Boletín de Matemáticas
Nueva Serie, Volumen X No. 2 (2003), pp. 59–67

EL INDICADOR DE INVOLUCIÓN

ALFONSO RÍDER MOYANO (*)
RAFAEL MARÍA RUBIO RUIZ (**)

Resumen. En este trabajo se construye una función que asocia a cada natural $n \geq 2$ el cardinal del subgrupo de involución, del anillo correspondiente $\mathbb{Z}/n\mathbb{Z}$. Se finaliza con algunos resultados parciales sobre el cálculo de elementos involutivos.

Abstract. In this paper we present a function which maps every natural number $n \geq 2$ into the order of the involution subgroup in the ring $\mathbb{Z}/n\mathbb{Z}$. We also study partial results about the computation of elements of order two in $\mathbb{Z}/n\mathbb{Z}$.

2000 Mathematics Subject Classifications: 11A07, 16U60.

0. Introducción

Es clásicamente conocido cómo el orden del subgrupo de unidades del anillo $\mathbb{Z}/n\mathbb{Z}$ viene determinado por la llamada función indicadora de Euler $\phi(n)$. En lo que sigue consideraremos el subgrupo del grupo de unidades, formado por aquellos elementos que son involutivos y de forma análoga al caso del grupo de unidades, nos proponemos desarrollar un indicador $i(n)$, que explicite el orden de dicho subgrupo de involución. Nuestro desarrollo utilizará únicamente, técnicas gaussianas, esto es, ligadas a los anillos de congruencias aritméticas. Recordemos que como consecuencia, aunque no directa, del Teorema de Cauchy se obtiene un resultado que afirma que si todos los elementos de un grupo son involutivos, entonces dicho grupo es isomorfo al producto directo de cierto número de copias de $\mathbb{Z}/2\mathbb{Z}$. En consecuencia, gracias a este resultado podríamos

(*) Alfonso Ríder Moyano. e-mail: ma1rimoa@uco.es
(**) Rafael María Rubio Ruiz. e-mail: ma1rurur@uco.es
Departamento de Matemáticas, Universidad de Córdoba
Campus de Rabanales, Edificio C2
Córdoba, 14071, España.

afirmar que la función $i(n)$, será una potencia de 2, hecho que nosotros probaremos haciendo uso únicamente, de las técnicas antes mencionadas y explicitando además el exponente de dicha potencia de 2, para el subgrupo de involución de cada $\mathbb{Z}/n\mathbb{Z}$.
Terminaremos nuestra exposición con algunos resultados parciales sobre el cálculo de elementos del grupo de involución, en algunos órdenes.

1. Preliminares

Recordemos que μ es involutivo en el anillo $\mathbb{Z}/n\mathbb{Z}$ cuando $\mu^2 \equiv 1(\text{mód. } n)$.

La siguiente equivalencia es evidente:

$$\mu^2 - 1 \equiv 0(\text{mód. } n) \Leftrightarrow n \mid \mu^2 - 1.$$

Aunque μ sea en principio cualquier entero, por pasar a las clases módulo n, no hay inconveniente en suponer siempre que $1 \leq \mu \leq n-1$ (el valor $\mu = 0$ se descarta pues conduce a $-1 \equiv 0$, o sea, $1 \equiv 0$, lo que no ocurre al ser $n \geq 2$).
Obsérvese que el conjunto $\mathcal{I}(n)$ de los elementos involutivos no es vacío, ya que $1 \in \mathcal{I}(n)$, además si $\mu \in \mathcal{I}(n)$, también $-\mu \in \mathcal{I}(n)$.
Por otra parte, los elementos involutivos forman un subgrupo del grupo $\Phi(n)$ de las unidades del anillo $\mathbb{Z}/n\mathbb{Z}$. En efecto, como $\Phi(n)$ es abeliano, la aplicación $x \mapsto x^2$ es un morfismo. Su núcleo es exactamente el conjunto $\mathcal{I}(n)$. En consecuencia, $\forall n \geq 2$, $i(n) \mid \varphi(n)$, siendo φ el indicador de Euler.

2. El indicador $i(n)$.

Proposición 2.1. *Sea n un número primo. Si $n = 2$, el único elemento involutivo del anillo $\mathbb{Z}/2\mathbb{Z}$ es el $\mu = 1$; si $n \geq 3$, los únicos elementos involutivos de $\mathbb{Z}/n\mathbb{Z}$ son los $\mu = 1, n-1$.*

Demostración: Sea $1 \leq \mu \leq n-1$ y supongamos que

$$n \mid \mu^2 - 1 = (\mu - 1)(\mu + 1).$$

Entonces, por la condición de Gauss, se deduce que

$$\begin{cases} n \mid \mu - 1 \Rightarrow \mu - 1 = 0 \Rightarrow \mu = 1, & \text{pues } 0 \leq \mu - 1 \leq n - 2 < n \\ n \mid \mu + 1 \Rightarrow \mu + 1 = n \Rightarrow \mu = n - 1, & \text{pues } 2 \leq \mu + 1 \leq n. \end{cases}$$

Si $n = 2$ los dos valores obtenidos claramente son coincidentes.

Proposición 2.2. *Sea $n = 2^m (m \geq 1)$. Si $m = 1$, el único elemento involutivo es el $\mu = 1$; si $m = 2$, los únicos elementos involutivos son los $\mu = 1, 3$; si $m \geq 3$, son elementos involutivos los cuatro valores*

$$\mu = 1, 2^{m-1} - 1, 2^{m-1} + 1, 2^m - 1,$$

y solamente ellos.

Demostración: El caso $n = 2$ ya ha sido aclarado. Si $n = 4$, sabemos que 1 y 3 son involutivos; el elemento restante, que es el 2, no puede ser involutivo porque ni siquiera es inversible.
Supongamos, pues, $m \geq 3$. Que $\mu = 1, 2^m - 1$, son involutivos ya se sabe; tomando

$$\mu = 2^{m-1} \mp 1,$$

se tiene

$$\mu^2 - 1 = 2^{2m-2} \mp 2^m = 2^m (2^{m-2} \mp 1),$$

que es un múltiplo de 2^m. Esta pareja es distinta de la trivial pues

$$\left.\begin{array}{rcl} 2^{m-1} \mp 1 = 1 & \Rightarrow & 2^{m-1} = \begin{cases} 2 \\ 0 \end{cases} \\ 2^{m-1} \mp 1 = 2^m - 1 & \Rightarrow & -2^{m-1} = \begin{cases} 0 \\ -2 \end{cases} \end{array}\right\} \Rightarrow 2^{m-2} = \begin{cases} 1 \\ 0, \end{cases}$$

siendo la primera relación imposible porque $m > 2$ y la segunda absurda.
Teniendo ya cuatro elementos involutivos distintos entre sí, se trata ahora de probar que son los únicos. Lo haremos por recurrencia sobre m:
a) Si $m = 3$, los restantes elementos 2,4,6 no pueden ser involutivos por no ser primos con él, módulo $n = 8$.
b) Sea $m > 3$ y supongamos nuestra afirmación cierta para $m - 1$. Dado un elemento μ, del margen $1 \leq \mu \leq 2^m - 1$, tal que $2^m \mid \mu^2 - 1$, existirá un entero c tal que $\mu^2 - 1 = 2^m c$, pero también se tendrá

$$2^{m-1} \mid \mu^2 - 1 \Leftrightarrow \mu^2 - 1 \equiv 0, \text{ (mód. } 2^{m-1}).$$

Por la hipótesis de inducción, se cumplirá

$$\mu \equiv \begin{cases} 1 \\ 2^{m-2} - 1 \\ 2^{m-2} + 1 \\ 2^{m-1} - 1 \end{cases}, \text{(mód. } 2^{m-1}).$$

Analizando estas posibilidades, tenemos

1) $\mu \equiv 1 \Rightarrow \exists h \in \mathbb{N}/\mu = 2^{m-1}h + 1$.
Si $h \geq 2$, el número μ se sale del margen $1 \leq \mu \leq 2^m - 1$, luego necesariamente

$$\begin{cases} h = 0 & \Rightarrow \mu = 1 \\ h = 1 & \Rightarrow \mu = 2^{m-1} + 1. \end{cases}$$

2) $\mu \equiv 2^{m-2} \mp 1 \Rightarrow \exists h \in \mathbb{N}/\mu = 2^{m-1}h + (2^{m-2} \mp 1)$.
Entonces,

$$\mu^2 - 1 = 2^{2m-2}h^2 + 2^m h(2^{m-2} \mp 1) + 2^{2m-4} \mp 2^{m-1} = 2^m c \Rightarrow$$

$$\Rightarrow 2^{m-1}h^2 + 2h(2^{m-2} \mp 1) + 2^{m-3} \mp 1 = 2c,$$

igualdad absurda porque, al ser $m > 3$, el primer miembro será un número impar, mientras que el segundo es par. Por tanto, esta alternativa no puede presentarse.

3) $\mu \equiv 2^{m-1} - 1 \Rightarrow \exists h \in \mathbb{N}/\mu = 2^{m-1}h + 2^{m-1} - 1$.
Si $h \geq 2$, el número μ se sale del margen $1 \leq \mu \leq 2^m - 1$, luego necesariamente

$$\begin{cases} h = 0 & \Rightarrow \mu = 2^{m-1} - 1 \\ h = 1 & \Rightarrow \mu = 2^m - 1. \end{cases}$$

Proposición 2.3. *Sea $p \geq 3$ un número natural primo y sea $\beta \geq 1$ natural. Entonces, los únicos elementos involutivos, módulo p^β, son los números*

$$1, p^\beta - 1.$$

Demostración: La haremos por recurrencia sobre β:
a) Si $\beta = 1$, basta aplicar la Proposición 3.1.
b) Supongamos el enunciado cierto para $\beta - 1$. Sea μ, con $1 \leq \mu \leq p^\beta - 1$, tal que $p^\beta \mid \mu^2 - 1$. Esto significa que existe un entero m tal que

$$\mu^2 - 1 = p^\beta m,$$

a la vez que implica la relación

$$p^{\beta-1} \mid \mu^2 - 1 \Leftrightarrow \mu^2 - 1 \equiv 0, \text{ (mód. } p^{\beta-1}).$$

Por la hipótesis de inducción, se cumplirá

$$\mu \equiv \begin{cases} 1 \\ p^{\beta-1} - 1 \end{cases}, \text{(mód. } p^{\beta-1}) \Rightarrow$$

$$\Rightarrow \mu = \begin{cases} p^{\beta-1}c + 1 \\ p^{\beta-1}d + (p^{\beta-1} - 1) = p^{\beta-1}(d+1) - 1 \end{cases} \Rightarrow$$

$$\Rightarrow \mu^2 - 1 = p^\beta m = \begin{cases} p^{2\beta-2}c^2 + 2p^{\beta-1}c \\ p^{2\beta-2}(d+1)^2 - 2p^{\beta-1}(d+1) \end{cases} \Rightarrow$$

$$\Rightarrow pm = \begin{cases} p^{\beta-1}c^2 + 2c \\ p^{\beta-1}(d+1)^2 - 2(d+1) \end{cases} \Rightarrow \begin{cases} p \mid 2c \\ p \mid -2(d+1) \end{cases} \Rightarrow \begin{cases} p \mid c \\ p \mid d+1, \end{cases}$$

pues p es primo con 2. Entonces,

$$\begin{cases} p \mid c \Rightarrow c = \begin{cases} 0 & \Rightarrow \mu = 1 \\ ph & \Rightarrow \mu = p^\beta h + 1 \end{cases} \\ p \mid d+1 \Rightarrow d+1 = \begin{cases} 0 & \Rightarrow \mu = -1 \\ pk & \Rightarrow \mu = p^\beta k - 1. \end{cases} \end{cases}$$

De los cuatro valores que salen para μ, el primero es uno de los que queríamos probar. El segundo y el tercero se descartan porque se salen del margen

$$1 \leq \mu \leq p^\beta - 1.$$

En el cuarto debe ser

$$k = 1 \Rightarrow \mu = p^\beta - 1,$$

que es el otro valor que queríamos obtener, pues de lo contrario μ vuelve a salirse del margen señalado.

Proposición 2.4. *Si p y q son primos entre sí, se cumple*

$$i(pq) = i(p)i(q).$$

Demostración: Al ser m.c.d.$(p, q) = 1$, se tiene el isomorfismo

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \mapsto \mathbb{Z}/(pq).$$

Si (a, b) se aplica en c, la condición $c^2 \equiv 1$, módulo pq, equivale a que

$$(a, b)^2 = (a^2, b^2) = (1, 1) \Leftrightarrow \begin{cases} a^2 \equiv 1, \text{ (mód. } p) \\ b^2 \equiv 1, \text{ (mód. } q). \end{cases}$$

Por tanto, en $\mathbb{Z}/(pq)$ hay tantos elementos involutivos como parejas formemos con uno de $\mathbb{Z}/p\mathbb{Z}$ y otro de $\mathbb{Z}/q\mathbb{Z}$, es decir, hay $i(p)i(q)$.

Proposición 2.5. *Sea $n \geq 2$ un número natural y sea*

$$n = 2^m p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

la factorización prima de n, con $p_1, p_2, \ldots, p_r \geq 3$, y $r = 0$ para los casos en que n sea potencia de 2. Entonces,

$$i(n) = \begin{cases} 2^r & si\ m \leq 1 \\ 2^{r+1} & si\ m = 2 \\ 2^{r+2} & si\ m \geq 3. \end{cases}$$

Demostración: Basta aplicar la Proposición 2.4, seguida de las 2.1, 2.2 y 2.3.

3. Sobre el grupo $\mathcal{I}(n)$

Presentamos en este capítulo, algunos pequeños resultados, que aunque elementales, creemos que pueden resultar sugestivos en referencia a la búsqueda de elementos involutivos.

Proposición 3.1. *Sea $q \geq 3$ impar. La mitad de los elementos de $\mathcal{I}(q)$ son pares y la otra mitad impares.*

Demostración: Sabemos que si $\mu \in \mathcal{I}(q)$, también $q - \mu \in \mathcal{I}(q)$. Ahora bien, por ser q impar, $q - \mu$ cambia de paridad respecto de μ.

Proposición 3.2. *Sea $q \geq 3$ impar. Si $\mu \in \mathcal{I}(q)$ es impar, también $\mu \in \mathcal{I}(2q)$.*

Demostración: Si μ es impar, el número $\mu^2 - 1$ es par, a la vez que múltiplo de q. Entonces,

$$\frac{\mu^2 - 1}{q}$$

es par, luego existe algún entero c tal que

$$\frac{\mu^2 - 1}{q} = 2c \Leftrightarrow \mu^2 - 1 = (2q)c \Leftrightarrow \mu^2 - 1 \equiv 0, \text{ (mód. 2q)}.$$

Como sabemos que para $q \geq 3$ impar, se tiene $i(q) = i(2q)$, al conocer los elementos involutivos, módulo q, tomando los impares, conoceremos la mitad de los elementos de $\mathcal{I}(2q)$. Si a cada uno de ellos, μ, le añadimos el elemento $2q - \mu$, quedan conocidos todos los elementos de $\mathcal{I}(2q)$. Por ejemplo,

$$\mathcal{I}(15) = \{1, 4, 11, 14\} \Rightarrow \mathcal{I}(30) = \{1, 11, 19, 29\}.$$

Proposición 3.3. *Si $p = 4q$, donde $q \geq 2$, en $\mathbb{Z}/p\mathbb{Z}$ hay cuando menos cuatro elementos involutivos distintos. A saber,*

$$1, 2q - 1, 2q + 1, 4q - 1.$$

Demostración: Para cada $k \geq 1$, se tiene que

$$\mu = 2kq \pm 1 \Rightarrow$$
$$\Rightarrow \mu^2 - 1 = 4k^2q^2 \pm 4kq = 4kq(kq \pm 1) \equiv 0, \text{ (mód. } 4q),$$

es decir, μ es involutivo.
Para $k = 1$, salen los valores

$$2q + 1, 2q - 1,$$

mientras que para $k = 2$ salen los

$$4q + 1 \equiv 1, 4q - 1.$$

Además, al ser $q \geq 2, se$ tiene

$$1 < 2q - 1 < 2q + 1 < 4q - 1,$$

luego los cuatro valores son distintos entre sí.

Obsérvese que si q es un primo impar, aplicando este teorema, quedan conocidos los cuatro únicos elementos de $\mathcal{I}(4q)$. Por ejemplo, $68 = 4 \cdot 17$, luego

$$\mathcal{I}(68) = \{1, 33, 35, 67\}.$$

Proposición 3.4. *Si $p = 8q$, donde $q \geq 3$ es impar, en $\mathbb{Z}/p\mathbb{Z}$ hay cuando menos ocho elementos involutivos distintos. A saber,*

$$1, 2q - 1, 2q + 1, 4q - 1, 4q + 1, 6q - 1, 6q + 1, 8q - 1.$$

Demostración: Para cada $k \geq 1$, se tiene que

$$\mu = 2kq \pm 1 \Rightarrow \mu^2 - 1 = 4k^2q^2 \pm 4kq = 4kq(kq \pm 1)$$

Si k es par, es claro que $4kq$ contiene el factor $8q$. Si k fuese impar, también lo es kq, a la vez que $kq \pm 1$ será par. En todo caso, por tanto, se llega a que

$$\mu^2 - 1 \equiv 0, \text{ (mód. 8q)}.$$

Para $k = 1, 2, 3, 4$ salen los elementos anunciados, los cuales son todos distintos por ser $q > 1$.

Observemos que análogamente al caso anterior, si q es un primo impar, aplicando este teorema, quedan conocidos los ocho únicos elementos de $\mathcal{I}(8q)$. Por ejemplo, $104 = 8 \cdot 13$, luego

$$\mathcal{I}(104) = \{1, 25, 27, 51, 53, 77, 79, 103\}.$$

Proposición 3.5. *Si* $p = 8q$, *donde*

$$q = \frac{r(r+1)}{2}, \text{ con } r \geq 0,$$

el elemento $2r + 1$ *es involutivo, módulo* p.

Demostración: Para $\mu = 2r + 1$ se tiene

$$\mu^2 - 1 = 4r^2 + 4r = 4r(r + 1) = 8q \equiv 0, \text{ (mód. } 8q),$$

porque uno de los factores r o $r + 1$ es par.

También será elemento involutivo $-\mu$, pues se tiene

$$8q - \mu = 8q - (2r + 1) = 4r(r + 1) - 2r - 1 = 4r^2 + 2r - 1.$$

Casi más interesante que saber que $\mu = 2r + 1$ es involutivo módulo el número $4r(r + 1)$ es observar que, de la igualdad

$$\mu^2 - 1 = 4r(r + 1),$$

deducimos que μ será involutivo en todos aquellos anillos $\mathbb{Z}/p\mathbb{Z}$ tales que

$$p \mid 4r(r + 1).$$

Dando sucesivos valores a r y tomando los posibles divisores del número $4r(r + 1)$, obtenemos todos aquellos módulos en los que un número impar genérico $2r + 1$ es involutivo. Así, a modo de ejemplo, obtenemos la tabla para los primeros impares:

r	$2r+1$	$4r(r+1)$	p
0	1	0	2,3,4,5,...
1	3	8	4,8
2	5	24	6,8,12,24
3	7	48	8,12,16,24,48
4	9	80	10,16,20,40,80
5	11	120	12,15,20,24,30,40,60,120
6	13	168	14,21,24,28,42,56,84,168
7	15	224	16,28,32,56,112,224
8	17	288	18,24,32,36,48,72,96,144,288

Un proceso similar puede tenerse para los números $\mu = 2r$, con $r \geq 1$, que sean pares: siendo

$$\mu^2 - 1 = 4r^2 - 1,$$

deducimos que μ es involutivo, módulo p, siempre que

$$p \mid 4r^2 - 1.$$

La correspondiente tabulación, para los primeros pares es

r	$2r$	$4r^2-1$	p
1	2	3	3
2	4	15	5,15
3	6	35	7,35
4	8	63	9,21,63
5	10	99	11,33,99
6	12	143	13,143
7	14	195	15,39,65,195
8	16	255	17,51,85,255

Bibliografía

[1] J.L. Alperin, B. Rowen. *Groups and Representations*, Springer-Verlag, New York, 1995.

[2] J. B. Fraleigh. *Algebra abstracta*, Addison-Wesley Iberoamericana, Wilmington, 1987.

[3] D. Gorenstein. *Finite Groups*, Chelsea Publishing Company, New York, 1980.

[4] N. Jacobson. *Basic Algebra* I,II. Freeman and Company, New York, 1985.

[5] A. Ríder, R. Rubio. *An Elemental Study of Groups whose Order is a Product of Two Primes.* Divulgaciones Matemáticas, **11** No. 1 (2003), 61–70.

[6] J. S. Robinson. *A Course in the Theory of Groups.* Springer-Verlag, New York, 1982.

[7] M. Suzuki. *Groups Theory.* Springer-Verlag, New York, 1982.

[8] I. Vinogradov. *Fundamentos de la Teoría de los Números.* MIR, Moscú, 1977.