Quiz 2

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

$\gcd(a,p) = \gcd(b,p) = 1$

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

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

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

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

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

2 Residuos cuadráticos de a) 17, b) 13

a) 17

$1^2 \equiv 1 \bmod 17$	$9^2 \equiv 13 \bmod 17$
$2^2 \equiv 4 \bmod 17$	$10^2 \equiv 15 \bmod 17$
$3^2 \equiv 9 \bmod 17$	$11^2 \equiv 2 \bmod 17$
$4^2 \equiv 16 \bmod 17$	$12^2 \equiv 8 \bmod 17$
$5^2 \equiv 8 \bmod 17$	$13^2 \equiv 16 \bmod 17$
$6^2 \equiv 2 \bmod 17$	$14^2 \equiv 9 \bmod 17$
$7^2 \equiv 15 \bmod 17$	$15^2 \equiv 4 \bmod 17$
$8^2 \equiv 13 \bmod 17$	$16^2 \equiv 1 \bmod 17$

Residuos $\{1, 2, 4, 8, 9, 13, 15, 16\}$

b) 13

$1^2 \equiv 1 \bmod 13$	$7^2 \equiv 10 \bmod 13$
$2^2 \equiv 4 \bmod 13$	$8^2 \equiv 12 \bmod 13$
$3^2 \equiv 9 \bmod 13$	$9^2 \equiv 3 \bmod 13$
$4^2 \equiv 3 \bmod 13$	$10^2 \equiv 9 \bmod 13$
$5^2 \equiv 12 \bmod 13$	$11^2 \equiv 4 \bmod 13$
$6^2 \equiv 10 \bmod 13$	$12^2 \equiv 1 \bmod 13$

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

3. Dados $Q=(4,5)$, $P(16,5)$ en $y^2 = x^3+9x+17$ sobre F_{23}

$Q = kp$

$2P$: $x_3 = \left(\frac{3(16)^2+9}{2(5)}\right)^2 - 2(16) = \left(\frac{3(3)+9}{10}\right)^2 - 9 = \left(\frac{18}{10}\right)^2 - 9 = (11)^2 - 9 = 6+14 = 20$

$y_3 = 11(16-20) - 5 = 11(10)+18 = 2+18 = 20$

$4P$: $x_3 = \left(\frac{3(20)^2+9}{2(20)}\right)^2 - 2(20) = \left(\frac{3(9)+9}{17}\right)^2 - 17 = \left(\frac{13}{17}\right)^2 - 6 = (17)^2+6 = 13+6 = 19$

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

$8P$: $x_3 = \left(\frac{3(19)^2+9}{2(20}\right)^2 - 2(19) = \left(\frac{3(16)+9}{17}\right)^2 - 15 = \left(\frac{217}{17}\right)^2 - 15 = \left(\frac{11}{17}\right)^2 + 8 = (2)^2+8 = 12$

$y_3 = (2)(19-12) - 20 = 14+3 = 17$

$9P$: $x_3 = \left(\frac{17-5}{12-16}\right)^2 - 16 - 12 = \left(\frac{12}{-4}\right)^2 - 28 = (-3)^2 + 18 = 9+18 = 4$

$y_3 = -3(16-4) - 5 = -3(12) - 5 = 10 - 5 = 5$

$k = 9$

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

q: cuerpo finito

$a, b \in F_q$ definen E sobre F_q / $y^2 = x^3+ax+b$ si la característica del cuerpo finito es distinta de 2 y 3 o $y^2 + xy = x^3 + ax^2 + b$ si la característica es 2.

Elementos $x_p, y_p \in F_q$ definen $P = (x_p, y_p) \in E(F_q)$. P es el punto base.

Orden n de P.

Alice escoge $\alpha = 4$, Bob $\beta = 8$ ¿Clave pública?

$2P$: $x_3 = \left(\frac{3(5)^2+10}{2(5)}\right)^2 - 2(5) = \left(\frac{85}{10}\right)^2 - 10 = \left(\frac{7}{10}\right)^2 - 10 = (2)^2 - 10 = 4+3 = 7$

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

$4P$: $x_3 = \left(\frac{3(7)^2+10}{2(4)}\right)^2 - 2(7) = \left(\frac{1}{8}\right)^2 - 1 = 5^2 - 1 = 24 = 11$

$y_3 =$

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

$2(4P)$.

$$x_3 = \left(\frac{3(11)^2+b}{2(2)}\right)^2 - 2(11) = \left(\frac{9}{4}\right)^2 - 9 = (12)^2 + 4 = 1+4 = 5$$

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

$P = 8P = (5,5)$ También $32P = 4(8P) = 4P$

$$\therefore \cancel{\beta} Q_A = 8Q_A = 4P = \underline{(11,2)}$$

5. a) Sea p primo impar. Encontrar los valores de c para que la congruencia $3x^2 - 2x + c \equiv 0 \bmod p$ tenga solución.

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

$$36x^2 - 24x + 12c \equiv 0 \bmod p$$

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

$$(6x-2)^2 \equiv 4 - 12c \bmod p$$

$$12c \equiv 4 - (6x-2)^2 \bmod p$$

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

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

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

$$c \equiv 12(-3x^2 + x) \bmod p$$

b) Analizar si tiene solución la congruencia en $p = 31$

$$x^2 - 2x + 6 \equiv 0 \bmod 31$$

$\mathbb{Z}_{31}$

$$x^2 - 2x + 6 \equiv 0 \bmod 31$$

$$4x^2 - 8x + 24 \equiv 0 \bmod 31$$

$$(2x-2)^2 + 20 \equiv 0 \bmod 31$$

$$(2x-2)^2 \equiv -20 \bmod 31$$

$$(2x-2)^2 \equiv 11 \bmod 31$$

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

$11 \notin$ Residuos

$\therefore$ La congruencia no es soluble.