Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 2

Prof. Samuel Feitosa

Aula 18

Resíduos Quadráticos

Definição 1. *Para todos a tais que $mdc(a,m) = 1$, a é chamado resíduo quadrático módulo m se a congruência $x^2 \equiv a \pmod m$ tem solução. Se ela não tem solução, então a é chamado de resíduo não quadrático módulo m.*

Exemplo 2. *Seja n um inteiro. Prove que se $2 + 2\sqrt{28n^2+1}$ é um inteiro, então é um quadrado perfeito.*

Se $2+2\sqrt{28n^2+1}$ é inteiro, o número $\sqrt{28n^2+1}$ é um racional e consequentemente devemos ter que $28n^2+1$ é o quadrado de um inteiro ímpar, digamos:

$$\begin{aligned} 28n^2+1 &= (2k+1)^2 \Rightarrow \\ 28n^2+1 &= 4k^2+4k+1 \Rightarrow \\ 7n^2 &= k(k+1) \end{aligned}$$

Devemos considerar dois casos: $7 \mid k$ ou $7 \mid k+1$. Além disso, lembremo-nos do seguinte fato:

Se $mdc(a,b) = 1$, e $a \cdot b = n^2$ então existem inteiros x e y tais que $a = x^2$ e $y = b^2$.

Como $mdc(k, k+1) = 1$, temos os dois casos para analisar:
Primeiro caso:

$$\begin{cases} k &= x^2 \\ (k+1)/7 &= y^2 \end{cases}$$

Assim, $1 = (k+1) - k = 7y^2 - x^2$. Analisando essa equação módulo 7, temos $x^2 \equiv -1 \pmod 7$. Entretanto, analisando os quadrados dos restos da divisão por 7, podemos notar que -1 não é um resíduo quadrático e consequentemente temos um absurdo.

Segundo caso:

$$\begin{cases} k/7 &= x^2 \\ k+1 &= y^2 \end{cases}$$

Daí, $2 + 2\sqrt{28n^2+1} = 2 + 2(2k+1) = 4(k+1) = (2y)^2$ e isso conclui o problema.

Em geral, se p é um primo da forma $4k+3$, -1 nunca é resíduo quadrático. Para ver isso, suponha que existe x tal que:

$$\begin{aligned} x^2 &\equiv -1 \pmod{p} \Rightarrow \\ (x^2)^{(p-1)/2} &\equiv (-1)^{(p-1)/2} \pmod{p} \Rightarrow \\ x^{p-1} &\equiv -1 \pmod{p}. \end{aligned}$$

Isso contradiz o teorema de Fermat.

Definição 3. *Se p denota um primo ímpar, então o símbolo de Legendre $\left(\frac{a}{p}\right)$ é definido por 1 se a é um resíduo quadrático, -1 se a não é um resíduo quadrático módulo p, e 0 se $p|a$.*

Teorema 4. *Se p é um primo ímpar. Então*

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

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

c) $a \equiv b \pmod{p}$ *implica que* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

d) Se $mdc(a,p) = 1$ *então* $\left(\frac{a^2}{p}\right) = 1$ *e* $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

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

Provemos inicialmente o item a) quando $mdc(a,p) = 1$. Em virtude do teorema de Fermat, perceba que se $mdc(a,p) = 1$ então:

$$p \mid a^{p-1} - 1 = (a^{p-1/2} + 1)(a^{p-1/2} - 1).$$

Daí, $a^{p-1/2} \equiv \pm 1 \pmod{p}$. Suponha que $\left(\frac{a}{p}\right) = 1$, então existe x tal que

$$\begin{aligned} x^2 &\equiv a \pmod{p} \Rightarrow \\ (x^2)^{\frac{p-1}{2}} &\equiv a^{\frac{p-1}{2}} \Rightarrow \\ x^{p-1} &\equiv a^{\frac{p-1}{2}} \end{aligned}$$

Pelo teorema de Fermat, a última congruência nos diz que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Suponha agora que $\left(\frac{a}{p}\right) = -1$, ou seja, que não existe x tal que $x^2 \equiv a \pmod{p}$. Assim, podemos

separar os números do conjunto $\{1, 2, \ldots, p-1\}$ em pares (i, j) onde $ij \equiv a \pmod p$ e $i \neq j$. Daí, o produto de todos esses pares é

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) &\equiv a \cdot a \cdot \ldots \cdot a \pmod p \\ &\equiv a^{\frac{p-1}{2}} \pmod p \end{aligned}$$

Usando o teorema de Wilson, concluímos que $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. Se $p \mid a$, $\left(\frac{a}{p}\right) \equiv 0 \equiv a^{\frac{p-1}{2}} \pmod p$. Os demais itens seguem de a).

Exemplo 5. *Suponha que p é um primo ímpar. Seja n o menor não-resíduo quadrático positivo módulo p. Prove que $n < 1 + \sqrt{p}$.*

Seja m o maior inteiro positivo tal que $mn > p$, ou seja, $(m-1)n < p < mn$. Assim, $0 < mn - p < n$ e consequentemente:

$$\begin{aligned} 1 &= \left(\frac{mn-p}{p}\right) \\ &= \left(\frac{mn}{p}\right) \\ &= \left(\frac{m}{p}\right) \cdot \left(\frac{m}{p}\right) \\ &= -\left(\frac{m}{p}\right) \end{aligned}$$

Daí, $m \geq n$ e

$$\begin{aligned} (n-1)^2 &< n(n-1) \\ &\leq n(m-1) \\ &< p. \end{aligned}$$

Portanto, $n - 1 < \sqrt{p}$.

Teorema 6. *(Lema de Thue) Sejam m um número natural e a um inteiro primo com m, então existem inteiros x e y tais que:*

1. $0 < |x|, |y| < \sqrt{m}$;
2. $ax \equiv y \pmod m$.

Demonstração. Considere o conjunto $\{au - v | u, v \in \mathbb{Z}, 0 \leq u, v \leq \lfloor \sqrt{p} \rfloor\}$. Como existem $\lceil \sqrt{p} \rceil^2 > p$ tais pares (u, v), existirão $(u_1, v_1) \neq (u_2, v_2)$ tais que

$$au_1 - v_1 \equiv au_2 - v_2 \pmod p$$

Sejam $x = v_1 - v_2$ e $y = u_1 - u_2$. Claramente ii) está satisfeito. Por construção, x, y não podem ser ambos nulos e, caso um deles seja, o outro também o será. Logo i) também é verdade.

Proposição 7. *Sejam $D \in \mathbb{Z}$ e $m \in \mathbb{N}$ inteiros relativamente primos tais que $-D$ é um resíduo quadrático módulo m. Então existem inteiros $k, x, y \in \mathbb{Z}$ com $0 < k \leq D$ e $0 < |x|, |y| < \sqrt{p}$ tais que:*

$$x^2 + Dy^2 = kp$$

Demonstração. Seja a tal que $a^2 \equiv -D \pmod{p}$ e x, y como no teorema anterior com $m = p$. Então, por um lado:

$$0 < x^2 + Dy^2 < (1 + D)p$$

e por outro lado,

$$x^2 + Dy^2 \equiv (a^2 + D)y^2 \equiv 0 \pmod{p}$$

Exemplo 8. *Seja $p > 3$ um primo ímpar tal que $\left(\frac{-3}{p}\right) = 1$, existem x e y tais que $x^2 + 3y^2 = p$.*

Pelo teorema anteiror, Exitem x, y, k tais que $x^2 + 3y^2 = pk$ com $|x|, |y| \leq \sqrt{p}$. Assim, $x^2 + 3y^2 < 4p$. Temos tres casos a considerar:
Primeiro caso: $x^2 + 3y^2 = 3p$. Devemos ter $x^2 \equiv 0 \pmod{3}$ e $x = 3x_0$. Daí, $3x_0^2 + y^2 = p$.

Segundo caso: $x^2 + 3y^2 = 2p$. Como $2p$ é par, devemos ter x e y ambos ímpares ou ambos pares. Em qualquer caso, $x^2 + 3y^2$ será múltiplo de 4 e consequentemente $2 \mid p$. Isso é um absurdo.

Terceiro caso: $x^2 + 3y^2 = p$. Não há o que fazer nesse caso.

Teorema 9. *(Lema de Gauss) Seja p um primo ímpar e a um inteiro tal que $mdc(a, p) = 1$, Considere os inteiros $a, 2a, \ldots, \frac{a(p-1)}{2}$ e seus restos módulo p. Se n denota o número desses restos que excedem $\frac{p}{2}$ então $\left(\frac{a}{p}\right) = (-1)^n$*

Demonstração. Sejam $r_1, r_2, \ldots r_n$ os resíduos que excedem $p/2$ e sejam $s_1, s_2, \ldots, s_k$ os resíduos restantes. Naturalmente todos esses restos são distintos e nenhum deles é nulo. Considere agora os números da forma $p - r_i$ e perceba que $0 < p - r_i < p/2$. Se tivéssemos $p - r_i \equiv s_j \pmod{p}$ para algum par (i, j), também teríamos $r_i + s_j \equiv 0 \pmod{p}$ e por conseguinte p dividiria a soma de dois números do conjunto $\{a, 2a, \ldots, \frac{a(p-1)}{2}\}$. Entretanto, isso é um absurdo porque a soma de quaisquer dois número desse conjunto é da forma ak com $0 < k < p$ e a não é divisível por p. Logo, os números da forma $p - r_j$ são todos distintos dos números da forma s_i e todos eles pertencem ao conjunto $\{1, 2, \ldots (p-1)/2\}$.

Como $n+k=(p-1)/2$, podemos concluir que:

$$\begin{aligned}
(p-r_1)(p-r_2)\dots(p-r_n)s_1s_2\dots s_k &= 1\cdot 2\cdot \dots \cdot \frac{p-1}{2} \Rightarrow \\
(-r_1)(-r_2)\dots(-r_n)s_1s_2\dots s_k &\equiv 1\cdot 2\cdot \dots \cdot \frac{p-1}{2} \pmod p \Rightarrow \\
(-1)^n r_1r_2\dots r_ns_1s_2\dots s_k &\equiv 1\cdot 2\cdot \dots \cdot \frac{p-1}{2} \pmod p \Rightarrow \\
(-1)^n a\cdot 2a\cdot \dots \cdot \frac{p-1}{2}a &\equiv 1\cdot 2\dots \frac{p-1}{2} \pmod p \Rightarrow \\
(-1)^n a^{(p-1)/2} &\equiv 1 \pmod p \Rightarrow \\
(-1)^n &\equiv a^{(p-1)/2} \pmod p.
\end{aligned}$$

Pelo critério de Euler, o resultado segue.

Teorema 10. *Se p é um primo ímpar e $mdc(a,2p)=1$, então $\left(\frac{a}{p}\right)=(-1)^t$ onde $t=\sum_{j=1}^{\frac{p-1}{2}}\left\lfloor \frac{ja}{p}\right\rfloor$ e $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.*

Demonstração. Consideraremos novamente o conjunto $\{a,2a,\dots,\frac{a(p-1)}{2}\}$ e usaremos a mesma notação do teorema anterior. Quando o inteiro ja é dividido por p, obtemos como quociente o número $\lfloor ja/p\rfloor$. Assim, podemos escrever:

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p\lfloor ja/p\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j$$

e

$$\begin{aligned}
\sum_{j=1}^{(p-1)/2} j &= \sum_{i=1}^{n}(p-r_i) + \sum_{j=1}^{n} s_j + \sum_{j=1}^{k} s_j \\
&= np - \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j
\end{aligned}$$

Substituindo na equação anterior, obtemos:

$$(a-1)\sum_{j=1}^{(p-1)/2} j = p\left(\sum_{j=1}^{(p-1)/2}\lfloor ja/p\rfloor - n\right) + 2\sum_{j=1}^{n} r_j$$

Como

$$\sum_{j=1}^{(p-1)/2} j = \frac{p^2-1}{8},$$

temos:

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{(p-1)/2} \lfloor ja/p \rfloor - n \pmod 2$$

Se a é ímpar, $n \equiv \sum_{j=1}^{(p-1)/2} \lfloor ja/p \rfloor \pmod 2$. Se $a = 2$, isto implica que $n \equiv (p^2-1)/8 \pmod 2$ pois $\lfloor 2j/p \rfloor = 0$ para $1 \leq j \leq (p-1)/2$. O resultado decorre do teorema anterior.

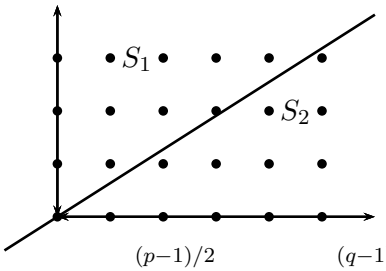
Exemplo 11. *Encontre todos os inteiros positivos n tais que $2^n - 1$ é divisível por 3 e $\frac{2^n-1}{3}$ tem um múltiplo da forma $4m^2+1$ para algum natural m.*

Teorema 12. *(Lei da reciprocidade quadrática) Se p e q são primos ímpares distintos, então*

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

Demonstração. Seja S o conjunto de todos os pares de inteiros (x, y) satisfazendo $1 \leq x \leq (p-1)/2, 1 \leq y \leq (q-1)/2$. O conjunto S possui $(p-1)(q-1)/4$. Suponha que exista um par (x, y) tal que $qx = py$. Como $mdc(p, q) = 1$, segue que $q \mid y$ e $p \mid x$. Entretanto, nos internvalos mencionados não existem tais múltilplos. Separemos então esse conjunto em dois outros mutuamente exclusivos:

$$\begin{aligned} S_1 &= \{(x,y) | qx > py\} \\ S_2 &= \{(x,y) | qx < py\} \end{aligned}$$



Os números de pares em S_1 e S_2 são $\sum_{x=1}^{(p-1)/2} \lfloor qx/p \rfloor$ e $\sum_{y=1}^{(q-1)/2} \lfloor py/q \rfloor$. Fazendo a contagem total de pares, temos:

$$\sum_{x=1}^{(p-1)/2} \lfloor qx/p \rfloor + \sum_{y=1}^{(q-1)/2} \lfloor py/q \rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

e, em virtude do teorema anterior, obtemos:

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

Exemplo 13. *Mostre que* $\dfrac{x^2-2}{2y^2+3}$ *nunca é um inteiro quando* x *e* y *são inteiros.*

Exemplo 14. *Seja* $q = 4^n + 1$ *onde* n *é um inteiro positivo. Prove que* q *é um primo se, e somente se,* $3^{\frac{q-1}{2}} \equiv -1 \pmod{q}$

Se q é um primo, então $q \equiv 2 \pmod 3$ e pela lei da reciprocidade quadrática temos:

$$\begin{aligned} 1 &= (-1)^{(q-1)/2\cdot 1} \\ &= \left(\frac{3}{q}\right)\left(\frac{q}{3}\right) \\ &= \left(\frac{3}{q}\right)(-1) \end{aligned}$$

Em virtude dessa equação e do critério de Euler, temos:

$$\begin{aligned} -1 &= \left(\frac{3}{q}\right) \\ &\equiv 3^{\frac{q-1}{2}} \pmod{q} \end{aligned}$$

Reciprocamente, se $3^{\frac{q-1}{2}} \equiv -1 \pmod{q}$, então $ord_q 3 = 4^n$. Como $ord_q 3 \mid \varphi(q)$, teremos $\varphi(q) = q - 1$, ou seja, q é primo.

Problemas Propostos

Problema 15. *Prove que se* p *é um primo maior que 3 então a soma dos resíduos quadráticos módulo* p *é divisível por* p*.*

Problema 16. *Mostre que se* a *é um resíduo quadrático módulo* m*, e* $ab \equiv 1 \pmod m$*, então* b *é também um resíduo quadrático. Prove que o produto dos resíduos quadráticos módulo* p *é congruente a* $+1$ *ou* -1 *módulo* p*.*

Problema 17. *Prove que se* p *é um primo da forma* $4k+3$*, e se* m *é o número de resíduos quadráticos menores que* $\frac{p}{2}$*, então:*

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2) \equiv (-1)^{m+k+1} \pmod p$$
$$2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1) \equiv (-1)^{m+k} \pmod p$$

Problema 18. *Seja* $q = 4^n + 1$ *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 19. *Os inteiros positivos* a *e* b *são tais que os números* $15a + 16b$ *e* $16a - 15b$ *são ambos quadrados de inteiros positivos. Qual é o menor valor possível que pode ter o menor desses números?*

Problema 20. *(Olimpíada Búlgara) Sejam m e n números naturais tais que*

$$A = \frac{(m+3)^n + 1}{3m}$$

é um inteiro. Prove que A é ímpar.

Problema 21.

a) Prove que para qualquer primo p, o número $\binom{2p}{p} - 2$ é divisível por p^2.

b) Mostre que se p é um primo e $0 \leq m < n < p$ então

$$\binom{np+m}{mp+n} \equiv (-1)^{m+n+1} p \pmod{p^2}$$

c) Prove que para qualquer primo $p > 3$, o número $\binom{2p-1}{p-1} - 1$ é divisível por p^3.

Problema 22. *Caracterize todos os inteiros que podem ser expressos na forma:*

a) $a^2 + ab + b^2$

b) $a^2 + 2b^2$

Problema 23. *Se n é um inteiro tal que $7n$ é da forma $a^2 + 3b^2$, prove que n também é dessa forma.*

Problema 24. *Encontre todos os inteiros positivos n para os quais existe um inteiro m tal que $m^2 + 9$ é um múltiplo de $2^n - 1$.*

Problema 25. *Mostre que dado qualquer primo p, existem inteiros x, y, z, w satisfazendo $x^2 + y^2 + z^2 - wp = 0$ e $0 < w < p$*

Problema 26. *Mostre que p é um divisor de ambos os números da forma $m^2 + 1$, $n^2 + 2$, se e somente se é um divisor de algum número da forma $k^4 + 1$.*

Problema 27. *Seja A o conjunto de todos os inteiros da forma $a^2 + 2b^2$, onde a e b são inteiros e $b \neq 0$. Mostre que p é um número primo e $p^2 \in A$, então $p \in A$.*

Problema 28. *Seja p um primo da forma $4k + 1$. Mostre que:*

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

Problema 29. *Mostre que se x não é divisível por 3, então $4x^2 + 3$ tem pelo menos um fator primo da forma $12n + 7$. Mostre que existem infinitos primos dessa forma.*

Problema 30. *Suponha que $\phi(5^m - 1) = 5^n - 1$ com m, n números naturais. Prove que $mdc(m, n) > 1$*

Problema 31. *(Coréia 2001) Seja $f : \mathbb{Z} \to \mathbb{Z}$. Dado um primo ímpar p, encontre todas as funções $f : \mathbb{Z} \to \mathbb{Z}$ satisfazendo as seguintes condições:*

1. *Se* $m \equiv n \pmod{p}$ *com* $m, n \in \mathbb{Z}$, *então* $f(m) = f(n)$

2. $f(mn) = f(m)f(n)$ *para quaisquer* $m, n \in \mathbb{Z}$.

Problema 32. *Para a congruência* $z^2 \equiv D \pmod{2^a}$, *onde* D *é ímpar e* a *é um natural, ser solúvel, é necesário e suficiente que* D *seja da forma* $2k+1, 4k+1$ *ou* $8k+1$ *de pendendo de* $a = 1, a = 2$ *ou* $a > 2$.

Problema 33. *(OBM 2007) Para quantos numeros inteiros* c, $-2007 \leq c \leq 2007$, *existe um inteiro* x *tal que* $x^2 + c$ *e múltiplo de* 2^{2007} *?*

Problema 34. *(Teorema de Wolstenhome) Se* $p \geq 5$ *é um primo, mostre que o numerador da fração*

$$\frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{p-1}$$

é múltiplo de p^2.

Problema 35. *Se* p *é um primo maior que* 3 *e* $q = \left\lfloor \frac{2p}{3} \right\rfloor$, *prove que*

$$\binom{p}{1} + \binom{p}{2} + \ldots \binom{p}{q}$$

é divisível por p^2.
(Dica: Use a identidade de Catalão e o teorema de Wolstenhome)

Referências

[1] E. Carneiro, O. Campos and F. Paiva, Olimpíadas Cearenses de Matemática 1981-2005 (Níveis Júnior e Senior), Ed. Realce, 2005.

[2] S. B. Feitosa, B. Holanda, Y. Lima and C. T. Magalhães, Treinamento Cone Sul 2008. Fortaleza, Ed. Realce, 2010.

[3] D. Fomin, A. Kirichenko, Leningrad Mathematical Olympiads 1987-1991, MathPro Press, Westford, MA, 1994.

[4] D. Fomin, S. Genkin and I. Itenberg, Mathematical Circles, Mathematical Words, Vol. 7, American Mathematical Society, Boston, MA, 1966.

[5] I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction to the Theory of Numbers.