

lo que implica realizar 36 productos.
Sin embargo,

$$a^{37} = a \,.\, a^{36} = a \,.\, (a^2)^{18} = a \,.\, (a^4)^9 = a \,.\, a^4 \,.\, (a^4)^8 = a \,.\, a^4 \,.\, a^{32}.$$

¿Cuántos productos necesito si actúo de esta manera? En primer lugar, 5 productos para calcular a^4 y a^{32} haciendo (cada flecha significa elevar al cuadrado):

$$a \to a^2 \to a^4 \to a^8 \to a^{16} \to a^{32}:$$

Con otros dos productos más, calculo a^{37}. En total, 7 productos frente a los 36 por el método ingenuo.

En realidad, hemos calcular la representación binaria del exponente, en este caso, $37 = 1 + 2^2 + 2^5$ ($37 = (100101)_2$). Este razonamiento es fácilmente extensible a cualquier otro exponente: si quiero calcular a^α siendo $\alpha =$ $2^k + \alpha_{k-1}.\,2^{2k-1} + \ldots + \alpha_2.\,2^2 + \alpha_1.\,2 + \alpha_0$, se tendrá que:

$$a^\alpha = a^{\alpha_0}.\,a^{\alpha_1 2}.\,a^{\alpha_2 2^2} \ldots a^{\alpha_{k-1} 2^{k-1}} a^{2^k}$$ ■

Ejemplo 3.15 *Calcular el resto de la división euclídea de* 2^{1010} *por* 23.

Como 23 es primo, es $\varphi(23) = 22$, y como $1010 = 45.22 + 20$, se tiene:

Por otra parte, $20 = 2^4 + 2^2$ es la representación binaria de 20

$2^{1010} \equiv 2^{20} \equiv 2^{16}2^4$, $\quad 2^2 \equiv 4 \pmod{23}$, $\quad 2^4 \equiv 16 (mod\ 23)$

$2^8 \equiv 64\ (mod\ 23) \equiv 3 (mod\ 23)$, $\ 2^{16} \equiv 9\ (mod\ 23)$,

$2^{1010} \equiv 2^{20} \equiv 2^{16}2^4 \equiv 144 \equiv 6\ (mod\ 23)$ ■

3.3 El grupo multiplicativo $\mathbb{Z}_p^*$ (con *p* número primo).

3.3.1 Polinomios con coeficientes en $\mathbb{Z}_p$

Lema 3.16 *Sea* $f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0$ *un polinomio con coeficientes enteros y* a *un número entero. Existe un polinomio* $g(x)$ *con grado* $d-1$ *y coeficientes enteros verificando* $f(x) = (x - a)\, g(x) + f(a)$.

Demostración.

Basta recordar la formula $(x^n - y^n) = (x - y)(x^{n-1} + x^{n-2}y + \ldots + x\, y^{n-2} + y^{n-1})$

$f(x) - f(a) = x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 - (a^d + a_{d-1}a^{d-1} + \ldots + a_1a + a_0)$

$= (x^d - a^d) + a_{d-1}\,(x^{d-1} - a^{d-1}) + \ldots + a_1(x - a)$

Aplicando la fórmula indicada todos los sumandos son múltiplos de $(x - a)$, con lo que se puede sacar factor común. Además, el exponente mayor de x corresponde a la expresión $(x^d - a^d) = (x - a)(x^{d-1} + x^{d-2}a + \ldots + x\, a^{d-2} + a^{d-1})$

Por tanto, se tiene $f(x) - f(a) = (x - a)g(x)$ con grado d -1. Esto es,

$f(x) = (x - a)\, g(x) + f(a)$ para todo entero a y para todo entero x. ■

Lema 3.17 *Sea* $f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0$ *un polinomio con coeficientes enteros y p un número entero primo. Entonces, la ecuación* $f(x) \equiv 0$ $(mod\ p)$ *tiene, a lo más, d soluciones en* $\mathbb{Z}_p$.*(Esto significa que el número de raíces de la ecuación en* $\mathbb{Z}_p$ *no excede al grado*)

Demostración.

Aplicando al resultado anterior congruencias p. Se verifica que:

$f(x) = (x - a)\, g(x) + f(a)$ $(mod\ p)$ para todo entero x.

Veamos las tesis por inducción sobre el grado d.

- Para $d = 1$: Si $f(x) = x + a_0$ $(mod\ p)$, es cierto, pues existe exactamente 1 solución $x \equiv (p\text{-}a_0)$ $(mod\ p)$.
- Supongamos cierto para d - 1 y veamos que es cierto para d.
- Sea $f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0$.

Si no existiesen raíces sería cierto, el número de raíces es 0 que es menor o igual que d.

Su pongamos que existe al menos una, sea a, $f(a) \equiv 0$ $(mod\ p)$.

Se verifica $f(x) = (x - a)\ g(x) + f(a)$ $(mod\ p) \equiv (x - a)\ g(x)$ $(mod\ p)$, siendo $g(x)$ un polinomio con grado d - 1. Con lo cual,

$$f(x) = (x - a)\ g(x) \equiv 0\ (mod\ p)$$

Por lo que, las raíces de $f(x)$ distintas de a serían raíces de $g(x)$. Además, $g(x)$ es un polinomio de grado d-1. Por hipótesis de inducción, a lo más, tiene d-1 raíces en $\mathbb{Z}_p$. En consecuencia, $f(x)$ tiene, a lo más, d raíces en $\mathbb{Z}_p$. ■

Lema 3.18 *Sea p un número entero primo, la congruencia* $x^{p-1} \equiv 1$ $(mod\ p)$ *tiene, exactamente, p* - 1 *raíces en* $\mathbb{Z}_p$.

Demostración.
Por el Pequeño Teorema de Fermat se sabe $a^{p-1} \equiv 1$ $(mod\ p)$, para todo a entero. Esto significa que que 1, 2, 3, …, p -1 son soluciones de la ecuación dada. Por otra parte, el lema anterior dice que a lo más tiene p -1 raíces. En consecuencia la ecuación dada tiene exactamente p raíces en $\mathbb{Z}_p$. ■

Lema 3.19 *Si* $d \mid p$-1, la congruencia $x^d \equiv 1$ $(mod\ p)$ *y tiene, exactamente*, *d soluciones en* $\mathbb{Z}_p$.

Demostración. Por el lema 3.15 sabemos que la congruencia tiene, a lo más, d soluciones.

Al ser $d \mid p$-1, existe k el cociente exacto de dividir p -1 entre d, esto es, $kd = p$-1.

Por otra parte, se verifica la identidad $x^k - 1 = (x - 1)(x^{k-1} + \ldots + x + 1)$.

Sustituyendo en dicha identidad x por x^d, se tiene:

$$x^{dk} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1), \text{ esto es,}$$

$$x^{p-1} - 1 = (x^d - 1)(x^{p-d-1} + x^{p-d-2} + \ldots + x^d + 1),$$

Como $x^{p-d-1} + x^{p-d-2} + \ldots + x^d + 1 \equiv 0$ $(mod\ p)$ tiene, a lo más, p - d -1 soluciones, si $x^d \equiv 1$ $(mod\ p)$ tuviese menos de d soluciones, entonces $x^{p-1} \equiv 1$ $(mod\ p)$ no tendría p - 1 soluciones, esto sería contradictorio. ■

3.3.2 Orden de un elemento en el anillo $(\mathbb{Z}_m^*, +, .)$

Definición 3.20 *Si a es un elemento de* $\mathbb{Z}_m^*$, *se llama orden de a en* $\mathbb{Z}_m^*$ *y se escribe* $ord_m(a)$, *al menor entero positivo d que verifica* $a^d \equiv 1$ $(mod\ m)$.

El teorema de Fermat justifica la existencia de enteros que verifican la condición:
Si a es un elemento de $\mathbb{Z}_m^*$, se verifica $a^{\varphi(m)} \equiv 1$ ($mod\ m$). En particular, $ord_m(a) \leq \varphi(n)$.

Ejemplo 3.21 Consideremos el grupo multiplicativo $\mathbb{Z}_7^*$, analicemos las potencias de 3

$3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$ y $3^6 = 1$, En $\mathbb{Z}_7^*$, ord(3) = 6.

Lema 3.22 *Si $a^n \equiv 1$ ($mod\ m$), entonces $ord_m(a)$ divide a n.*

Demostración. Sea n con $a^n \equiv 1$ ($mod\ m$) y llamemos d a $ord_m(a)$. Es $d \leq n$, pues d es el menor entero positivo que cumple la condición. Consideremos la división euclídea de n por d: $n = q.d + r$ con $0 \leq r < d$, observar que al ser $d \leq n$ es $q \geq 1$.

$$1 = a^n = a^{qd+r} = (a^d)^q \,.\, a^r = a^r,$$

Por definición de orden, $r = 0$.

Lema 3.23 *Sea a un entero con $mcd(a, m) = 1$. Si $a^e \equiv a^f \equiv 1$ ($mod\ m$), entonces $a^d \equiv 1$ ($mod\ m$), donde $d = mcd(e, f)$.*

Demostración.
Si $d = mcd(e, f)$ existen números enteros x e y tales que $d = ex + fy$. En cuyo caso, se tiene $a^d \equiv a^{ex+fy} \equiv (a^e)^x \,.\, (a^f)^y \equiv 1$ ($mod\ m$). ■

Lema 3.24 *Sean a y b enteros con $ord_p(a) = r$ y $ord_p(b) = s$ en $\mathbb{Z}_p^*$. Si r y s son coprimos, el orden de ab en $\mathbb{Z}_p^*$ es igual a r.s.*

Demostración. Llamemos d al orden de ab.

Se verifica que $(ab)^{rs} \equiv (a^r)^s\ (b^s)^r \equiv 1$ ($mod\ p$). Por el lema anterior d divide a rs. Supongamos que $d \neq rs$, existe $k \neq 1$ tal que $dk = rs$, es más existe un número primo q que divide a k (cualquier número primo de la descomposición en factores de k), $rs = dk = dqt$, esto es $\frac{rs}{q} = dt$ es múltiplo de d. En consecuencia, $(ab)^{rs/q} \equiv 1(mod\ p)$.

Puesto que $mcd(r, s) = 1$ y q es divisor de rs, q dividirá uno de ellos, pero no a los dos a la vez. Supongamos que divide a r (sería análogo si dividiese a s) y no divide a s.

Se verifica, $1 \equiv (ab)^{rs/q} \equiv (a)^{rs/q}(b^s)^{r/q} \equiv (a)^{rs/q}$ ($mod\ p$)

Además, al ser $ord_p(a) = r$, se verifica $(a)^r \equiv 1$ ($mod\ p$)

Como $r = \frac{r}{q}.q$ y $\frac{rs}{q} = \frac{r}{q}.s$ y q no divide a s, se verifica que $mcd\left(\frac{rs}{q}, r\right) = mcd\left(\frac{r}{q}s, \frac{r}{q}q\right) = \frac{r}{q}.mcd(s, q) = \frac{r}{q}$

Se ha obtenido $(a)^r \equiv 1$ ($mod\ p$) y $(ab)^{rs/q} \equiv 1$ ($mod\ p$) $mcd\left(\frac{rs}{q}, r\right) = \frac{r}{q}$. Por el lema 3.23, se tiene que $(a)^{r/q} \equiv 1(mod\ p)$, siendo $r/q < r$, lo que contradice que $ord_p(a) = r$.

Por tanto $d = rs$. ■

Teorema 3.25 *Si p es primo, existe* $a \in \mathbb{Z}_p^*$, *tal que*

$$\mathbb{Z}_p^* = \{a, a^2, a^3, \dots, a^{p-1}\}$$

Esto significa que $\mathbb{Z}_p^*$ *es un grupo* ***cíclico*** *y que a se dice que es un* ***generador*** *de* $\mathbb{Z}_p^*$.

Demostración. Sea $\prod_{i=1}^{n} {p_i}^{e_i}$ la factorización en primos de $p - 1$. ${p_i}^{e_i}$ y ${p_i}^{e_i-1}$ son divisores de $p - 1$. Por tanto, se verifica que $x^{{p_i}^{e_i}} \equiv 1(mod\, p)$ tiene exactamente ${p_i}^{e_i}$ soluciones y $x^{{p_i}^{e_i-1}} \equiv 1(mod\, p)$ tiene exactamente ${p_i}^{e_i-1}$ soluciones. Por tanto, existe alguna solución de la primera congruencia que no lo es de la segunda, esto es, existe a_i verificando ${a_i}^{{p_i}^{e_i}} \equiv 1(mod\, p)$, pero ${a_i}^{{p_i}^{e_i-1}} \not\equiv 1(mod\, p)$. En consecuencia, el orden de a_i es divisor de ${p_i}^{e_i}$, pero no de ${p_i}^{e_i-1}$, por tanto, el orden de a_i es ${p_i}^{e_i}$.

Considerando $a = \prod_{i=1}^{n} a_i$, al ser ${p_i}^{e_i}$ y ${p_j}^{e_j}$ coprimos para $i \neq j$, se verifica que $ord_p(a) = ord_p(\prod_{i=1}^{n} a_i) = \prod_{i=1}^{n} ord_p(a_i) = \prod_{i=1}^{n} {p_i}^{e_i} = p - 1$.

Por tanto, se verifica $a^{p-1} \equiv 1$ $(mod\, p)$, pero $a^i \not\equiv 1$ $(mod\, p)$ para $1 \le i < p - 1$.

Si existiesen i, j, $1 \le i < j \le p-1$, verificando $a^i \equiv a^j$ $(mod\, p)$, se tendría $a^{j-i} \equiv 1$ $(mod\, p)$, siendo $j - i < p - 1$, pero el orden de a en $\mathbf{Z}_p$ es $p - 1$. Por tanto, $a^i \not\equiv a^j$ $(mod\, p)$, para todo i, j, $1 \le i < j \le p-1$. Todas las potencias a, a^1, $a^2, \dots, a^{p-1}$ son distintas, esto es, $\mathbb{Z}_p^* = \{a, a^2, a^3 \dots, a^{p-1}\}$. ■

Corolario 3.26 (Teorema de Wilson)

$$p \text{ es primo} \Leftrightarrow (p - 1)! \equiv -1\ (mod\, p)$$

Demostración.
Si p es primo, como la ecuación $x^{p-1} - 1 \equiv 0$ $(mod\, p)$ tiene como únicas soluciones 1, 2, …, $p - 1$, se tiene

$$x^{p-1} - 1 \equiv (x - 1)\,(x - 2) \dots (x - p + 1)\ (mod\, p).$$

Sustituyendo x por 0 se tiene $(-1)^{p-1}(p - 1)! \equiv -1$ $(mod\, p)$.
Si p es primo impar, se sigue $(p - 1)! \equiv -1$ $(mod\, p)$. El único primo par es $p = 2$, y se verifica, $1! = 1 \equiv -1$ $(mod\, 2)$.
Recíprocamente, si $(p - 1)! \equiv -1$ $(mod\, p)$, se verifica existe $k \in \mathbf{Z}$ tal que $(p - 1)! + 1 = kp$. Si p tuviese un divisor menor o igual que $(p - 1)$, sería divisor de $(p - 1)!$. Al verificarse la igualdad también lo sería de 1, por lo que sería 1. En consecuencia p es primo. ■