Resíduos Quadráticos

Como já sabemos, em teoria dos números, propriedades de primos são sempre bem vindas - todas são incrivelmente úteis para nosso estudo de olimpíadas - E uma das propriedas mais interessantes dos nossos queridos primos são os resíduos quadráticos. Você pode já ter ouvido falar deles em problemas de alguma olímpiada e ter se perguntad: afinal, o que é essa técnica e o que de interessante ela nos traz? Com esse material, esperamos que você não precise mais se perguntar nada sobre resíduos quadráticos!

• 1: Afinal, o que são os resíduos quadráticos?

Fazendo problemas de teoria dos números é muito comum nos depararmos com quadrados perfeitos enquanto olhamos pra divisibilidades. É natural nos perguntarmos: O que podemos fazer com eles? Resíduos quadráticos são a resposta!

Inicialmente, vejamos algumas propriedades dos quadrados perfeitos $\pmod p$, onde p é primo:

- **Teorema 1:** Se $\exists\, x$ tal que $x^2 \equiv a \pmod p$, então essa equação tem exatamente duas soluções

Prova:

$$x^2 \equiv y^2 \pmod p \Rightarrow p \mid x^2 - y^2 \Rightarrow p \mid (x-y)(x+y) \Rightarrow x \equiv \pm y \pmod p$$

Logo, as únicas duas soluções são x e $-x$.

- *Definição 1 (Símbolo de Legendre):* se p é um primo, definimos:

$$\left(\frac{a}{p}\right) = \left\{ \begin{array}{ll} 1 & \text{se } \exists\, x \text{ tal que } p \mid x^2 - aep \nmid a \\ -1 & \text{se } \nexists\, x \text{ tal que } p \mid x^2 - a \\ 0 & \text{se } p \mid a \end{array} \right\}$$

Se $(\frac{x}{p}) = 1$, chamamos x de um resíduo quadrático módulo p. Assim, temos, por exemplo $(\frac{5}{3}) = -1$, pois $\nexists\, x$ tal que $x^2 \equiv 5 \pmod 3$ e $(\frac{13}{5}) = 1$, pois $2^2 \equiv 13 \pmod 5$

- **Teorema 2:** Existem exatamente $\frac{p-1}{2}$ resíduos quadráticos módulo p de 1 a p-1

  Prova: Os números $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ são todos diferentes módulo p. Pelo teorema 1, isso facilmente implica este teorema!

- **Teorema 3:** $x^{\frac{p-1}{2}} \equiv (\frac{x}{p}) \pmod p$

  Prova: Seja g uma raiz primitiva módulo p, se $\left(\frac{x}{p}\right) = 0$, o problema não é tão difícil. Caso contrário, seja x_0 tal que $g^{x_0} \equiv x$. Sabemos que x_0 é par $\iff \left(\frac{x}{p}\right) = 1$

$$\Rightarrow x^{\frac{p-1}{2}} \equiv (g^{x_0})^{\frac{p-1}{2}} = (g^{\frac{p-1}{2}})^{x_0} \equiv (-1)^{x_0} = \left(\frac{x}{p}\right)$$

- **Teorema 4:** $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

  Prova: Isso é consequência direta do Teorema 3!

Agora que já sabemos algumas propriedades básicas dos resíduos quadráticos, vamos tentar alguns problemas!

1. Prove que todo número da forma $8k+1$ é um resíduo quadrático $\pmod{2^k}$
2. Prove que existe um natural não resíduo quadrático $\pmod{p}$ menor que $\sqrt{p}+1$
3. Prove que a soma de todos os resíduos quadráticos $\pmod{p}$ é divisível por p

• 2: Qualquer primo pode dividir isso?

Já sabemos que uma das coisas mais úteis em problemas de teoria dos números é olhar para primos que dividem algum dos números dados em enunciados, então por que não achar propriedades legais para esses primos para números específicos?

- *Quais primos podem dividir números da forma x^2+1?*

  Resposta: Apenas primos $p \equiv 1 \pmod 4$

  Prova:

  $$p \mid x^2+1 \Rightarrow -1 \equiv x^2 \pmod p \Rightarrow \left(\frac{-1}{p}\right) = 1, \text{ mas } \left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \Rightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

  Sabemos que $(-1)^{\frac{p-1}{2}} = 1 \iff \frac{p-1}{2}$ é par $\iff p-1$ é multiplo de 4, que nos dá a resposta!

  Corolário: se $p \equiv 3$, $p \mid a^2+b^2 \Rightarrow p \mid a, b$

- *E se eu tentar fazer Bhaskara pra* $\pmod p$*, será que dá certo?*

  Resposta: Sim! (Mais ou Menos)

  Prova: Queremos saber quando existe e achar explicitamente x tal que

  $$ax^2+bx+c \equiv 0 \pmod p$$

  Onde a, b, c são fixos e $p \nmid a$. Algo natural é tentar repetir a prova de Bhaskara:

  $$ax^2+bx+c \equiv 0 \quad (\div a) \Rightarrow x^2+\frac{b}{a}x \equiv -\frac{c}{a} \quad (+\frac{b^2}{4a^2}) \Rightarrow x^2+\frac{b}{a}x+\frac{b^2}{4a^2} \equiv \frac{b^2}{4a^2}-\frac{c}{a}$$
  $$\Rightarrow (x+\frac{b}{2a})^2 \equiv \frac{b^2-4ac}{4a^2}$$

  Chegamos num impasse, será que teremos como achar um x tal que essa última equação tenha uma solução? A resposta é sim! Desde que $\left(\frac{b^2-4ac}{p}\right) = 0$ ou 1. Vamos chamar $\sqrt{x}$ um dos números t tal que $t^2 \equiv x \pmod p$ (veja que $\sqrt{x}$ nem sempre existe). Então, se $\sqrt{b^2-4ac}$ existe, vamos precisar de

  $$x+\frac{b}{2a} \equiv \pm\frac{\sqrt{b^2-4ac}}{2a} \Rightarrow x \equiv \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

  Que funciona trocando na equação original. Então sabemos quando qualquer quadrática tem raiz $\pmod p$! (É necessário e suficiente que)

  $$\left(\frac{b^2-4ac}{p}\right) = 0 \text{ ou } 1$$

- **Teorema 5 (Lei da reciprocidade quadrática):** Se p, q são primos ímpares, temos:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

É fácil olhar para esse teorema e se perguntar: **"POR QUÊ? COMO? ONDE?"** e é assim que todo mundo fica da primeira vez. Mas vejamos como pode ser comum tentar chegar nesse teorema:

Imagine que você está fazendo um problema de olimpíada e se depara com um $\left(\frac{3}{p}\right)$, onde p é um primo ímpar qualquer. Pode ser que você não saiba calcular isso, mas você com certeza consegue calcular $\left(\frac{p}{3}\right)$. ele é 1 se $p \equiv 1 \pmod 3$ e -1 se $p \equiv 2 \pmod 3$ então será que não existe jeito nenhum de ligar esses dois? A resposta é sim! Mas a prova é relativamente bem extensa, então, para não deixarmos esse artigo desnecessariamente grande, essa solução pode ser encontrada no *Livro do Gugu*: *"Um Passeio com Primos* junto com outras soluções de problemas conhecidos no meio olímpico!

• 3: Como vou aplicar isso em problemas de olimpíada?

1. *Se eu quiser achar muitos primos dividindo um número de alguma forma?*

   Essa pergunta pode parecer não muito fácil de se deparar do nada assim, então vamos trazer um problema da OBM pra mostrar como podemos nos ver nessa situação:

   (OBM 2017) Demonstre que, para todo n inteiro positivo, existem inteiros positivos a e b, sem fatores primos em comum, de modo que $a^2 + 2017b^2$ possui mais de n fatores primos distintos.

   Solução: Aqui já podemos ver claramente como funcionaria um problema em que queremos achar muitos divisores de um mesmo número: Agora, como vamos achar os primos que dividem esse número? Para diminuirmos nossas contas, vamos fixar $b = 1$, assim, basta achar a tal que $a^2 + 2017$ tem quantos divisores primos eu quiser: Para que, para o $p \in \mathbb{P}$, exista a tal que $p \mid a^2 + 2017$ é necessário e suficiente que $\left(\frac{-2017}{p}\right) = 1$ como 2017 é primo, por reciprocidade quadrática:

$$\left(\frac{2017}{p}\right)\left(\frac{p}{2017}\right) = (-1)^{\frac{2016(p-1)}{4}} = 1$$

   Se tomarmos $p \equiv 1 \pmod{2017}$ (existem infinitos desses, por dirichlet), basta que $\left(\frac{-1}{p}\right) = 1 \Rightarrow 4 \mid p - 1$ então, tomando $p \equiv 1 \pmod{4 \cdot 2017}$ necessariamente temos uma solução $\pmod p$. Assim, sejam $p_1, p_2, \ldots, p_n$ n primos da forma $4 \cdot 2017k + 1$. Sabemos que $\forall i \in \{1, 2, \ldots, n\} \exists a_i$ tal que $p_i \mid a_i^2 + 2017$. Finalmente, por TCR, existe um $A \in \mathbb{N}$ tal que

$$\begin{cases} A \equiv & a_1 & \pmod{p_1} \\ A \equiv & a_2 & \pmod{p_2} \\ \vdots & & \vdots \\ A \equiv & a_n & \pmod{p_n} \end{cases}$$

   Tomando $a = A$, temos que $p_1 p_2 \ldots p_n \mid a^2 + 2017$, como queríamos.

2. *Eu consigo achar um primo que não deveria dividir isso!*

   Existem alguns problemas em que usamos resíduos quadráticos para chegar num absurdo, procurando primos que fazem um quadrado deixar um resto não quadrático, por exemplo. Para exemplificar, temos o seguinte problema:

   (Exemplo): Sejam m, $n \geq 3$ inteiros positivos ímpares. Prove que $2^m - 1 \nmid 3^n - 1$

   Solução: Vamos supor por absurdo que existem m,$n \geq 3$ tais que $2^m - 1 \mid 3^n - 1$.

   Seja $p \in \mathbb{P}$ tal que $p \mid 2^m - 1 \mid 3^n - 1$ como m, n são ímpares, sabemos que

$$ord_p 2 \equiv ord_p 3 \equiv 1 \pmod 2 \Rightarrow \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$$

   Mas $\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{12}^{(*)}$ e $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1 \iff p \equiv \pm 1 \pmod 8$

   Assim,

$$p \equiv \pm 1 \pmod{12}, p \equiv \pm 1 \pmod 8 \Rightarrow p \equiv \pm 1 \pmod{24}$$

   (testando os casos, esses são os únicos números que cumprem os dois $\pmod{24}$)

   Logo, $2^m - 1$ vai ser a multiplicação de primos da forma $24k \pm 1 \Rightarrow 2^m - 1 \equiv \pm 1 \pmod{24}$ O que é um absurdo!
   Assim, existe um primo que não é da forma $24k \pm 1$ que divide $2^m - 1$, esse primo não pode dividir $3^n - 1$. Como queríamos demonstrar ■

• 4: Problemas Propostos

1. Prove que todo primo da forma $4k + 1$ pode ser escrito como soma de dois quadrados.

2. **(OBM 2021)** Determine todas as triplas (a, b, c) de inteiros não negativos tais que

$$a^2 + b^2 + c^2 = abc + 1$$

3. Sejam $a > 2$, $n > 1$ inteiros tais que $a^n - 2^n$ é quadrado perfeito. Prove que a é par.

4. **(IMO 2008)** Prove que existe um número infinito de inteiros positivos n tais que $n^2 + 1$ tem um divisor primo maior do que $2n + \sqrt{2n}$.

5. Prove que se a não é um quadrado perfeito, existem infinitos primos p tais que $\left(\frac{a}{p}\right) = 1$ e infinitos tais que $\left(\frac{a}{p}\right) = -1$

6. **(OBM 2007)** Para quantos números inteiros c, $-2007 \leq c \leq 2007$, existe um inteiro x tal que $x^2 + c$ é múltiplo de 2^{2007}?

7. Prove que, para todo polinômio $P \in \mathbb{Z}[x]$ com grau 2, $P(x) = a(bx + c)^2$ para alguma tripla $(a, b, c) \in \mathbb{Z}^3$ ou, para todo p primo grande, existe n tal que $p \mid P(n), p^2 \nmid P(n)$