Quiz 2 Mariana Rizo Z. A01423985

1.- $a, b \in \mathbb{Z}$ p y primo

$mcd(a,p) = mcd(b,p) = 1$

entonces

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$$

$$\left(\frac{ab^2}{p}\right) = \left(a^{\frac{p-1}{2}}\right)\left(b^{\frac{p-1}{2}}\right)^2 \pmod p$$

$$= \left(a^{\frac{p-1}{2}}\right)\left(b^{p-1}\right) \pmod p$$

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

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

$\square$

2.- a) 17

$1^2 \equiv 1$	$6^2 \equiv 2$	$11^2 \equiv 2$	$16^2 \equiv 1$
$2^2 \equiv 4$	$7^2 \equiv 15$	$12^2 \equiv 8$	$17^2 \equiv 0$
$3^2 \equiv 9$	$8^2 \equiv 13$	$13^2 \equiv 16$	Residuos:
$4^2 \equiv 16$	$9^2 \equiv 13$	$14^2 \equiv 9$	$\{1, 2, 4, 8, 9, 13, 15, 16\}$
$5^2 \equiv 8$	$10^2 \equiv 15$	$15^2 \equiv 4$	

b) 13

$1^2 \equiv 1$	$3^2 \equiv 9$	$5^2 \equiv 12$	$7^2 \equiv 10$	$9^2 \equiv 3$	$11^2 \equiv 4$
$2^2 \equiv 4$	$4^2 \equiv 3$	$6^2 \equiv 10$	$8^2 \equiv 12$	$10^2 \equiv 9$	$12^2 \equiv 1$

Residuos: $\{1, 3, 4, 9, 10, 12\}$

3.- $Q = (4,5)$ $\quad P = (16,5)$ $\quad E: y^2 = x^3 + 9x + 17$

en $\mathbb{F}_{23}$

$Q = kP \quad k = 9$

$2P$

$$x_3 = \left(\frac{3(16)^2 + 9}{2(5)}\right)^2 - 2(16)$$

$$= \left(\frac{3(3) + 9}{10}\right)^2 - 9 = \left(\frac{18}{10}\right)^2 - 9 = (11)^2 - 9$$

$$= 6 + 14 = 20$$

$$y_3 = 11(16 - 20) - 5 = 11(19) + 18 = 2 + 18 = 20$$

$4P = (20,20) \oplus (20,20)$

$$x_3 = \left(\frac{3(20)^2 + 9}{2(20)}\right)^2 - 2(20) = \left(\frac{3(9) + 9}{17}\right)^2 - 17$$

$$= \left(\frac{13}{17}\right)^2 + 6 = (17)^2 + 6 = 13 + 6 = 19$$

$$y_3 = 17(20 - 19) - 20 = 17 + 3 = 20$$

$8P = (19,20) \oplus (19,20)$

$$x_3 = \left(\frac{3(19)^2 + 9}{2(20)}\right)^2 - 2(19) = \left(\frac{3(16) + 9}{17}\right)^2 - 15$$

$$= \left(\frac{2 + 9}{17}\right)^2 - 15 = \left(\frac{11}{17}\right)^2 + 8 = (2)^2 + 8$$

$$= 12$$

$$y_3 = (12)(19 - 12) - 20 = 14 + 3 = 17$$

$P \oplus rP = (16, 5) \oplus (12, 17)$

$x_3 = \left(\frac{17-5}{12-16}\right)^2 - 16 - 12 = \left(\frac{12}{-4}\right)^2 - 28$

$= (-3)^2 + 18 = 9 + 18 = 4$

$y_3 = -3(16-4) - 5 = -3(12) - 5$

$= 10 + 5 = 5$

$= (4, 5)$ $\square$

4 = $(q, a, b, P, n) = (13, 10, 6, (5, 5), 7)$

$\alpha = 4$ $\beta = 8$ ¿llave pública?

$4(5, 5)$ F_{13} $q = 10$

$2(5, 5)$

$x_3 = \left(\frac{3(5)^2 + 10}{2(5)}\right)^2 - 2(5) = \left(\frac{85}{10}\right)^2 - 10 = \left(\frac{7}{10}\right)^2 - 10$

$= (2)^2 - 10 = 4 + 3 = 7$

$y_3 = 2(5-7) - 5 = -4 - 5 = -9 = 4$

$4P = 2(7, 4)$

$x_3 = \left(\frac{3(7)^2 + 10}{2(4)}\right)^2 - 2(7) = \left(\frac{1}{8}\right)^2 - 1 = 5^2 - 1$

$25 - 1 = 11$

$y_3 = 5(7-11) - 4 = -20 - 4 = -24 = 2$

$4P = (11, 2) = Q_A$

$\beta Q_A = \gamma Q_4 = 8(4P)$

$2(4P) = (11,2) \oplus (11,2)$

$x_3 = \left(\frac{3(11)^2+10}{2(2)}\right)^2 - 2(11) = \left(\frac{9}{4}\right)^2 - 9$

$= (12)^2 + 4 = 1 + 4 = 5$

$y_3 = 12(11-5) - 2 = 12(6) - 2 = 7 - 2 = 5$

$8P = (5,5) = P$

y sabemos que $32P = 4(8P) = 4(P)$

entonces $\beta Q_A = 8 Q_A = 4P = (11,2)$

$\therefore$ la clave pública es $(11,2)$

5.- $3x^2 - 2x + c \equiv 0 \pmod{p}$

$4(3)\{3x^2 - 2x + c\} \equiv 0 \pmod{p}$

$36x^2 - 24x + 12c \equiv 0 \pmod{p}$

$(6x-2)^2 + 12c - 4 \equiv 0 \pmod{p}$

$(6x-2)^2 \equiv 4 - 12c \pmod{p}$

$12c \equiv 4 - (6x-2)^2 \pmod{p}$

$c \equiv (12^{p-2})(4 - (6x-2)^2) \pmod{p}$

$c \equiv (12^{p-2})(4 - (36x^2 - 12x + 4)) \pmod{p}$

$\equiv (12^{p-2})(-36x^2 + 12x) \pmod{p}$

$\equiv 12(1^{p-2})(-3x^2 + x) \pmod{p}$

$c \equiv 12(-3x^2 + x) \pmod{p}$

b) $\mathbb{Z}_{31}$ $\quad x^2-2x+6 \equiv 0 \pmod{31}$

$$4x^2-8x+24 \equiv 0 \pmod{31}$$

$$(2x-2)^2+20 \equiv 0 \pmod{31}$$

$$(2x-2)^2 \equiv -20 \pmod{31}$$

$$(2x-2)^2 \equiv 11 \pmod{31}$$

Los residuos cuadráticos de 31 son:

$\{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}$

Ya que 11 no se encuentra dentro de estos valores,

la congruencia no es soluble.