Seminario de Curvas Elípticas
1. Cúbicas racionales

Página del seminario: `http://www.cmat.edu.uy/~tornaria/2007/ELL/`

1. Leer la introducción del libro de Silverman y Tate.
2. Mostrar que $x^2 + y^2 = 3$ no tiene puntos racionales:
   (a) Ver que alcanza probar que
   $$X^2 + Y^2 = 3Z^2$$
   no tiene solución con X, Y, Z enteros sin factores comunes.
   (b) Ver que X e Y no pueden ser divisibles por 3.
   (c) Concluir que $X^2 + Y^2$ no puede ser múltiplo de 3.
3. Leer la demostración de que una curva elíptica es un grupo conmutativo en el libro de Silverman y Tate (p. 18–20).
4. Leer el ejercicio 1.11 de Silverman y Tate (p. 34).
5. Considerar la curva $y^2 = f(x)$, siendo f un polinomio de grado 3 con coeficientes racionales.
   (a) Mostrar que los puntos singulares son los puntos de la forma $(x, 0)$ con x una raíz múltiple de f.
   (b) Concluir que los puntos singulares son racionales (sugerencia: las raices dobles de un polinomio racional de grado 3 son necesariamente racionales).
6. Leer los ejercicios 1.15 y 1.16 de Silverman y Tate (p. 35–36).
7. En este ejercicio se demuestra la Conjetura de Fermat para $n = 4$. Si $x^4 + y^4 = z^4$ tiene solución en enteros positivos, entonces también $x^4 + y^4 = w^2$ tendrá solución. Sea x, y, w una tal solución con w el mínimo posible. Entonces x^2, y^2, w es una terna pitagórica primitiva. Asumiendo (sin pérdida de generalidad) que x es impar, podemos escribir
   $$x^2 = m^2 - n^2, \qquad y^2 = 2mn, \qquad w = m^2 + n^2,$$
   con m y n enteros positivos relativamente primos, no ambos impares.
   (a) Mostrar que
   $$x = r^2 - s^2, \qquad n = 2rs, \qquad m = r^2 + s^2,$$
   con r y s enteros positivos relativamente primos, no ambos impares.
   (b) Mostrar que r, s, y m son relativamente primos dos a dos. Usando que $y^2 = 4rsm$ concluir que r, s, y m son todos cuadrados, digamos a^2, b^2, y c^2.
   (c) Mostrar que $a^4 + b^4 = c^2$, y que esto contradice la minimalidad de w.