Resíduos Quadráticos

Guilherme Zeus Moura
zeusdanmou@gmail.com

0 Objetivo

Secretamente, o objetivo da aula é confeccionar um material mais completo sobre Resíduos Quadráticos, com a ajuda de vocês.

1 Teoria

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

Exemplo 1
Olhando mod 4, os resíduos quadráticos são 0 e 1. Olhando mod 5, os resíduos quadráticos são 0, 1 e 4. Olhando mod 7, os resíduos quadráticos são 0, 1, 4 e 2.

Proposição 2
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 $x, y \in \left\{0, 1, 2, \ldots, \frac{p-1}{2}\right\}$. □

Definição 3 (Símbolo de Legendre)
Seja p um primo e $a \in \mathbb{Z}$.

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

Exemplo 2
$\left(\frac{1}{5}\right) = 1$. $\left(\frac{2}{5}\right) = -1$.

Teorema 4 (Critério de Euler)
Sejam p um primo ímpar e $a \in \mathbb{Z}$. Então

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

Demonstração. Se a é multiplo de p, então

$$a^{(p-1)/2} \equiv 0 \equiv \left(\frac{a}{p}\right).$$

Se a é resíduo quadrático não nulo, então existe y tal que $a \equiv y^2$. Portanto,

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

Considere o polinômio

$$P(x) = x^{p-1} - 1 = \underbrace{\left(x^{(p-1)/2} - 1\right)}_{Q(x)} \underbrace{\left(x^{(p-1)/2} + 1\right)}_{R(x)}.$$

Como $P(x)$ possui grau $p-1$, ele possui no máximo $p-1$ raízes (contando multiplicidade). Note que $1, 2, \ldots, p-1$ são raízes de $P(x)$ e, consequentemente, são todas as raízes de $P(x)$.

Como $Q(x)$ possui no máximo $(p-1)/2$ raízes e todos os $(p-1)/2$ resíduos quadráticos não nulos são raízes de $Q(x)$, eles são todas as raízes de $Q(x)$.

Desse modo, os não residuos quadraticos não nulos são raízes de $P(x)$, mas não de $Q(x)$, e portanto são raízes de $R(x)$. Logo, para a não multiplo de p e não resíduo quadrático, vale

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

$\square$

Corolário 5
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 6
-1 é resíduo quadrático mod p se, e somente se, $p \equiv 1 \pmod{4}$.

Teorema 7 (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 8

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 9

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?

Solução. Considere o polinômio $P(x) = x^4 + 1$.

$P(x)$ é irredutível em $\mathbb{Z}[x]$, pois se fosse redutível, teria que ser redutível em polínômios de segundo grau. Portanto, seria

$$x^4 + 1 = (x^2 + qx \pm 1)(x^2 + rx \pm 1).$$

Podemos testar que não existem valores de q, r que funcionam.

Já em $\mathbb{Z}_p[x]$:

- Se $p = 2$,
$$x^4 + 1 \equiv (x + 1)^4.$$
- Se -1 é resíduo quadrático ($i^2 \equiv -1$) então
$$x^4 + 1 = x^4 - i^2 = (x^2 + i)(x^2 - i).$$
- Se 2 é resíduo quadrático ($q^2 \equiv 2$) então
$$x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2 + 1)^2 - (qx)^2 = (x^2 + 1 + qx)(x^2 + 1 - qx).$$
- Se -2 é resíduo quadrático ($r^2 \equiv -2$) então
$$x^4 + 1 = x^4 - 2x^2 + 1 - (-2)x^2 = (x^2 + 1)^2 - (rx)^2 = (x^2 - 1 + rx)(x^2 - 1 - rx).$$

Mas,

$$\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right),$$

logo pelo menos um entre -2, 2 ou 1 é resíduo quadrático.

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.

Solução. $4xy - x - y$ é quadrado perfeito se, e somente se, $16xy - 4x - 4y$ é quadrado perfeito. Porém,

$$16xy - 4x - 4y = (4x - 1)(4y - 1) - 1.$$

Suponha que é um quadrado perfeito. Logo, $(4x - 1)(4y - 1) = k^2 + 1$.

Como $4x - 1 \equiv 3 \pmod 4$, existe algum primo $p \equiv 3 \pmod 4$ tal que $p \mid 4x - 1$. Logo,

$$p \mid k^2 + 1,$$

que é um absurdo, pois -1 não é resíduo quadrático mod p, para $p \equiv 3 \pmod 4$.

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.

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.