Folhas de exercícios VII

Fernando Ferreira

Introdução à Teoria dos Números
2018/2019

1. Seja E a seguinte curva elíptica sobre os racionais: $y^2 = x^3 + 17$. Considere os pontos $P = (-1, 4)$ e $Q = (2, 5)$.

   (a) Verifique que estes pontos estão na curva

   (b) Calcule $P + Q$ e $P - Q$.

   (c) Calcule $2Q$.

2. Uma solução racional da equação $y^2 = x^3 - 2$ é $(3, 5)$. Encontre uma solução racional com $x \neq 3$ considerendo a linha tangente a este ponto e computando o segundo ponto de interseção.

3. Seja E a seguinte curva elíptica sobre o corpo $\mathbb{Z}/13\mathbb{Z}$: $y^2 = x^3 + 3x + 8$.

   (a) Verifique que os pontos $(1, 5)$, $(1, 8)$ e $(9, 7)$ estão na curva.

   (b) Liste os nove elementos de $E(\mathbb{Z}/13\mathbb{Z})$. (Sugestão: para facilitar as contas (1) ache os quadrados de $\mathbb{Z}/13\mathbb{Z}$; (2) percorra x com os valores de $\mathbb{Z}/13\mathbb{Z}$ e veja quando os valores $x^3 + 3x + 8$ são quadrados; (3) não se esqueça do $\mathcal{O}$.)

   (c) Calcule $(1, 8) + (9, 7)$ e $(1, 5) + (1, 8)$.

4. Seja E a seguinte curva elíptica sobre os racionais: $y^2 = x^3 - 2x + 4$. Considere os pontos $P = (0, 2)$ e $Q = (1/4, 15/8)$.

   (a) Verifique que estes pontos estão na curva.

   (b) Calcule $P + Q$. Interprete o resultado geometricamente.

5. Seja E a curva elíptica sobre o corpo finito $K = \mathbb{Z}/5\mathbb{Z}$ definida pela equação $y^2 = x^3 + x + 1$.

   (a) Liste os nove elementos de $E(K)$.

   (b) Qual a estrutura de $E(K)$ como produto de grupos cíclicos?

6. Seja E uma curva elíptica sobre $\mathbb{R}$. Mostre que o grupo $E(\mathbb{R})$ não é finitamente gerado.

7. Seja p um primo congruente com 2 módulo 3. Considere E_p a curva elíptica sobre o corpo finito $\mathbb{Z}/p\mathbb{Z}$ definida pela equação $y^2 = x^3 + 1$. O objetivo deste exercício é demonstrar que a cardinalidade de E_p é $p + 1$.

   (a) Mostre que a aplicação de $(\mathbb{Z}/p\mathbb{Z})^*$ para si próprio dada por $x \rightsquigarrow x^3$ é sobrejetiva. (Sugestão: use o pequeno teorema de Fermat.)

   (b) Demonstre o objetivo deste exercício tendo em atenção que a aplicação de $\mathbb{Z}/p\mathbb{Z}$ para si próprio dada por $x \rightsquigarrow x^3 + 1$ é uma bijeção.

8. Suponha que a equação $y^2 = x^3 + ax + b$, com $a, b \in \mathbb{Q}$, define uma curva elíptica. Mostre que existe outra equação $y^2 = x^3 + Ax + B$, com $A, B \in \mathbb{Z}$ cujas soluções (racionais) estão em bijeção com as soluções (racionais) de $y^2 = x^3 + ax + b$.