Unidades de $\mathbb{Z}_n$

Susana Puddu

1. Introducción.

Sea $n \in \mathbb{N}$, $n > 1$. Si en el conjunto

$$\mathbb{Z}_n = \{\, a \in \mathbb{Z} \,/\, 0 \leq a < n \,\}$$

definimos las operaciones $+$ y $\cdot$ en la forma

$$a + b = r_n(a + b)$$

$$a.b = r_n(ab)$$

(donde $r_n(c)$ denota el resto de la división de c por n), resulta que $(\mathbb{Z}_n\,,\,+\,,\,\cdot)$ es un anillo conmutativo.
Sea $\mathcal{U}_n$ el conjunto de unidades de este anillo, es decir,

$$\mathcal{U}_n = \{\, a \in \mathbb{Z}_n \,/\, \exists\, b \in \mathbb{Z}_n \text{ que satisface } a.b = 1 = b.a \,\}.$$

Teniendo en cuenta la definición del producto en $\mathbb{Z}_n$, se tiene que $a.b = 1$ en $\mathbb{Z}_n$ sii $r_n(ab) = 1$ sii $ab \equiv 1 \quad (n)$. Luego, dado $a \in \mathbb{Z}_n$, $\exists\, b \in \mathbb{Z}_n$ tal que $ab = 1 = ba$ sii la ecuación de congruencia $aX \equiv 1 \quad (n)$ tiene una solución b tal que $0 \leq b < n$, lo que ocurre si, y sólo si, $(a, n) = 1$.
Se tiene entonces que

$$\mathcal{U}_n = \{\, a \in \mathbb{Z}_n \,/\, (a, n) = 1 \,\}.$$

Siendo $\mathcal{U}_n$ el conjunto de unidades del anillo conmutativo $(\mathbb{Z}_n\,,\,+\,,\,\cdot)$, resulta que $(\mathcal{U}_n\,,\,\cdot)$ es un grupo abeliano finito de orden

$$|\,\mathcal{U}_n| = \#\{\, a \in \mathbb{Z}_n \,/\, (a, n) = 1 \,\} = \varphi(n),$$

donde φ es la función de Euler (recordemos que si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, con p_i primos positivos distintos y $\alpha_i \in \mathbb{N}$, entonces $\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \dots p_r^{\alpha_r - 1}(p_r - 1)$).

Nuestro objetivo es caracterizar el grupo abeliano $\mathcal{U}_n$. Para ello, primero en la sección 2 estudiaremos el caso en que n es primo. Luego, en la sección 3, el caso en que $n = 2^\alpha$, con $\alpha \in \mathbb{N}$, $\alpha \geq 2$ y en la sección 4, el caso $n = p^\alpha$, con p primo, $p > 2$ y $\alpha \in \mathbb{N}$, $\alpha \geq 2$. Por último, en la sección 5, caracterizaremos $\mathcal{U}_n$ $\forall n \in \mathbb{N}$, $n \geq 2$, a partir de la factorización de n como producto de primos.

2. El caso $n = p$, con p primo.

Probaremos en esta sección que si p es un primo positivo, entonces $\mathcal{U}_p \simeq \mathbb{Z}_{p-1}$. Para ello, necesitaremos la noción de exponente de un grupo finito.

Definición: Sea $(G\,,\,\cdot)$ un grupo finito. Definimos el *exponente* de G como

$$\exp(G) = \min\{\, k \in \mathbb{N} \,/\, x^k = 1 \quad \forall\, x \in G \,\}$$

Observación: Si $(G\,,\,\cdot)$ es un grupo finito, $|G| \in \{\, k \in \mathbb{N} \,/\, x^k = 1 \quad \forall\, x \in G \,\}$. Luego, $\exp(G)$ está bien definido (pues $\{\, k \in \mathbb{N} \,/\, x^k = 1 \quad \forall\, x \in G \,\} \neq \emptyset$) y $\exp(G) \leq |G|$.

Ejemplos:

i) Si $G = \mathbb{Z}_m$ entonces $|G| = m$ y $\exp(G) = m$

ii) Si $G = \mathbb{Z}_6 \oplus \mathbb{Z}_{12}$ entonces $|G| = 72$ y $\exp(G) = 12$

iii) Si $G = \mathbb{Z}_6 \oplus \mathbb{Z}_{15}$ entonces $|G| = 90$ y $\exp(G) = 30$

iv) Si $G = D_{10} = \langle s\,,\,\rho\,;\, s^2 = 1 = \rho^{10}\,,\, s\rho = \rho^{-1}s\rangle$ entonces $|G| = 20$ y $\exp(G) = 10$

v) Si $G = D_9 = \langle s\,,\,\rho\,;\, s^2 = 1 = \rho^{9}\,,\, s\rho = \rho^{-1}s\rangle$ entonces $|G| = 18$ y $\exp(G) = 18$

vi) Si $G = \mathcal{H} = \langle i\,,\,j\,;\, i^4 = 1 = j^4\,,\, ij = j^3 i\rangle$ entonces $|G| = 8$ y $\exp(G) = 4$

vii Si $G = S_4$, el grupo de permutaciones de 4 elementos, entonces $|G| = 24$ y $\exp(G) = 12$

Veamos ahora algunas propiedades de $\exp(G)$.

Proposición 2.1. *Sea $(G\,,\,\cdot)$ un grupo finito. Entonces* $\exp(G) \mid |G|$.

Demostración: Sea $e = \exp(G)$ y sea $m = |G|$. Sean $q, r \in \mathbb{Z}$ tales que $m = e.q + r$ y $0 \leq r < e$.
Como $x^e = 1 = x^m$ para todo $x \in G$, entonces $x^r = x^{m-e.q} = x^m.(x^e)^{-q} = 1$ para todo $x \in G$.
Si fuese $r \neq 0$, entonces resultaría que $r \in \{\, k \in \mathbb{N} \,/\, x^k = 1 \quad \forall\, x \in G \,\}$. Pero como e es el mínimo de este conjunto y $r < e$, esto no puede ocurrir.
Luego $r = 0$ y, así, $e \mid m$. ▫

Proposición 2.2. *Sea $(G\,,\,\cdot)$ un grupo finito. Entonces $ord(x) \mid \exp(G)$ para todo $x \in G$.*

Demostración: Sea $e = \exp(G)$ y sea $x \in G$. Como $y^e = 1$ para todo $y \in G$ entonces, en particular, $x^e = 1$, de donde $ord(x) \mid e$. ▫

Proposición 2.3. Sea G un grupo abeliano y sean $x, y \in G$ tales que $ord(x) = n$ y $ord(y) = m$. Entonces existe en G un elemento de orden $[n : m]$.

Demostración: Sean $r, s \in N$ tales que $[n : m] = r.s$, $(r : s) = 1$, $r \mid n$ y $s \mid m$. Dejamos a cargo del lector demostrar que dados n y m siempre existen r y s que satisfacen estas condiciones. Veremos que $x^{\frac{n}{r}}.y^{\frac{m}{s}}$ tiene orden $r.s = [n : m]$

Es claro que $(x^{\frac{n}{r}}.y^{\frac{m}{s}})^{r.s} = (x^n)^s.(y^m)^r = 1$. Si $(x^{\frac{n}{r}}.y^{\frac{m}{s}})^k = 1$ entonces elevando a la s se tiene que $x^{\frac{n}{r}.s.k} = 1$ y elevando a la r se tiene que $y^{\frac{m}{s}.r.k} = 1$ de donde $n \mid \frac{n}{r}.s.k$ y $m \mid \frac{m}{s}.r.k$. Como $n \mid \frac{n}{r}.s.k$ entonces $\frac{n}{r}.s.k = n.q$ para algún $q \in \mathbb{Z}$ y por lo tanto $s.k = r.q$ de donde $r \mid s.k$. Análogamente, $m \mid \frac{m}{s}.r.k$ implica que $s \mid r.k$. Por lo tanto $r \mid k$ y $s \mid k$ pues r y s son coprimos. Luego, por la misma razón, $r.s \mid k$. ▫

Proposición 2.4. *Sea $(G\,,\,\cdot)$ un grupo finito. Si G es abeliano entonces $\exists\, x \in G$ tal que $ord(x) = \exp(G)$.*

Demostración: Sea $x \in G$ tal que $ord(x) \geq ord(g)$ para todo $g \in G$ (tal x existe pues G es finito), y sea $s = ord(x)$. Veamos primero que $ord(y) \mid s$ para todo $y \in G$.
Sea $y \in G$ y sea $m = ord(y)$. Como G es un grupo abeliano, por la proposición 2.3. existe $z \in G$ tal que

$$ord(z) = [s, m] = \frac{sm}{(s, m)},$$

y como $ord(x) \geq ord(g)$ para todo $g \in G$, en particular, $s = ord(x) \geq ord(z) = \dfrac{sm}{(s, m)}$, de donde $(s, m) \geq m$. Pero $(s, m) \mid m$. Luego debe ser $(s, m) = m$ y, por lo tanto, $m \mid s$.
Luego, $ord(y) \mid s$ para todo $y \in G$ y, en consecuencia, $y^s = 1$ para todo $y \in G$. Esto implica que

$$\exp(G) = \min\{\, k \in \mathbb{N} \,/\, x^k = 1 \quad \forall\, x \in G \,\} \leq s.$$

Pero, por la proposición 2.2., $s = ord(x) \mid \exp(G)$, de donde $s \leq \exp(G)$.
Luego, $\exp(G) = s = ord(x)$. ▫

Observación: La hipótesis "G es abeliano" en la proposición anterior es esencial. Por ejemplo, si $G = S_3$ es el grupo de permutaciones de 3 elementos, entonces $\exp(G) = 6$ y G no contiene elementos de orden 6.

Proposición 2.5. *Sea $(G\,,\,\cdot)$ un grupo abeliano finito. Entonces G es cíclico si, y sólo si $\exp(G) = |G|$.*

Demostración: Si G es cíclico entonces existe $x \in G$ tal que $ord(x) = |G|$. Como $\exp(G) \mid |G|$, por la proposición 2.1., y como $ord(x) \mid \exp(G)$, por la proposición 2.2., teniendo en cuenta que $ord(x) = |G|$ resulta que $\exp(G) = |G|$.
Recíprocamente, si $\exp(G) = |G|$, sea $x \in G$ tal que $ord(x) = \exp(G)$ (su existencia está garantizada por la proposición 2.4., ya que G es abeliano). Entonces $ord(x) = |G|$, de donde resulta que G es cíclico. ▫

Observación: También aquí la hipótesis "G es abeliano" es esencial. Por ejemplo, si $G = D_5 = \langle s\,,\,\rho\,;\, s^2 = 1 = \rho^5\,,\, s\rho = \rho^{-1}s\rangle$ entonces $\exp(G) = 10 = |G|$, pero G no es cíclico.

Sea $(K\,,\,+\,,\,\cdot)$ un cuerpo. Si K^* denota el conjunto de elementos no nulos de K, entonces $(K^*\,,\,\cdot)$ es un grupo abeliano. Probaremos, usando propiedades del exponente que, cuando K es finito, este grupo es cíclico.

Teorema 2.6. *Sea $(K\,,+\,,\cdot)$ un cuerpo. Si K es finito, entonces $(K^*\,,\cdot)$ es cíclico.*

Demostración: Sea $e = \exp(K^*)$ y sea $f \in K[X]$ el polinomio $f = X^e - 1$.
Como $x^e = 1$ para todo $x \in K^*$, entonces $f(x) = 0$ para todo $x \in K^*$. Siendo f un polinomio en una variable, de grado e y con coeficientes en el cuerpo K, entonces f tiene a lo sumo e raíces en K. Luego, $|K^*| = \#K^* \leq e$. Pero, por la proposición 2.1., $e = \exp(K^*) \mid |K^*|$. Luego debe ser $e = |K^*|$. Como $(K^*\,,\cdot)$ es un grupo abeliano finito y $\exp(K^*) = e = |K^*|$ entonces, por la proposición 2.5., K^* es cíclico. ▫

Si p es un primo positivo, entonces $(\mathbb{Z}_p\,,+\,,\cdot)$ es un cuerpo finito y

$$\mathcal{U}_p = \{\, a \in \mathbb{Z}_p \,/\, (a,p) = 1 \,\} = \mathbb{Z}_p^*.$$

Luego, $\mathcal{U}_p = \mathbb{Z}_p^*$ es un grupo cíclico de orden $\varphi(p) = p - 1$. Por lo tanto, se tiene el siguiente

Corolario 2.7. *Si p es un primo positivo, entonces $\mathcal{U}_p \simeq \mathbb{Z}_{p-1}$.*

3. El caso $n = 2^\alpha$, con $\alpha \geq 2$.

Estudiaremos por separado los casos $\alpha = 2$ y $\alpha \geq 3$. Probaremos primero que si $\alpha = 2$ entonces $\mathcal{U}_{2^\alpha} \simeq \mathbb{Z}_2$ y luego que, para $\alpha \geq 3$, $\mathcal{U}_{2^\alpha} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha-2}}$.

Si $\alpha = 2$ entonces $\mathcal{U}_{2^\alpha} = \mathcal{U}_4$ es un grupo abeliano de orden $\varphi(4) = 2$ y, por lo tanto, isomorfo a $\mathbb{Z}_2$.

Sea ahora $\alpha \in \mathbb{N}$, $\alpha \geq 3$.

Como $|\mathcal{U}_{2^\alpha}| = \varphi(2^\alpha) = 2^{\alpha-1}$, el siguiente lema muestra que para probar nuestra afirmación, basta encontrar $x \in \mathcal{U}_{2^\alpha}$ de orden 2 e $y \in \mathcal{U}_{2^\alpha}$ de orden $2^{\alpha-2}$ tales que $x \notin \langle y \rangle$.

Lema 3.1. *Sea $\alpha \geq 3$ y sea G un grupo abeliano de orden $2^{\alpha-1}$. Si existen $x, y \in G$ tales que $ord(y) = 2^{\alpha-2}$, $ord(x) = 2$ y $x \notin \langle y \rangle$ entonces $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha-2}}$.*

Demostración: Sea $f : \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha-2}} \longrightarrow G$ la aplicación definida por $f(i,j) = x^i.y^j$. Veremos que f es un isomorfismo de grupos.

f es un morfismo:

Teniendo en cuenta que $ord(x) = 2$, $ord(y) = 2^{\alpha-2}$ y que G es abeliano, se tiene que
$f((i,j) + (r,s)) = f(r_2(i+r), r_{2^{\alpha-2}}(j+s)) = x^{r_2(i+r)}.y^{r_{2^{\alpha-2}}(j+s)} = x^{i+r}.y^{j+s} =$
$= x^i.y^j.x^r.y^s = f(i,j).f(r,s).$

f es un monomorfismo:

Supongamos que $f(i,j) = 1$ para algún $0 \leq i < 2$, $0 \leq j < 2^{\alpha-2}$. Entonces $x^i.y^j = 1$, de donde $x^i.x^i.y^j = x^i$, es decir, $x^{2i}.y^j = x^i$. Siendo $x \in G$ un elemento de orden 2 resulta entonces que $x^i = y^j$ y, por lo tanto, $x^i \in \langle y \rangle$. Como $0 \leq i < 2$ y $x \notin \langle y \rangle$, entonces debe ser $i = 0$.

Luego, $1 = x^i.y^j = y^j$, de donde $2^{\alpha-2} = ord(y) \mid j$ y, como $0 \leq j < 2^{\alpha-2}$, resulta que $j = 0$. Por lo tanto $i = 0 = j$.

f es sobre:

Sea $H = Imf$. Siendo f un monomorfismo, H es un subgrupo de G y $f : \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha-2}} \longrightarrow H$ es un isomorfismo. Luego $H \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha-2}}$, de donde resulta que H es un subgrupo de G de orden $2^{\alpha-1}$. Como por hipótesis $|G| = 2^{\alpha-1}$, entonces $H = G$. ▫

Probaremos ahora que 5 tiene orden $2^{\alpha-2}$ en $\mathcal{U}_{2^\alpha}$.

Lema 3.2. *Para todo* $k \in \mathbb{N}$, $k \geq 3$, $5^{2^{k-3}} \equiv 1 + 2^{k-1} \quad (2^k)$.

Demostración: Por inducción en k. Si $k = 3$, $5^{2^{3-3}} = 5 \equiv 5 = 1 + 2^{3-1} \quad (2^3)$. Supongamos ahora que la afirmación es cierta para un $k \geq 3$, es decir, que $5^{2^{k-3}} \equiv 1+2^{k-1} \quad (2^k)$ para un $k \geq 3$. Entonces, $5^{2^{k-3}} = 1 + 2^{k-1} + q.2^k$ para algún $q \in \mathbb{Z}$.
Luego,

$$5^{2^{k-2}} = (5^{2^{k-3}})^2 =$$

$$= (1 + 2^{k-1} + q.2^k)^2 = 1 + 2^{2(k-1)} + q^2.2^{2k} + 2.2^{k-1} + 2.q.2^k + 2.2^{k-1}.q.2^k =$$

$$= 1 + 2^k + q.2^{k+1} + 2^{2(k-1)} + (q^2 + q).2^{2k} \equiv$$

$$\equiv 1 + 2^k \quad (2^{k+1})$$

pues $2(k-1) \geq k+1$ y $2k \geq k+1$, ya que $k \geq 3$.

Por lo tanto,

$$5^{2^{k-2}} \equiv 1 + 2^k \quad (2^{k+1}),$$

es decir, la afirmación es cierta para $k+1$, como queríamos probar. ▫

Proposición 3.3. *Sea* $\alpha \in \mathbb{N}$, $\alpha \geq 3$. *Entonces* 5 *tiene orden* $2^{\alpha-2}$ *en* $\mathcal{U}_{2^\alpha}$.

Demostración: Por el lema 3.2.,

$$5^{2^{\alpha-2}} \equiv 1 + 2^\alpha \quad (2^{\alpha+1}) \quad \text{y} \quad 5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \quad (2^\alpha).$$

Luego,

$$5^{2^{\alpha-2}} \equiv 1 \quad (2^\alpha) \quad \text{y} \quad 5^{2^{\alpha-3}} \not\equiv 1 \quad (2^\alpha),$$

es decir, $5^{2^{\alpha-2}} = 1$ y $5^{2^{\alpha-3}} \neq 1$ en $\mathcal{U}_{2^\alpha}$. Por lo tanto, $ord(5) \mid 2^{\alpha-2}$ y $ord(5) \nmid 2^{\alpha-3}$. Luego debe ser $ord(5) = 2^{\alpha-2}$. ▫

Ahora caracterizaremos $\mathcal{U}_{2^\alpha}$.

Teorema 3.4. *Sea* $\alpha \in \mathbb{N}$, $\alpha \geq 3$. *Entonces* $\mathcal{U}_{2^\alpha} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha-2}}$.

Demostración: Por el lema 3.1. y la proposición 3.3., basta encontrar $x \in \mathcal{U}_{2^\alpha}$ de orden 2 tal que $x \notin \langle 5 \rangle$. Claramente $2^\alpha - 1 \in \mathcal{U}_{2^\alpha}$ tiene orden 2. Veamos que $2^\alpha - 1 \notin \langle 5 \rangle$.

Como $\langle 5\rangle$ es un subgrupo cíclico de $\mathcal{U}_{2^\alpha}$, de orden $2^{\alpha-2}$, entonces contiene un único elemento de orden 2: $5^{2^{\alpha-3}}$ (recordemos que si G es un grupo cíclico de orden m y d es un divisor de m, entonces G contiene exactamente $\varphi(d)$ elementos de orden d). Luego, basta ver que $5^{2^{\alpha-3}} \not\equiv 2^\alpha - 1 \quad (2^\alpha)$.
Si fuese $5^{2^{\alpha-3}} \equiv 2^\alpha - 1 \quad (2^\alpha)$ entonces, por el lema 3.2., $1 + 2^{\alpha-1} \equiv -1 \quad (2^\alpha)$.
Luego, $2^{\alpha-1} \mid 2$. Siendo $\alpha \geq 3$, esto no puede ocurrir. Luego, $x = 2^\alpha - 1$ tiene orden 2 en $\mathcal{U}_{2^\alpha}$ y $x \notin \langle 5\rangle$. □

4. El caso $n = p^\alpha$, con p primo impar y $\alpha \geq 2$.

Probaremos que si p es un primo, $p > 2$ y $\alpha \in \mathbb{N}$, $\alpha \geq 2$, entonces $\mathcal{U}_{p^\alpha} \simeq \mathbb{Z}_{p^{\alpha-1}(p-1)}$. Para ello, primero encontraremos $x, y \in \mathcal{U}_{p^\alpha}$ tales que $ord(x) = p^{\alpha-1}$ y $ord(y) = p - 1$.
Para encontrar un elemento de orden $p^{\alpha-1}$ necesitaremos probar primero el siguiente

Lema 4.1. *Sea p un primo, $p > 2$. Entonces, $\forall\, k \geq 2$, $(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \quad (p^k)$.*

Demostración: Por inducción en k. Si $k = 2$,

$$(1+p)^{p^{2-2}} = 1 + p \equiv 1 + p = 1 + p^{2-1} \quad (p^2).$$

Supongamos ahora que la afirmación es cierta para un $k \geq 2$, es decir, que

$$(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \quad (p^k).$$

Entonces, $(1+p)^{p^{k-2}} = 1 + p^{k-1} + q.p^k$ para algún $q \in \mathbb{Z}$. Luego,

$$(1+p)^{p^{k-1}} = \left((1+p)^{p^{k-2}}\right)^p = (1 + p^{k-1} + q.p^k)^p =$$

$$= \sum_{i=0}^{p} \binom{p}{i} (1 + p^{k-1})^i . (q.p^k)^{p-i} \equiv$$

$$\equiv (1 + p^{k-1})^p + p.(1 + p^{k-1})^{p-1}.q.p^k \equiv (1 + p^{k-1})^p \quad (p^{k+1})$$

pues, $\forall\, 0 \leq i \leq p-2$, $k + 1 \leq 2k \leq k(p-i)$ y, por lo tanto, $p^{k+1} \mid (p^k)^{p-i}$.
Por otra parte,

$$(1 + p^{k-1})^p = \sum_{j=0}^{p} \binom{p}{j} (p^{k-1})^j \equiv 1 + p.p^{k-1} + \frac{p-1}{2} p^{2k-1} \equiv 1 + p^k \quad (p^{k+1})$$

pues, $\forall\, 3 \leq j \leq p$, $p^{k+1} \mid (p^{k-1})^j$ ya que $k + 1 \leq 3(k-1) \leq j(k-1)$, p es impar y $p^{k+1} \mid p^{2k-1}$ ya que $k + 1 \leq 2k - 1$.
Luego,

$$(1+p)^{p^{k-1}} \equiv 1 + p^k \quad (p^{k+1})$$

como queríamos probar. ▫

El lema 4.1. nos permitirá ahora encontrar el elemento de orden $p^{\alpha-1}$ que estábamos buscando.

Proposición 4.2. *Sea $\alpha \in \mathbb{N}$, $\alpha \geq 2$, y sea p un primo positivo impar. Entonces $1+p$ tiene orden $p^{\alpha-1}$ en $\mathcal{U}_{p^\alpha}$.*

Demostración: Por el lema 4.1.

$$(1+p)^{p^{\alpha-1}} \equiv 1 + p^\alpha \quad (p^{\alpha+1}) \quad \text{y} \quad (1+p)^{p^{\alpha-2}} \equiv 1 + p^{\alpha-1} \quad (p^\alpha).$$

Luego,

$$(1+p)^{p^{\alpha-1}} \equiv 1 \quad (p^\alpha) \quad \text{y} \quad (1+p)^{p^{\alpha-2}} \not\equiv 1 \quad (p^\alpha),$$

es decir, $(1+p)^{p^{\alpha-1}} = 1$ y $(1+p)^{p^{\alpha-2}} \neq 1$ en $\mathcal{U}_{p^\alpha}$. Por lo tanto, en $\mathcal{U}_{p^\alpha}$, $ord(1+p) \mid p^{\alpha-1}$ y $ord(1+p) \nmid 2^{\alpha-2}$. Luego, $ord(1+p) = p^{\alpha-1}$. ▫

La siguiente proposición garantiza la existencia de un elemento de orden $p-1$ en $\mathcal{U}_{p^\alpha}$.

Proposición 4.3. *Sea p un primo positivo impar y sea $\alpha \in \mathbb{N}$. Si a es un generador del grupo cíclico $\mathcal{U}_p$, entonces $a^{p^{\alpha-1}}$ tiene orden $p-1$ en $\mathcal{U}_{p^\alpha}$.*

Demostración: Como $|\mathcal{U}_{p^\alpha}| = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$ y $a \in \mathcal{U}_{p^\alpha}$, entonces $\left(a^{p^{\alpha-1}}\right)^{p-1} =$
$= a^{p^{\alpha-1}(p-1)} \equiv 1 \quad (p^\alpha)$.

Supongamos ahora que $\left(a^{p^{\alpha-1}}\right)^k \equiv 1 \quad (p^\alpha)$. Entonces, $\left(a^{p^{\alpha-1}}\right)^k \equiv 1 \quad (p)$.

Como $a^p \equiv a \quad (p)$ entonces $a^{p^{\alpha-1}} \equiv a \quad (p)$. Luego, $a^k \equiv 1 \quad (p)$ de donde resulta que $p-1 \mid k$, ya que, en $\mathcal{U}_p$, $ord(a) = |\mathcal{U}_p| = p-1$. ▫

Ahora sí estamos en condiciones de caracterizar $\mathcal{U}_{p^\alpha}$.

Teorema 4.4. *Sean p un primo, $p > 2$ y $\alpha \in \mathbb{N}$, $\alpha \geq 2$. Entonces $\mathcal{U}_{p^\alpha} \simeq \mathbb{Z}_{p^{\alpha-1}(p-1)}$.*

Demostración: Por la proposición 4.2., $\exists\, x \in \mathcal{U}_{p^\alpha}$ de orden $p^{\alpha-1}$ y, por la proposición 4.3., $\exists\, y \in \mathcal{U}_{p^\alpha}$ de orden $p-1$. Como $(p^{\alpha-1}, p-1) = 1$, entonces $[p^{\alpha-1}, p-1] = p^{\alpha-1}(p-1)$. Sea $g = x.y \in \mathcal{U}_{p^\alpha}$. Como $\mathcal{U}_{p^\alpha}$ es un grupo abeliano finito, resulta que

$$ord(g) = ord(x.y) = [ord(x), ord(y)] = [p^{\alpha-1}, p-1] = p^{\alpha-1}(p-1) = \varphi(p^\alpha) = |\mathcal{U}_{p^\alpha}|.$$

Luego, $\mathcal{U}_{p^\alpha}$ es un grupo cíclico de orden $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ y por lo tanto se tiene que $\mathcal{U}_{p^\alpha} \simeq \mathbb{Z}_{p^{\alpha-1}(p-1)}$. ▫

Observación: De la demostración del teorema anterior y de la proposición 4.3. se deduce que si a es un generador de $\mathcal{U}_p$ (con p primo, $p > 2$), entonces $(1+p).a^{p^{\alpha-1}}$ es un generador de $\mathcal{U}_{p^\alpha}$.

5. El caso general.

Como hemos caracterizado $\mathcal{U}_{p^\alpha}$ para todo primo positivo p y $\alpha \in \mathbb{N}$, para caracterizar $\mathcal{U}_n$ para todo $n > 1$, utilizaremos la factorización de n como producto de primos.

Proposición 5.1. *Sean $m, k \in \mathbb{N}$, $m, k \geq 2$. Si $(m,k) = 1$, entonces $\mathcal{U}_{m.k} \simeq \mathcal{U}_m \oplus \mathcal{U}_k$.*

Demostración: Sea $f : \mathcal{U}_{m.k} \longrightarrow \mathcal{U}_m \oplus \mathcal{U}_k$ la aplicación definida por $f(a) = (r_m(a), r_k(a))$.

Probaremos que f está bien definida (i.e., que si $a \in \mathcal{U}_{m.k}$ entonces $f(a) \in \mathcal{U}_m \oplus \mathcal{U}_k$) y que es un isomorfismo.

f está bien definida:
Sea $a \in \mathcal{U}_{m.k}$. Es claro que $r_m(a) \in \mathbb{Z}_m$. Luego, para probar que $r_m(a) \in \mathcal{U}_m$, basta ver que $(r_m(a), m) = 1$.
Sea $d = (r_m(a), m)$. Entonces $d \mid m$ y $d \mid r_m(a)$. Como $a = m.q + r_m(a)$, para algún $q \in \mathbb{Z}$, resulta que $d \mid m$ y $d \mid a$. Luego $d \mid m.k$ y $d \mid a$ y, en consecuencia, $d \mid (a, m.k)$. Como $a \in \mathcal{U}_{m.k}$ entonces $(a, m.k) = 1$. Por lo tanto, $d = 1$.
Hemos probado entonces que $r_m(a) \in \mathcal{U}_m$. Análogamente, $r_k(a) \in \mathcal{U}_k$.

Dejamos a cargo del lector verificar que f es un morfismo.

f es biyectiva:

Como $(m,k) = 1$, por el teorema Chino del resto, dados $b, c \in \mathbb{Z}$ existe un único $a \in \mathbb{Z}$ tal que $a \equiv b \quad (m)$, $a \equiv c \quad (k)$ y $0 \leq a < m.k$.
Teniendo en cuenta que, $\forall\, 0 \leq b < m$, $a \equiv b \quad (m)$ es equivalente a $r_m(a) = b$ y que, $\forall\, 0 \leq c < k$, $a \equiv c \quad (k)$ es equivalente a $r_k(a) = c$, se tiene que dado $(b, c) \in \mathcal{U}_m \oplus \mathcal{U}_k$ existe un único $a \in \mathbb{Z}_{m.k}$ tal que $r_m(a) = b$ y $r_k(a) = c$.

Veamos que $a \in \mathcal{U}_{m.k}$. Supongamos que existe un primo p tal que $p \mid a$ y $p \mid m.k$. Entonces, $p \mid a$ y $p \mid m$, o $p \mid a$ y $p \mid k$, lo que implica que $p \mid b$ y $p \mid m$, o $p \mid c$ y $p \mid k$, ya que $a \equiv b \quad (m)$ y $a \equiv c \quad (k)$. Luego, $p \mid (b, m)$ o $p \mid (c, k)$, lo cual es absurdo pues $b \in \mathcal{U}_m$ y $c \in \mathcal{U}_k$. Por lo tanto, $(a, m.k) = 1$. Hemos probado entonces que $\forall (b, c) \in \mathcal{U}_m \oplus \mathcal{U}_k$ existe un único $a \in \mathcal{U}_{m.k}$ tal que $f(a) = (b, c)$. ▫

Corolario: *Dado $n \in \mathbb{N}$, $n > 1$, si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, con p_i primos positivos distintos y $\alpha_i \in \mathbb{N}$, entonces $\mathcal{U}_n \simeq \mathcal{U}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathcal{U}_{p_r^{\alpha_r}}$.*

Demostración: Por inducción en r. El resultado es trivial si $r = 1$. Supongamos que

$$\mathcal{U}_{p_1^{\alpha_1} \dots p_r^{\alpha_r}} \simeq \mathcal{U}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathcal{U}_{p_r^{\alpha_r}}$$

para un $r \in \mathbb{N}$. Sea p_{r+1} un primo positivo distinto de $p_1, \dots, p_r$ y sea $\alpha_{r+1} \in \mathbb{N}$. Entonces $(p_1^{\alpha_1} \dots p_r^{\alpha_r}, p_{r+1}^{\alpha_{r+1}}) = 1$ y, por lo tanto, aplicando la proposición 5.1., se tiene que

$$\mathcal{U}_{p_1^{\alpha_1} \dots p_{r+1}^{\alpha_{r+1}}} \simeq \mathcal{U}_{p_1^{\alpha_1} \dots p_r^{\alpha_r}} \oplus \mathcal{U}_{p_{r+1}^{\alpha_{r+1}}} \simeq \mathcal{U}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathcal{U}_{p_r^{\alpha_r}} \oplus \mathcal{U}_{p_{r+1}^{\alpha_{r+1}}}$$

como queríamos probar. ▫

Ejemplos:

i) $\mathcal{U}_{21} = \mathcal{U}_{3.7} \simeq \mathcal{U}_3 \oplus \mathcal{U}_7 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6$

ii) $\mathcal{U}_{72} = \mathcal{U}_{2^3.3^2} \simeq \mathcal{U}_{2^3} \oplus \mathcal{U}_{3^2} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6$

iii) $\mathcal{U}_{980} = \mathcal{U}_{2^2.5.7^2} \simeq \mathcal{U}_{2^2} \oplus \mathcal{U}_5 \oplus \mathcal{U}_{7^2} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{42}$

iv) $\mathcal{U}_{1350} = \mathcal{U}_{2.3^3.5^2} \simeq \mathcal{U}_2 \oplus \mathcal{U}_{3^3} \oplus \mathcal{U}_{5^2} \simeq \mathbb{Z}_{18} \oplus \mathbb{Z}_{20}$

v) $\mathcal{U}_{2^{32}.3^{23}.7^4.17} \simeq \mathcal{U}_{2^{32}} \oplus \mathcal{U}_{3^{23}} \oplus \mathcal{U}_{7^4} \oplus \mathcal{U}_{17} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{30}} \oplus \mathbb{Z}_{2.3^{22}} \oplus \mathbb{Z}_{6.7^3} \oplus \mathbb{Z}_{16}$

Ejercicios:

1. Encontrar un generador de $\mathcal{U}_{7^{15}}$ y uno de $\mathcal{U}_{13^4}$
2. Determinar el exponente de $\mathcal{U}_{3.11.31}$, de $\mathcal{U}_{2.5.7^2.13}$ y de $\mathcal{U}_{2^8}$
3. Determinar cuántos elementos de orden 15 hay en $\mathcal{U}_{99}$. ¿Y de orden 12?
4. Hallar todos los $n \in \mathbb{N}$ tales que $\mathcal{U}_n \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6$
5. Hallar todos los $n \in \mathbb{N}$ tales que $\mathcal{U}_n$ es cíclico
6. ¿Cuántos subgrupos de orden 5 tiene $\mathcal{U}_{300}$? ¿Cuántos subgrupos de orden 15 tiene $\mathcal{U}_{225}$?
7. Usando que un grupo cíclico de orden n tiene elementos de orden d, para todo d tal que $d \mid n$, probar que si p es un primo positivo impar entonces -1 es un cuadrado en $\mathbb{Z}_p$ si, y sólo si, p es de la forma $4k+1$