

Resíduos Quadráticos

Juan Pablo Lins

Semana Olímpica 2026 - N2 - Vitória, ES

Dado um primo $p > 2$, queremos determinar critérios de existência de soluções para a equação

$$x^2 \equiv d \pmod{p}.$$

Se essa equação admite solução (isto é, d é um quadrado perfeito módulo p), dizemos que d é um *resíduo quadrático* módulo p .

Lema 1. *Há exatamente $\frac{p-1}{2}$ resíduos quadráticos módulo p . A saber, são eles*

$$0^2, 1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2 \pmod{p}$$

Definição 1 (Símbolo de Legendre). Dados $p > 2$ primo e $a \in \mathbb{Z}$ qualquer, definimos o *símbolo de Legendre* como

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } p \nmid a \text{ e } a \text{ é um resíduo quadrático módulo } p \\ 0, & \text{se } p \mid a \\ -1, & \text{caso contrário} \end{cases}$$

Proposição 1 (Critério de Euler). *Seja $p > 2$ um primo e $a \in \mathbb{Z}$ qualquer. Então*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Corolário 1 (Propriedades). *O símbolo de Legendre tem as seguintes propriedades:*

- i) *se $a \equiv b \pmod{p}$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
- ii) *$\left(\frac{a^2}{p}\right) = 1$ se $p \nmid a$.*
- iii) *$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, ou seja, -1 é resíduo quadrático módulo p se, e somente se, $p \equiv 1 \pmod{4}$.*
- iv) *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$*

Teorema 1 (Lei da Reciprocidade Quadrática).

1. *Sejam p e q primos ímpares distintos. Então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

2. *Seja p um primo ímpar. Então*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod{8} \\ -1 & \text{se } p \equiv \pm 3 \pmod{8} \end{cases}$$

Problemas

Problema 1. Determine se -90 é resíduo quadrático módulo 1019 ou não.

Problema 2. Calcule $\left(\frac{44}{103}\right)$, $\left(\frac{-60}{1019}\right)$ e $\left(\frac{2010}{1019}\right)$.

Problema 3. Seja $p > 2$ um primo. Mostre que $\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) = 0$.

Problema 4. Sejam p um primo ímpar e c um inteiro que não é múltiplo de p . Prove que

$$\sum_{a=0}^{p-1} \left(\frac{a(a+c)}{p}\right) = -1.$$

Problema 5. Seja p um primo ímpar. Mostre que

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

Problema 6. Seja p um primo. Mostre que existem $x, y \in \mathbb{Z}$ tais que $x^2 + y^2 + 1$ é múltiplo de p .

Problema 7. Existem inteiros m e n tais que

$$5m^2 - 6mn + 7n^2 = 1985 \quad ?$$

Problema 8. Seja $p > 3$ primo. Se existe um inteiro a com $p \mid a^2 - a + 3$, mostre que existe um inteiro b tal que $p \mid b^2 - b + 25$.

Problema 9. Seja p um primo ímpar. Mostre que o menor não resíduo quadrático positivo de p é menor que $\sqrt{p} + 1$.

Problema 10. Sejam M um inteiro e p um primo ímpar. Mostre que a sequência

$$M, M+1, \dots, M+2\lfloor\sqrt{p}\rfloor$$

contém um elemento que não é resíduo quadrático módulo p (e portanto, em particular, não é múltiplo de p).

Problema 11. Seja p um primo. Mostre que

1. se p é da forma $4n+1$ então $p \mid n^n - 1$.
2. se p é da forma $4n-1$, então $p \mid n^n + (-1)^{n+1} \cdot 2n$.

Problema 12. Prove que se $10^{2n} + 8 \cdot 10^n + 1$ tem fator primo da forma $60k+7$, então n e k são pares.

Problema 13 (Ibero 2003). Definem-se as sequências $(a_n)_{n \geq 0}$ e $(b_n)_{n \geq 0}$ por $a_0 = 1$, $b_0 = 4$,

$$a_{n+1} = a_n^{2001} + b_n \quad \text{e} \quad b_{n+1} = b_n^{2001} + a_n, \quad n \geq 0.$$

Demonstre que 2003 não divide nenhum dos termos dessas sequências.

Problema 14. Demonstre que existem infinitos primos da forma $3k+1$ e $3k-1$.

Problema 15. Sejam x e y inteiros positivos. Prove que $4xy - x - y$ não é um quadrado perfeito.

Problema 16. Seja a um inteiro positivo que não é quadrado perfeito. Mostre que existem infinitos primos p para os quais $\left(\frac{a}{p}\right) = -1$.

Problema 17. Seja $F_n = 2^{2^n} + 1$ o n -ésimo número de Fermat.

- (a) (Euler) Prove que todo fator primo de F_n é da forma $k \cdot 2^{n+1} + 1$.
- (b) (Lucas) Prove que, se $n \geq 2$, então todo fator primo de F_n é da forma $k \cdot 2^{n+2} + 1$.
- (c) Mostre que $2^{2^5} + 1$ é composto.

Problema 18. Se n é um inteiro positivo tal que $7n$ é da forma $a^2 + 3b^2$, mostre que n também é.

Problema 19 (Putnam 1991). Seja p um primo ímpar. Quantos elementos tem o conjunto

$$\{x^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\} \cap \{y^2 + 1 \mid y \in \mathbb{Z}/p\mathbb{Z}\}?$$

Problema 20 (Taiwan 1997). Seja $k = 2^{2^n} + 1$ para algum $n \in \mathbb{N}$. Prove que k é primo se, e somente se, k é um divisor de $3^{\frac{k-1}{2}} + 1$.

Problema 21. Prove que $2^n + 1$ não tem fatores primos da forma $8k + 7$.

Problema 22 (TST Turquia 2021). Seja n um inteiro positivo. Prove que o número

$$\frac{20 \cdot 5^n - 2}{3^n + 47}$$

nunca é inteiro.

Problema 23. Mostre que não existem inteiros positivos x e y tais que $x^2 + 3xy - 2y^2 = 122$.

Problema 24 (IMOSL 2012). Encontre todas as triplas (x, y, z) de inteiros positivos tais que $x \leq y \leq z$ e

$$x^3(y^3 + z^3) = 2012(xyz + 2).$$