Introducción a la Teoría de Números
6. Formas Cuadráticas — Curvas Elípticas

1. ¿Cuáles de los siguientes números son suma de dos cuadrados? Escribir aquellos que lo sean como suma de dos cuadrados.

$$-389,\ 12345,\ 91210,\ 729,\ 1729,\ 68252$$

2. Encontrar un entero positivo que tenga por lo menos tres representaciones diferentes como suma de dos cuadrados, sin contar signos ni orden de los sumandos.

3. Escribir 2001 como suma de tres cuadrados.

4. Mostrar que si un número natural es suma de dos cuadrados racionales, entonces también es suma de dos cuadrados enteros.

5. Sea p un primo impar. Mostrar que $p = x^2 + 2y^2$ si y sólo si $p \equiv 1, 3 \pmod 8$.

6. Mostrar que dados cuatro enteros consecutivos cualesquiera, al menos uno de ellos no se representa como suma de dos cuadrados.

7. Un *número triangular* es un número que es suma de los primeros m enteros para algún $m > 0$. Si n es un número triangular, mostrar que $8n^2$, $8n^2 + 1$ y $8n^2 + 2$ pueden ser escritos como suma de dos cuadrados.

8. Mostrar que $13x^2+36xy+25y^2$ y $58x^2+82xy+29y^2$ son equivalentes a la forma x^2+y^2, y encontrar enteros x e y tales que $13x^2 + 36xy + 25y^2 = 389$.

9. ¿Cuáles son los discriminantes de las formas $199x^2-162xy+33y^2$ y $35x^2-96xy+66y^2$? ¿Son equivalentes?

10. Escribir una ecuación $E:\ y^2 = x^3+ax+b$ sobre un cuerpo K tal que $-16(4a^3+27b^2) = 0$. ¿Qué es lo que falla al tratar de definir la ley de grupo en $E(K)$?

11. Una solución racional a la ecuación $y^2 = x^3 - 2$ es $(3, 5)$. Encontrar otra solución racional (con $x \neq 3$) considerando la recta tangente en $(3, 5)$.

12. Sea E la curva elíptica sobre el cuerpo finito $K = \mathbb{Z}/5\mathbb{Z}$ definida por

$$y^2 = x^3 + x + 1.$$

    (a) Listar los 9 elementos de $E(K)$.

    (b) ¿Cuál es la estructura de $E(K)$ como producto de grupos cíclicos?

13. Sea E la curva elíptica definida por la ecuación $y^2 = x^3 + 1$. Para cada primo $p \geq 5$, sea N_p el cardinal de $E(\mathbb{Z}/p\mathbb{Z})$. Por ejemplo, $N_5 = 6$, $N_7 = 12$, $N_{11} = 12$, $N_{13} = 12$, $N_{17} = 18$, $N_{19} = 12$, $N_{23} = 24$, $N_{29} = 30$. Enunciar una conjetura para el valor de N_p cuando $p \equiv 2 \pmod p$.