Olimpíada Brasileira de Matemática

Resíduos Quadráticos

N3 – Professor Matheus Secco

1 Introdução

Estamos interessados em estudar congruências do tipo $x^2 \equiv a \pmod n$, onde x é inteiro e n é inteiro positivo. Quando existe x satisfazendo esta última congruência, dizemos que a é resíduo quadrático módulo n. Fatorando $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ em produto de primos, pelo Teorema Chinês dos Restos, basta resolvermos $x^2 \equiv a \pmod{p_i^{\alpha_i}}$, $1 \leqslant i \leqslant n$ e depois juntarmos as peças. Desta maneira, nosso roteiro será o seguinte:

(i) Estudar os resíduos quadráticos módulo 2^m.

(ii) Introduzir o símbolo de Legendre e estudar os resíduos quadráticos módulo p, onde p é primo ímpar.

(iii) Estudar os resíduos quadráticos módulo p^m, onde p é primo ímpar.

2 Potências de 2

O seguinte teorema classifica completamente os resíduos quadráticos ímpares módulo 2^m, onde $m \geqslant 3$ é inteiro positivo. Os resíduos quadráticos módulo 2 e 4 são fáceis de serem encontrados.

Teorema 1 *Um inteiro ímpar a é resíduo quadrático módulo $2^m, m \geqslant 3$ se, e somente se, é da forma $8k+1$, com k inteiro.*

Demonstração: Provaremos inicialmente que se a é r.q módulo 2^m, então $a \equiv 1 \pmod 8$. De fato, temos que $x^2 \equiv a \pmod 8$, pois $m \geqslant 3$ e os resíduos quadráticos ímpares módulo 8 são exatamente os números da forma $8k+1$.
Feito isso, provaremos agora que se $a = 8k+1$, então existe um inteiro x tal que $x^2 \equiv a \pmod{2^m}$. A prova será por indução em m, sendo o caso $m = 3$ trivial. Suponha então que existe x_0 tal que $x_0^2 \equiv a \pmod{2^m}$. Tome

$$x' = x_0 + 2^{m-1}$$

e veja que

$$x'^2 = x_0^2 + 2^m x_0 + 2^{2m-2}.$$

Como $m \geqslant 3$, segue que

$$x'^2 \equiv x_0^2 + 2^m x_0 \pmod{2^{m+1}}.$$

Por outro lado, temos que $x_0^2 = 2^m \ell + a$, $\ell \in \mathbb{Z}$ e há duas possibilidades: ℓ par ou ℓ ímpar.
Se ℓ é par, temos que $x_0^2 \equiv a \pmod{2^{m+1}}$ e concluímos a indução.
Por outro lado, se ℓ é ímpar, temos que $x'^2 \equiv 2^m(\ell + x_0) + a \pmod{2^{m+1}}$. Como ℓ e x_0 são ímpares, segue que $\ell + x_0$ é par e então $x'^2 \equiv a \pmod{2^{m+1}}$, como queriamos.
Nos dois casos, conseguimos concluir a indução e, portanto, provamos o resultado. $\square$

3 Primos

3.1 Resultados Iniciais

Teorema 2 *Sejam* p *um primo ímpar e* a *um inteiro não divisível por* p*. Caso a congruência* $x^2 \equiv a(\bmod p)$ *possua solução, ela tem exatamente duas. Mais ainda, se* x_0 *é uma destas soluções, a outra é* $-x_0$*.*

Demonstração: Se x_0 é uma destas soluções, então claramente $-x_0$ também é e devemos mostrar que x_0 e $-x_0$ são diferentes módulo p, o que é evidente, pois p é primo ímpar. Por fim, precisamos mostrar que não há mais do que duas soluções para esta congruência. Sendo y uma outra solução, temos que $y^2 - x_0^2 \equiv 0(\bmod p)$ e então $(y + x_0)(y - x_0) \equiv 0(\bmod p)$, o que nos dá $y \equiv -x_0(\bmod p)$ ou $y \equiv x_0(\bmod p)$, o que mostra que só há duas soluções de fato. □

Teorema 3 *Seja* p *um primo ímpar. Dentre os números* $1, 2, \ldots, p-1$*, exatamente* $\frac{p-1}{2}$ *são resíduos quadráticos e* $\frac{p-1}{2}$ *não são resíduos quadráticos.*

Demonstração: É fácil ver que os resíduos quadráticos sáo os números

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

□

3.2 Símbolo de Legendre

Definição 1 *Sendo* p *um primo ímpar e* a *um inteiro não divisível por* p*, definimos o símbolo de Legendre* $\left(\frac{a}{p}\right)$ *por:*

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

Se a *é múltiplo de* p*, definimos* $\left(\frac{a}{p}\right) = 0$*.*

As demonstrações dos teoremas a seguir podem ser encontradas em livros clássicos de Teoria dos Números.

Teorema 4 *(Critério de Euler) Se* p *é um primo ímpar e* a *é um inteiro não divisível por* p*, então*

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

Corolário: Este resultado mostra por exemplo que -1 é resíduo quadrático módulo p, onde p é primo ímpar, se, e somente se, p é da forma $4k + 1$.

Teorema 5 *(Multiplicatividade) O símbolo de Legendre é completamente multiplicativo, ou seja, se* a *e* b *são inteiros, temos que*

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

Corolário: O produto de dois resíduos quadráticos é um resíduo quadrático; o produto de dois não resíduos quadráticos também é um resíduo quadrático e por fim, o produto de um não resíduo quadrático por um resíduo quadrático não é um resíduo quadrático.

Teorema 6 *Sendo* p *um primo ímpar, temos que*

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

Teorema 7 *(Reciprocidade Quadrática) Se p e q são primos ímpares distintos, então*

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

4 Potências de primo

Teorema 8 *Seja $k \geqslant 1$. Se p é um primo ímpar que não divide a e x_k é tal que*

$$x_k^2 \equiv a \pmod{p^k},$$

então existe x_{k+1} tal que

$$x_{k+1} \equiv x_k \pmod{p^k},$$
$$x_{k+1}^2 \equiv a \pmod{p^{k+1}}.$$

Demonstração: Afirmamos que existe $0 \leqslant t \leqslant p-1$ tal que $x_{k+1} = x_k + tp^k$ satisfaz o desejado. Inicialmente, veja que sempre temos $x_{k+1} \equiv x_k \pmod{p^k}$. Para finalizar, veja que

$$(x_k + tp^k)^2 = x_k^2 + 2tx_kp^k + t^2p^{2k} \equiv x_k^2 + 2tx_kp^k \pmod{p^{k+1}}.$$

Sendo $x_k^2 = p^k\ell + a$, obtemos que

$$(x_k + tp^k)^2 \equiv p^k(2tx_k + \ell) + a \pmod{p^{k+1}}.$$

Como $2x_k$ é primo com p, existe t tal que $2tx + k + \ell$ é múltiplo de p e então conseguimos obter o desejado. □

Corolário: Seja p um primo ímpar e a inteiro não divisível por p. Então a é resíduo quadrático módulo p^k, $k \geqslant 1$ inteiro, se, e somente se, a é resíduo quadrático módulo p.

5 Problemas

Problema 1 Determine se as equaçõe modulares a seguir possuem solução:

(a) $x^2 + 4x - 3 \equiv 0 \pmod{51}$

(b) $2x^2 - 4x + 1 \equiv 0 \pmod{13}$

(c) $x^2 - x + 1 \equiv 0 \pmod{91}$

(d) $x^2 - 3x + 5 \equiv 0 \pmod{16}$

(e) $x^2 - 6x + 7 \equiv 0 \pmod{15}$

Problema 2 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 3 Existem inteiros m e n tais que

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

Problema 4 Seja p um primo maior do que 3. Se existe um inteiro a tal que $p|a^2 - a + 3$, prove que existe um inteiro b tal que $p|b^2 - b + 25$.

Problema 5 Seja p um primo. Mostre que existem x e y inteiros tais que $x^2 + y^2 + 1$ é divisível por p.

Problema 6 Seja p um primo ímpar. Mostre que o menor não resíduo quadrático positivo de p é menor que $\sqrt{p} + 1$.

Problema 7 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 8 (Putnam 1991) Seja p um primo ímpar. Quantos elementos tem o conjunto

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

Problema 9 Prove que para todo n inteiro positivo, qualquer divisor primo de $n^4 - n^2 + 1$ é da forma $12k + 1$, onde k é inteiro.

Problema 10 Sejam x e y inteiros positivos. Prove que $4xy - x - y$ não é um quadrado perfeito.

Problema 11 Seja p um número primo. Mostre que

(a) Se p é da forma $4n + 1$, então $p | n^n - 1$.

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

Problema 12 Mostre que se x e y são inteiros, então $\frac{x^2-2}{2y^2+3}$ nunca é um número inteiro.

Problema 13 (Taiwan 1997) Seja $q = 2^{2^n} + 1$, onde n é um inteiro positivo. Prove que q é um primo se, e somente se, $3^{\frac{q-1}{2}} \equiv -1 \pmod q$.

Problema 14 (IMO 1996) Os inteiros positivos a e b são tais que os números $15a + 16b$ e $16a - 15b$ são ambos quadrados perfeitos. Qual é o menor valor possível que pode ter o menor destes dois números?

Problema 15 (Coréia 1999) Encontre todos os inteiros positivos n tais que $2^n - 1$ é divisível por 3 e $\frac{2^n-1}{3}$ possui um múltiplo da forma $4m^2 + 1$ para algum inteiro positivo m.

Problema 16 Sejam $m, n \geqslant 3$ inteiros positivos ímpares. Prove que $2^m - 1$ não divide $3^n - 1$.

Problema 17 (Taiwan) Sejam m e n inteiros positivos tais que $\varphi(5^m - 1) = 5^n - 1$. Prove que $\text{mdc}(m, n) > 1$.

Problema 18 (Bulgária 1998) Sejam m e n inteiros positivos tais que $A = \frac{(m+3)^n+1}{3m}$ é inteiro. Prove que A é ímpar.

Problema 19 (Banco IMO 1998) Encontre todos os inteiros positivos n para os quais existe um inteiro m tal que $m^2 + 9$ é múltiplo de $2^n - 1$.

Problema 20 (OBM 2007) Para quantos números inteiros c, $-2007 \leqslant c \leqslant 2007$, existe um inteiro x tal que $x^2 + c$ é múltiplo de 2^{2007}?

Problema 21 Seja $F_n = 2^{2^n} + 1$ o n-ésimo número de Fermat. Prove que para todo $n \geqslant 2$, todo fator primo de F_n é da forma $k \cdot 2^{n+2} + 1$, onde k é inteiro.

Problema 22 (OBM-U 2010) Prove que se $10^{2n} + 8 \cdot 10^n + 1$ tem um fator primo da forma $60k + 7$, onde n e k são inteiros não negativos, então n e k são pares.

Problema 23 (Ibero 2003) As sequências (a_n) e (b_n) são definidas como a seguir: $a_0 = 1, b_0 = 4$ e para $n \geqslant 0$,

$$a_{n+1} = a_n^{2001} + b_n, b_{n+1} = b_n^{2001} + a_n.$$

Prove que 2003 não divide nenhum dos termos destas sequências.

Problema 24 Seja a um inteiro positivo que não é quadrado perfeito. Então existem infinitos primos p para os quais $\left(\frac{a}{p}\right) = -1$.

Problema 25 (Mathlinks Contest 2004) Sejam $a_1, a_2, \ldots, a_{2004}$ inteiros não negativos tais que $a_1^n + a_2^n + \ldots + a_{2004}^n$ é quadrado perfeito para todo inteiro positivo n. Qual é o maior número possível de a_i's que são não nulos?

Problema 26 (Moldávia 2005) Sejam f, g funções dos inteiros positivos nos inteiros positivos tais que:

(i) g é sobrejetiva.

(ii) $2f(n)^2 = n^2 + g(n)^2$ para todo n inteiro positivo.

(iii) $|f(n) - n| \leqslant 2004\sqrt{n}$ para todo n inteiro positivo.

Prove que f possui infinitos pontos fixos.

Problema 27 (Romênia 2004) Seja p um primo ímpar e defina

$$f(x) = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) x^{i-1}.$$

(a) Prove que f é divisível por $x - 1$, mas não por $(x-1)^2$ se, e somente se, $p \equiv 3 (\mathrm{mod}\, 4)$.

(b) Prove que se $p \equiv 5 (\mathrm{mod}\, 8)$, então f é divisível por $(x-1)^2$, mas não é divisível por $(x-1)^3$.

Problema 28 (IMO 2008) Prove que existem infinitos inteiros positivos n tais que n^2+1 possui um divisor primo maior do que $2n + \sqrt{2n}$.

Problema 29 (Ibero 2008) Seja $P(x) = x^3 + mx + n$ um polinômio com coeficientes inteiros com a seguinte propreidade: se x e y são inteiros tais que $P(x) - P(y)$ é divisível por 107, então $x - y$ também é divisível por 107. Prove que m é múltiplo de 107.

Problema 30 Seja p um primo da forma $4n + 1$, n inteiro positivo. Calcule

$$\sum_{k=1}^{p-1} \left(\left\lfloor \frac{2k^2}{p} \right\rfloor - 2 \left\lfloor \frac{k^2}{p} \right\rfloor \right).$$