Revista INTEGRACION
Departamento de Matemáticas UIS
Vol. 5, No. 2, julio-diciembre 1987

Restos cuadráticos y generadores en el grupo $\langle Z'_m , \bullet , 1 \rangle$

CARLOS LEZAMA*

En el número antepasado de la revista Integración [1] se trataron los siguientes aspectos del grupo $\langle Z'_m , \bullet , 1 \rangle$:

1. Una condición necesaria y suficiente para que el grupo sea cíclico es que $m = 2, 4, p^\alpha, 2p^\alpha$, con p primo, $p \neq 2$, $\alpha \geq 1$.

2. Una condición necesaria y suficiente para que $g \in Z'_n$ sea generador es que g no satisfaga $g^{\frac{\phi(m)}{q}} \cong 1$ (mód. p), para cada divisor primo q de $\phi(m)$.

3. Siendo g un generador de Z'_p, existen $t, u \in Z_p$ tales que $(g + p^t)^{p-1} = 1 + pu$ y $t \nmid u$, siendo $g + pt$ un generador para Z'^{α}_p.

El problema de determinar un generador para Z'_p cuando p es muy grande, no ha sido resuelto en el sentido de que ningún algoritmo conduce directamente al generador. Un método indirecto es el dado en 2, pero es muy laborioso cuando $p - 1$ tiene muchos divisores primos distintos.

En el presente artículo se darán algunos criterios que son útiles para «simplificar» un poco el método indirecto antes mencionado. Básicamente se tra-

* Profesor Auxiliar, Departamento de Matemáticas, Universidad Industrial de Santander, Bucaramanga, Colombia.

tará el siguiente aspecto: Conocida la forma del primo p, decidir qué elementos con seguridad no son generadores de Z'_p y qué elementos pueden ser generadores de Z'_p.

1.0 Proposición:

Sea $R_p = \{ a \in Z'_p / (\frac{a}{p}) = 1$ **Entonces:**

(i) $R_p \neq \emptyset$;
(ii) $R_p < Z'_p$

Demostración:

(i) Puesto que la congruencia $X^2 \equiv 1$ (mód. p) tiene como soluciones 1 y p - 1, se tiene que 1 es resto cuadrático mód. p, esto es, $\left(\frac{1}{p}\right) = 1$. Por tanto, $1 \in R_p$.

(ii) Sean $a, b \in R_p$. Entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$. Entonces las congruencias $X^2 \equiv a, b$ (mód. p) tienen solución. Sean éstas X_o, Y_o tales que $X_o^2 \equiv a$ (mód. p), $Y_o^2 \equiv b$ (mód. p). Entonces $X_o^2 Y_o^2 \equiv ab$ (mód. p), esto es, $(X_o Y_o)^2 \equiv ab$ (mód. p). Luego la congruencia $X^2 \equiv ab$ (mód. p) tiene solución. Por tanto, ab es resto cuadrático mód p, esto es, $\left(\frac{ab}{p}\right) = 1$, $ab \in R_p$ □

2.0 Corolario:

R_p es el subgrupo de Z'_p cuyo orden es $1/2(p - 1)$

Demostración:

El número de restos cuadráticos mód. p es $1/2(p - 1)$. Por tanto, $|R_p| = 1/2(p - 1)$. Siendo Z'_p cíclico, se tiene el resultado. Además, es obvio que R_p es cíclico. Por tanto, existe $h \in R_p$ tal que $\langle h \rangle = R_p$ □

3.0 Ejemplos:

3.1 Hallar R_7

Puesto que $2^{\frac{7-1}{2}} = 2^3 \equiv 1$ (mód. 7), se tiene que $\left(\frac{2}{7}\right) = 1$; por tanto, $2 \in R_7$. Además, $|2| = 3$. Luego, $\langle 2 \rangle = R_7$, esto es, $R_7 = \{1, 2, 4\}$ •

3.2 Hallar R_{13}

Como $2^6 \not\equiv 1$ (mód. 13), $\left(\frac{2}{13}\right) = -1$. Por tanto, $2 \notin R_{13}$. Ahora, $3^6 \equiv 1$ (mód. 13). Así, $\left(\frac{3}{13}\right) = 1$, esto es, $3 \in R_{13}$. Pero $|3| = 3 \neq 6$. Por tanto, 3 no es generador para R_{13}. Sin embargo, $4^6 \equiv 1$ (mód. 13), $\left(\frac{4}{13}\right) = 1$, $4 \in R_{13}$. $|4| = 6$. Luego, $R_{13} = \langle 4 \rangle = \{1, 4, 3, 12, 9, 10\}$ •

Los ejemplos anteriores muestran que no siempre 2 y 3 son residuos cuadráticos mód. p. Sin embargo, existen resultados sobre el carácter cuadrático de tales números. Tales resultados son:

(a) $2 \in R_p \Leftrightarrow p \equiv 1,7$ (mód. 8) ⇔ (véase, por ej. [2], p. 75).

(b) $3 \in R_p \Leftrightarrow p \equiv 1,11$ (mód. 12) (véase, por ej. [2], p. 138).

Consecuencia inmediata de los resultados anteriores es la siguiente proposición:

4.0 Proposición:

i) 2 no es generador de Z'_p para $p \equiv 1,7$ (mód. 8)

(ii) 3 no es generador de Z'_p para $p \equiv 1,11$ (mód. 12)

Demostración:

(i) Puesto que $p \equiv 1,7$ (mód. 8), el resultado (a) garantiza que $2 \in R_p$. Por tanto, $2^{1/2(p-1)} \equiv 1$ (mód. p). Luego, $|2| \leq 1/2(p - 1) < p - 1 = |Z'_p|$. Así, $\langle 2 \rangle \neq Z'_p$.

(ii) Análoga a la parte (i), utilizando el resultado (b) ■

Una pregunta inmediata después de analizar el alcance de la proposición anterior es la siguiente: ¿Es 2 generador de Z'_p cuando $p \equiv 3,5$ (mód. 8), y es 3 generador de Z'_p cuando $p \equiv 5,7$ (mód. 12)?

Veamos algunos casos particulares:

1. Para $p = 11 = 8 \cdot 1 + 3$, se tiene que $2^{10} \not\equiv 1 \not\equiv 2^2$ (mód. 11). Por tanto, $\langle 2 \rangle = Z'_{11}$.

2. Para $p = 43 = 8 \cdot 5 + 3$, se tiene que $2^{14} \equiv 1$ (mód. 43). Por tanto, $\langle 2 \rangle \neq Z'_{43}$.

3. Para $p = 13 = 8 \cdot 1 + 5$, se tiene que $2^6 \not\equiv 1 \not\equiv 2^4$ (mód. 13). Por tanto, $\langle 2 \rangle = Z'_{13}$.

4. Para $p = 109 = 8 \cdot 13 + 5$, se tiene que $2^{36} \equiv 1$ (mód. 109). Por tanto, $\langle 2 \rangle \neq Z'_{109}$.

5. Para $p = 17 = 12 \cdot 1 + 5$, se tiene que $3^6 \not\equiv 1$ (mód. 17). Por tanto, $\langle 3 \rangle = Z'_{17}$.

6. Para $p = 41 = 12 \cdot 3 + 5$, se tiene que $3^8 \equiv 1$ (mód. 41). Por tanto, $\langle 3 \rangle \neq Z'_{41}$.

7. Para $p = 7 = 12 \cdot 0 + 7$, se tiene que $3^2 \not\equiv 1 \not\equiv 3^3$ (mód. 7). Por tanto, $\langle 3 \rangle = Z'_7$.

8. Para $p = 103 = 12 \cdot 8 + 7$, se tiene que $3^{34} \equiv 1$ (mód. 103). Por tanto, $\langle 3 \rangle \neq Z'_{103}$.

Por los 8 ejemplos anteriores, la respuesta a la pregunta es:
¡NO NECESARIAMENTE!

Sin embargo, bajo ciertas condiciones adicionales, se puede garantizar que 2 y 3 son generadores para algunos grupos Z'_{2p+1} y Z'_p, respectivamente. Esto se verá en las dos proposiciones siguientes:

5.0 Proposición:

$$\text{Si } p = 4K + 1 \text{ entonces } \langle 2 \rangle = Z'_{2p+1}$$

Demostración:

Puesto que $\varnothing(2p+1) = 2p$, 2 es generador para Z'_{2p+1} si $2^p \not\equiv 1 \not\equiv 2^2$ (mód. $2p+1$).

Como $4 \not\equiv 1$ (mód. $2p+1$), queda por considerar el otro caso.

Si $2^p \not\equiv 1$ (mód. $2p+1$), entonces $2 \notin R_{2p+1}$ y, por tanto, $\left(\frac{2}{2p+1}\right) = 1$; pero $\left(\frac{2}{2p+1}\right) = (-1)^{\frac{(2p+1)^2-1}{8}}$

Así que $-1 = (-1)^{\frac{(2p+1)^2-1}{8}}$. Por tanto, $-1 = (-1)^{\frac{p^2+p}{2}}$ Esta igualdad se tiene si $p = 4K + 1$, como puede comprobarlo el lector.

6.0 Corolario: Si $p = 4K + 3$ entonces $\langle -2 \rangle = Z'_{2p+1}$

Demostración:

Procediendo en forma análoga a como se hizo en la proposición, debe cumplirse que $\left(\frac{-2}{2p+1}\right) = -1$ para que -2 sea generador de Z'_{2p+1}.

Pero $\left(\frac{-2}{2p+1}\right) = \left(\frac{2}{2p+1}\right)\left(\frac{-1}{2p+1}\right) = (-1)^{\frac{p(p+1)}{2}} \cdot (-1)^p$

Por tanto, $1 = (-1)^{\frac{p(p+1)}{2}}$. Esta igualdad se tiene si $p = 4K + 3$, como se deduce de la proposición anterior □

7.0 Proposición: Si $p = 2^K + 1$, $K > 1$ entonces $\langle 3 \rangle = Z'_p$

Demostración:

$\varnothing(p) = 2^K$. Por tanto, 3 es generador para Z'_p si $3^{\frac{2^K}{2}} \not\equiv$ (mód. p), esto es, si $\left(\frac{3}{2^K+1}\right) = -1$.

Ahora,

$\left(\frac{3}{2^K+1}\right) = \left(\frac{2^K+1}{3}\right) = \left(\frac{2}{3}\right) = -1$.* Por tanto, se tiene el resultado ■

* La ley de reciprocidad cuadrática y el hecho de que $a \equiv b$ (mód. p) implican $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ (véase, por ejemplo, [3], p.88-91).

Respecto al elemento -3, se tiene el siguiente resultado:

$-3 \in R_p \longleftrightarrow p = 6K + 1$ (véase, por ej., [3], p. 100).

Por tanto, para primos p de la forma $6K + 1$, se garantiza que -3 no es generador de Z_p^*.

En cuanto al elemento -1, se tiene que $|-1| = 2$.

Sin embargo, ello no garantiza que -1 sea siempre resto cuadrático mód. p, ya que $\left(\frac{-1}{p}\right) = 1 \longleftrightarrow p = 4K + 1$ (véase, por ej., [3], p. 88).

Lo que sí se puede afirmar es que -1 no es generador de Z_p^*.

8.0 Tabla de mínimos generadores para Z_p^*, $2 < p < 100$:

p	g	p	g	p	g	p	g
3	2	19	2	43	3	71	7
5	2	23	5	47	5	73	5
7	3	29	2	53	2	79	3
11	2	31	3	59	2	83	2
13	2	37	2	61	2	89	3
17	3	41	6	67	2	97	5

Obsérvese que en 12 de los 24 casos, 2 es generador y en 6 de los casos, 3 es generador.

Obsérvese también que no todo g es primo

Extendiendo las anteriores observaciones a los 167 primos impares menores que 1000, se tiene lo siguiente:

- En 67 casos, 2 es mínimo generador.
- En 40 casos, 3 es mínimo generador.
- En 15 casos, el mínimo generador no es primo.

Posiblemente por tales observaciones (extendidas a muchos más casos) es que se le ha dedicado mayor atención a los elementos 2 y 3, como restos cuadráticos y generadores.

9.0 Tabla de mínimos generadores de R_p, $2 < p < 100$:

p	h	p	h	p	h	p	h
3	1	19	4	43	9	71	2
5	4	23	2•	47	2•	73	6
7	2•	29	4	53	4	79	2
11	3•	31	7	59	3•	83	3•
13	4	37	3	61	4	89	5
17	2	41	2	67	4	97	2

• Cualquier elemento diferente de 1, genera a R_p

A manera de ejemplo, los 44 restos cuadráticos mód. 89 son:

$$R_{89} = \langle 5 \rangle = \{ 1, 5, 25, 36, 2, 10, 50, 72, 4, 20, 11, 55, 8, 40, 22, 21, 16, 80, 44, 42, 32, 71, 88, 84, 64, 53, 87, 79, 39, 17, 85, 69, 78, 34, 81, 49, 67, 68, 73, 9, 45, 47, 57, 18 \} = \{ 5^0, 5^1, 5^2, \ldots, 5^{43} \}.$$

Obsérvese que 2 y 4 son restos cuadráticos mód. 89. Sin embargo, no son generadores de R_{89}.

REFERENCIAS

[1] LEZAMA Carlos, ACEVEDO Francisco, AVENDAÑO Enrique. «El grupo $< Z'_n, \cdot, 1 >$» *Revista Integración*. Vol. 4, No. 2 (1986), p. 5-11.

[2] BURTON Jones. *Teoría de los números*. Programex Editora S.A., México, 1969.

[3] VINOGRADOV I.M. *Fundamentos de la Teoría de los Números*. Editorial MIR, Moscú, 1977.