RAÍCES CUADRADAS EN $\mathbb{F}_p^*$

(p IMPAR)

DADO $a \in \mathbb{F}_p^*$, QUEREMOS

- SABER SI $a \equiv \square \ (p)$
- EN TAL CASO, HALLAR $b \in \mathbb{F}_p^*$ / $b^2 \equiv a \ (p)$

OBS:
- A LO SUMO HAY DOS TALES b, YA QUE UN TAL b ES RAÍZ DEL POLINOMIO $x^2 - a \in \mathbb{F}_p[X]$, QUE TIENE GRADO 2.
- SI b ES SOL, ENTONCES $-b$ TAMBIÉN

$\rightsquigarrow$ SI $a \equiv \square \ (p)$, TIENE DOS (EXACTAMENTE) RAÍCES $\square$.

DEF (SÍMBOLO DE LEGENDRE): SEA $a \in \mathbb{F}_p^*$.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{si } a \equiv \square \ (p) \\ -1, & \text{si } a \not\equiv \square \ (p) \end{cases}$$

LO EXTENDEMOS A $\mathbb{F}_p$ PONIENDO $\left(\frac{0}{p}\right) := 0$.

PROP: $\left(\frac{*}{p}\right)$ ES MULTIPLICATIVO. ES DECIR,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

(EN OTRAS PALABRAS, $\mathbb{F}_p^* \to \{\pm 1\}$ ES MORF.; $a \mapsto \left(\frac{a}{p}\right)$)

DEM:
- SI $a \equiv x^2$ Y $b \equiv y^2$, ENTONCES $ab \equiv (xy)^2$
- SI $a \equiv x^2$ Y $ab \equiv$ [illegible] y^2, ENTONCES $b \equiv (y/x)^2$

$\rightsquigarrow$ RESTA VER QUE SI $a, b \not\equiv \square$, ENTONCES ab [illegible] $\equiv \square$...

LEMA: SEA g PRIMITIVA. SEAN $x \in \mathbb{Z}$, Y SEA $a = g^x$.
ENTONCES, $a \equiv \square \pmod{p}$ SII x ES PAR.

DEM: $\Leftarrow$) SI $x = 2y$, ENTONCES $(g^y)^2 \equiv a$.

$\Rightarrow$) EJERCICIO.

$\boxtimes_{\text{LEMA}}$

TAL x ES ÚNICO MOD $p-1$; POR ESO ESTÁ BIEN HABLAR SOBRE SU PARIDAD...

AHORA SÍ: SUP $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right) = -1$. ENTONCES,

$a = g^x$, $b = g^y$, CON x, y IMPARES.

LUEGO, $ab = g^{x+y}$ ES UN CUADRADO, PUES $x+y$ ES PAR.

$\boxtimes_{\text{PROP}}$

EJEMPLO: SEA $f(X) = aX^2 + bX + c \in \mathbb{F}_p[X]$.
SEA $D = b^2 - 4ac$. ENTONCES, LA CANTIDAD DE RAÍCES DE f ES $1 + \left(\frac{D}{p}\right)$.

LEY DE RECIPROCIDAD CUADRÁTICA (GAUSS):

SEAN p, q PRIMOS IMPARES. ENTONCES,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

DEM: NO ES FÁCIL...

EJEMPLO:

$$\left(\frac{3}{31}\right) = \left(\frac{31}{3}\right)(-1)^{\frac{(3-1)(31-1)}{4}} = \underbrace{\left(\frac{1}{3}\right)}_{1}\underbrace{(-1)^{\frac{60}{4}}}_{-1} = -1$$

↓ "DIFÍCIL", 31 ES GRANDE

1: "FÁCIL", 3 ES CHICO

−1: FÁCIL

CALCULAR EL SÍMBOLO DE LEGENDRE ES FÁCIL.

PROP: $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

DEM: • SI $\left(\frac{a}{p}\right)=1$: ESCRIBAMOS $a=b^2$. ASÍ,

$a^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \ (p)$, POR FERMAT.

• SI $\left(\frac{a}{p}\right)=-1$: EJERCICIO.

∎

SABIENDO QUE $\left(\frac{a}{p}\right)=1$, ¿CÓMO HALLAMOS UNA RAÍZ CUADRADA DE a?

VEREMOS: SI $p \equiv 3 \ (4)$, $b = a^{\frac{p+1}{4}}$ SIRVE.

(EN EL PRÁCTICO)

EJEMPLO: SUPONGAMOS $p \equiv 5 \ (8)$ (Y POR LO TANTO $p \equiv 1 \ (4)$).

ENTONCES, $m = \frac{p+3}{8}$ ES ENTERO.

→ QUEDA ENTONCES EL CASO $p \equiv 1 \ (8)$ (DIFÍCIL)

SEA $x = a^{\frac{p+3}{8}}$, Y SEA $c = x^2$.

AFIRMO: $c \equiv \pm a \ (p)$.

DEM: BUP $(c/a)^2 \equiv 1 \ (p)$. EN EFECTO,

$$(c/a)^2 = \frac{a^{\frac{p+3}{2}}}{a^2} = a^{\frac{p-1}{2}} \equiv 1 \ (p) \ \checkmark$$

SI $c \equiv a \ (p)$, LISTO. ¿QUÉ PASA SI $c \equiv -a \ (p)$?

$\rightsquigarrow$ SI d ES TAL QUE $d^2 \equiv -1 \ (p)$, ENTONCES

$(dx)^2 \equiv (-1)(-a) \ (p)$, Y LISTO!

OBS: UN TAL d EXISTE PUES $p \equiv 1 \ (4)$ (VER PRÁCTICO)

¿CÓMO HALLARLO?

VALE: $p \equiv 1 \ (4) \Rightarrow$ ESTA EC. TIENE SOL.

EJ: SI $p = \alpha^2 + \beta^2$ CON $\alpha, \beta \in \mathbb{Z}$, ENTONCES

$0 \equiv \alpha^2 + \beta^2 \ (p) \Rightarrow \quad -1 \equiv (\alpha/\beta)^2 \ (p) \ldots$

ADEMÁS: SI $|\alpha, \beta|$ ES SOL, ENTONCES

$|\alpha|, |\beta| < \sqrt{p}$; ESTO NOS DA UNA CAJA "CHICA" EN LA QUE BUSCAR LA SOL...