# RAICES CUADRADAS EN CUERPOS PRIMOS DE CARACTERISTICA *P*

por

J. M. MARTINEZ SANCHEZ

## 1. INTRODUCCIÓN

Dado un cuerpo K, podemos establecer un homomorfismo de anillos $\varphi : Z \to K$ definido del siguiente modo:

*a)* $\varphi(n) = 1 + \ldots + 1 = n \,.\, 1$ si $n \geqslant 0$ ; $1 \in K$.
*b)* $\varphi(-n) = -\varphi(n)$.

Si $\varphi$ es inyectivo, Z es isomorfo a un anillo de K, y por consiguiente K contiene un subcuerpo isomorfo a Q; en este caso se dice que K es de característica cero.

Si $\varphi$ no es inyectivo, *ker* $\varphi$ es un ideal de Z, luego como Z es anillo principal *ker* $\varphi = (p)$, $p \in Z$, de forma que $Z/(p)$ se identifica con un subanillo de K, lo cual implica que $Z/(p)$ es un anillo íntegro y consecuentemente $p$ es un número primo.

$Z/(p)$ es el anillo de las congruencias mod. $p$, consta de $p$ elementos. Ahora bien, como todo anillo íntegro finito es un cuerpo y ademas todo cuerpo finito es conmutativo, $Z/(p)$ se identifica a un subcuerpo conmutativo de K. En este caso se dice que K es de característica $p$. A los cuerpos $Z/(p)$ los designaremos $\Gamma p$.

*Definición 1.* Un cuerpo K se dice finito si *card*(K) = $n$, $n \in N$.

Tanto Q como $\Gamma p$ son los subcuerpos mínimos de un cuerpo K y reciben el nombre de cuerpos primos.

*Definición 2.* Un cuerpo se llama perfecto si es de característica cero, o si siendo de característica $p$ coincide con el subcuerpo $K^p$.

Como consecuencia de que todo cuerpo primo es perfecto, sabemos que todo elemento de $\Gamma p$ admite raíz *p-esima* en $\Gamma p$.

## 2. RAICES CUADRADAS DE LOS ELEMENTOS DE $\Gamma p$ ($p > 2$).

Sea $x \in \Gamma p$, $x$ admite raíz p-ésima, pero no ocurre lo mismo con las raíces cuadradas, ya que si $p \neq 2$ existen elementos en $\Gamma p$ que son cuadrados de elementos de $\Gamma p$ y otros no son.

*Ejemplos:*

*a)* En $\Gamma_3$ 0 y 1 admiten raíz cuadrada y no admite el 2.

*b)* En $\Gamma_5$ admiten raíz cuadrada el 0, 1 y 4, pero el 2 y 3 carecen de raíz cuadrada.

*c)* En $\Gamma_7$ poseen raíz cuadrada los elementos 0, 1, 2, 4, y no poseen raíz cuadrada los elementos 3, 5 y 6.

Es inmediato dar una condición suficiente para que un elemento $x \in \Gamma p$ admita raíz cuadrada en $\Gamma p$, basta conque sea cuadrado perfecto en N. En efecto: si $x = a^2 \in N$ como $x \in \Gamma p \Longrightarrow x < p \Longrightarrow$ $\Longrightarrow a < p \Longrightarrow a \in \Gamma p$. (Nota: excluimos el cero de $\Gamma p$.)

*Proposición 1.ª:* Si un elemento $x \in \Gamma p$ posee una raíz cuadrada en $\Gamma p$, entonces admite otra, cumpliéndose las siguientes condiciones:

*a)* Las dos raíces son únicas.

*b)* Si $p > 2$ las raíces son distintas; si $p = 2$ doble.

*Demostración:* Si $x \in \Gamma p$ y por hipótesis $x = a^2$ con $a \in \Gamma p$, entonces $(p - a)^2 = p^2 - 2ap + a^2 = (p - 2a)\, p + a^2 = a^2 = x$; luego si $a^2 =$ $= x \Longrightarrow (p - a)^2 = x$.

*b)* $a \neq p - a$, pues si $a = p - a \Longrightarrow 2a = p$, en contra de ser $p$ primo $\neq 2$. Si $p = 2$ $a = 1$ y $p - a = 2 - 1 = 1$ es la raíz doble.

*a)* Si $a^2 = x$ y $a'^2 = x$ con $a$ y $a' \in \Gamma p$ tenemos que $a^2 - a'^2 =$ $= 0 \Longrightarrow (a + a')\,(a - a') = 0$, por ser $\Gamma p$ cuerpo carece de divisores de cero, es decir, $a + a' = 0$ ó $a - a' = 0$, luego $a = p - a'$ ó $a = a'$.

### 3. Ecuaciones de segundo grado en $\Gamma p$.

Sea $ax^2 + bx + c = 0$ (1) una ecuación de segundo grado con coeficiente en $\Gamma p$, $a \neq 0$. Entonces existe un elemento $\overline{a} \in \Gamma p$ tal que $a\overline{a} =$ $= 1 \in \Gamma p$ y podemos escribir la ecuación (1) en la forma

$$x^2 + \overline{a}bx + \overline{a}c = 0 \qquad [2]$$

y poniendo $\overline{a}b = m$, $\overline{a}c = n$ tenemos:

$$x^2 + m\,x + n = 0. \qquad [3]$$

Sea $\overline{2}$ el inverso de 2 en $\Gamma p$, podemos escribir [3]:

$$(x + \overline{2}m)^2 = (\overline{2}m)^2 + (p - n) \qquad [4]$$

y la investigación de las raíces de (1) queda reducida a obtener las raíces cuadradas del elemento de $\Gamma p = (\overline{2}m)^2 + (p - n)$.

*Definición:* Damos el nombre de discriminantes de la ecuación

$$ax^2 + bx + c = 0 \quad \text{a} \quad D = (\overline{2}m)^2 + (p - n).$$

Se pueden presentar los casos siguientes:

1. D admite dos raíces cuadradas en $\Gamma p$:

$D = d^2$, $D = (p - d)^2$, entonces la ecuación $x^2 + mx + u = 0$ tiene las raíces $x_1 = d + (p - \overline{2}m)$, $x_2 = (p - d) + (p - \overline{2}m)$.

2. $D = 0 \in \Gamma p$.

La ecuación $x^2 + mx + n = 0$ admite la raíz doble: $x_1 = p - \overline{2}m = x_2$. En este caso $(\overline{2}m)^2 = n$.

3. D no admite raíces cuadradas en $\Gamma p$, entonces la ecuación $x^2 + mx + n = 0$ carece de raíces en $\Gamma p$.

Como consecuencia de lo anterior, obtenemos la siguiente

*Proposición 2.ª* $[\overline{2^2} + k(k+1)] \in \Gamma p$ admite raíces cuadradas en $\Gamma p$.

*Demostración*: La ecuación $x^2 + x + p - k(k+1) = 0$ admite las raíces $x_1 = k$ y $x_2 = p - (k+1)$, en efecto:

$k^2 + k + p - k(k+1) = p = 0$.
$[p - (k+1)]^2 + [p - (k+1)] + p - k(k+1) = p^2 - 2(k+1)p + (k+1)^2 + p - (k+1) + p - k(k+1) = [p - 2(k+1)]p + k^2 + 2k + 1 + (p - k) + (p - 1) + (p - k^2) + (p - k) = [k^2 + (p - k^2)] + [2k + 2(p - k)] + [1 + (p - 1)] = 0$ y como el discriminante de la ecuación es $D = \overline{2}^2 + k(k+1)$ queda desmotrada la proposición 2.ª

*Ejemplos:*

1) Resolver en $\Gamma_7$ las ecuaciones $x^2 + x + 1 = 0$ y $x^2 + x + 5 = 0$

$x^2 + x + 1 = x^2 + x + (7 - 2 \cdot 3) = 0 \qquad x_1 = 2, x_2 = 7 - 3 = 4$
$x^2 + x + 5 = x_2 + x + (7 - 1 \cdot 2) = 0 \qquad x_1 = 1, x_2 = 7 - 2 = 5$

2) Resolver en $\Gamma_{23}$ las ecuaciones $x^2 + x + 3 = 0$, $x^2 + x + 17 = 0$

$x^2 + x + 3 = x^2 + x + (23 - 4 \cdot 5) = 0 \qquad x_1 = 4, x_2 = 23 - 5 = 18$
$x^2 + x + 17 = x^2 + x + (23 - 2 \cdot 3) = 0 \qquad x_1 = 2, x_3 = 23 - 3 = 20$

3) Hallar en $\Gamma_{29}$ las raíces cuadradas de 5 y 13.

$5 = \overline{2}^2 + 3.4$, ya que

$$\overline{2} = \frac{29 + 1}{2} = 15,$$

$\overline{2}^2 = 15^2 = 22$ y $22 + 12 = 5$, luego 5 es el discriminante de la ecuación $x^2 + x + (29 - 3.4) = 0$, cuyas soluciones son $x_1 = 3$ y $x_2 = 25$; por último, como $x_2 = d + (p - 15) = d + 14 = 25$, $d = 11$ y $d' = 18$, es decir, que $11^2 = 5$ y $18^2 = 5$.

$13 = \overline{2}^2 + 4.5$ es el discriminante de $x^2 + x + (29 - 4.5) = 0$, $x_1 = 4$, $x_2 = 24$ y $x_2 = d + 14 = 24 \quad d = 10$, $d' = 19$, son las raíces cuadradas de 13 en $\Gamma_{29}$.

4) Raíces cuadradas de 30 en $\Gamma_{37}$.

$$30 = \overline{2}^2 + 1.2, \overline{2} = \frac{37 + 1}{2} = 19; d = 1 + \overline{2} = 20, d' = 17.$$

Como consecuencia de la proposición 2.ª tenemos la siguiente

*Proposición 3.ª* La ecuación $x^2 + mx + p - m^3(m+1) = 0$ tiene solución en $\Gamma p$.

*Proposición 4.ª* Si la ecuación $x^2 + mx + n = 0$ tiene la raíz $x_1$, entonces también tiene la $x_2 = (p - m) + (p - x_1)$.

*Demostración:* Si $D = d^2 = (p - d)^2$ entonces $x_1 = \frac{d}{} + (p - \overline{2}m)$ y $x_2 = (p - d) + (p - \overline{2}m)$, sumando $x_2 + x_1 = 2(p - \overline{2}m) = p - m$, luego $x_2 = (p - m) + (p - x_1)$.

## 4. Condiciones en las que los elementos de $\Gamma p$ admiten raiz cuadrada.

El grupo multiplicativo de $\Gamma p$ es cíclico de orden $p - 1$, como consecuencia se tiene que $x^{p-1} = 1$ para todo $x \in \Gamma p$.

*Definición:* Se dice que $x \in \Gamma p$ es una raíz primitiva de $\Gamma p$ si para todo elemento y de $\Gamma p$ existe un entero $s$, $0 \leqslant s \leqslant p - 1$ tal que $y = x^s$.

Por tanto, $x$ engendra el grupo multiplicativo de $\Gamma p$, cuyos elementos son $x, x^2, -, x^{p-1}$ y tal que $x^i \neq x^j$ *sii* $i \neq j$, $x^{p-1} = 1$.

Teorema 1.º Si $x$ es una raíz primitiva de $\Gamma p$, entonces $x$ no admite raíz cuadrada en $\Gamma p$.

*Demostración:* Si $x = a^2$, $a \in \Gamma p$, entonces como $p - 1 = 2e$, tendríamos que $x^e = a^{2e} = a^{p-1} = 1$, $0 < e < p - 1$, luego $x^e = 1$, $0 < < e < p - 1$ en contra de la hipótesis de que $x$ es una raíz primitiva de $\Gamma p$.

*Corolario:* La condición necesaria para que un elemento de $\Gamma p$ admita raíz cuadrada es que no sea raíz primitiva de $\Gamma p$.

Tenemos los elementos de $\Gamma p$ clasificados así:

*i)* Elementos que engendran un grupo cíclico de orden $p - 1$ o raíces primitivas de $\Gamma p$ y que no admiten raíces cuadradas.

*ii)* Elementos que engendran un subgrupo cíclico de orden $q < < p - 1$, estos elementos pueden o no tener raíz cuadrada.

Si un elemento $y$ no es raíz primitiva de $\Gamma p$, sea $q$ el menor entero menor que $p$ que cumple $y^q = 1$, entonces como para todo $x \in \Gamma p$ se verifica que $x^{p-1} = 1$, tenemos que $y^{p-1} = y^q$, pero como $q < p - 1$ se cumple que $q \mid p - 1$, luego $p - 1 = k \cdot q$, y puede suceder, puesto que $p - 1$ es par, que $k$ sea par o no.

El siguiente teorema nos caracteriza estos elementos.

Teorema 2. Sea $y$ un elemento de $\Gamma p$, sea $q$ el menor entero, $q < p - 1$, tal que $y^q = 1$ se verifica:

*a)* Si $q = p - 1/k$, donde $k$ es par, entonces $y$ admite raíz cuadrada en $\Gamma p$.

*b)* Si $q = p - 1/k$, donde $k$ es *impar*, entonces $y$ no admite raíz cuadrada en $\Gamma p$.

*Demostración:*

*a)* Sea $y^{p-1/2i} = 1$; el subgrupo cíclico de orden $k$ engendrado por $y$ tiene los siguientes elementos: $y_1 y^2, \ldots, y^q = 1$ con $q = p^{-1}/_{2i}$.

Sea $x$ una raíz primitiva de $\Gamma p$: $x_1 x^2_1, - x^{p-1} = 1$, con $x^i \neq x^j$

si y sólo si $i \neq j$, son todos los elementos de $\Gamma p$. Por consiguiente $y = x^s$ mediante multiplicaciones sucesivas tenemos:

$$y^{p-1/2t} = (x^s)^{p-1/2t} = x^{s\,p-1/2t} = 1, \text{ luego } x^{s(p-1/2t} = x^{p-1} \text{ o}$$

$$x^{s(p-1)/2t} = x^o, \text{ lo que implica:}$$

$$\frac{s\,(p-1)}{2t} = p - 1 \text{ ó } \frac{s\,(p-1)}{2t} = 0$$

es decir $s = 2t$ ó $s = 0$, de donde $y = x^{2t}$ ó $y = x^o = 1$, prescindiendo de éste caso trivial, $y = (x^t)^2$, poniendo $a = x^t$ tenemos que $y = a^2$ admite raíz cuadrada en $\Gamma p$.

*b)* Basta demostrar el recíproco de *a)*, es decir, que si un elemento tiene raíz cuadrada en $\Gamma p$, entonces el menor entero $q$, tal que $y^q = 1$ es de la forma $^{p-1}/_{2t}$. En efecto, si $y = a^2$, sea $x$ una raíz primitiva de $\Gamma p$ tenemos que $a = x^t$ e $y = x^{2t}$, luego $y^q = x^{2tq} = 1$ pero como $x$ es raíz primitiva y el menor entero que cumple $x^{2tq} = 1$ es $p - 1$, tenemos que $2tq = p - 1$, lo que implica $q = {}^{p-1}/_{2t}$ Q. E. D.

Resuminos los resultados anteriores en el siguiente

Teorema 3. La condición necesaria y suficiente para que un elemento de $\Gamma p$ admita raíz cuadrada en $\Gamma p$ es que sea potencia par de alguna raíz primitiva de $\Gamma p$.

*Demostración:* La condición es suficiente: $y = x^{2s} = (x^s)^2$, poniendo $x^s = a$ tenemos $y = a^2$.

La condición es necesaria: si $y = x^{2s+1}$ siendo $x$ raíz primitiva de $\Gamma p$, $x$ no se puede expresar como potencia par de ningún elemento de $\Gamma p$, pues en caso contrario $x$ tendría raíz cuadrada en $\Gamma p$, en contra de las hipótesis de que $x$ era raíz primitiva, luego y sólo se puede expresar como potencia de exponente impar de elementos de $\Gamma p$.

*Consecuencia* 1. Si $x$ es una raíz primitiva, todas sus potencias pares son los elementos de $\Gamma p$ que admite raíz cuadrada. Por tanto en $\Gamma p$ hay

$$\frac{p-1}{2}$$

elementos que admite raíz cuadrada y

$$\frac{p-1}{2}$$

elementos que no la admiten. (El cero excluido.)

*Consecuencia* 2. Si $p-1/_2$ es el menor entero para el cual $y^{p-1}/_2 = 1$ entonces $y$ engendra un subgrupo cíclico de orden $p - 1/_2$ de $\Gamma p$, cuyos elementos $y, y^2, y^3, —, y^{p-1}/_2$ son todos los elementos de $\Gamma p$ que poseen raíz cuadrada. En efecto, como $y = a^2$, $a = x^t$, $y = x^{2t}$ todas son potencias pares de $x$ y todas son distintas, luego son todas las potencias pares de $x$ en $\Gamma p$.

Consecuentemente, $y$, $y^2$, $y^3$, — , $y^{p-1}/_2$ no son raíces primitivas de $\Gamma p$.

*Consecuencia* 3. Si $x$ es un elemento de $\Gamma p$ que no posée raíz cuadrada y $q = {}^{p-1}/_2$ es el menor entero para el cual $x^q = p - 1$, entonces $x$ es raíz primitiva de $\Gamma p$.

*Consecuencia* 4. Si $z^{p-1}/_2 = p-1$, pero existe otro entero $q < {}^{p-1}/_2$ tal que $z^q = 1$ ó $z^q = p - 1$, entonces $z$ ni es raíz primitiva ni admite raíz cuadrada en $\Gamma p$.

TEOREMA 4.

*a)* Si $y = p - 1$ admite raíces cuadradas en $\Gamma p$ hay

$$\frac{p-1}{2}$$

elementos de $\Gamma p$ en total, se excluye el cero, tales que ellos y sus opuestos admiten raíz cuadrada en $\Gamma p$ y otros

$$\frac{p-1}{2}$$

elementos que ni ellos ni sus opuestos admiten raíces cuadradas en $\Gamma p$.

*b)* Si $y = p - 1$ no admite raíz cuadrada a $\Gamma p$, entonces para todo elemento de $\Gamma p$ él o su opuesto admite raíz cuadrada pero no ambos.

*Demostración:*

*a)* $p - 1 = d^2$, sea $x$ una raíz primitiva de $\Gamma p$ y pongamos $d = x^t$, entonces $p - 1 = x^{2t}$. Sea ahora $a = b^2$, $b \in \Gamma p$ como $a = x^\alpha$, $b = x^\beta$, tenemos que $a = x^{2\beta}$ y $x^{2t} \cdot x^{2\beta} = (p - 1)a$, luego $x^{2(t+\beta)} = pa - a = (a - 1)\, p + p - a = p - a$, lo que nos dice que $p - a = d_1{}^2$ con $d_1 = x^{t+\beta}$.

*b)* $p - 1 = d^s$, $s$ = impar, sea $x$ raíz primitiva de $\Gamma p$ y sea $d = x^t$, es decir, $p - 1 = x^{st}$, $st = i$ impar. Sea $a = b^2$, $b \in \Gamma p$ $a = x^\alpha$, $b = x^\beta$, luego $a = x^{2\beta}$ tenemos, como antes, $x^{st} \cdot x^{2\beta} = (p - 1)\, a\, x^{st+2\beta} = pa - a = (a - 1)\, p + (p - a) = p - a$ y como $st + 2\beta$ es $i$ impar, resulta en virtud del teorema 3, que $p - a$ no tiene raíz cuadrada en $\Gamma p$, pero si la tiene $a$.

En el caso en que $p - 1 = a^2$ tenemos que $p = a^2 + 1$, luego $a$ tiene que ser par, pues en caso contrario $a^2$ sería impar y $p = a^2 + 1$ sería par en contra de ser $p$ número primo distinto de 2. Por consiguiente, $a = 2\alpha$, $a^2 = 4\alpha^2$ y $p = 4\alpha^2 + 1$, poniendo $k = \alpha^2$ tenemos que $p = 4k + 1$.

El recíproco que no se verifica en Z, basta fijarse en el caso de $p = 13$, si se cumple en $\Gamma p$. Veamos el siguiente lema.

*Lema.* En todo cuerpo $\Gamma p$ se verifica que si $p = 4k + 1$, entonces $p - 1 = a^2$.

*Demostración:* Si $p = 4k + 1$, entonces $p - 1 = 4k$, sea $x$ una raíz primitiva de $\Gamma p$ y sea $k = x^t$, $2 = x^s$, entonces $x^{2s} \cdot x^t = p - 1$, es decir, $x^{2s+t} = p - 1$ elevando al cuadrado $[x^{2s+t}]^2 = (p-1)^2 = 1$, es decir, $x^{4s+2t} = x^{p-1}$, luego $4s + 2t = p - 1$ tenemos finalmente, $4s + 2t = 4k$, $2s + t = 2k$ y $t = 2(k - s)$ poniendo $k - s = r$, obtenemos que $t = 2r$, luego $k = x^t = x^{2r} = (x^r)^2$, poniendo $x^r = \alpha$, $k = \alpha^2$ y $p - 1 = (2\alpha)^2$ escribimos $2\alpha = a$ y tenemos, por último, $p - 1 = a^2$. C. Q. D.

Entonces, si $p - 1$ no admite raíces cuadradas en $\Gamma p$, $p$ no es de la forma $4k + 1$, luego $p$ tiene que ser de la forma $4k + 3$. El teorema 4 lo podemos enunciar así:

TEOREMA 5. Sea $\Gamma p$ un cuerpo primo de característica $p \neq 0$, se verifica que:

*a)* Si $p \equiv 1$, mód. 4, existen, en $\Gamma p$, $^{p-1}/_2$ elementos en total, tales que ellos y sus opuestos admiten raíz cuadrada y los $^{p-1}/_2$ elementos restantes ni ellos ni sus opuestos, $^{p-1}/_2$ en total, admiten raíz cuadrada en $\Gamma p$.

*b)* Si $p \equiv 3$, mód. 4, todo elemento de $\Gamma p$ o su opuesto admite raíz cuadrada en $\Gamma p$, pero no ambos simultáneamente.

Obtenemos los corolarios siguientes:

*Corolario 1.* Si $p = 4k + 1$, entonces $k \in \Gamma p$ admite raíz cuadrada en $\Gamma p$.

*Corolario 2.* Si $p = 4k + 1$, entonces $p - 1$ admite raíz cuadrada en $\Gamma p$.

*Corolario 3.* Si $p = 4k + 3$, entonces $p - 1$ no admite raíz cuadrada en $\Gamma p$.

*Corolario 4.* Si $p = 4k + 3$, entonces o $p - 2$ ó $p - k - 1$, o ambos, admiten raíz cuadrada en $\Gamma p$.

*Ejemplos:*

1. ¿Posee 10 raíz cuadrada en $\Gamma_{13}$? ¿Y 17 en $\Gamma_{19}$?

Como $13 = 4 \cdot 3 + 1$, si 10 posee raíz cuadrada en $\Gamma_{13}$ también la posee $13 - 10 = 3$ y recíprocamente. Pero $3 = 3$, $3^2 = 9$, $3^3 = 1$, luego $q = 3$, $q = 13 - 1/4$, $k = 4$ par, por tanto 3 posee raíz cuadrada en $\Gamma_{13}$ y lo mismo sucede con 10 ($6^2 = 7^2 = 10$).

En la segunda interrogante $19 = 4 \cdot 4 + 3$, luego si 17 tiene raíz cuadrada en $\Gamma_{19}$, $2 = 19 - 17$ no tiene y si 2 admite raíz cuadrada 17 no la admite. Como $2 = 2$, $2^4 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 13$, $2^6 = 7$, $2^7 = 14$, $2^8 = 9$, $2^9 = 18$ tenemos que $2^{^{19-1}/_2} = 19 - 1$, por tanto 2 es raíz primitiva de $\Gamma_{19}$ y 17 tiene, por consiguiente, raíz cuadrada en $\Gamma_{19}$.

2. Hallar todos los elementos de $\Gamma_{17}$ que posee raíz cuadrada.

Puesto que $17 = 4 \cdot 4 + 1$, cuatro elementos y sus cuatro opuestos poseen raíz cuadrada. Como 4 posee siempre raíz cuadrada, tenemos que 1, 4, 16, 13 posee raíz cuadrada, lo mismo con 9 y 8. Los cuadrados de estos elementos también poseen raíz cuadrada $8^2 = 13$, $13^2 = 2$, y

tenemos 1, 2, 4, 8, 9, 13, 15, 16 son todos los elementos perdidos, ya que $15 = 17 - 2$.

3. Hallar una raíz primitiva de $\Gamma_{11}$.

Como $11 = 2 \cdot 4 + 3$ y 4 posee raíz cuadrada en $\Gamma_{11}$ se deduce que 7 no posee raíz cuadrada en $\Gamma_{11}$. Entonces: $7^1$, $7^2 = 5$, $7^3 = 3$, $7^4 = 3$, $7^5 = 10$ y al ser $7^{11-1}/_2 = 11 - 1$, 7 es una raíz primitiva de $\Gamma_{11}$. Ahora es fácil hallarlas todas, puesto que basta tomar las potencias de exp. impar de 7 y excluir las que engendran subgrupos de ord. menor que 11.

Es decir, 7, $2 = 7^3$, $10 = 7^5$, $6 = 7^7$, $8 = 7^9$ y excluir el 10, pues $10^2 = 1$, luego las raíces primitivas de $\Gamma_{11}$ son {2, 6, 7, 8}.

## 5. Aplicaciones a la sistematización de los conjuntos $\Gamma p(m)$ de ecuaciones cuadraticas.

Si bien ahora podemos dar algunas proposiciones para la resolución de algunas ecuaciones de 2º grado en $\Gamma p$, lo principal será discutir la solución de las mismas.

*Proposición 5.* Si $p \equiv 1$ (mód. 4) y la ecuación $x^2 + mx + n = 0$, tiene solución en $\Gamma p$, entonces también le tiene la ecuación $x^2 + m'x + p - n = 0$, siendo $m'$ la raíz cuadrada de $p - m^2$.

*Demostración:* En efecto como $m^2$ admite raíz cuadrada en $\Gamma p$ también la admite $p - m^2$, sea $m'$ como indicábamos. El discriminante de $x^2 + mx + n = 0$ es $D = \overline{2}^2 m^2 + p - n$ y posee raíces cuadradas en $\Gamma p$, luego lo mismo le ocurre a $D' = p - D = n + p - \overline{2}^2 m^2$, pero este es el discriminante de la ecuación $x^2 + m'x + p - n = 0$, ya que: $D' = \overline{2}^2 m'^2 + n = \overline{2}^2 (p - m^2) + n = p - \overline{2}^2 m^2 + n = p - D$, y la ecuación $x^2 + m' x + p - n = 0$ tiene solución en $\Gamma p$. Q. E. D.

*Proposición 6.* Si $p \equiv 3$, mód. 4, y la ecuación $x^2 + mx + a^2 = 0$ no admite solución en $\Gamma p$, entonces la ecuación $x^2 + 2a\,x + m' = 0$, donde $m' = (\overline{2}m)^2$ admite solución en $\Gamma p$.

*Demostración:* El discriminante de $x^2 + mx + a^2 = 0$ es $D = (\overline{2}n)^2 + p - a^2$ que no admite raíces cuadrada en $\Gamma p$, luego en virtud del teorema 5 $p - D = a^2 + p - (\overline{2}m)^2$ sí admite raíces cuadradas, pero $D' = p - D$ es el discriminante de $x^2 + 2ax + m' = 0$, luego esta ecuación admite soluciones en $\Gamma p$. Q. E. D.

Sea ahora el conjunto $\Gamma p(m)$ de ecuaciones $x^2 + mx + n = 0$, con $m$ fijo y $n$ recorriento todo $\Gamma p$, entonces $D = (\overline{2}m)^2 + p - n$ toma todos los valores de $\Gamma p$ una sola vez y en virtud del teorema hay $p - 1/2$ valores de D que admiten raíz cuadrada en $\Gamma p$ y otras $p - 1/2$, valores de D, que no admiten raíz cuadrada, tenemos, por tanto, el teorema siguiente:

Teorema 6. Sea $\Gamma p(m)$ el conjunto de las ecuaciones de la forma $x^2 + mx + n = 0$ con $m$ fijo y $n$ recorriendo todo $\Gamma p$. Entonces:

*a)* Existe $p - 1/2$ ecuaciones de $\Gamma p(m)$ que tienen dos raíces distintas.

*b)* Existe $p - 1/2$ ecuaciones de $\Gamma p(m)$ que no admiten solución.

*e)* Existe una única ecuación de $\Gamma p(m)$ que tiene una raíz doble.

*Demostración:* Basta ver *c)*, para ello $D = 0$, pero $D = (\overline{2m})^2 + (p - n)$, tenemos que $(\overline{2m})^2 + (p - n) = 0$, es decir $(\overline{2m})^2 = n$, pero al ser $m$ fijo sólo hay un valor de $n \in \Gamma p$ que verifique la igualdad, por tanto, sólo hay una ecuación de raíces dobles.

## BIBLIOGRAFIA

1. Van Der Waerden. *Modern Algebra.* Vol. I.

2. Samuel, Pierre. *Theorie Alg. des Nombres.*

3. Godement, Roger. *Cours d'Algebre.*

(R. 8 - V - 68)