# Tercer tarea

Manuel Díaz Díaz y Gerardo Rubén López Hernández

December 4, 2022

1) Dada la curva $y^2 = x^3 + x + 1 mod(103)$ y el punto $(6, 29)$ aplique el teorema de Hasse o el teorema con que se obtiene el orden del grupo, para obtener el orden del grupo de puntos de la curva y obtenga todos sus puntos.

2) Dada la curva $y^2 = x^3 + x + 1 mod(10403)$ , encuentre un factor de 10403.

3) Dada la Curva $y^2 = x^3 + x + 4 mod(53)$ y la curva $y^2 = x^3 + 16x + 11 mod(53)$ muestre que son isomorfas y de el isomorfismo.

4) Sea la curva $y^2 = x^3 + x + 1 mod(71)$ y el punto $P = (18, 61)$ encuentre $m$ tal que $mP = (59, 6)$.

   Dado el cifrado en Ecies con parámetros $E(y^2 = x^3 + x + 1, (18, 61), m, (59, 6), 71)$ descifre el siguiente mensaje. Los caracteres son tomados módulo 26, es decir a=0=26, b=1,..., z=25:

   ((23,0),21),((13,1),47),((9,1),57),((44,0),25),((39,1)11),((64,1),53),((5,1),26)

5) Describa tres ataques cibernéticos y en que consiste el computo forense.