Folhas de exercícios V

Fernando Ferreira

Introdução à Teoria dos Números
2018/2019

1. (a) Seja p um primo ímpar. Mostre que um polinómio $X^2 + bX + c \in (\mathbb{Z}/p\mathbb{Z})[X]$ tem raízes em $\mathbb{Z}/p\mathbb{Z}$ se, e somente se, b^2-4c é um quadrado módulo p.

   (b) Seja K um corpo de característica diferente de 2. Em que condições é que um polinómio $X^2 + bX + c \in K[X]$ tem raízes em K?

2. Seja $n = mr$ com $m, r \in \mathbb{N} \setminus \{1\}$ e $m \perp r$. Considere-se $a \in \mathbb{Z}$ tal que $a \perp n$. Mostre que a é resíduo quadrático módulo n se, e somente se, a é resíduo quadrático módulo m e a é resíduo quadrático módulo r.

3. Seja p um primo ímpar. Mostre que, para qualquer inteiro m coprimo com p, o número de soluções da equação $x^2 \equiv m \pmod{p}$ é $1 + \left(\frac{m}{p}\right)$.

4. Calcule os seguintes símbolos de Legendre: $\left(\frac{3}{97}\right)$, $\left(\frac{3}{389}\right)$, $\left(\frac{5!}{7}\right)$, $\left(\frac{19}{31}\right)$, $\left(\frac{11}{37}\right)$, $\left(\frac{97}{101}\right)$, $\left(\frac{31}{167}\right)$ e $\left(\frac{5}{160465489}\right)$.

5. Seja p primo com $p \equiv 3 \pmod{4}$ e considere-se a, com $a \perp p$, um resíduo quadrático. Mostre que $a^{(p+1)/4}$ é uma raiz quadrada de a módulo p. (Sugestão: use o critério de Euler.)

6. Use a lei da reciprocidade quadrática de Gauss para mostrar que, para p primo com ≥ 5,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1, 11 \pmod{12} \\ -1 & \text{se } p \equiv 5, 7 \pmod{12} \end{cases}$$

7. Use a lei da reciprocidade quadrática para caracterizar os primos p, com $p > 5$, para os quais 5 é resíduo quadrático. (Sugestão: inspire-se no exercício anterior.)

8. Mostre que 7 é um resíduo quadrático módulo um primo ímpar p diferente de 7 se, e somente se, p é congruente com 1, 3, 9, 19, 25 ou 27 módulo 28. (Sugestão: inspire-se nos exercícios anteriores.)

9. Sejam m e n números naturais ímpares. Mostre que $\frac{mn-1}{2}$ tem a mesma paridade que $\frac{m-1}{2} + \frac{n-1}{2}$.

10. Calcule o símbolo de Jacobi $\left(\frac{123}{917}\right)$. Deste cálculo pode concluir que 123 é resíduo módulo 917 ou que 123 é não resíduo quadrático módulo 917?

11. Calcule os seguintes símbolos de Legendre sem fatorizar números (excetuando fatores que são potências de 2): $\left(\frac{91}{167}\right)$, $\left(\frac{1801}{8191}\right)$, $\left(\frac{3083}{3911}\right)$ e $\left(\frac{43691}{65537}\right)$.

12. Usando o critério de Euler, calcule $4^{48} \pmod{97}$. Note que 97 é primo.

13. Mostre que a equação $x^2 \equiv 5 \pmod{2^{13}-1}$ tem duas soluções nos naturais x com $x < 2^{13}$. (Note que $2^{13}-1$ é um número primo.)

14. Seja p um número primo ímpar. Use o facto do grupo $(\mathbb{Z}/p\mathbb{Z})^*$ ser cíclico para mostrar diretamente que $\left(\frac{-3}{p}\right) = 1$ quando $p \equiv 1 \pmod{3}$. (Sugestão: há um elemento $c \in (\mathbb{Z}/p\mathbb{Z})^*$ de ordem 3 (justifique); mostre que $(2c+1)^2 = -3$.)

15. Seja p primo ímpar tal que $p \equiv 1 \pmod{5}$. Mostre diretamente que $\left(\frac{5}{p}\right) = 1$ pelo método do exercício anterior. (Sugestão: tome-se $c \in (\mathbb{Z}/p\mathbb{Z})^*$ de ordem 5 e mostre que $(c+c^4)^2 + (c+c^4) - 1 = 0$, etc.)

16. Seja p um primo ímpar. Mostre que se q é primo e $q \mid (2^p - 1)$, então $q \equiv \pm 1 \pmod{8}$. (Sugestão: mostre que $2^{(p+1)/2}$ é uma raíz quadrada de 2 módulo q.)

17. Sejam p e $2p+1$ ambos números primos (diz-se que p é um primo de Sophie Germain). Suponha que $p \equiv 3 \pmod{4}$.

    (a) Mostre que $2^p \equiv 1 \pmod{2p+1}$. (Sugestão: calcule $\left(\frac{2}{2p+1}\right)$ de duas formas distintas.)

    (b) Mostre que $2^{251} - 1$ não é primo de Mersenne.

18. Mostre que 3 é um não resíduo quadrático módulo os primos de Mersenne maiores do que 3.

19. Seja p um primo ímpar. Mostre que o produto P de todos os resíduos quadráticos $\pmod{p}$ satisfaz $P \equiv (-1)^{(p+1)/2} \pmod{p}$. (Sugestão: se g é raiz primitiva módulo p, então g^2, g^4, g^6, ..., g^{p-1} são os resíduos quadráticos módulo p.)

20. (a) Seja K um corpo, $b \in K$ e $n \in \mathbb{N}$ ímpar. Mostre que

$$b^n + 1 = (b+1)(b^{n-1} - b^{n-2} + \ldots b^2 - b + 1).$$

    (b) Um *primo de Fermat* é um primo da forma $2^n + 1$, com $n \in \mathbb{N}$. Mostre que se $2^n + 1$ é um primo de Fermat então n é uma potência de 2.

    (c) Seja $F_n = 2^{2^n} + 1$. Fermat conjeturou que todos os números desta forma são primos. De facto, F_0, F_1, F_2, F_3 e F_4 são primos (calcule-os!). Mas F_5 não é primo (vá à Wikipédia para ver a fatorização de F_5 obtida por Euler). Não se sabe se há mais primos de Fermat.

21. Seja p um primo de Fermat.

    (a) Mostre que cada não resíduo quadrático módulo p é um gerador de $(\mathbb{Z}/p\mathbb{Z})^*$.

    (b) Mostre que 5 é gerador de $(\mathbb{Z}/p\mathbb{Z})^*$, exceto quando $p = 5$.

22. Seja a um inteiro positivo e p e q primos ímpares com $p \perp a$ e $q \perp a$ tais que $p + q \equiv 0 \pmod{4a}$.

    (a) Mostre primeiro que se a é ímpar, então $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

    (b) Mostre que $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

23. (a) Dado um número natural k, então $\left(\frac{-3}{6k-1}\right) = -1$.

    (b) Seja n um número inteiro. Dado um número natural k, mostre que $6k - 1$ não divide $n^2 + n + 1$. (Note que $4n^2 + 4n + 4 = (2n + 1)^2 + 3$.)

24. Neste exercício use um computador (por exemplo, o programa SAGE).

    (a) Aplique o teste de Solovay-Strassen ao número 56052361 para várias bases. Que conclusão é que pode tirar?

    (b) Aplique o teste de Solovay-Strassen ao número 2301745249 para várias bases. Que conclusão é que pode tirar?

    (c) Aplique o teste de Solovay-Strassen ao número 7427466391 para várias bases. Que conclusão é que pode tirar?

25. Quais são os números naturais menores do que 20 que são soma de dois quadrados inteiros? E de três quadrados? E de quatro quadrados?

26. Mostre que de quatro inteiros consecutivos, pelo menos um deles não é soma de dois quadrados naturais. (Sugestão: considere os quadrados módulo 8.)

27. Mostre que se um número natural é soma de dois quadrados racionais então é soma de dois quadrados naturais. (Sugestão: use a caracterização dos números naturais que são soma de dois quadrados naturais.)