Resíduos Quadráticos

Guilherme Zeus Moura
zeusdanmou@gmail.com

§1 Teoria

Definição 1 Dizemos que a é *resíduo quadrático* mod n se, e somente se, $x^2 \equiv a$ possui solução mod n.

Proposição 1 Seja p um primo ímpar. Existem exatamente $(p+1)/2$ resíduos quadráticos mod p. Eles são:

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Demonstração. Estes são todos os resíduos quadráticos pois $(p-x)^2 \equiv x^2 \pmod{p}$.

Eles são distintos pois:

$$\begin{aligned} x^2 \equiv y^2 \pmod{p} &\iff p \mid x^2 - y^2 \\ &\iff p \mid (x-y)(x+y) \\ &\iff p \mid (x-y) \text{ ou } p \mid (x+y) \\ &\iff y \equiv \pm x \pmod{p}, \end{aligned}$$

que é impossível para $x, y \in \left\{0, 1, 2, \ldots, \frac{p-1}{2}\right\}$. $\square$

Definição 2 (Símbolo de Legendre) Seja p um primo e $a \in \mathbb{Z}$.

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

Teorema 2 (Critério de Euler) Sejam p um primo ímpar e $a \in \mathbb{Z}$. Então

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

Corolário Sejam p um primo ímpar e $a, b \in \mathbb{Z}$.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Corolário -1 é resíduo quadrático mod p se, e somente se, $p \equiv 1 \pmod{4}$.

Teorema 3 (Lei da Reciprocidade Quadrática) Sejam p e q primos ímpares distintos. Temos:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}};$$
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Usando os dois teoremas a seguir, podemos determinar se a é resíduo quadrático mod n apenas olhando módulo as potências de 2 que dividem n e módulo os primos ímpares que dividem n.

Teorema 4 Sejam p primo ímpar e $a, k \in \mathbb{Z}$ com $k > 0$. Se $x^2 \equiv a \pmod{p^k}$, existe $t \in 0, 1, \ldots, p-1$ tal que $(x+tp)^2 \equiv a \pmod{p^{k+1}}$.

Teorema 5 Sejam a um inteiro ímpar e $n \geq 3$. a é resíduo quadrático mod 2^n se, e somente se, $a \equiv 1 \pmod{8}$.

§2 Problemas

Problema 1 Existe algum polinômio irredutível em $\mathbb{Z}[x]$, mas redutível mod p para todo p primo?

Problema 2 **(Vietnam TST)** Seja $n \in \mathbb{N}$. Prove que $2^n + 1$ não tem fator primo da forma $8k - 1$.

Problema 3 Existem inteiros m, n tais que $5m^2 - 6mn + 7n^2 = 1985$?

Problema 4 Seja p um primo. Mostre que existem inteiros x, y tais que $x^2 + y^2 + 1$ é divisível por p.

Problema 5 **(OBM)** Prove que se $10^{2n} + 8 \cdot 10^n + 1$ tem fator primo da forma $60k + 7$, então n e k são pares.

Problema 6 **(OBM)** Demonstre que, dado um inteiro positivo n qualquer, existem inteiros positivos a e b primos entre si tais que $a^2 + 2017b^2$ possui ao menos n fatores primos distintos.

Problema 7 Prove que para todo inteiro positivo n, qualquer divisor primo de $n^4 - n^2 + 1$ é da forma $12k + 1$.

Problema 8 Sejam x e y inteiros positivos. Prove que $4xy - x - y$ não é quadrado perfeito.

Problema 9 Sejam p um primo ímpar e c um inteiro não múltiplo de p. Prove que

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

Problema 10 Seja p um primo ímpar. Prove que o menor inteiro positivo que não é resíduo quadrático mod p é menor que $\sqrt{p} + 1$.

Problema 11 Seja p um primo. Prove que:

(a) Se p é da forma $4k + 1$, então $p \mid k^k - 1$.

(b) Se p é da forma $4k - 1$, então $p \mid k^k + (-1)^{k+1} 2k$.

Problema 12 **(IMO)** Os inteiros positivos a e b são tais que $15a + 16b$ e $16a - 15b$ são ambos quadrados perfeitos positivos. Encontre o menor valor que pode tomar o menor desses quadrados.

Problema 13 **(IMO)** Prove que existe um número infinito de inteiros positivos n tais que $n^2 + 1$ tem um fator primo maior que $2n + \sqrt{2n}$.

Problema 14 Suponha que $a_1, a_2, \ldots, a_{2019}$ são inteiros positivos tais que $a_1^n + a_2^n + \cdots + a_{2019}^n$ é quadrado perfeito para todos os inteiros positivos n. Qual é a quantidade mínima de a_i's que devem ser iguais a zero?

Problema 15 Encontre todos os inteiros positivos n tais que n é resíduo quadrático mod x, para todo x maior que n.

Problema 16 Encontre todos os inteiros positivos n tais que $2^n - 1 \mid 3^n - 1$.

Problema 17 **(Banco IMO)** Suponha que, para um certo primo p, os valores que o polinômio de coeficientes inteiros $ax^2 + bx + x$ toma $2p - 1$ inteiros consecutivos são quadrados perfeitos. Prove que $p \mid b^2 - 4ac$.

Problema 18 Seja n um inteiro positivo. Prove que $2^{3^n} + 1$ tem ao menos n fatores primos distintos da forma $8k + 3$.

Problema 19 Mostre que, para cada inteiro positivo n, exitem inteiros $k_0, k_1, \ldots, k_n$ maiores que 1 e primos entre si tais que $k_0 k_1 \cdots k_n - 1$ é o produto de dois inteiros consecutivos.

Problema 20 Sejam a e b inteiros positivos. Mostre que $\frac{a^{+1}}{b^2-5}$ não é inteiro.

Referências

1. *Resíduos Quadráticos*, Valentino Amadeus Sichinel.
2. *Quadratic residues*, Brilliant.
   https://brilliant.org/wiki/quadratic-residues/
3. *Teoria dos Números - Um passeio com primos*, Fabio E. Brochero Martinez, Carlos Gustavo T. de A. Moreira, Nicolau C. Saldanha, Eduardo Tengan.